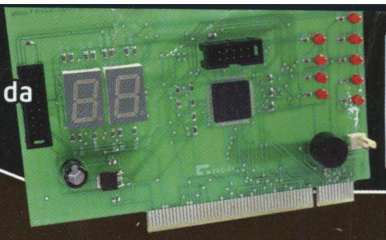
Service Pack 3
Novidades do último pacote de atualizações para o Windows XP

Manutenção
Cenários para uso da placa POST Saber



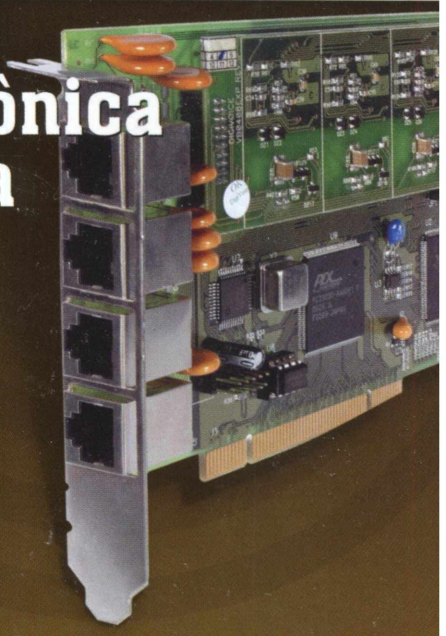
Projetos de Redes
Testamos o software concorrente do Visio
Profissionalismo e baixo custo

www.revistapcecia.com.br

PC &CIA

Conta telefônica mais barata

PABX VoIP falando com telefonia tradicional
Saiba como integrar essa solução



SABER

ANO 7 - Nº 82 - Junho/2008 - Europa €4,30 - Brasil R$13,90

Gaming PC



- Sofisticação no mercado local
- Opções prontas ou faça você mesmo?
- Testes revelam as soluções mais rápidas
- Para quem busca simplesmente o melhor!

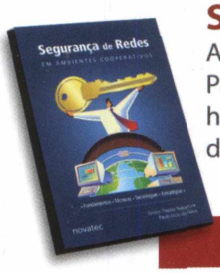
Redes Windows mais seguras

VPN com Vista e Server 2008
Configuração passo a passo

ISSN 1519-5267

LITERATURA TÉCNICA

Que não pode faltar em sua biblioteca

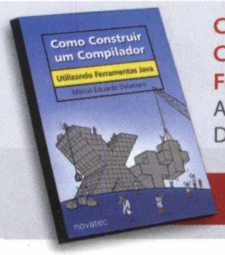


Segurança de Redes em Ambientes Cooperativos

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.

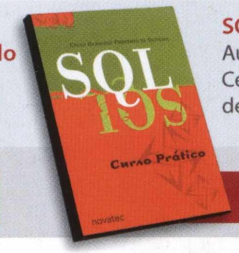
R$ 81,00

LANÇAMENTO



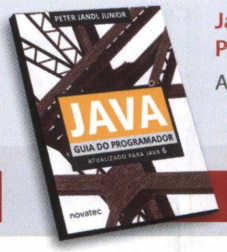
Como Construir um Compilador Utilizando Ferramentas Java
Autor: Márcio Eduardo Delamaro

R$ 69,00



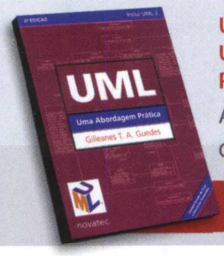
SQL - Curso Prático
Autor:
Celso Henrique Poderoso de Oliveira

R$ 42,00



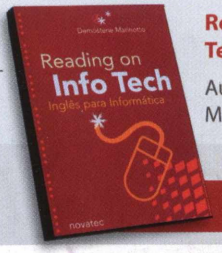
Java Guia do Programador
Autor: Peter Jandl Junior

R$ 119,00



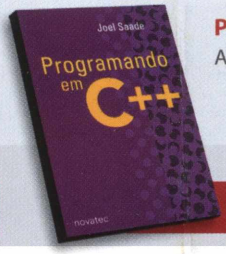
UML - Uma Abordagem Prática
Autor: Gilleanes T. A. Guedes

R$ 69,00



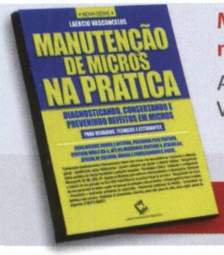
Reading on Info Tech – 2ª edição
Autor: Demóstene Marinotto

R$ 39,00



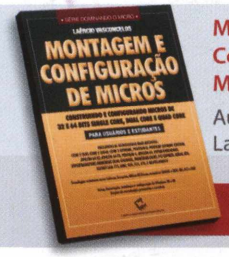
Programando em C++
Autor: Joel Saade

R$ 79,00



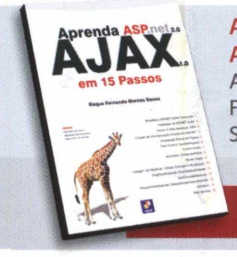
Manutenção de micros na prática
Autor: Laércio Vasconcelos

R$ 99,00



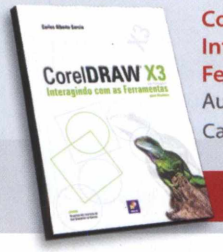
Montagem e Configuração de Micros
Autor:
Laércio Vasconcelos

R$ 39,00



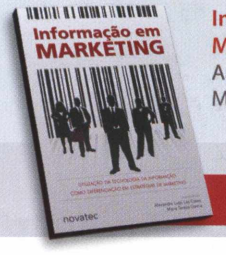
Aprenda ASP.NET AJAX em 15 Passos
Autor: Roque Fernando Marcos Sousa

R$ 53,10



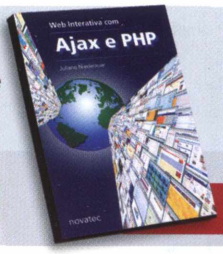
CorelDRAW X3 - Interagindo com as Ferramentas
Autor:
Carlos Alberto Garcia

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.

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, Gabriel Marques, 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
Christiane Aguiar

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
Arquivo Ed. Saber

Impressão
São Francisco Gráfica e Editora

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



Fernando Ramos

Há alguns meses realizamos alguns comentários sobre a sofisticação do mercado brasileiro de computadores e durante a produção desta edição tivemos a oportunidade de enxergar esse fenômeno mais de perto. Imagine a configuração de hardware necessária para rodar o Crysis, um dos mais badalados jogos da atualidade, com elevado nível de detalhes e resolução de imagem, tal como 1680x1050. Se até bem pouco tempo as opções para realizar esse sonho de consumo se restringiam a entrar em contato com uma revenda especializada e aguardar algumas semanas para receber todos os componentes e montar o micro, hoje a história é bem diferente.

Primeiro, vale ressaltar que o mercado que atende ao chamado nicho do "faça você mesmo"(do inglês DIY, Do-It-Yourself) está mais aquecido do que nunca. Placas-mãe com chipset Intel X48 ou NVIDIA 790, placas de vídeo Radeon HD 3870 X2 ou GeForce 9800GX2, fontes de potência real acima de 500W e gabinetes de alta performance térmica, em resumo está muito mais fácil encontrar componentes topo de linha como estes, à pronta entrega. E o que é melhor: até mesmo os usuários que precisam de hardware desse nível de performance – inclusive para rodar outros tipos de softwares -, mas não se sentem à vontade para montar seu próprio sistema, podem atualmente fazer o pedido junto a algum fabricante de grife e receber a máquina após alguns dias.

Como de costume, mais uma vez conseguimos reunir diversas configurações e submetê-las a uma longa bateria de testes, a fim de obter e demonstrar as evidências que nos levam à solução mais interessante. Os detalhes você confere a partir da página 8.

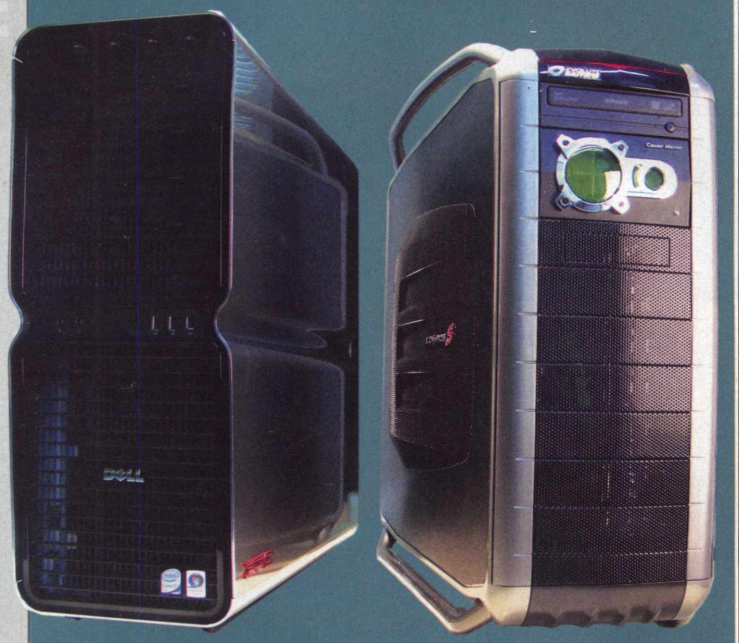
Aproveito ainda para destacar o bom trabalho realizado por vários colegas da equipe em relação a soluções para redes. Que tal um software de custo acessível para fazer projetos e assim poder realizar um trabalho com maior profissionalismo mesmo nos ambientes de rede de pequeno porte? Além disso, você também encontrará nesta edição duas soluções interessantes para segurança de redes, uma para ambientes Linux com um software do tipo IPS (sistema de prevenção de intrusos) e outra para configurar uma VPN (rede virtual privada) usando as novas tecnologias da dupla Windows Vista e Server 2008. E se você procura uma solução para diminuir drasticamente os custos com conta telefônica em sua empresa, prosseguindo com a série voz sobre IP desta vez o Flávio demonstra como integrar um PABX VoIP à rede de telefonia tradicional.

No mais, sinta-se convidado para nos enviar seus comentários, ou mesmo para discutir algumas opções de investimento.

Bons negócios e até a próxima!

fernando@editorasaber.com.br

Os artigos assinados são de exclusiva responsabilidade de seus autores. É vedada a reprodução total ou parcial dos textos e ilustrações desta Revista, bem como a industrialização e/ou comercialização dos aparelhos ou idéias oriundas dos textos mencionados, sob pena de sanções legais. As consultas técnicas referentes aos artigos da Revista deverão ser feitas exclusivamente por cartas, ou e-mail (A/C do Departamento Técnico). São tomados todos os cuidados razoáveis na preparação do conteúdo desta Revista, mas não assumimos a responsabilidade legal por eventuais erros, principalmente nas montagens, pois tratam-se de projetos experimentais. Tampouco assumimos a responsabilidade por danos resultantes de imperícia do montador. Caso haja enganos em texto ou desenho, será publicada errata na primeira oportunidade. Preços e dados publicados em anúncios são por nós aceitos de boa fé, como corretos na data do fechamento da edição. Não assumimos a responsabilidade por alterações nos preços e na disponibilidade dos produtos ocorridas após o fechamento.



Gaming PC 8

HARDWARE

Manutenção com a POST
Saber a tiracolo 23

Computação verde 26



REDES

Asterisk: o nome da revolução no mercado de telefonia – Parte 2 28

Redes seguras com VPN 34

Softwares para projetos de redes 44

SISTEMAS OPERACIONAIS

Proteja sua rede com um IPS 47

Windows XP Service Pack 3 52

Controladores de domínio Windows Server 2008 – Parte 1 56

Certificação Microsoft MCTS – Parte Final 60



Editorial 03
Segurança High-Tech 05
Seção do Leitor 06
Notícias 07

O tal do vício



Jansen C. Sena
Mestre em segurança de redes e administração de sistemas pelo Instituto de Computação da Unicamp, certificado pelo Linux Professional Institute, professor e consultor. www.jsena.info

Há coisas que se tornam estranhas quando isentas de qualquer racionalidade, sobretudo aos olhos daqueles com condições suficientes para entender o absurdo de tais situações. A caminho de Porto Alegre, para participar da 9ª edição do Fórum Internacional de Software Livre, onde apresentaria uma palestra sobre segurança de redes e software livre, presenciei uma dessas situações.

Devido a problemas meteorológicos na capital gaúcha (comuns nessa época do ano), logo veio o anúncio por parte do piloto: pousaríamos em Florianópolis até que fosse permitido o vôo até Porto Alegre.

Alheia a segurança coletiva, a prudência nem sempre se equilibra com planos pessoais. Após alguns minutos em solo catarinense, a aeronave ficou um pouco distante do aeroporto. Apesar da porta ter sido aberta, os passageiros permaneceram a bordo. Alguns, inclusive eu, se levantaram a fim de alongar-se um pouco, para relaxar antes da viagem continuar.

No mesmo vôo estava Sérgio Amadeu, amigo já conhecido de outros eventos do gênero, um dos nomes mais ativos do software livre no cenário nacional e com quem comecei a conversar. Após algum tempo, sem fazer qualquer esforço, era possível perceber que havia alguma discussão tornando-se cada vez mais calorosa na frente da aeronave. Era uma senhora que reinvindicava à tripulação, o direito de fumar um cigarro na porta da aeronave. Alertada a respeito da óbvia proibição, a senhora propôs descer pela escada conectada à aeronave para fumar o seu cigarro a alguns metros do avião, na pista do aeroporto. Novamente, outra negativa por parte da tripulação. Após ameaças de acender o cigarro, apesar das instruções de segurança, não houve outra saída senão alertar a já descontrolada senhora que a polícia seria acionada para resolver a questão caso o centro das discussões, o cigarro, fosse de fato, aceso.

Na ameaça de atrasar mais ainda o vôo graças ao desejo de fumar da senhora, outros passageiros entraram na discussão. Eis que o vôo foi liberado, antes que a situação tomasse maiores proporções. A porta foi fechada e a senhora resolveu voltar à sua poltrona, mas ainda resmungando: "Agora eu vou fumar um cigarro de qualquer jeito. Lá atrás, dentro do banheiro...". O culpado por tudo isso? O vício. Sem demora uma reflexão ocupou meus pensamentos, numa espécie de fusão entre o assunto de meu compromisso e a situação que acabava de presenciar: pelo mesmo motivo, muitos usuários se viciam em determinadas soluções a ponto de desconsiderar outras alternativas, mesmo que elas, racionalmente, representem mais vantagens sobre aspectos econômicos e tecnológicos. É o vício que faz com que muitos usuários do Windows protejam-se afirmando que o GNU/Linux é mais difícil para o usuário final, mesmo sabendo do crescimento de instituições que vêm adotando-o em seus ambientes. O mesmo acontece com relação ao OpenOffice (ou sua vertente canarinha, o Br-Office) quando comparado com o Microsoft Office. Por vezes, a única razão para tal defesa é o vício.

O mesmo paralelo permanece sobre segurança. É o vício em não mudar certas rotinas e hábitos de trabalho que torna a implantação de procedimentos de segurança uma tarefa árdua e pouco aceita pelos usuários. Proteger "pen drives" corporativos com uma rotina de criptografia para garantir a segurança das informações diante das comuns perdas desses pequenos meios de armazenamento, é um processo simples e eficaz. Entretanto, o fato de ter uma senha para acessar os dados seria, provavelmente, um motivo de rejeição por parte dos usuários.

...pelo mesmo motivo, muitos usuários acabam se viciando em determinadas soluções a ponto de desconsiderar outras, mesmo que estas, racionalmente, representem mais vantagens sobre aspectos econômicos e tecnológicos, por exemplo.

Infelizmente, da mesma maneira que para a senhora fumante, nem sempre outras alternativas são capazes de controlar o desejo de tragar um cigarro, não existem soluções semelhantes para vencer a resistência e o vício dos usuários em determinadas soluções. É preciso, para cada caso, lançar mão da criatividade para encontrar uma solução eficaz. Aí está o maior desafio. **PC**

Servidor de bate papo

Sobre a matéria publicada na edição anterior, gostaria de contribuir com uma dica a respeito da necessidade de ter um servidor DNS para cadastrar o domínio no Pidgin (Windows),pois tive problemas para conectar mesmo usando o IP que cadastrei na máquina virtual Openfire. A solução é a edição do arquivo hosts do windows XP (armazenado na pasta C:\WINDOWS\system32\drivers\etc), como o exemplo a seguir:

127.0.0.1 localhost
192.168.0.50 openfire

Desse modo, acesso minha VM Openfire em um servidor Mandriva 2008 com VMware 1.0.4 e funcionou muito bem. Espero que possa ajudar alguém.
João Batista P. Sousa

Agradecemos sua colaboração João, com certeza irá ajudar.



Compatibilidade do PCI Express

As novas placas gráficas PCI-Express 2.0 são compatíveis com as placas-mãe PCI Express 16x ou terei que fazer um upgrade? Eu tenho uma placa-mãe ECS C51GM-M com placa gráfica XFX 7300 GT (256 MB de memória) e um processador AMD X2 3800+. Nesta placa-mãe posso instalar um processador Phenom 9600?
Miguel Rodrigues
Recife - PE

Em teoria, não há problema de compatibilidade com as versões do PCI Express. Mas não podemos deixar de lembrar que no tempo da predominância do AGP, houve problemas pelo fato de que alguns fabricantes implementaram medidas para contornar as restrições, o que resultou no dano de várias placas-mãe. Até o momento não temos nenhum relato desse tipo de problema com o PCI Express. A C51GM-M não é compatível com o Phenom. A lista de processadores compatíveis com essa placa-mãe pode ser vista no link **http://www.ecs.com.tw/ECSWebSite/Support/CPU_Support_Model.aspx?detailid=653&MenuID=69&LanID=0.**

vPro e Raid

Depois de ter lido a edição nº 69 referente ao VPro, esperei para adquirir uma placa-mãe compatível. Comprei a DQ35MP da Intel, mas estou com o seguinte problema: estou configurando os HDs em RAID 1 (Mirroring) através do Setup e tive vários problemas para instalar o Windows XP Professional, pois o driver necessário, instalado durante a instalação através do pressionamento da tecla F6, não funcionava, seja o fornecido com o produto ou o disponibilizado no site. Num determinado momento, coloquei um mas era para ter colocado outro, troquei e para minha surpresa deu certo. Acredito que os arquivos corretos estavam divididos nos dois disquetes. Depois de ter instalado o Windows (com SP2), comecei a instalar os programas e não estou entendendo porque aparecem dois HDs e por que os programas só estão apenas em um. Li também a edição nº 56 "RAID de HDs" no Linux e entendi um pouco mais como funciona, mas não consegui aplicar ao XP PRO SP2. Acessei no site da Intel para ver sobre o Intel Matrix Storage, mas as versões disponíveis no site são incompatíveis com meu sistema.
Daniel A. Nascimento
São Paulo - SP

Depois de configurar a controladora SATA do Southbridge para o modo de operação RAID, no Setup, você deve acessar o firmware de configuração do RAID ainda durante o POST, para só então partir para a instalação do XP. Esse passo foi executado normalmente? Se puder nos enviar uma foto da tela do firmware da controladora RAID da Intel, será útil para identificarmos o problema.

Resolução de Vídeo

Adquiri há pouco um monitor de 19" para substituir um que chegou ao final de sua vida útil e então me deparei com o problema. O computador utiliza a placa-mãe PC Chips m863g v1.Os drivers que encontrei para a placa de vídeo não dão suporte ao formato 1440x900. O que fazer pra resolver o problema sem ter que adquirir outra placa de vídeo que suporte essa resolução? Tentei ver se atualizações de BIOS resolveriam mas não consegui.
Carlos Alberto

Geralmente a resolução máxima das interfaces de vídeo onboard está limitada à quantidade de memória reservada para elas. Verifique qual é a quantidade de memória alocada para o vídeo. Se já estiver no máximo, não há outra solução além de adquirir uma nova placa. Dificilmente nesse caso uma atualização do VBIOS ajudará.

@ 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

O Linux vai dividir um espaço o Windows no XO

A Microsoft fechou um acordo com a OLPC (One Laptop per Child), que passa a oferecer o Windows como opção de sistema operacional no laptop XO.

Depois de enfrentar problemas com a adoção do Linux e até anúncios controversos de alguns membros de governos que compraram o produto, como "veio com Linux tal, mas vamos trocar para Windows", esse acordo põe fim à resistência que o XO sofria em alguns países.

Há planos de oferecer no futuro o dual boot para disponibilizar os dois sistemas, e também transferir a interface Sugar para o Windows.

LG disponibiliza nova unidade óptica multi formato

Com preço sugerido de R$ 855, a LG oferece o Super Multi Blue GGC-H20L, uma unidade óptica combo oferecendo suporte à leitura de mídia Blu-Ray e HD-DVD, e leitura e gravação de mídia CD e DVD, que também tem integrada a tecnologia Lightscribe, (a impressão diretamente na superfície da mídia). A interface de conexão é a Seral ATA.

O GGC-H20L pode ler mídias Blu-ray e HD-DVD single ou dual-layer. A velocidade de leitura das mídias Blu-ray é de 6x.



VIA Technologies incentiva o desenvolvimento em Linux e o ITX é oficializado como padrão

Ampliando seu incentivo no mundo Linux, a VIA Technologies disponibiliza um portal para os desenvolvedores *em código aberto*. O endereço do portal é **http://linux.via.com.tw** e no momento foram disponibilizados os drivers dos chipsets CN896, CX700/M e VX700 para o Ubuntu 8.04 e o Suse Linux Enterprise Desktop 10. Em breve serão disponibilizados a documentação e o código-fonte. Além disso, também está nos planos para esse ano o fórum e o controle de bugs.

De outro lado, o formato ITX, a plataforma para sistemas compactos criada há alguns anos, terá uma das suas variações, a Pico-ITX, transformada em padrão. A VIA vai transferir para o Small Form Factor Special Interest Group (SFF-SIG), um organismo internacional dedicado à criação e padronização em mini-notes, UMPC´s, controladoras e módulos, como padrão oficial. A SFF-SIG vai redigir documento específico orientando todo o mercado e promover e ampliar o número de fornecedores e clientes que criam e comercializam computadores (SBCs) compatíveis com Pico-ITX.

Queda da pirataria no Brasil

A BSA (*Business Software Alliance*) apresentou o 5º Estudo Anual Global de Pirataria de Software, que apontou queda no índice de pirataria no Brasil. Essa queda foi de 1%, e ao total acumula 5% em dois anos. Entretanto, mesmo diante desses números, o valor do prejuízo aumentou. Ao todo foram pesquisados 108 países, onde em 64 houve queda e apenas em 11 houve aumento. Os Estados Unidos são o país com menor índice de pirataria (20%), porém acumula o maior prejuízo, totalizando mais de 8 bilhões de dólares.

As conclusões do estudo quando à redução são atribuídas à intensificação da globalização entre os países em mercados emergentes; tecnologias de proteção (como o DRM) e novos modelos de negócios (o software como serviço). Quanto ao aumento, o problema está no crescimento nos setores de bens de consumo e pequenos negócios, onde o combate é muito mais difícil, além da popularização do acesso de banda larga.





Gaming PC

Ao que tudo indica, o nicho de TI focado nos gamers engrenou de vez, com diversos fabricantes oferecendo sistemas otimizados para as necessidades desse público. Apresentamos três opções e testamos várias outras, todas disponíveis no Brasil.

Parece que o mercado brasileiro "acordou" para o nicho focado nas necessidades dos jogadores, sejam eles "apreciadores da arte" ou *cyber athletes*. No mundo, já há alguns anos, vários integradores, como a Alienware e a Falcon Northest, oferecem produtos de alta performance não apenas para jogadores, mas para qualquer outro usuário que precise de tal poder. Tentar oferecer uma configuração que atenda a esse público é o que integradores locais tentam fazer há anos, sem muito sucesso.

No Brasil, quem desejava ter uma máquina realmente poderosa tinha que contar com um fornecedor que entendesse realmente o perfil de jogador ou fazer uma peregrinação em diversas lojas para achar os dispositivos sonhados, ou até mesmo, encomendar fora do país, principalmente quando o dispositivo era algo recém-lançado.

Várias tentativas e experimentações foram feitas, a fim de identificar as tendências não apenas do segmento de gamers, mas também de outros, como *media centers* e sistemas compactos. Mas apenas agora, com os incentivos que o governo ofereceu ao mercado, os integradores têm uma condição real de oferecer algo que atenda aos nichos, no caso os gamers, e não algo que se limita a ser rotulado para tal. Podemos resumir em uma palavra o sentimento que existia: frustração.

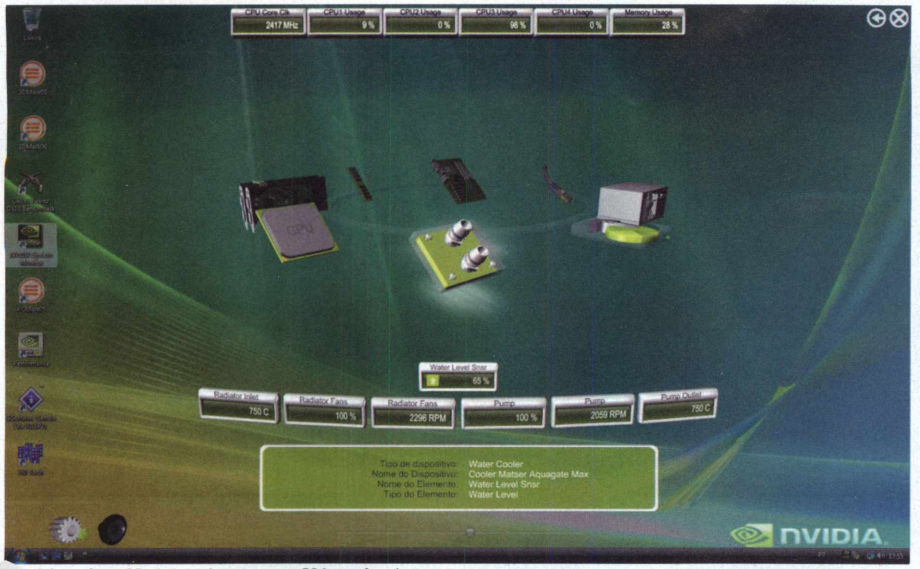
Hoje, o *gap* entre o lançamento no exterior e aqui é bem menor, e por algumas vezes, inexistente, o que demonstra que o mercado está atingindo maturidade suficiente para justificar essas ações por parte dos grandes fabricantes.

Algumas opções

Antes, como comentamos, praticamente não havia máquinas de alta performance prontas, de "grife" ou qualquer outro integrador nacional. O usuário precisava ter conhecimento acerca dos produtos ou ter um vendedor de confiança para comprar seu equipamento. Hoje, alguns fabricantes oferecem boas opções, que não ficam devendo para muitas configurações DIY (o famoso *Do-It-Yourself*, ou faça você mesmo), além do fato de que a venda é totalmente legal, com nota fiscal e os impostos devidamente pagos. Numa rápida pesquisa na internet, podemos achar alguns deles.



Anderson C. D. Costa
Técnico de TI com mais de 10 anos de experiência na área de manutenção e integração de hardware, com especialização nos mecanismos de refrigeração de PCs.



F1. A interface 3D de monitoramento ESA em funcionamento.

Um exemplo é a *Preview*, que pode ser considerada uma das empresas pioneiras no mercado a oferecer máquinas diferenciadas do modelo tradicional. E por "modelo tradicional" entenda como sendo máquinas com configuração modesta e sem apelo estético, ou melhor, sem qualquer apelo a não ser uma condição "facilitada" de compra.

São três linhas bem destacadas no site, agrupadas sob soluções: casa, jogos e empresa. Há um destaque para o *Preview Workstation*, que não está sob nenhum desses agrupamentos. Embora exista uma configuração definida, a *Preview* oferece a possibilidade de personalizar alguns dos componentes que integram o computador.

Dentro das soluções para jogos, há quatro produtos: o Platinum, o Platinum Over e o Exclusive série limitada, que são baseados nos processadores Intel Core 2 Quad, e mais um Exclusive, baseado no processador AMD Athlon 64 X2. Todos utilizam GPUs NVIDIA GeForce série 8000, embora o Exclusive com processador AMD utilize uma placa-mãe dotada de vídeo onboard da ATI.

Os mais poderosos da linha são os Platinum, que são overclockados de fábrica. O Platinum usa o Core 2 Quad QX6750 de 3GHz para 4 GHz, e o Platinum Over usa um Q6600 de 2.4GHz operando a 3GHz.

Seguindo um caminho similar, existe a Login, que também faz parte do time de integradores que procuraram se diferenciar do modelo tradicional, mas que focou sua atividade principalmente no norte e nordeste do país, conforme as informações fornecidas em seu site.

Suas configurações não são tão sofisticadas, mas não deixam de oferecer qualidade, integrando pelo menos dispositivos da classe *mainstream*.

A linha da Login que pode atender aos gamers é a LOG HiPower, que possui quatro modelos: dois baseados no Core 2 Duo E6600 e outros dois baseados no Core 2 Quad Q6600. Todos usam GPUs ATI/AMD Graphics Radeon HD 2600PRO ou XT (apenas em uma das configurações baseada no Core 2 Quad).

O *Blackbird* 002 é a opção oferecida pela HP aos gamers, que aliás tem um apelo e tanto: utiliza a placa-mãe Asus Strike Extreme, que utiliza um chipset NVIDIA, o nForce 680i SLI. Alguns detalhes técnicos chamam atenção, é que dentre as opções oferecidas pela HP, são disponibilizadas duas com placas de vídeo ATI. Se está em CrossFire, ou apenas em Multi Head, (suporte para mais monitores) não fica claro. O que consta em fóruns na internet é que o BIOS feito pela HP suporta o CrossFire e também é compatível com qualquer Asus Strike Extreme. Infelizmente não tivemos a oportunidade de realizar tal teste.

A HP é uma das grifes de computador que está presente há anos no Brasil, porém, até o fechamento da edição, esse produto não constava da linha de produtos disponíveis para comercialização local. Tradicionalmente, a HP mantém um intervalo entre lançamentos no exterior e aqui no mercado local.

Em mãos

É claro que não ficaríamos limitados a uma pesquisa na internet. É importante reconhecer que os modelos citados já têm reconhecimento e espaço no mercado. De qualquer forma, ainda há aqueles que preferem montar sua própria configuração e, além disso, existem vários outros integradores entrando na disputa por um lugar ao sol nesse nicho que fica mais disputado a cada dia.

Uma máquina personalizada

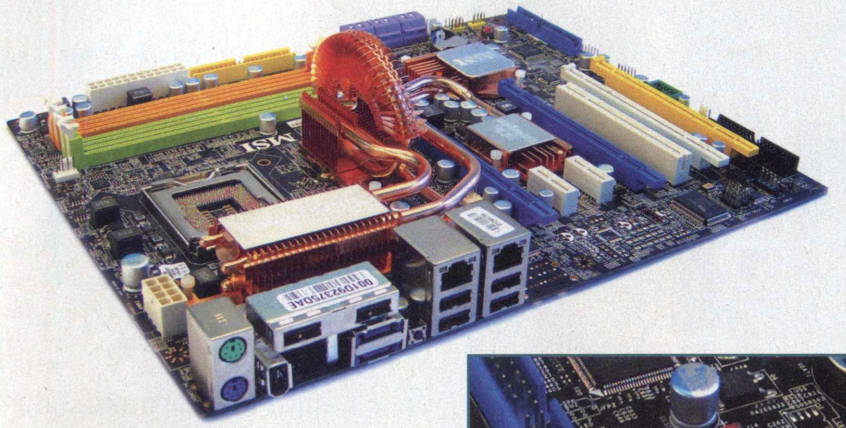
Qualquer gamer que optar por montar o seu sistema, com certeza vai começar a partir da placa de vídeo. Ao ter condições de adquirir a melhor, a escolha vai recair sobre a GeForce 8800 Ultra ou 9800 GX2. Vai optar também por uma placa-mãe com um chipset poderoso, como um X38 ou X48 da Intel, ou mesmo algum da NVIDIA, como o maduro nForce 680 ou os recentemente lançados 780i ou 790i, sendo que esses dois últimos também se valem da iniciativa ESA – *Enthusiast System Archteture*. Outra escolha óbvia é o processador Core 2 Quad ou Extreme, dependendo das intenções do gamer. A memória vai ser de no mínimo 2GB de baixa latência, algo que os fabricantes de boa qualidade já oferecem em alguma das suas linhas.

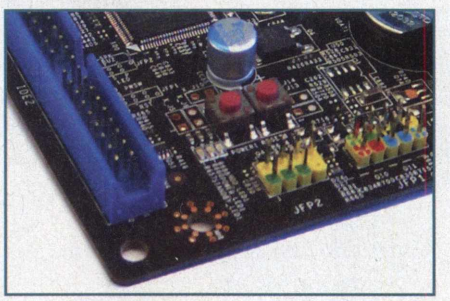
NVIDIA 780i e 790i

Num primeiro momento, a NVIDIA lançou dois chipsets da família nForce 700, o 780i SLI, o 790i SLI e 790i Ultra SLI, todos para o segmento *high-end*, que é onde as *games machines* se "alimentam". A família já cresceu, sendo composta por outros modelos para os segmentos *mainstream, value e entry-level*. Note o que sufixo "i" é um indicativo direto de que o chipset é para processadores Intel. Para os modelos AMD, é adicionado o "a".

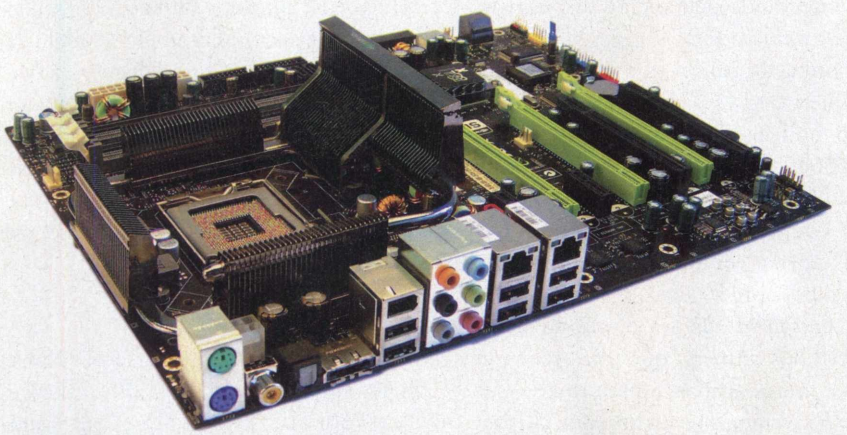
A diferença essencial entre o 780i SLI e os 790i é o suporte à memória e ao FSB. O 780i utiliza memória DDR2 de até 1333MHz. Os 790i têm FSB de 1600MHz, e a freqüência da DDR3 é de 1600MHz para o 790i SLI e 2000MHz para o 790i Ultra SLI. Outra exclusividade dos 790i é o suporte ao Quad SLI, que é o emprego de duas GeForce 9800 GX2.

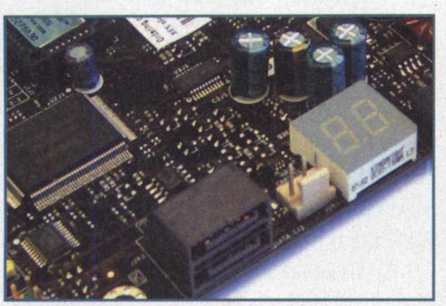
Além dessas características, a série nForce 700 apresenta algumas novidades, como o ESA e um upgrade do SLI, o 3way

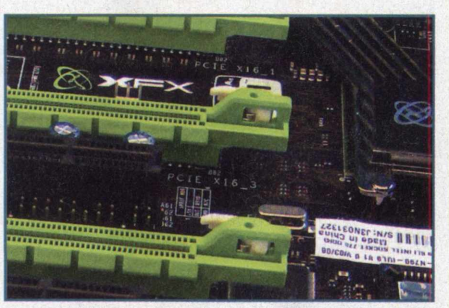




F2. A MSI P7N Diamond é integrada com o nForce 780i. Note os *micro-switches* para ligar e resetar o equipamento, uma facilidade nos processos de testes e manutenção. O sistema de refrigeração é robusto.







F3. A XFX N790i- IUL9, que usa a versão Ultra do nForce 790i. Note o display do *POST integrado*, o conector SATA e o tipo de travas dos slots PCI Express.

SLI, que possibilita a utilização de até 3 placas de vídeo, aumentando o poder de processamento gráfico.

O ESA foi apresentado ao público há alguns meses e alguns produtos compatíveis também foram lançados, mas o principal, a placa-mãe, levou um pouco mais de tempo. Especulou-se que a NVIDIA enfrentou problemas na integração dessa tecnologia, que é um dos apelos presentes na série nForce 700. Mas reiteramos, foi apenas especulação, e agora as placas-mãe já estão no mercado e com o ESA em operação (**figura 1**).

Relembrando um pouco, o ESA é um padrão para monitoramento de dispositivos, os quais obrigatoriamente devem ser compatíveis com ela, e que se vale da interface USB para fazer a comunicação entre o sistema e o dispositivo em si. O fato de usar o barramento USB torna a sua implementação muito simples, bastando conectar o chicote a um *header* livre e pronto, dispositivo monitorado. Ele é identificado pelo Windows como um Dispositivo de Interação Humana, bem como um teclado ou mouse.

O monitoramento em si sempre é muito bem-vindo, ainda mais se o seu uso é facilitado e a interface mais atraente. A NVIDIA realmente caprichou nesse aspecto, pois há dois modos de monitoramento. O primeiro podemos chamar de padrão, que exibe uma janela de tamanho discreto, com o nome do dispositivo e a grandeza monitorada acerca do dispositivo, como temperatura ou rotação de ventoinha. O outro é 3D, com uma representação visual de cada dispositivo passível de monitoramento.

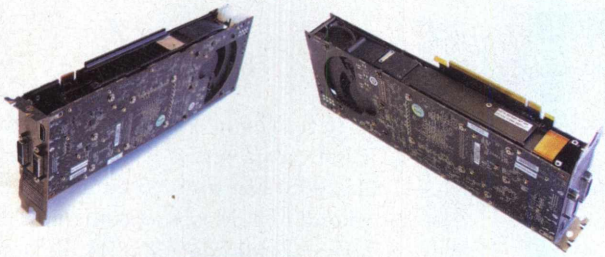
Esse software de monitoramento faz parte do NVIDIA *System Tools*, e o monitoramento não está limitado a dispositivos ESA. O ESA, em principio, é um mecanismo que estará presente em fontes de alimentação, watercoolers e gabinetes. Os dispositivos ESA utilizados são da Cooler Master, o watercooler Aquagate Max e a fonte de alimentação Real Power ESA 1000W. Como o ESA trabalha "em cima" da USB, a conexão (e a desconexão) pode ser feita a "quente" e o monitor reconhecerá o dispositivo imediatamente.

O 3way SLI é a outra novidade do nForce 700. É uma pena que no momento são poucas as aplicações que se valem de todo o poder oferecido pelo uso de três placas de vídeo simultaneamente. Diante desse cenário, o ganho fica limitado ao campo da teoria.

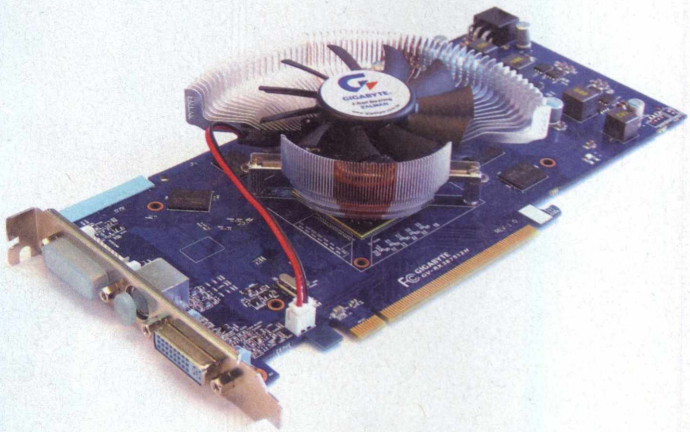
Ao contrário do que se pode imaginar, o 3way SLI não é suportado pela geração 9000 da GeForce, sendo apenas pelas 8800GTX e Ultra. Considerando o Quad SLI, se a 9800 GX2 suportasse operação em 3way, não seria Quad SLI, mas algo como Hex SLI, já que seriam seis GPUs em operação conjunta. Quem sabe no futuro veremos essa "limitação" resolvida.

A placa-mãe com o 780i utilizada nos testes é a MSI P7N Diamond (**figura 2**), e a 790i é a XFX N790i- IUL9 (**figura 3**). No caso, essa XFX utiliza o 790i Ultra.





F4. A GeForce 9800 GX2, a mais nova e potente integrante da família. Note o arranjo das placas, o cooler "compartilhado" e a ponte SLI posicionada na base, próximo ao espelho. Observando com atenção são utilizadas duas pontes sobrepostas.



F5. A Radeon HD 3870, um design dentro do padrão visto em diversos modelos. Essa é da Gigabyte e utiliza um cooler da Zalman.

Ambas possuem detalhes que indicam claramente que o produto é para quem quer performance e, sobretudo, gosta de testar o sistema antes de montá-lo no gabinete. Para facilitar esse procedimento, foram integrados dois *micro-switches*, um homólogo ao botão liga/desliga e o outro é o *reset*. Na XFX, ela está na extremidade esquerda da placa-mãe, ao lado do último slot. É uma boa posição, considerando os seguintes cenários: teste em bancada, ficar fora da trajetória das placas de expansão, e o gabinete ter um bom espaço interno, como é o caso do Cosmos S, facilitando os testes e manutenção.

Já no caso da MSI, os botões estão na frente dos slots. Não é uma boa posição, pois, conforme a instalação das placas, o acesso aos botões é dificultado. Mas para compensar, ela não tem um jumper de ClearCMOS, mas sim um *micro-switch* no painel I/O ATX. Para um profissional ou usuário avançado, tal posição é muito prática. É um recurso que, conforme o cenário, pode ser tanto uma facilidade como um "calcanhar de Aquiles".

Por fim, a bridge SLI. Na XFX ela é rígida, empregando uma PCB (placa de circuito impresso) e os conectores necessários, sendo um para o SLI e o outro para o 3way SLI. Na MSI, são empregados três *bridges* flexíveis: dois curtos para o SLI e um mais longo, que é usado em conjunto com os outros para "fechar" o 3way SLI. A sua configuração lembra um enlace na forma do número "8".

GeForce 9800 GX2

A GeForce 9800 GX2 (**figura 4**) é o novo topo da NVIDIA, sendo dotada de dois GPUs em uma mesma placa de vídeo, o que, em teoria, duplica a capacidade de processamento gráfico do sistema.

A NVIDIA adotou uma solução interessante na GeForce 9800 GX2: são realmente duas placas de vídeo fisicamente independentes e ligadas através de uma ponte (*bridge*) SLI. Mesmo com toda essa independência, elas compartilham o cooler e a interface PCI Express x16. Muitos criticam tal saída, porém, de um modo ou de outro, foi uma implementação bem superior se comparada ao impacto negativo da utilização do bridge AGP para PCI Express, utilizada na geração 5 da GeForce.

Ela é dotada de 256 *Stream processors* e conta com 1GB de memória em uma interface de 512 bits. Além desses incrementos, sempre existentes quando uma nova família é lançada, a 9800GX2 suporta a API DX10 (um elemento padrão em qualquer lançamento atual) e é capaz de acelerar o processamento de vídeo de alta definição através do PureVideo HD. A interface HDMI e o suporte a revisão 2.0 do barramento PCI-Express complementam as especificações básicas.

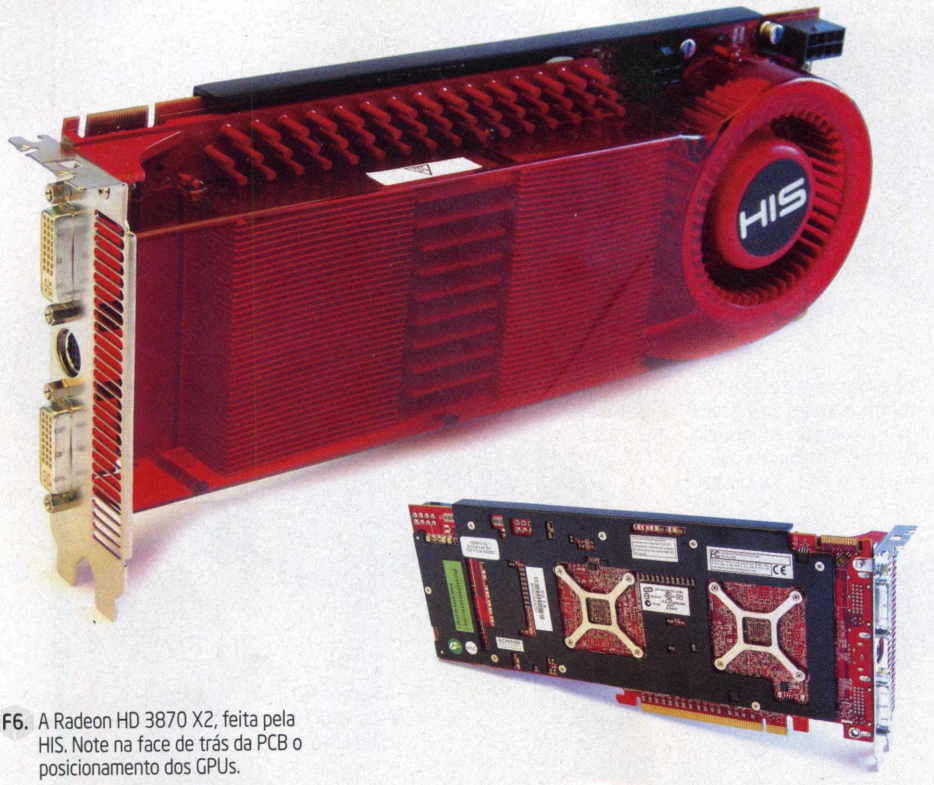
Há também o Quad SLI, que já comentamos ao falar do nForce 790i. O que não fica claro é se essas especificações são de apenas um GPU GeForce 9800 GX2, ou se são a soma de duas unidades. Tal como nas gerações anteriores, as conexões de monitor são DVI.

O consumo de energia é uma das maiores preocupações da indústria de PCs na atualidade e a NVIDIA integrou alguns recursos de gerenciamento, a exemplo do *Hybrid Power* que é configurado através de um Painel de Controle desenvolvido pela própria empresa, mas que por ora só está disponível nos chipsets para a plataforma AMD.

ATI Radeon HD 3870 e 3870 X2

Antes de a AMD comprá-la, a ATI deu alguma canseira na NVIDIA quando lançou a série Radeon X, iniciada com a X800. A nova série, que foi continuada com a X1000, entrou na era da alta definição com a HD X2000 e, mais recentemente, foi lançada a mais nova integrante, a HD 3000.

Cada GPU HD 3870 é dotado de 320 *Stream processor*. Na X2 esse número é duplicado, de modo que, pelo menos em teoria, esta é, sem dúvida, uma configuração de respeito.



F6. A Radeon HD 3870 X2, feita pela HIS. Note na face de trás da PCB o posicionamento dos GPUs.

Questões financeiras

Devido a limitações financeiras, muitos acabarão ficando com alguma placa de vídeo da série GeForce 7000, que tem preços convidativos atualmente ou, pelo menos, tentar adquirir uma GeForce 8600. Claro que há as opções da ATI/AMD com a série Radeon, mas que, nos últimos tempos, não têm obtido um grande apelo junto ao público.

A HD 3800 tem suporte para vídeo em HD (*High Definition* – Alta Definição) através do Avivo HD, sendo capaz de exibir imagens superiores a 1080p (utilizando uma conexão Dual DVI) e, é claro, mediante a utilização de conexões HDMI integral, com vídeo e som de 5.1. Há, também, suporte ao DirectX 10.1, OpenGL 2.0, PCI Express 2.0 e à sua tecnologia de gerenciamento de energia, a ATI Power Play. A interface de memória é de 256 bits suportando GDDR3 e 4.

A HD 3870 (**figura 5**) utiliza um design tradicional, sem novidades. Se não fosse pelo modelo de cooler adotado na unidade testada, ela facilmente ocuparia apenas um slot do sistema. Já a HD 3870 X2 (**figura 6**) é diferente. Ao contrário da NVIDIA, que optou por utilizar duas placas de vídeo, a ATI preferiu utilizar dois GPU's numa mesma placa. E deu o nome de CrossFire X ao utilizar as duas GPU's. Teoricamente, o CrossFire X já vem ativado de fábrica, mas existem informações de que, alguns modelos, precisam ser configurados manualmente.

Para a NVIDIA, não foi problema utilizar duas placas, já que os modelos top de linha, mesmo quando utilizavam apenas uma PCB, ocupavam o espaço de duas placas de qualquer jeito. A opção da NVIDIA garante funcionamento e, além do mais, já é um caminho conhecido pela empresa. Trocando em miúdos, é uma forma de oferecer um produto multi-GPU rapidamente sem a necessidade de realizar mais pesquisas.

A solução da ATI é tecnicamente mais refinada, já que esse design sugere que os GPUs são capazes de se comunicar diretamente, sem o risco de haver gargalos nessa comunicação. Claro que deve haver algum mecanismo, mesmo que seja de uso do próprio circuito, para desligar um dos GPU's, visando o gerenciamento de energia.

A ATI também deu um nome à utilização de duas HD 3870 X2: CrossFireX, que permite escalar duas, três ou quatro das GPUs.

Instalando e configurando

A instalação do sistema operacional, no caso, o Windows Vista, não teve segredos ou qualquer tipo de problema. A plataforma que demandou alguma atenção foi a da NVIDIA, pois há dois pacotes de *drivers* nForce disponíveis no site.

Em vários casos, o mecanismo de seleção tem várias opções, mas sempre remete ao mesmo arquivo. Mas, no caso do nForce 7, se escolhermos o 780i ou algum 790i, é indicada a versão 9.64 de 18 de março de 2008. Esse arquivo também suporta o nForce 680. Mas, se escolhermos o 780a, a versão indicada é a 18.11, de 9 de abril de 2008, que suporta o 750a, 710a, Geforce8300, o nForce8200/nForce 730a e o Geforce8200/720a.

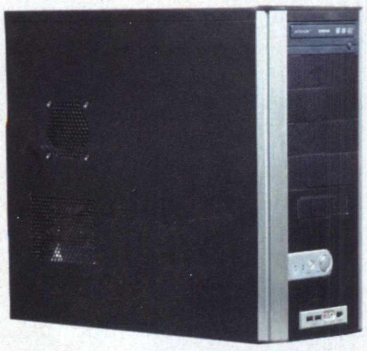
Ao instalar um pacote não indicado, o sistema ficava simplesmente instável. A explicação para isso estava bem debaixo dos nossos narizes: um dos pacotes é para as implementações baseadas em CPU's Intel e a outra, para AMD. Em suma, não é apenas uma brincadeira com rótulo, há outras diferenças, nem que essas se limitem à configuração.

Já com a placa-mãe de chipset Intel, não houve problemas, foi uma instalação bem tranqüila.

Com o lançamento das GeForce 9000, a NVIDIA evidentemente lançou um novo Forceware exclusivo para elas, com número de versão iniciado em 174. O primeiro *release* do driver (174.53) suportava apenas a 9800 GX2 e a 9600GS, e o segundo (174.74) incluiu o suporte aos outros modelos. Para as GeForce 8000, o último lançado até o fechamento dessa edição foi o 169.25.

Para as Radeon HD 3000, em especial a HD 3870 X2, o CrossFireX só está disponível a partir da versão 8.3 do Catalyst. Nós utilizamos a versão 8.4.

Optamos pelo conservadorismo na configuração do processador e das memórias, utilizando os valores nominais, sem *overclock*.



F7. O Flame da Evolute, empresa utilza vários produtos da Cooler Master.



F8. O Celerety: versão avaliada veio integrada com um leitor de Blu-Ray. A predominância desses modelo é da Gigabyte



F9. O Comet, top de linha da Evolute, usando duas GeForce 8800 Ultra em SLI, refrigeradas por um watercooler. O CPU também recebeu o mesmo tratamento.

Evolute Gaming Flame e Celerity

Na edição anterior, noticiamos o lançamento dos três modelos da *Evolute Gaming*, e tivemos a oportunidade de testá-los nessa edição.

Pode soar estranho analisar dois modelos simultaneamente, mas isso é facilmente explicado: a configuração do sistema (CPU, placa-mãe, memória, placa de vídeo e HD) é igual. As diferenças entre o Flame e o Celerity se resumem ao gabinete, fonte de alimentação, cooler da CPU e drive óptico.

Ambos são integrados com o Core 2 Quad Q6600 de 2.4GHZ operando em *overclock* de 3GHz, a placa-mãe utilizada é a Gigabyte GA-P35-DS3 com 4GB de memória RAM fabricada pela OCZ, a placa de vídeo também é da Gigabyte, baseada no GeForce 8800GT, HD Western Digital Caviar de 500GB e um leitor de cartões.

O Flame (**figura** 7) utiliza vários produtos da Cooler Master, como o gabinete Centurion 5, o cooler Hyper TX2, a fonte de alimentação Extreme Power 500W e uma unidade de DVD-RW da LG.

Já o Celerity, usa maciçamente produtos da Gigabyte: o gabinete 3D Aurora 570 Black, o cooler G-Power Pro e a fonte de alimentação Odin GT 550W. A primeira leva dos Celerity empregava uma unidade óptica Blu-ray.

A Evolute optou por utilizar produtos de linha de marcas de qualidade e também de reconhecimento no mercado. A montagem é bem feita, privilegiando a organização e o fluxo de ar interno. Foi uma escolha bem acertada, já que assim, dá liberdade de upgrade ao usuário.

Aliás, é bom que se diga que o upgrade feito pelo usuário sempre foi um assunto encarado com um certo tabu pelos fabricantes, uma vez que eles não têm como aferir com precisão se o usuário, ou a pessoa à qual ele delegou a operação, tem o conhecimento ou a competência necessárias. Assim, tais processos só eram permitidos nas assistência técnicas autorizadas e com poucas opções. A Evolute nos informou que o usuário pode fazer um upgrade, porém, é necessário que entre em contato com o Suporte Técnico para que seja registrado, no histórico daquela unidade, a permissão de abertura para upgrade. O controle de histórico de cada unidade é feito através de números de série.

O *overclock* das unidades testadas funcionou muito bem, e notamos que houveram cuidados com a configuração da temporização da memória, definida manualmente.

Evolute Gaming Comet

O Comet é o topo de linha da Evolute, é dotado de uma configuração agressiva para o gamer que não se contenta com nada inferior ao máximo de performance. Seguindo a mesma linha dos seus irmãos Flame e Celerity, são empregados produtos de marcas reconhecidas no mercado e componentes de alta performance.

A Evolute nos informou que essa é uma configuração de referência, já que o Comet poderá ser configurado conforme as necessidades (e desejos) do usuário.

A unidade enviada para testes, que não é uma versão comercial, mas apenas para demonstração, estava integrada com



F10. O XPS é a aposta da Dell no segmento de games.

um processador Core 2 Quad Q6600 de 2.4GHZ, 2GB de memória RAM da OCZ (pertencente à série Reaper HPC de 1066 MHZ), placa-mãe EVGA com chipset nForce 680i, dois HDs Western Digital Raptor X de 150GB operando em RAID 0, duas placas de vídeo EVGA GeForce 8800 Ultra operando evidentemente em SLI, sendo que essa é uma versão com *overclock* de fábrica que utiliza um *waterblock* digno de respeito.

A Cooler Master está fortemente presente nesse modelo, com dois watercoolers, o Aquagate S1 para o processador e o Aquagate Max para as placas de vídeo, a fonte de alimentação ESA 1000W que, como o nome sugere, é compatível com o ESA da NVIDIA, e o gabinete Cosmos S, que pode ser encarado como uma uma versão "tunada" dos Cosmos testado em edições anteriores.

A configuração de referência da versão comercial do Comet é integrada com um processador Core 2 Extreme QX9650, 4GB de memória RAM e fonte de alimentação Cooler Master Real Power Pro de 1250W, além do Windows Vista Ultimate de 64 bits.

Mesmo sendo uma unidade de demonstração, os dispositivos que compõem o Comet são potentes tanto em suas características técnicas como no visual. Por exemplo, a OCZ Reaper HPC, dotada de dissipadores com *heatpipes*, as janelas do Raptor X, os waterblocks da placa de vídeo e o gabinete Cosmos S que, com suas dimensões avantajadas, permite que os dois watercoolers sejam instalados dentro dele sem maiores problemas. Conforme dito, o Cosmos S possui várias características similares às do Cosmos original, mas tem alguns detalhes, como o botão liga/desliga, que não é um *push-button*, mas do tipo membrana. Basta ter contato com sua superfície para provocar o acionamento.

Por último, mas não menos importante, a placa-mãe EVGA. A EVGA e a XFX tipicamente são os primeiros fabricantes a oferecerem produtos de alta performance baseados em soluções da NVIDIA. O design de refrigeração da placa-mãe se vale de *heatpipes* e não se limita aos Northbridge e Southbridge (chips Ponte Norte e Sul do chipset, respectivamente), estendendo-se ao circuito regulador de tensão (Vcore) do processador. Os micro-switches evidentemente estão presentes.

Além dos testes com o Windows Vista Ultimate de 64 bits, também realizamos alguns com a versão de 32 bits.

Dell XPS 720

Há alguns anos, a Dell decidiu entrar no mercado de games lançando a série XPS, e fez algum barulho no mundo, já que, até então, não eram muitas as opções oferecidas para gamers.

O XPS 720 (**figura 10**) tem algumas configurações, porém a mais poderosa não está disponível no Brasil. O modelo testado utiliza um processador Core 2 Duo E6850 de 3GHz, placa de vídeo GeForce 8800 Ultra, 4GB de memória Corsair Dominator, dois HDs em RAID 0 e um DVD-RW. Evidentemente, ele já vem com um sistema operacional instalado que, no caso, é o Windows Vista Ultimate de 32 bits.

Como em diversos modelos, a Dell utiliza um design próprio, inconfundível, e não foi diferente com o XPS. A aparência (e o peso) sugere que o gabinete tenha acabamento em aço escovado, mas é de plástico com um acabamento similar e muito bem feito.

As suas linhas inspiram velocidade, algo como uma turbina de alta capacidade, com um pequeno toque retrô. Complementando esse visual *high-tech*, foram integrados LEDs para iluminação no painel frontal e também no traseiro. São 16 opções de cor com controle de intensidade e efeitos, como luz estro-

boscópica, pisca-pisca, intercâmbio de cores e (para quem não aprecia esses adornos) desligar tudo. Esse adorno visual é controlado por um software pré-instalado no sistema, o Quick Set, e por mais absurdo que pareça, também pelo BIOS!

Ao olhar o painel traseiro, uma surpresa: o formato do XPS é o BTX, o que explica o seu peso. Geralmente gabinetes BTX são mais pesados que os ATX.

As dimensões do gabinete são bem grandes, o que lhe proporciona um ótimo espaço interno. Além do cooler característico do formato BTX, logo abaixo dele, existe mais uma ventoinha para auxiliar na refrigeração da placa de vídeo. As GeForce 8800 costumam ser integradas com uma espécie de carenagem em cima do cooler para otimizar o fluxo de ar, mas nesse caso , ela é aberta, o que explica a presença da ventoinha. Os HDs estão posicionados na traseira do HD, onde seria o espaço reservado às fontes de alimentação no formato ATX.

A Dell costuma projetar o hardware que utiliza, e com o XPS não seria diferente. A placa-mãe emprega o chipset NVIDIA 680i, com três PCIs, três PCI Express x16, um PCI Express x1, oito portas USB (sendo duas frontais) e duas *Firewire*, uma frontal e outra traseira.

Notamos um fato curioso: a unidade testada é na cor prata, e como já comentamos, utiliza uma GeForce 8800 Ultra (informado pelas propriedades do sistema). Mas no site da Dell Brasil, só estão disponíveis modelos na cor preta. Outro ponto curioso encontrado no site, é uma menção discreta à possibilidade de o XPS receber uma configuração SLI. Porém, ao configurar o sistema, não encontramos nenhuma opção para a adição de uma segunda placa de vídeo. Existe opção para a Ageia PhysX (que hoje é da NVIDIA), mas não para uma segunda opção de placa de vídeo e pior, nada de 8800 Ultra, apenas GTX e modelos de menor capacidade.

Não vamos classificar isso como um problema, pois, em outras oportunidades, já percebemos que a Dell, quando contatada pelo telefone, pode oferecer condições ou promoções bem convidativas que não são divulgadas no site, o que pode explicar a ausência desse modelo testado no site.



F11. O G15 Gaming Keyboard da Logitech, uma das opções mais apreciadas pelos gamers.

Acessórios

Até algum tempo, qualquer acessório com algum design diferenciado era rotulado como "para gamer". Ainda havia o agravante dos jogos serem vistos como coisa de criança, e os jovens e adultos, que apreciavam esse entretenimento, sofriam alguma marginalização, sem nos esquecermos das diversas piadinhas. Atualmente a história é bem diferente.

Além da separação em definitivo da relação entre gamer e criança, temos opções de qualidade que são verdadeiramente focadas nas necessidades (e também desejos) de um gamer, seja apenas um aficionado que não abre mão da qualidade, ou um profissional que precisa de bons produtos para obter o seu melhor desempenho.

Alguns marcas se consagraram nesse nicho, como a Zalman com o seu fone de ouvido 5.1, a Razer com os seus teclados, mouses e pads, a Saitek com os seus *joysticks* e, claro, a Logitech, além de outras marcas. Sendo um nicho promissor, e mais maduro do que nunca, outros fabricantes também entraram na onda. Ora oferecendo qualidade, fator que acaba elitizando um produto, ora preço, que é mais importante para as massas, contribuem, e muito, com a popularização do segmento.

Foram testados três teclados e dois mouses para games. Começando pelas marcas de elite, temos o Logitech G15 Gaming Keyboard e o G5 Laser Mouse, o Microsoft SideWinder Mouse e, por fim, o Game Pad Action Strike e o teclado Combat Strike, ambos da Leadership.

O teclado G15 Gaming Keyboard (**figura 11**) pode ser encarado como uma evolução do G11, algo como uma versão expandida. O design é essencialmente o mesmo entre os dois, porém o G15 é maior, com mais botões de macro, e o LCD não é integrado ao teclado, mas ao estilo *clamshell*, podendo ser fechado ou aberto quando desejado. As teclas têm *backlight*, com dois níveis de intensidade e pode ser desligado. Em ambientes mais escuros, proporciona um visual atraente, com um ar *sci-fi*. Em tempo, os níveis de intensidade das teclas é ajustado em conjunto com a do LCD.

Sem o driver, o LCD não tem qualquer função, exibindo apenas o logotipo da Logitech. Após a instalação do driver, que inclui o respectivo painel de controle, podemos usufruir dele. Em tempo, a integração do LCD com o sistema operacional só é compatível com o Windows Vista, através do recurso SideShow, que é a capacidade de exibir informações em um display secundário.

Incluídos no driver, estão os applets de exibição de data e hora, contagem de tempo (*countdown e stopwatch*), monitor do servidor de e-mail POP3, monitor de performance (uso do CPU e da memória) e monitor de mídia. Há outros dois applets, o *G-Series Keyboard Profiler* e o *Scripting*



F12. O G5 Laser Mouse que, assim como o G15, também é um dos alvos de desejo dos gamers. No detalhe, o compartimento dos pesos.

Mouses de alta resolução

Mouses com resolução alta, para muitos, é apenas uma questão de velocidade de movimentação do ponteiro, o que chega a ser irritante de tão arisco que fica o manuseio. Mas, percebemos a necessidade deles ao usar monitores de 20" ou superiores. Nos monitores 4:3 utilizando resoluções "tradicionais", como a 1024x768 ou 1280x1024, um mouse de alta resolução é apenas chato, por ser rápido demais. Mas nos monitores *widescreen* a partir de 20" utilizando resoluções de 1680x1050 ou 1900x1600, eles fazem a diferença, pois nesses casos, o mouse tem área suficiente para se deslocar e manter uma velocidade confortável de utilização.

Utilizamos dois monitores, um da Dell e um da Acer, de 22" e 24" respectivamente. Ao usar a resolução de 800dpi, para deslocar o ponteiro do canto inferior ao superior, era necessário dar uma "levantadinha" no mouse para ter espaço para manuseá-lo. Em resoluções menores, era um tormento. Já acima de 1600 ou superior, o movimento era perfeito.

Assim, ao comprar um monitor grande, não se esqueça de considerar a troca do seu mouse.

Display, que não exibiram nada no LCD. Já entre os dependentes do sistema operacional, no caso providos pelo Slide Show, estão o Windows Mail e o Media Player, onde respectivamente é exibido o número de e-mails não lidos e a música em execução, bem como sua duração. Como o sistema utilizado para o teste do G15 usava um chipset NVIDIA, o gerenciador do G15 identificou e automaticamente instalou um *applet* acerca do software de monitoramento incluído no driver.

Essa capacidade de identificação automática também se estende aos jogos instalados no sistema. Existindo algum suporte, o perfil é automaticamente instalado. Por exemplo, o Crysis é um jogo DX10 suportado pelo G15 e que, por ser utilizado em nossas baterias de teste, já estava instalado no sistema. Quando instalamos o driver, a presença do jogo foi identificada e o perfil carregado sem qualquer dificuldade após a confirmação do usuário. Quando o Crysis é executado, o seu logotipo aparece no LCD enquanto ele é inicializado, e durante o jogo, é exibido o status da energia, do armamento e do modo da Nanosuit.

Além do painel, o G15 é dotado de 18 teclas macro. Em conjunto com as teclas M1, M2 e M3, é possível acessar rapidamente conjuntos de macros previamente configurados. Claro que outros perfis podem ser criados, mas para utilizá-los será preciso acessar o gerenciador do G15 para fazer a seleção. Através do botão MR, gravamos rapidamente uma macro e também definimos um tecla G para ela.

Outros botões presentes são os referentes à navegação do display LCD, multimídia (com direito a controle de volume com potenciômetro) e tecla mudo. A conexão ao PC é através da porta USB. Aproveitando esse fato, são integradas duas portas USB para a instalação de pen drives ou acessórios dessa natureza. A propósito, o cabo mede aproximadamente 1.8m

Quanto aos outros detalhes, as suas teclas têm a altura padrão de qualquer outro teclado, bem como o curso de acionamento, sendo bem macio sem deixar de ser firme. O layout do teclado é o Inglês Internacional, que é uma das opções presentes ao escolher o idioma Português do Brasil.

O G5 Laser Mouse (**figura 12**) é o companheiro mais comum do G15. E um detalhe muito importante: a Logitech tem dois mouses com esse mesmo nome, mas que se diferenciam por três pontos: o código do produto, a cor e a presença de botões laterais de navegação. O modelo testado tem o código 931376 e apenas um botão de navegação lateral. Outra diferença, descrita nas especificações técnicas do site, diz respeito à velocidade de transmissão que é de 1000 por segundo, contra 500 por segundo da unidade testada. Já o driver, informa que a transmissão é de 1000.

É empregado um sensor laser, ou seja, maior precisão sem o incômodo do feixe colorido dos mouses ópticos. Sua resolução máxima é de 2000dpi, com configuração padrão de passos de 800 e 400. Através do software que o acompanha, é possível colocar mais dois passos intermediários, além de mudar todos os valores. Há um indicador com três LEDs para indicar a velocidade. Se forem usados os cinco passos, ao selecionar os valores intermediários, serão acendidos dois LEDs.

Todos os botões podem ter suas funções personalizadas. Vários mouses têm os botões laterais que geralmente são atribuídos à navegação de páginas, exatamente as funções Avançar e Voltar. Esses botões foram integrados junto à roda, que ao ser pressionada lateralmente terá essas funções.



F13. Sidewinder Mouse, o mouse para gamers da Microsoft. No detalhe, o display e a gaveta de pesos.



F14. O *Game Pad Action Strike* da Leadership, compacto, prático e com acionamento macio. O curso das teclas é o que normalmente encontramos em qualquer teclado.

Um dos pontos fortes do G5 é a possibilidade de ajustar seu peso e, conseqüentemente, o equilíbrio. Para tal, há um compartimento que abriga os pesos. Ao total são 4 pesos de 4,5 gramas e outros 4 de 1,7 gramas.

Embora grande parte dos negócios da Microsoft seja Windows e Office, a empresa também possui sua linha de hardware, como os dispositivos de entrada. O primeiro, que foi o Natural Keyboard, fez muito sucesso à sua época. O SideWinder é uma marca popular entre os usuários em geral, quando se fala de controladores de jogo com qualidade. Claro que os profissionais e entusiastas vão conhecer outras marcas e não raro, ter outras opiniões.

O *SideWinder Mouse* (**figura 13**) apresenta um design relativamente discreto com pequenas excentricidades, como os botões laterais ressaltados e o compartimento de pesos, que é uma espécie de gaveta e, por fim, um display que exibe a configuração de DPI e o status de gravação e execução de macros.

Sua resolução é de até 2000dpi e há três botões de seleção na mesma linha da roda, em cima do corpo do mouse. A primeira velocidade é, evidentemente, a de 2000dpi, e as demais são de 800 e de 400dpi. Além dos botões que indicam claramente qual é a velocidade presente, há um pequeno display que exibe o valor definido. O limite é 2000, mas esses valores podem ser alterados através do software que acompanha o driver. Também utiliza sensor Laser, assim como o G5 da Logitech.

Ele suporta a gravação de macros, iniciadas por um discreto botão à esquerda do seu corpo. O display LED exibe um ícone indicativo de que uma macro é gravada e também quando uma está em uso.

A gaveta que abriga os pesos no SideWinder suporta até três blocos. São fornecidos quatro, sendo três de 10 gramas e um de 5 gramas. Além disso, são fornecidos os *sliders* de três materiais diferentes. Um acessório fornecido, que é muito interessante, é a âncora para o cabo do mouse que impede que o cabo fique deslizando e, conseqüentemente, arrastando o mouse junto a ele. Essa âncora tem um compartimento que abriga os pesos e também os *sliders*.

Por fim, os teclados da Leadership. O *Game Pad Action Strike* (**figura 14**) é um teclado otimizado para jogos, contendo apenas as teclas necessárias para a movimentação do personagem bem como a seleção de armamentos e acessórios inerentes ao jogo, além de serem posicionadas numa trajetória que claramente foi planejada para oferecer conforto ergonômico.

Ao centro, as teclas são posicionadas de um modo similar ao teclado numérico de qualquer outro teclado, mas as demais são posicionadas numa trajetória circular, facilitando o acionamento. Além das letras (movimento) e dos números (seleção de armas), foi incluído no design as teclas de função (F1 a F12) que abrigam funções "administrativas" dos jogos, como salvar e carregar o jogo, dentre outras.

Notamos alguns cuidados, como por exemplo, as teclas ESC e de ajuste de volume. Além de serem um pouco afastadas e terem uma forma diferenciada, elas oferecem maior resistência ao serem pressionadas, evitando o acionamento acidental, uma inconveniência comum ao



F15. O Combat Strike pode ser encarado como uma fusão entre o Action Strike e um teclado de 84 teclas. No detalhe, portas USB Integradas.

Elementos em comum

Notamos que esses sistemas oferecem uma configuração baseada no processador Core 2 Quad Q6600 em conjunto com a Gigabyte P35. Essa escolha não é totalmente por acaso, já que a P35, além de ser integrada com um bom chipset, é fabricada no Brasil, o que a torna muito atraente por se valer dos benefícios fiscais do PPB (Processo Produtivo Básico). A placa de vídeo tipicamente é da NVIDIA, poucos usam ATI/AMD e, quando ocorre, normalmente se opta por modelos da geração anterior, a HD 2000.

Já existem novas gerações de chipsets além do P35, mas ele não é necessariamente antigo. O que aconteceu, e que pode realçar tal impressão, é que a Intel lançou novos chipsets num espaço de tempo menor do que o normalmente praticado. As demais configurações, bem como os tipos de dispositivos, são parecidos, e naturalmente serão diferentes de um para outro fabricante.

utilizar teclados tradicionais. Foi integrado um LED cuja única função é indicar que o teclado está conectado ao computador. Em tempo, ele utiliza a interface USB.

Com um conjunto de teclas reduzidas, evidentemente suas dimensões são menores. Sua estrutura, de corpo circular, tem a superfície ligeiramente inclinada e ainda conta com ajustes de altura, caso necessário, para melhorar o conforto. Os pés de borracha oferecem um bom "grip", deixando-o bem firme à superfície na qual está acomodado. No mínimo, o Action Strike vai proporcionar algum conforto na utilização, pois o posicionamento entre ele o mouse vai reduzir a tensão nas mãos, braços e ombros.

É claro que a posição de algumas teclas, como as WASD, é igual a de qualquer teclado. Será necessário algum tempo para se acostumar com ele, para "calibrar a mão". Mas de qualquer forma, elas foram ajustadas para proporcionar conforto e, conseqüentemente, uma diminuição no tempo de reposta do jogador.

O Combat Strike (**figura 15**) é um teclado similar aos antigos de 84 teclas (sem o teclado numérico e com algumas teclas em outras posições), porém com um Action Strike integrado à sua esquerda. Note que a diferença entre o Action Strike e a implementação junto ao Combat Strike é a ausência das teclas de função. Para o Combat Strike, um conjunto de teclas de função adicional seria redundante. Ele também é dotado das teclas multimídia.

E por incrível que pareça, o Action e o Combat Strike têm algo em comum com o G15 da Logitech: o layout do teclado, o Inglês Internacional.

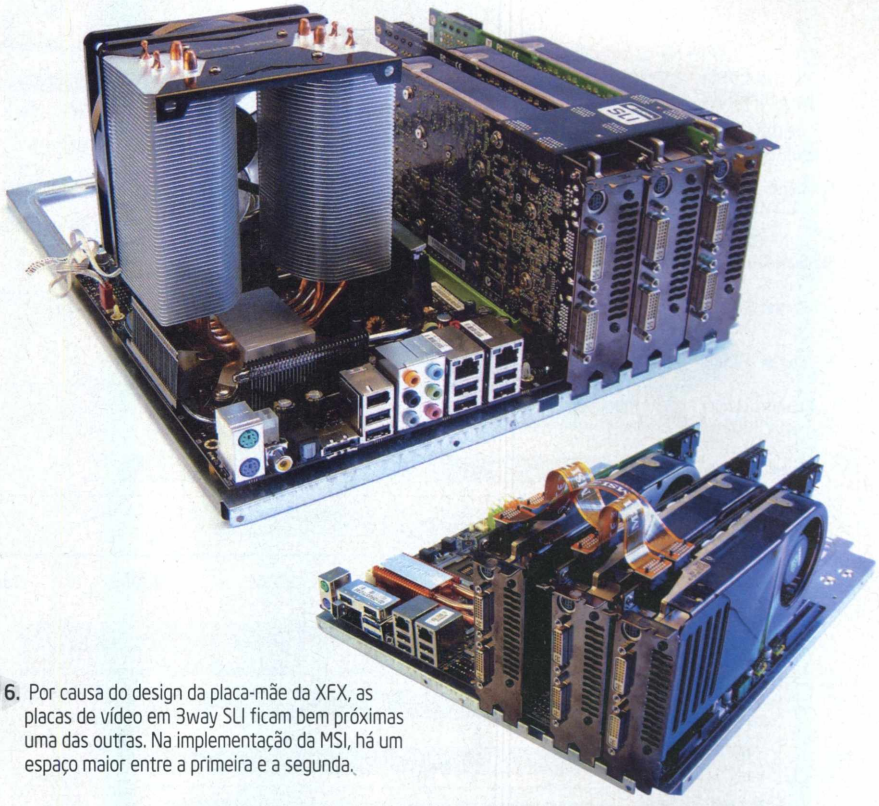
Como não montar uma Gaming PC

Sistemas de alta performance são invariavelmente mais complexos e, conseqüentemente, possuem uma quantidade maior de pontos críticos. E, exatamente por empregar componentes de qualidade, é que devem ser manuseados e configurados com o maior cuidado possível. É uma relação inversamente proporcional: o que lhe dá poder também pode ser o maior ponto fraco.

Ao surgir a necessidade (ou apenas o desejo) de adquirir uma máquina de alta performance para jogos, vários pontos devem ser levados em consideração. Vamos aos tópicos:

- Economia burra: ao montar um sistema de alta performance, seu custo será maior, principalmente se comparado às opções disponíveis nos grandes magazines pelo Brasil afora. Performance e preço costumam caminhar lado a lado, sempre em direção ao "cume da montanha" e por vezes, o céu. Para uma máquina ter alguma performance, seus dispositivos devem ser escolhidos levando em consideração o equilíbrio entre eles. Por exemplo: por que comprar um Core 2 Quad, se a placa-mãe tem um chipset de baixa performance, além de ter componentes de baixa qualidade? Ou então, ter um excelente conjunto de placa-mãe, memória, CPU e placa de vídeo, e comprar uma fonte genérica, ou pior, comprar um modelo de marca mas de potência inferior à necessária? Resumindo: não é muito útil ter apenas um componente poderoso se as demais partes do conjunto não apresentarem, além da qualidade, o equilíbrio;

- Objetivo do uso: Por ser um sistema naturalmente poderoso, uma Gaming PC pode ter capacidade de realizar outras tarefas, como exibição e edição multimídia. Portanto, ao definir a configuração, não deixe de considerar essas possibilidades de uso;
- Bom senso: não se esqueça de que ao compor uma Gaming PC, os periféricos e acessórios fazem a diferença. Imagine ter uma configuração dual GPU que permite usufruir de todos os recursos visuais de um jogo, mas ter um monitor de 15 polegadas, um teclado de R$ 20 e um mouse de R$ 10... Ou então, que tal uma placa de vídeo de baixa performance com um mouse de 400dpi e uma tela de 22 polegadas com resolução de 1900 x 1200? Ou ainda, uma interface de som com 7.1 canais combinada com caixas estéreo?
- Limites de aquisição: eles sempre vão existir, mas conforme a situação, podem ser a diferença entre ter uma máquina realmente de alta performance ou ter apenas uma de performance acima da média. Como já dissemos, performance e preço andam de mãos dadas, ou seja, quanto maior a performance, maior será o preço, com raríssimas exceções;
- Ansiedade: na empolgação de definir uma configuração poderosa, vários problemas podem acontecer. O mais típico é o susto ao ver o preço. Se o preço não assustou, a chateação pode ser resumida em uma palavra: compatibilidade. Algumas placas-mãe *high-end* se valem de dispositivos de refrigeração mais sofisticados, com maior volume, que podem impedir o uso de determinados modelos de cooler, seja o tradicional a ar ou um watercooler. Ainda há a questão da disponibilidade de slots. A cada dia que passa, o PCI tradicional vai cedendo espaço para o PCI Express x1. Outra questão, é a disposição dos slots da placa-mãe escolhida. O uso de um arranjo com duas placas de vídeo, via de regra, impedirá o uso de algum slot, exatamente aquele que estava reservado para a sua placa de som de estimação;
- Muitos podem questionar sobre a possibilidade de se jogar com máquinas menos poderosas. Claro que é possível. Mas em qual configuração? Lembre-se de que "Alta performance" é diferente de "performance". O "alta" já define que será utilizado o melhor e não apenas o possível.
- Não há como fazer grandes economias em uma Gaming PC de qualidade que não irá frustar a experiência de uso. Reiteramos que a definição da configuração deve ser pautada pelo equilíbrio dos recursos e não concentrada na potência de apenas um dispositivo.



F16. Por causa do design da placa-mãe da XFX, as placas de vídeo em 3way SLI ficam bem próximas uma das outras. Na implementação da MSI, há um espaço maior entre a primeira e a segunda.

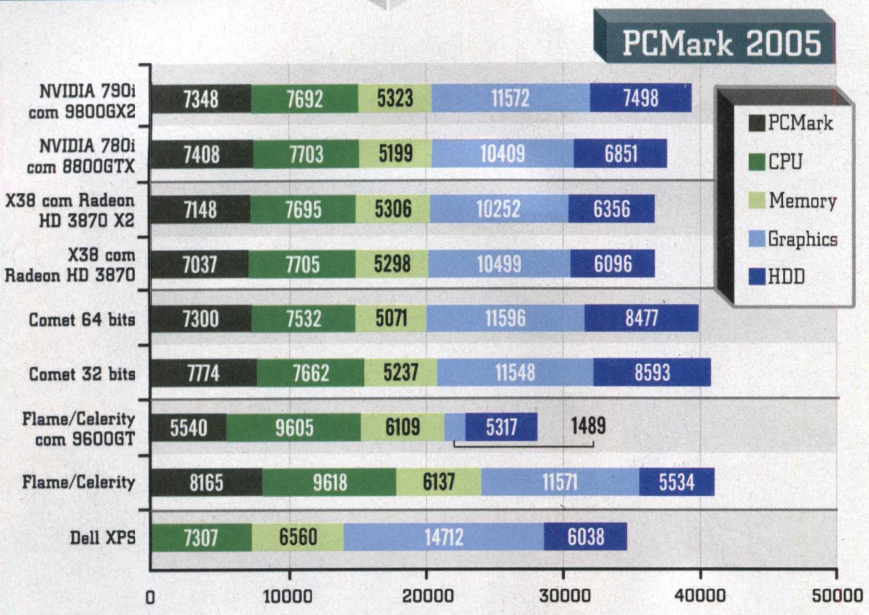
Processos de manutenção

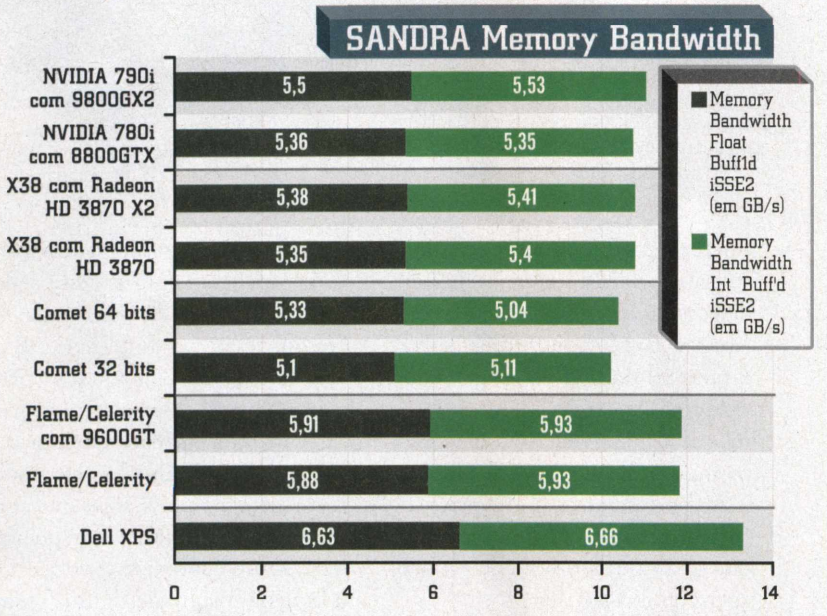
Em máquinas de alta performance, como são tipicamente as Gaming Machines, o processo de manutenção não se limita a reinstalar o sistema, instalar os drivers, manter os softwares de proteção atualizados, etc. Ele vai além, exigindo muito mais do profissional.

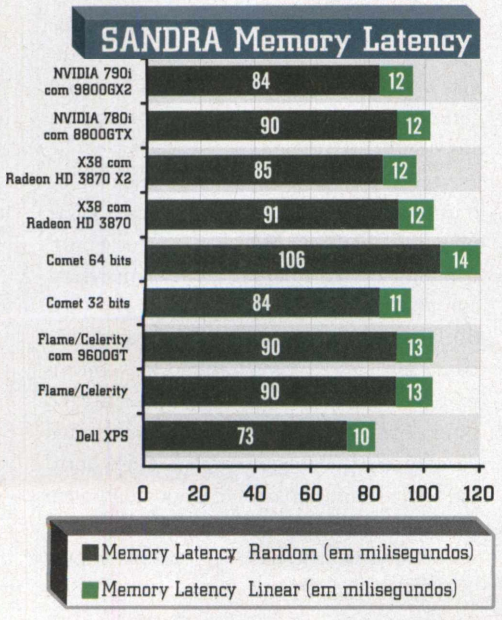
Quando uma máquina dessa natureza apresenta algum problema, é improvável que ele será resolvido rapidamente. Para evitar um consumo excessivo de tempo, é preciso, antes de mais nada, fazer um "reconhecimento do terreno". É claro que se o sistema foi montado por você mesmo, evidentemente esse passo pode ser pulado.

Um fato curioso, comum a sistemas de alta performance, é que por ser mais complexo, ele pode apresentar problemas por motivos simples como: poeira acumulada, um chicote que se soltou e impediu o funcionamento de alguma ventoinha do sistema, ou que apresenta baixa rotação quando deveria estar em alta;, uma configuração que voltou ao *default* e a alteração não foi percebida, ou ainda alterada intencionalmente, porém não revertida à sua condição original, etc.

Se o sistema emprega algo menos comum, como um watercooler, é preciso estar preparado para manuseá-lo, o que exige um conjunto de ferramentas e outros materiais apropriados. Essas ferramentas servem para o manuseio das mangueiras e abraçadeiras, como estiletes e chaves canhão, e os outros materiais são: um recipiente para armazenar o fluído, um pano para enxugar algum eventual vazamento (por menor ele seja) e um outro para acomodar as partes desmontadas, além de algum tipo de proteção para os componentes do sistema, caso não seja possível remover







todo o watercooler, um funil para recolocar o fluído, um pedaço de mangueira para realizar algum teste com a bomba ou substituir um segmento, fita veda-rosca, etc.

O manuseio de placas em SLI é relativamente simples, pois há espaço entre as placas para manuseio e, assim, uma pode ser retirada sem interferir na outra. Porém, em 3way SLI, nem sempre essa facilidade está presente. Por exemplo, na placa-mãe da XFX, os slots PCI Express x16 usam um tipo de trava de retenção de alavanca lateral. Devido ao seu design, se for necessário remover a placa de vídeo mais distante da CPU, é necessário remover todas, já que não há espaço para acessar a alavanca, destravar e remover apenas uma (**figura 16**).

Ainda sobre o 3way SLI, notamos que as placas de vídeo ficam muito próximas umas da outras, o que faz dessa área do sistema um ponto térmico crítico, demandando alguns cuidados ao escolher o gabinete em si e os elementos de refrigeração, que serão necessários para manter a integridade térmica do sistema. Em resumo, são apenas detalhes, mas que não devem ser negligenciados no processo de manutenção.

Os testes

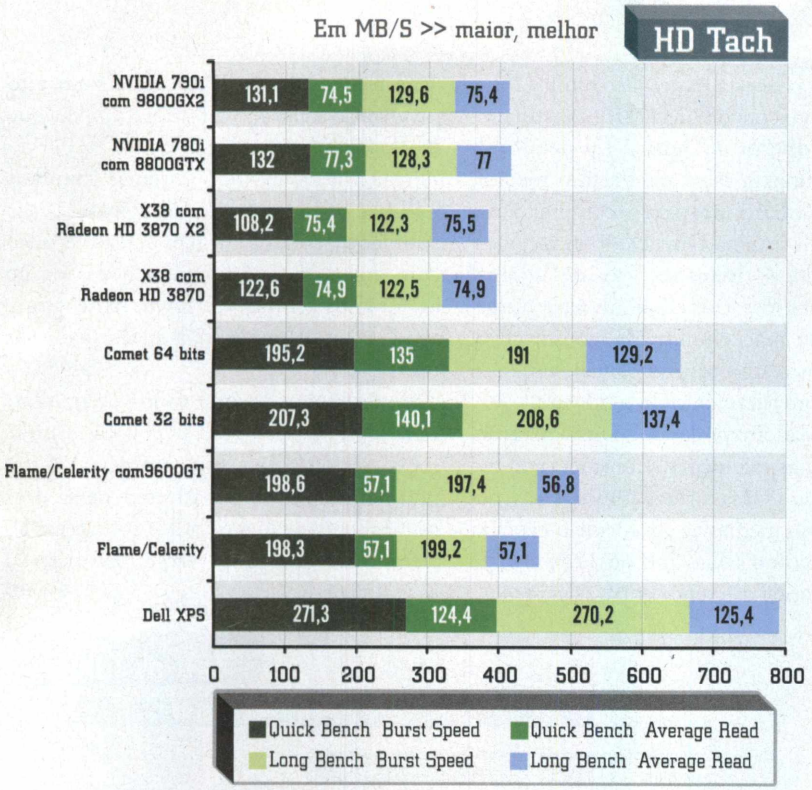
Em se tratando de máquinas configuradas para jogos, os *benchmarks* evidentemente serão focados para esse uso. Foram utilizadas as suítes PCMark2005, 3Dmark05 e 3Dmark06 da Futuremark, o Call of Juarez Benchmark e o módulo de *benchmark* de GPU do Crysis. Além deles, também analisamos a performance de disco com o HD Tach e também de memória com o SiSoft Sandra.

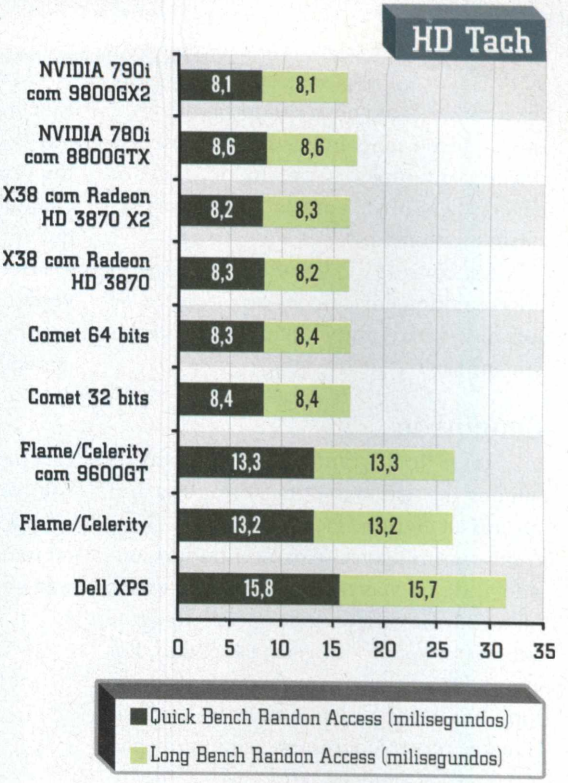
Pelo fato dos produtos em teste contemplarem três sistemas prontos, optamos por organizar os produtos avulsos em conjunto, constituindo sistemas personalizados.

Então temos os seguintes conjuntos: nForce 790i com GeForce 9800GX2, nForce 780i com GeForce 8800GTX, Intel X38 com Radeon HD 3870 e HD 3870 X2. O processador utilizado foi um Core 2 Quad Q6600 em freqüência nominal, ou seja, 2.4GHz. Tínhamos também uma 9600GT da Zogis e optamos por utilizar o hardware do Flame para testá-la.

Nas configurações personalizadas, utilizamos o HD Raptor da Western Digital, memórias Patriot DDR2 e DDR3, DVD-RW da TSST, fontes de alimentação e coolers da Cooler Master, respectivamente a série Real Power Pro e o Hyper 212.

Antes de continuar, duas más notícias. Uma acerca do 3way SLI e outra com o CrossFireX: ambos não funcionaram. Começando pelo 3way SLI, foram utilizadas três 8800GTX, mas o sistema apresentou instabilidades durante a execução de qualquer *benchmark*, do tradicional *freeze* à tela azul. Os erros de tela azul foram os mais diversos possíveis, surgindo de operações simples, que não exigiam poder do sistema. O *freeze* se manisfesta do nada: bastava deixar o sistema parado. Entretanto, a instalação do sistema operacional, bem como dos drivers, ocorreu sem problemas.

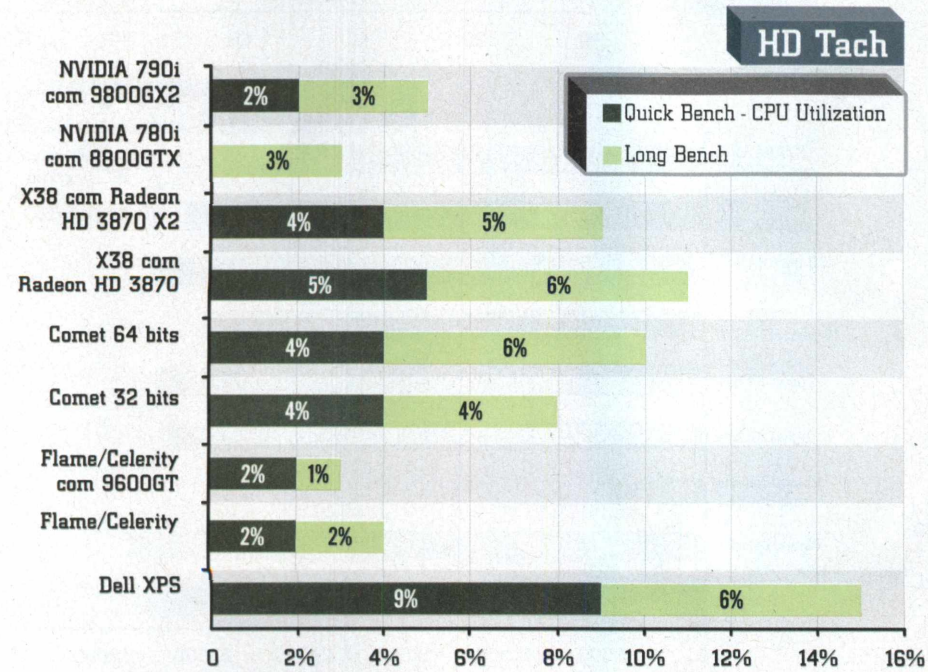




Recomendamos que o uso de um arranjo SLI seja feito com placas iguais, ou seja, não basta ter o mesmo GPU, elas devem ser do mesmo fabricante, modelo e série. As três unidades se valiam do GPU GeForce 8800GTX, porém não eram do mesmo fabricante, sendo uma da XFX, uma da Asus e uma terceira *Reference Design*. Se levar ao extremo o significado de palavra, então as placas eram no máximo similares, porém não iguais. Então fica o recado: se usar o 3way SLI, use três placas rigorosamente iguais e, preferencialmente, compre as três no mesmo lugar.

Considerando o DirectX 9, o Flame e o Celerity da Evolute Gaming, já que usam a mesma configuração, obtiveram a melhor média. O ponto de equilíbrio entre o DX9 e DX10 foi o Dell XPS.

Agora para o DirectX 10, os melhores sistemas foram o Comet e o sistema baseado no nForce 790i com a GeForce 9800GX2. Vale ressaltar que o Comet testado não estava com a sua configuração comercial, o que poderia ter feito a diferença.



Nos testes de dispositivos de armazenamento, sempre chamam atenção os testes de velocidade de pico (*burst speed*) e média (*average speed*), que é o mais relevante para o uso diário. É claro que os modelos que utilizam RAID 0 vão apresentar o melhor resultado. Com base no HD Tach, em *burst* o Dell XPS com os seus HDs Seagate de 72000 RPM obteve o melhor resultado, o que é um tanto curioso, já que o Comet utiliza HDs WD Raptor X de 10000RPM. Contudo, o poder dos WD Raptor X se evidenciou ao obter a maior velocidade média. Se a referência for o PC Mark, o Comet tem o melhor resultado com boa vantagem.

Menções honrosas

Com o mercado de sistemas focados em games e de alta performance aquecido, alguns podem perguntar acerca da ausência de alguns produtos, como o chipset Intel X48, o AMD 780 e 790FX, e o emprego de configurações com o Athlon 64 X2 e, principalmente, o Phenom.

Um fato concreto que observamos é que todos os fabricantes que oferecem Gaming Machines utilizam soluções Intel

e NVIDIA (CPUs, Chipsets e GPUs). Até mesmo por causa desse comportamento, é que se torna mais interessante apresentar outras configurações, porém, por motivos *diversos*, não foi possível contemplá-las nesse momento.

Um consolo é que todos eles já foram apresentados em edições anteriores e de um modo mais amplo, não focado apenas em games.

Conclusão

Nosso foco principal foi mostrar as opções de sistemas para jogos, seja um pronto ou do tipo "faça você mesmo", bem como alguns dispositivos de entrada. Considerando apenas o computador, já temos uma enorme variedade de opções, imagine considerar todo o universo envolvido. Por isso, outros elementos acabaram ficando de fora, como monitores, interfaces e caixas de som, controladores em geral (gamepad ou alavanca), móveis, etc.

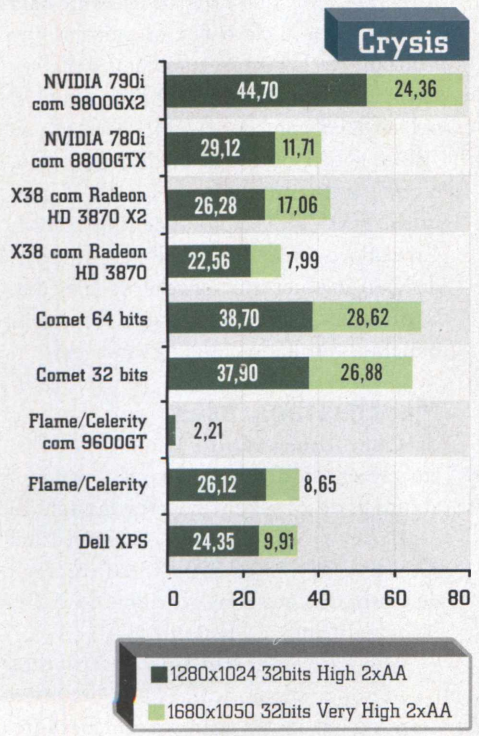
Apresentamos opções para vários gostos, desde aqueles que querem um sistema pronto para usar aos que vêem a definição da configuração como parte do prazer.

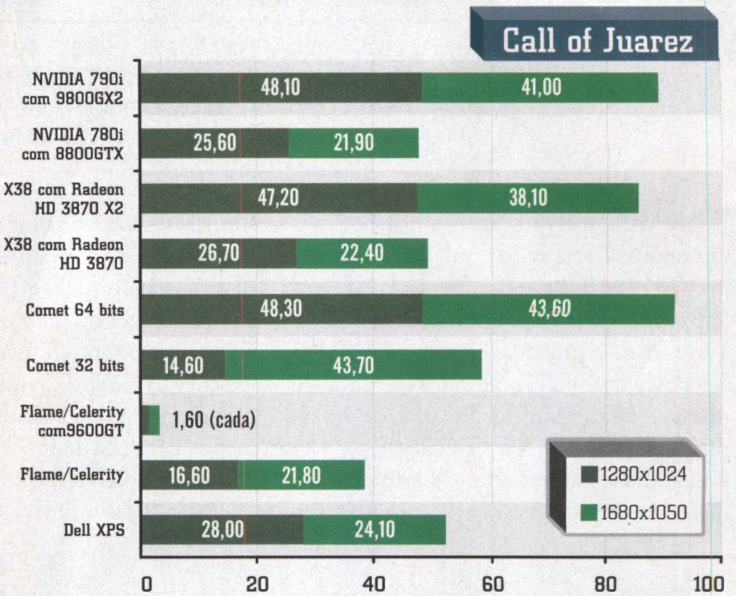
Assim como aconteceu com os sistemas que não estavam totalmente preparados para os primeiros processadores Dual Core, agora vemos a repetição do cenário com as placas de vídeo dotadas de dois GPUs.

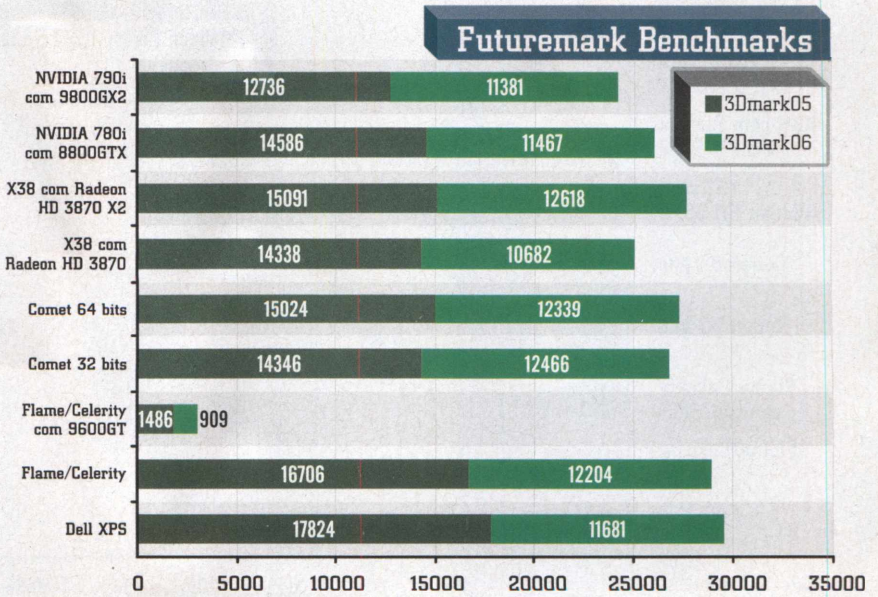
As novas interfaces de vídeo multi-GPU, em conjunto com o DirectX 10, constituem um belo divisor de águas. Tal detalhe é importante para saber qual será o melhor conjunto de hardware para se comprar. Para que ter um sistema DirectX 10 se os jogos selecionados só usam recursos de alguma versão anterior? É melhor investir numa arquitetura mais equilibrada, conforme já comentamos. Do contrário, não se terá o melhor aproveitamento do hardware.

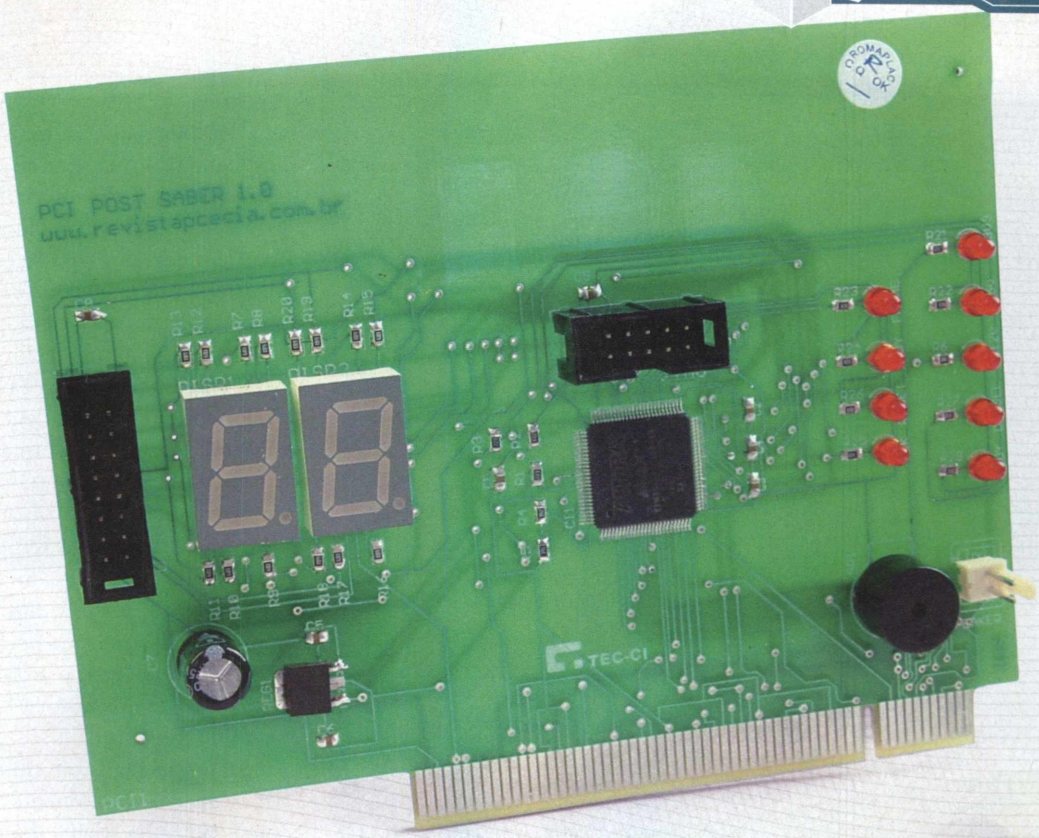
O verdadeiro poder dessa nova geração está nas altas resoluções. Considerando resoluções hoje classificadas como baixas, ou no máximo medianas conforme o critério adotado, como 1024x768 ou 1280x1024, não há grande diferença entre as gerações. Mas nas resoluções maiores e com alto nível de detalhes, elas mostram do que são capazes.

Há anos já existem sistemas com dois CPUs, e os bi, tri e quadrinucleares já são realidade. Só agora surgem placas de vídeo com dois GPUs. Assim fica a dúvida no ar: quanto tempo vai levar para surgiu um GPU multinuclear? Será que vai levar mais tempo que o CPU, ou elas estão mais próximas do que todos imaginam? Lembrando que, para breve (que pode ser meses ou anos), está prometida outra grande quebra de paradigma nessa área que é a integração das CPUs com as GPUs num único chip. Mas isso é história para as futuras edições... **PC**







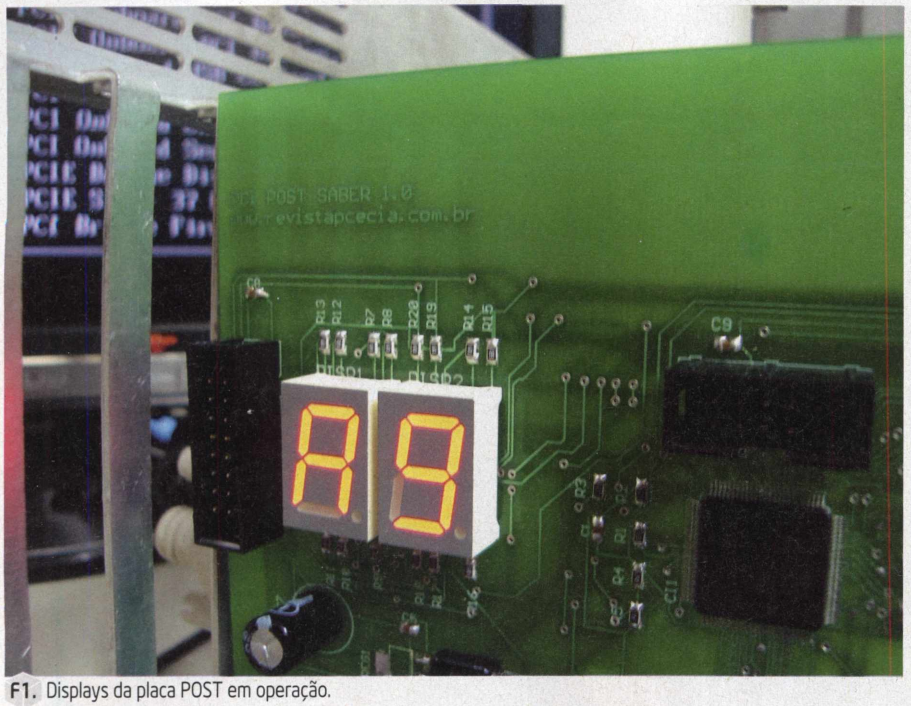


Manutenção com a POST Saber a tiracolo



Anderson C. D. Costa
Técnico de TI com mais de 10 anos de experiência na área de manutenção e integração de hardware, com especialização nos mecanismos de refrigeração de PCs.

Os cenários de manutenção são os mais diversos possíveis. Assim, quanto mais ferramentas tivermos à disposição, mais preparados estaremos para enfrentar essa diversidade e assim caminhar para o sucesso. Nesta matéria relataremos algumas experiências com a POST Saber.



F1. Displays da placa POST em operação.

Não importa qual seja a situação, se é uma montagem de um sistema novo, upgrade ou mesmo uma tarefa de manutenção cotidiana, sem um mínimo de ferramentas apropriadas, inevitavelmente, perderemos um tempo que poderia ser facilmente poupado.

Em qualquer negócio, tempo é dinheiro, e na manutenção de PCs não é diferente. A realização de um bom trabalho no menor tempo possível pode significar a existência de um espaço na agenda para atender um cliente a mais no dia, aumentando a produtividade e também o saldo no caixa. Do contrário, deixar de atender um cliente que estava previsto, pode resultar em prejuízos que vão além da queda do saldo do caixa.

A POST na prática

A placa POST é uma ferramenta que pode nos auxiliar em qualquer processo, nem que seja apenas para monitoramento do comportamento do sistema sob suspeita. Exemplificando, podemos usar a POST não apenas em computadores que estão com defeito, mas também em computadores novos que estão sendo montados e também em upgrades.

Por vezes, perdemos um tempo precioso por causa de pequenos detalhes que podem ser facilmente poupados com a POST. Ela não faz milagres mas, com certeza, lhe indica o caminho para a realização de um.

Vamos considerar a situação de um sistema que não liga. O termo "não liga" é absurdamente amplo, principalmente na cabeça de um usuário. Esse "não liga" pode ser traduzido em diversas formas, sendo as mais comuns:

- Não liga MESMO;
- Não liga, mas o sistema é energizado (que é o entendimento mais comum);
- O monitor não liga/vídeo não é exibido;
- O Windows não inicia ou apresenta erros de inicialização.

Considerando o entendimento mais comum, sem uma POST vamos à situação de análise mais simples, porém dispendiosa: a troca de peças aleatória, até achar o problema. Isso se não for feita a reinstalação do Windows antes disso.

Não há dúvidas quanto à eficiência da troca de peças. Mas, para contemplar todas as condições possíveis, o cenário ideal é carregar pelo menos um sistema inteiro na mala ou pelo menos ter acesso a um rapidamente, sem comprometer um outro sistema em funcionamento que esteja presente no local, considerando que seja possível utilizá-lo para tal. Esse sistema é escolhido com base no perfil dos clientes. A condição mais restritiva é quando se faz necessário ter dois ou mais sistemas, se o perfil for misto e se o cliente exigir um tempo de resPOSTa extremamente curto para a resolução de problemas.

Além do valor para se ter esse equipamento à mão, temos que enfrentar outros problemas como a pouca praticidade de transporte (nem todo técnico ou profissional de manutenção tem carro) e também a segurança e integridade dos dispositivos (mesmo desmontado, uma mala grande chama atenção, e também é necessário usar acomodações apropriadas). Temos também a questão do tempo consumido para realizar a tarefa. Se o problema é identificado "de primeira", ótimo, mas do contrário, começa a peregrinação para localizar e solucionar o problema, processo este que pode consumir várias horas preciosas de trabalho.

A situação mais comum do técnico é ter à mão apenas componentes mais baratos, como coolers, ou de fácil manuseio mecânico, como memórias e placas em geral. O resto não é utilizado por se tratar de itens mais caros, como processadores e placas-mãe, pois a substituição vai depender da aprovação do cliente, o que por vezes não ocorre imediatamente.

A troca de peças também tem um outro inconveniente: podemos até mesmo resolver o problema, mas isso não significa que o dispositivo trocado esteja realmente com defeito. Um problema pode se evidenciar devido à utilização de uma configuração de BIOS incorreta, por exemplo, ou até mesmo a população incorreta dos slots de expansão, que pode resultar no conflito de recursos da placa-mãe.

Com o objetivo de facilitar o entendimento, citaremos alguns cenários onde a POST efetivamente nos poupou grande tempo na resolução dos problemas encontrados.

Cenário 1 – Teste de bancada

Na matéria de placas-mãe de baixo custo, publicada na edição 80, tivemos problemas com um módulo de memória em uma das placas-mãe com chipset Intel 945G. O erro indicado nos displays da POST era o C1, que tipicamente está relacionado com o chipset e este, por sua vez, com a memória do sistema (**figura 1**). Os módulos de memória

foram substituídos e o sistema inicializou corretamente.

Tínhamos certeza que o módulo não estava com defeito. Assim, as opções para tal comportamento eram compatibilidade ou mau contato dos módulos com os slots. Por sabermos que o módulo era compatível, sobrou apenas a opção de mau contato.

Cientes dessa possibilidade, concentramo-nos na análise da situação para concluir se realmente era mau contato ou simplesmente um condição de erro desconhecida. Com o foco nesse problema, realizamos a inserção dos módulos com maior cuidado e, logo na primeira tentativa, o módulo respondeu e o sistema iniciou e funcionou sem problemas.

Os testes de bancada compõem um cenário mais simples, já que, teoricamente, temos mais material disponível à mão do que em campo. Mas, sem uma POST, a possibilidade desse módulo ser descartado num primeiro momento é bem grande, o que poderia resultar no desperdício de recursos.

Cenário 2 - Teste de montagem

Este caso aconteceu recentemente, durante o teste de uma placa-mãe com um Core 2 Extreme da série QX9000. No caso, o BIOS era um Award/Phoenix versão 6.00PG, a POST retornou o código 18 e o sistema não foi iniciado.

O código 18 diz respeito à identificação do processador utilizado. Diante disso, pudemos concluir que a versão atual do BIOS não suportava o processador utilizado.

Dependendo da situação, a inicialização é até possível, mas a funcionalidade do sistema é bem limitada, por vezes travando no cabeçalho de inicialização. Mesmo que não trave no cabeçalho e o sistema operacional seja inicializado, ainda há riscos de travamento durante a atualização, o que não é nada bom, principalmente se travar no momento da gravação do Boot Block.

Há duas soluções totalmente seguras: utilizar um processador que seja compatível com a versão presente do BIOS na placa-mãe possibilitando a sua inicialização e, conseqüentemente, a atualização para uma versão mais nova que suporte o processador, ou remover o chip de memória Flash-ROM e atualizá-lo num gravador externo apropriado.

Cenário 3 - Manutenção em Campo

Esse caso foi mais simples, exibindo o código C0 que é um indicativo de problemas relacionados ao chipset. Todos os dispositivos offboard foram removidos para a realização do teste e, mesmo assim, o erro continuou. Os demais componentes foram instalados numa placa-mãe nova e todos, sem exceção, funcionaram corretamente, o que decretou o defeito da placa-mãe anterior.

Cenário 4 - Limitações do POST

Observamos que a atual versão da POST apresenta incompatibilidade com determinados modelos de placa-mãe, geralmente modelos *entry-level* com vídeo onboard de diversos fabricantes. Para citar três, temos a ECS P4M800PRO-M2, a Asus P5VD2-VM e a Biostar K8M800 Micro AM2. Além do vídeo onboard, elas têm em comum o fato de integrarem chipsets da VIA Technologies, que têm o hábito de não seguir à risca a especificação do barramento PCI, o que acaba gerando problemas com diversas marcas de placa POST, inclusive modelos da Ultra-X, que são conhecidos como "A" referência nesse tipo de produto.

Nas vezes que enfrentamos esse problema, era exibido o código 10 e o sistema não inicializava. A inicialização era simplesmente interrompida e, conseqüentemente, nada era exibido na tela. Quando isso ocorre, o primeiro pensamento que vem à mente é que a POST não foi útil e pior, ainda agravou a situação. Geralmente, independente da placa POST utilizada, a atenção sempre recai sobre os displays que exibem o código, mas há outros LEDs que indicam a presença de sinais e, conseqüentemente, o estado real do sistema.

Nesse caso, o LED que deve ser observado é o CLK, o último da primeira coluna da esquerda para a direita. Quando o computador está saudável, o estado normal desse LED é ficar piscando intermitentemente enquanto o sistema estiver ligado. Se ele estiver desligado ou ligado, pode existir algum problema no gerador de clock da placa-mãe, o que pode estar por trás dos problemas na inicialização do sistema, ou mesmo travamentos ou reset aleatório.

Por exemplo, imagine um parque de máquinas que tenha qualquer uma das três placas-mãe citadas acima. A POST não exibirá nenhum código, mas sabemos que o LED CLK, em todas elas, fica piscando, o que indica que o clock está "fluindo" no sistema. Assim, se nos depararmos com uma em que o CLK esteja simplesmente ligado ou desligado, podemos considerar que a unidade está com problemas no gerador de clock e, conseqüentemente, com defeito.

Em resumo, além de nos atentarmos ao código, é muito importante também dar atenção aos LEDs presentes na placa POST.

Cenário 5 - Sistema morto

Excetuando os casos de incompatibilidade, onde a POST apresenta um código sem qualquer referência, nem que seja classificado como reservado, pode significar que a placa-mãe está morta.

Nesses casos, o display LED exibe os caracteres 00 (zero-zero), indicativo de que o sistema nem chegou a ser inicializado. Usando com referência o LED CLK, se ele estiver apagado, é a prova definitiva da morte da placa-mãe, ou na melhor das hipóteses, com um sério problema intermitente, como algum curto entre as camadas do PCB, dentre outras possibilidades.

Ao se deparar com uma situação assim, é conveniente que todos os slots PCI da placa-mãe sejam testados, para reduzir a chance de condenar uma placa-mãe com problema apenas nos slots PCI. Sem slots PCI, por exemplo, a placa-mãe tem utilização limitada, podendo ser aproveitada em outro sistema mais simples.

Conclusão

Conforme comentamos no início, para realizar qualquer trabalho precisamos ter um conjunto de ferramentas eficiente e, no trabalho com integração e manutenção de hardware, uma placa POST é uma adição fundamental para se obter maior eficiência na execução das tarefas, reduzindo os riscos de um diagnóstico demorado ou errado.

Mas lembre-se de que a POST não se limita a exibir um código, pois quando existe algum problema de compatibilidade, como citado acima, ainda podemos lançar mão de outras referências oferecidas por ela, a exemplo da sinalização de LEDs, como o CLK. Aliás, a análise dos LEDS não deixa de ser importante, mesmo quando a POST exibe normalmente os códigos indicando problemas que nem sempre podem ser facilmente percebidos. **PC**



Computação verde

Cada vez mais a indústria do hardware e componentes de infra-estrutura está preocupada com a ecologia. Será mesmo? Veja agora como se orientar para que suas próximas compras não te tragam problemas.

Marcus Brandão de Moura

A que ponto chegamos

Aquele comercial do Greenpeace (**www.greenpeace.org/brasil**) que mostra imagens de graves distúrbios climáticos e em seguida entram os slides: "lembra quando sua geração sonhava em mudar o mundo?", uma pausa e depois o outro slide "parabéns, vocês conseguiram" (**http://br.youtube.com/watch?v=wCmO3OCZX6Q**), representou um "dedo na ferida" de muitos setores industriais.

Maiores discussões à parte, em geral os europeus estão mais preocupados com a ecologia e preservação do meio ambiente do que os americanos, e é da Europa que partem muitas das iniciativas para se poluir cada vez menos.

Não se trata apenas de políticas de marketing. São verdadeiros tratados e acordos que atingem muitas áreas industriais. Esses tratados sugerem ações não somente sobre produtos, mas também ao longo de toda sua cadeia produtiva, desde as matérias–primas até sua colocação no comércio varejista

Em que temos que prestar atenção

Utilizar produtos que atendam às especificações desses tratados e acordos não é só uma bondade de nossa parte. Para um cliente final, pessoa física, até pode parecer, mas para você, técnico, prestador de serviço e profissional da área de Tecnologia da Informação, é uma obrigação na qual tem que estar atento.

- Ah, mas funciona da mesma forma.

Esquece isso, amigo leitor. Não, não funciona da mesma forma.

Ao prestar um serviço, preocupe-se também com os novos requisitos dos acordos "ecológicos" e recomende objetivamente somente a compra de material que atende a esses requisitos. Se não o fizer, a empresa para a qual prestou serviço poderá enfrentar problemas para obter certificações internacionais de conformidade e qualidade de serviços e produtos. Imagina uma empresa perdendo uma certificação internacional em sua área, como, por exemplo, a ISO 9000, só porque você não especificou os produtos corretos na ocasião da compra. Se isso acontecer, você terá problemas.

Vamos fazer um resumo dos principais protocolos a serem seguidos internacionalmente. Esteja atento a eles.

O primeiro e mais conhecido de todos é o programa americano Energy Star, da EPA (Environmental Protection Agency - Agência de Proteção Ambiental - **www.energystar.gov**). Esse programa visa a certificar produtos que atendam às suas especificações referentes ao consumo de energia elétrica. O produto contemplado recebe o direito de ostentar um selo que nos é muito conhecido (**figura 1**).

O Energy Star é um dos mais antigos e importantes protocolos, desde pelo menos 1994 nós já temos visto esse selo nas telas de abertura de alguns computadores. Na realidade, o protocolo Energy Star se atualiza periodicamente. A versão atual, 4.0 série 1, é de julho de 2007.

A próxima diretriz é quase uma recomendação que caiu nas graças do mercado. É aplicada mais especificamente aos plás-

ticos e materiais similares, que quando são queimados costumam exalar aquela conhecida fumaça bem escura e densa, e vapores halógenos que além de serem poluentes, atacam o trato respiratório de quem estiver por perto.

Para evitar isso, alguns plásticos e principalmente cabos elétricos e para telecomunicações, como nossos cabos de rede, tanto de par trançado quanto de fibra óptica, devem seguir a orientação LSZH (Low Smoke, Zero Halogen – Pouca Fumaça, Nenhum Halogênio).

Continuando nos protocolos, temos também o TCO Development (**www.tcodevelopment.com**), que é mais amplo e completo. Ele trata de emissões eletromagnéticas, ergonomia, ecologia e consumo de energia dos equipamentos em ambiente de escritório, tais como computadores, monitores, teclados, telefones celulares, impressoras e até mesmo mobiliário de escritório. Os monitores são os produtos mais certificados pelo TCO Development, portanto, não compre um monitor sem este selo (**figura 2**).

Dentre os principais protocolos, a RoHS (*Restriction on the use of Hazardous Substances* – Restrição ao Uso de Substâncias Nocivas - **http://www.rohs.gov.uk**), uma diretiva nascida na Comunidade Européia, é o mais recente. Ela especifica que ao longo de toda a cadeia produtiva de um produto, não sejam empregadas substâncias altamente poluentes e metais pesados. São elas: chumbo (Pb), cádmio (Cd), mercúrio (Hg), cromo hexavalente (Cr-VI), polibromato bifenílico (PBB) e éter polibromato difenílico (PBDE).

Mais uma diretiva interessante. Mas preste mais atenção ao chumbo. Lembrou de algo? Não? A solda. Isso mesmo, a chamada solda de rádio é composta de 40% de chumbo, os outros 60% são de estanho. Ah, sim.

Pois é, agora suas placas terão que usar ligas especiais nas soldas. Essas ligas fundem a uma temperatura de aproximadamente 227 graus Celsius, contra 180 graus da liga tradicional. A nova liga de solda dá um acabamento mais esbranquiçado e opaco, lembrando uma solda velha e com mau contato, a chamada solda fria. Ao contrário dos outros protocolos, o RoHS ainda não possui um logo ou selo próprio, por isso fique atento aos dois mais usados (**figura 3**).

O que fazer agora?

É simples, inicialmente só especifique produtos que ostentem esses selos, mesmo que sejam um pouco mais caros.

Os cabos de rede merecem uma atenção especial porque eles têm que ser LSZH e RoHS. No Brasil, eles já estão presentes e são regularmente comercializados.

Tudo mais que for movido à energia elétrica tem que ostentar os selos dos protocolos Energy Star e TCO.

Para facilitar sua vida, abandone a indicação dos monitores CRT para ambiente de escritório, você não se arrependerá. Veja que um monitor de 19" CRT Samsung 997MB consome 90W/hora em condição normal de uso; já o Samsung 931BW, de 19" LCD, consome apenas 42W/hora. É menos da metade.

Na edição 77, página 15, é possível ver no artigo "Upgrade de processador" que existem versões do microprocessador Intel Core 2 Duo com consumo elétrico em idle de 22, 12 e 8W/hora. Priorize os de baixo consumo elétrico.

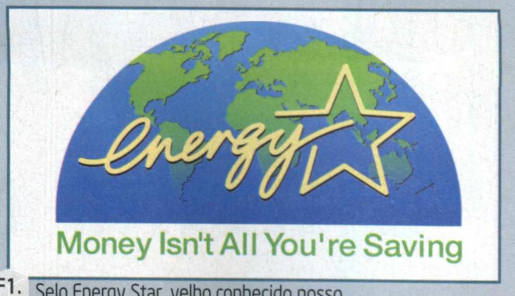
Os discos rígidos mais modernos consomem menos energia elétrica do que seus antecessores, mas nenhum disco com motor é páreo para os novíssimos discos SSD (*Solid State Disk*). O problema é que estes discos são muito caros e isso ainda os tornam inviáveis em ambiente residencial.

Conclusão

Os protocolos são muito importantes para as empresas. Não cometa o erro de indicar qualquer equipamento para seus clientes SOHO ou corporativos, eles perderão tanto quanto você com isso.

Como um cenário de aumento das tarifas de energia elétrica está se delineando, a substituição de monitores CRT pelos LCD em computadores novos é extremamente aconselhável, principalmente porque a diferença de preço está muito pequena.

Indicando equipamentos compatíveis com Energy Star, TCO e RoHS, além de cabos LSZH e RoHS, você mostrará aos seus clientes que está atento e atualizado em relação ao mercado internacional. Isso é muito bom para qualquer profissional. Sempre foi. Até a próxima. **PC**



F1. Selo Energy Star, velho conhecido nosso.



F2. Selo TCO Development, procure nos monitores LCD ou CRT (estes, ainda podem ostentar o selo TCO'03).





F4. Dois selos muito usados para identificar produtos que atendem à diretiva RoHS.

Asterisk: O nome da revolução no mercado de telefonia

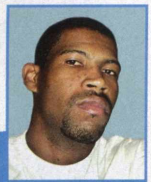
Parte 2

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

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

Na edição anterior aprendemos a instalar o Asterisk no Debian Linux e a configurar ramais SIP (Session Initiation Protocol) em Softphones, telefones IP e em um adaptador ATA (Adaptador para Telefone Analógico). Além disso, tivemos a oportunidade de construir um plano de discagem simples que indica ao Asterisk o que deve ser feito quando ele recebe uma chamada. Ao final da matéria anterior, tínhamos então um PABX funcional, permitindo a realização de chamadas entre seus ramais.

Nessa edição iremos ampliar um pouco mais nossos horizontes, pois além de realizar chamadas entre ramais VoIP, aprenderemos a integrar o Asterisk com a rede pública de telefonia (PSTN - Public Switched Telephone Network), o que nos permitirá realizar chamadas para telefones convencionais a partir de nosso PABX. Também criaremos uma URA (Unidade de Resposta Audível) simples para atender nossas ligações, apresentando opções de atendimento a todos que ligarem para nossa instituição. Vamos lá!



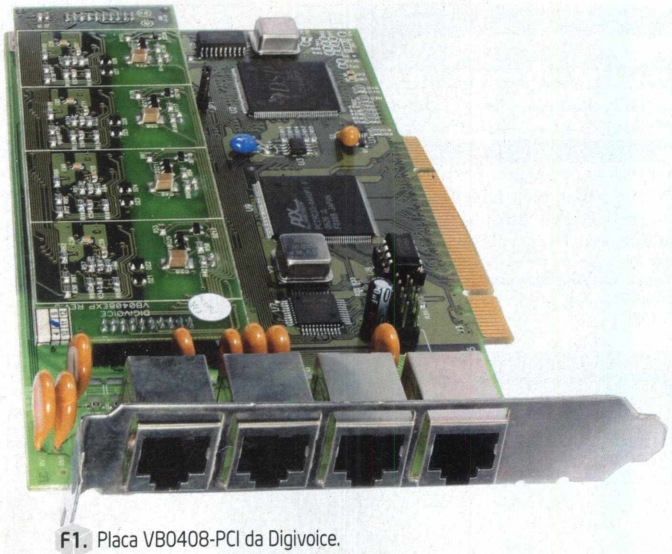
Flávio de Souza Oliveira
Mestre em Administração e Segurança de Sistemas pela Unicamp. Certificado LPI, atualmente trabalha na Callink - Serviços de Callcenter, em Uberlândia/MG

Cenário

Após a conclusão da primeira etapa de nosso trabalho, possuímos um PABX instalado com ramais SIP configurados em diversos tipos de equipamentos e que, por sua vez, conseguem realizar chamadas entre si. Nessa etapa faremos a integração deste PABX com a rede telefônica convencional através da utilização de uma placa que contém o que chamamos de porta FXO (Foreign eXchange Office).

Existem basicamente dois tipos de portas de interface analógica que devem ser entendidos para seguirmos com essa integração. Uma delas é a porta FXO, projetada para receber um sinal da operadora de telefonia, o famoso tom de discagem, ou seja, que é ligada diretamente à linha telefônica recebida da operadora. Existe também o que chamamos de porta FXS (*Foreign eXchange Subscriber*), que oferece tom de discagem, como é o caso da porta do dispositivo ATA na qual conectamos o aparelho de telefone analógico da matéria anterior.

Para a interligação entre nosso PABX e uma linha telefônica convencional instalaremos no servidor a placa VB0408-PCI da Digivoice (**www.digivoice.com.br**), que pode trabalhar com até 8 linhas analógicas e tem recursos interessantes para gravação de voz e para integração com equipamentos convencionais de PABX (**figura 1**). Além de permitir que nossos ramais possam realizar chamadas para telefones convencionais, também utilizaremos essa placa para atender as chamadas que chegarem através das linhas conectadas a ela com nossa URA.



F1. Placa VB0408-PCI da Digivoice.

```
flavio@ares: ~
Arquivo Editar Ver Terminal Abas Ajuda
hercules:~# cd /usr/src/
hercules:/usr/src# ln -s asterisk-1.4.17 asterisk
hercules:/usr/src# tar -zxvf voicerlib-4.0.9.5.tar.gz
voicerlib-4.0.9.5/Makefile
voicerlib-4.0.9.5/configure
voicerlib-4.0.9.5/driver/linux/Makefile
voicerlib-4.0.9.5/driver/linux/vlibd_load.sh
voicerlib-4.0.9.5/driver/linux/vlibdrv.c
voicerlib-4.0.9.5/driver/linux/vlibdrv.h
voicerlib-4.0.9.5/driver/linux/vlibd.debian
voicerlib-4.0.9.5/driver/linux/vlibd.init
voicerlib-4.0.9.5/driver/linux/vlibd.sysconfig
voicerlib-4.0.9.5/firmware/boot294.i00
voicerlib-4.0.9.5/firmware/boot300.i00
voicerlib-4.0.9.5/firmware/bootel.i00
```

F2. Preliminares antes da compilação.

```
flavio@ares: ~
Arquivo Editar Ver Terminal Abas Ajuda
hercules:/usr/src# cd /usr/src/voicerlib-4.0.9.5/src_linux/
hercules:/usr/src/voicerlib-4.0.9.5/src_linux# make && make install
cc -fPIC -c -std=gnu99 -D__LINUX__ -DLINUX26 -lpthread -DCCS_ENABLE -fPIC -D_GN
_SOURCE -Wall -DTWOBYTEDATA -DMODULE -D__LINUX__ -Dvlibd -DLINUX26  linux_api.c
linux_api.c: In function 'digivoice_starttimer':
linux_api.c:542: warning: passing argument 2 of 'digivoice_beginthread' from in
ompatible pointer type
linux_api.c: In function 'digivoice_stoptimer':
linux_api.c:560: warning: passing argument 1 of 'digivoice_cancelthread' makes
ointer from integer without a cast
linux_api.c: In function 'digivoice_beginthread':
linux_api.c:601: warning: pointer targets in passing argument 2 of 'pthread_att
_getstacksize' differ in signedness
linux_api.c: In function 'dg_DisableDebug':
```

F3. Compilação dos fontes.

```
flavio@ares: ~
Arquivo Editar Ver Terminal Abas Ajuda
hercules:/usr/src/voicerlib-4.0.9.5/src_linux# cd /usr/src/voicerlib-4.0.9.5/driver/linux
hercules:/usr/src/voicerlib-4.0.9.5/driver/linux# make && make install && make config
Building kernel modules with default options...

make -C /lib/modules/2.6.18-4-k7/build -I/usr/include/asm/mach-default/ SUBDIRS=/usr/src/
voicerlib-4.0.9.5/driver/linux modules
make[1]: Entrando no diretório `/usr/src/linux-headers-2.6.18-4-k7'
  Building modules, stage 2.
  MODPOST
make[1]: Saindo do diretório `/usr/src/linux-headers-2.6.18-4-k7'
Building kernel modules with default options...

make -C /lib/modules/2.6.18-4-k7/build -I/usr/include/asm/mach-default/ SUBDIRS=/usr/src/
voicerlib-4.0.9.5/driver/linux modules
```

F4. Compilação do driver.

Instalação

Após a instalação física da VB0408 na máquina, precisamos fazer a instalação dos drivers para que, assim, o sistema operacional e o Asterisk sejam capazes de interagir com ela, lembrando que todos os procedimentos administrativos que apresentaremos aqui devem ser executados utilizando o usuário root.

A placa da Digivoice vem acompanhada de um CD intitulado Kit Integrador, no qual podemos encontrar os drivers tanto para Linux quanto para Windows. Na versão do CD que utilizamos, encontramos uma pasta chamada Linux que contém dois arquivos compactados: dgvchannel-0.9.5.tar.gz e voicerlib-0.4.9.5.tar.gz.

Considerando que seu CDROM foi montado no diretório /media/cdrom, copie os dois arquivos citados para o diretório /usr/src com o comando cp /media/cdrom/Linux/*.tar.gz /usr/src, acesse o diretório de fontes (cd /usr/src), crie um link simbólico chamado asterisk apontando para os fontes do Asterisk compilados na matéria anterior (no nosso caso ln -s asterisk-1.4.17 asterisk). Em seguida, efetue a descompactação da voicerlib com o comando tar -zxvf voicerlib-0.4.9.5.tar.gz (**figura 2**), acesse a pasta src_linux dentro do diretório recém-criado (cd /usr/src/voicerlib-4.0.9.5/src_linux no nosso caso) e compile os fontes com o comando make && make install (**figura 3**). Feito isso, acesse o diretório do driver (cd /usr/src/voicerlib-4.0.9.5/driver/linux) e compile com o comando make && make install && make config (**figura 4**).

Ao contrário da maioria das placas construídas para trabalhar com o Asterisk, a VB0408 não foi baseada nas placas da Digium (**www.digium.com**), empresa criada por Mark Spencer (**http://en.wikipedia.org/wiki/Mark_Spencer**) e que está por trás do desenvolvimento do Asterisk. Dessa forma, ela não utiliza o canal ZAP, configurado através do arquivo /etc/asterisk/zapata.conf e que normalmente é utilizado para esse tipo de integração. A Digivoice criou um canal próprio chamado DIGIVOICE, cujos arquivos fontes se encontram no arquivo dgvchannel copiado anteriormente do Kit Integrador.

Para instalar o canal DIGIVOICE, acesse novamente o diretório dos arquivos fonte (cd /usr/src), efetue a descompactação do dgvchannel com o comando tar -zxvf dgvchannel-0.9.5.tar.gz (**figura 5**), acesse o diretório recém-criado (cd dgvchannel-0.9.5) e compile com o comando make && make install && make install_config (**figura 6**). Ao final desse passo teremos o driver da VB0408 e o canal DIGIVOICE instalados, restando apenas efetuar a configuração.

Configuração

A configuração do canal DIGIVOICE é feita através do arquivo /etc/asterisk/digivoice.conf (**figura 7**), cujos parâmetros dependem diretamente da forma como as linhas analógicas foram ligadas à VB0408.

```
flavio@ares: ~
Arquivo Editar Ver Terminal Abas Ajuda
hercules:/usr/src# tar -zxvf dgvchannel-0.9.5.tar.gz
./dgvchannel-0.9.5/
./dgvchannel-0.9.5/app_dgccb.c
./dgvchannel-0.9.5/dgvchannel.h
./dgvchannel-0.9.5/CHANGELOG
./dgvchannel-0.9.5/step_2.conf
./dgvchannel-0.9.5/step_8.conf
./dgvchannel-0.9.5/auto_conf_dgv.c
./dgvchannel-0.9.5/step_4.conf
./dgvchannel-0.9.5/step_5.conf
./dgvchannel-0.9.5/LICENSE
./dgvchannel-0.9.5/step_1.conf
./dgvchannel-0.9.5/digivoice.conf
./dgvchannel-0.9.5/chan_dgv.c
./dgvchannel-0.9.5/step_6.conf
```

F5. Descompactação do dgvchannel.

```
flavio@ares: ~
Arquivo Editar Ver Terminal Abas Ajuda
hercules:/usr/src# cd dgvchannel-0.9.5
hercules:/usr/src/dgvchannel-0.9.5# make && make install && make install_config
./create_config.sh "/usr/src/asterisk/include"
4095
Checking Asterisk version at /usr/src/asterisk/include/asterisk... 1.4.17
 * assuming Asterisk version 1.4
 * found stringfield in ast_channel
 * found 'indicate' with data
 * found second extended ast_channel_alloc
 * found extended ast_channel_alloc
 * found send_digit_end with duration
config.h complete.
gcc -std=gnu99 -pipe -fPIC -Wall -Wmissing-prototypes -Wmissing-declarations  -I/usr/src/
asterisk/include -D_REENTRANT -D_GNU_SOURCE -D__LINUX__     -c -o chan_dgv.o chan_dgv.c
```

F6. Compilação do dgvchannel.

```
flavio@ares: ~
Arquivo Editar Ver Terminal Abas Ajuda
[general]
allow_slinear=0
allow_alaw=1
allow_ulaw=1
allow_gsm=0
consolelanguage=br

[allportsconfig]
default_callprogress=cp_default.cfg
detectiontype = 1
dialtype = 1
afterdialpause=1000
ringbacktone1 = tone1
ringbacktone2 = tone1
ringbacktimes = 1000,4000,1000,4000
busytone1 = tone1
busytone2 = tone1
busytimes = 250,250,250,250

[groups]
group = 1
ports => 1

[port_config]
context=entrada
tx_gain = -6
rx_gain = 0
echocan=4
echotraining=400
signalling=fxo
gen_dtmf=1
gen_ringback=1
gen_busy=1
dtmf_to_asterisk=2
callprogress=cp_default.cfg
language=pt_BR
silence_threshold=-36
dialtone_timeout=3000
wait_dialtone=1
relaxdtmf=1
faxdetection=1
ports => 1-4
<ce.conf" [converted] 42L, 660C written 7,0-1          All
```

F7. Arquivo de configuração do canal DIGIVOICE.

```
flavio@ares: ~
Arquivo Editar Ver Terminal Abas Ajuda
>vlibd: vlib_init_module - Starting loading driver...
vlibd: Module /dev/vlibd using major number 254
vlibd: Driver Version: 4.0.9.5
vlibd: VoicerLib Device Driver was loaded successfully!
vlibd->init_plx: Probing Device Name: vlibd
vlibd->plx_countcards: 1 Cards Found.
vlibd->plx_probe: ->Probing card number 0
eth0: no IPv6 routers present
hercules:/etc/asterisk#
```

F8. Inicialização dos drivers.

```
flavio@ares: ~
Arquivo Editar Ver Terminal Abas Ajuda
[default]
exten => 7000,1,Dial(SIP/7000,20,t)
exten => 7001,1,Dial(SIP/7001,20,t)
exten => 7002,1,Dial(SIP/7002,20,t)

exten => 6000,1,Answer()
exten => 6000,2,PlayBack(demo-thanks)
exten => 6000,3,HangUp()

exten => _0X.,1,Dial(DGV/G1/${EXTEN:1},40,Tt)

"extensions.conf" 11L, 255C written      11,0-1        All
```

F9. Configuração para deixar plano de discagem acessível

No nosso caso, onde utilizamos apenas uma linha, orientados pelo manual do produto preparamos um cabo com um conector RJ45, ligamos a linha telefônica aos pinos 1 e 2, que correspondem à primeira porta Digivoice e conectamos o cabo à entrada CN1 da placa.

No arquivo digivoice.conf foram alterados apenas dois parâmetros, todas as demais configurações foram mantidas com os valores default. Na seção groups da figura 7, alteramos a opção ports de 1-4 para 1, indicando que possuímos apenas uma linha analógica habilitada, que ela está ligada à primeira porta da placa e que desejamos associá-la ao grupo 1 (ou 1º canal DIGIVOICE). A outra opção alterada se encontra na seção port_config, na qual o parâmetro context foi alterado de from-pstn para entrada. Realizadas essas configurações, reinicie a máquina para verificar se os módulos são carregados corretamente durante a inicialização do sistema.

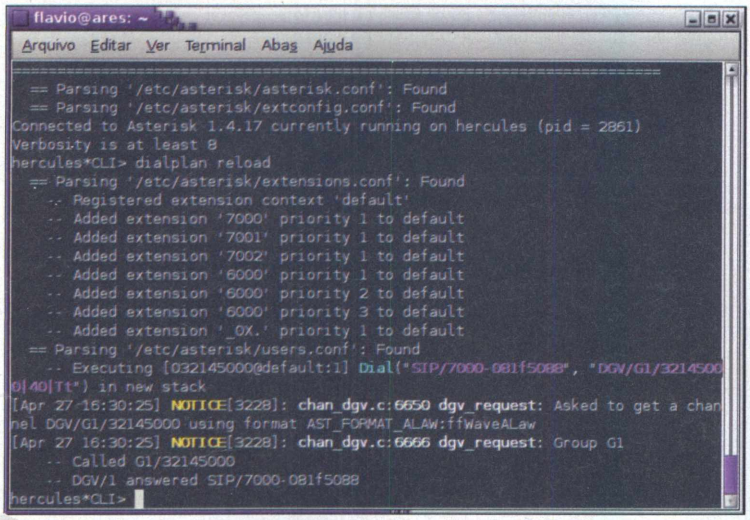
Ao final da inicialização, execute o comando dmesg, no qual é possível verificar as mensagens de inicialização dos drivers (**figura 8**).

Plano de discagem

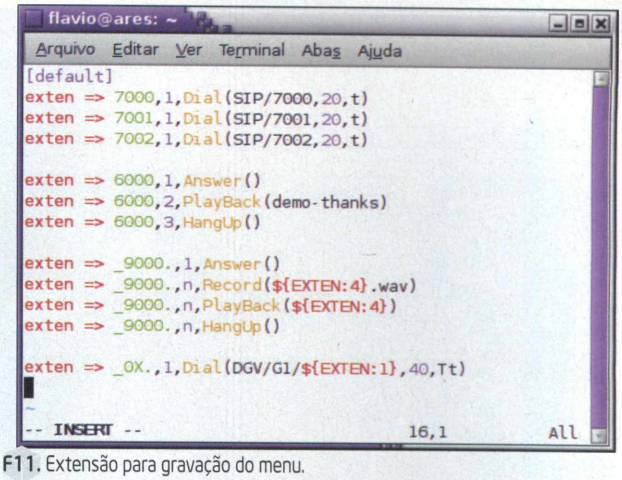
Uma vez configurado o canal DIGIVOICE, precisamos torná-lo acessível em nosso plano de discagem. Para isso, basta acrescentar a extensão: exten =>0X.,1,Dial(DGV/G1/${EXTEN:1},40,Tt), como na **figura 9**.

Vamos agora entender um pouco mais o que essa nova linha de configuração significa:

- **1.Primeiro parâmetro [_0X.]**: Como mencionamos na edição anterior, é possível criar expressões regulares para comparar com os dígitos recebidos pelo PABX. Nesse caso, temos uma expressão regular simples que combina com qualquer seqüência de números iniciada por 0 e com no mínimo 3 dígitos. Veja na tabela 1 um resumo dos



F10. Carga das alterações do plano de discagem.



F11. Extensão para gravação do menu.

caracteres especiais que podem ser utilizados na construção de expressões regulares e, na tabela 2, alguns exemplos de expressões.

- **2. Segundo parâmetro** [1]: como visto na edição anterior, esse parâmetro corresponde à prioridade ou seqüência de execução;

- **3. Terceiro parâmetro [Dial (DGV/G1/${EXTEN:1},40,Tt)]**: vamos agora analisar os argumentos da aplicação Dial. Note o primeiro parâmetro repassado, indicando o canal a ser chamado (DGV/G1), e verifique que pela primeira vez em nosso plano de discagem não se trata de um canal SIP e sim de um novo tipo de canal, chamado DGV. O número a ser repassado para o canal DGV vem da variável EXTEN, que contém os dígitos discados pelo usuário e recebidos pelo PABX. Entretanto, o número não pode ser repassado integralmente, pois precisamos eliminar o zero inicial que foi utilizado apenas para indicar que se trata de uma chamada externa. Para isso, configuramos um offset de 1 dígito que é feito através do ":1" que vemos logo após a variável EXTEN.

Com essa configuração basta digitar zero, seguido do número que discaríamos normalmente em um telefone comum, para realizarmos ligações externas a partir de nossos ramais SIP. Após ter editado o arquivo de configuração, acesse a CLI (asterisk -vvvvvr) e digite o comando dialplan reload para carregar as alterações do plano de discagem (**figura 10**). O resultado de uma chamada pode ser acompanhado via CLI, como também podemos observar nesta figura.

Expressão	Descrição
-	Início de um padrão.
.	Trata-se de um coringa, corresponde a um ou mais dígitos.
[47-9]	Quaisquer dígitos dentro das chaves, no exemplo temos o dígito 4 e todos 7 a 9.
X	Dígito de 0 a 9.
Z	Dígito de 1 a 9.
N	Dígito de 2 a 9.

T1. Descompactação do dgvchannel.

Extensão	Descrição
_9XXX	Qualquer número de 4 dígitos iniciado por 9.
_9.	Qualquer número que comece com 9.
_[7-9]XXXXXXX	Qualquer número de 8 dígitos iniciado por 7, 8 ou 9.

T2. Exemplos de expressões regulares.

URA

Agora que já podemos realizar chamadas através da rede telefônica convencional, falta atender as ligações que chegam através dela. Para isso, vamos criar uma URA simples que atenderá as ligações de entrada, agradecerá o contato e oferecerá um menu com três opções, conforme texto do **quadro 1**.

```
Obrigado por ligar para a XYZ software!
Tecle 1 para desenvolvimento;
Tecle 2 para suporte;
Ou aguarde...
```

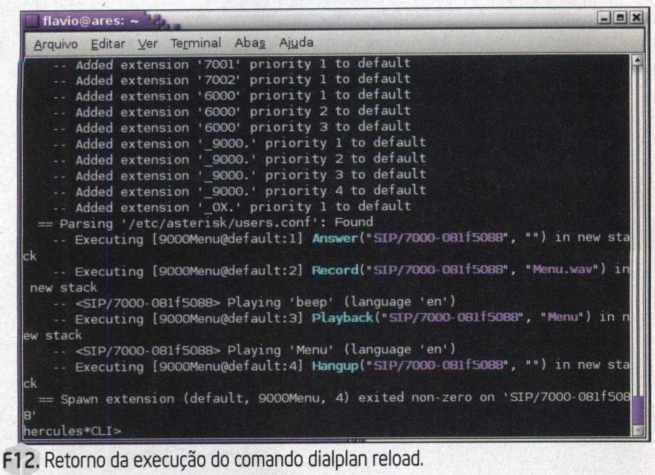
Q1. Script da URA

Gravando o menu

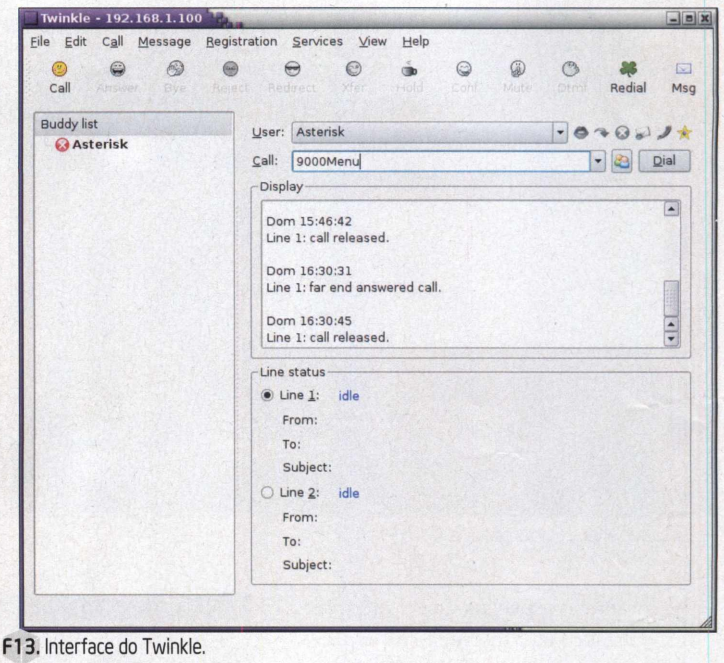
Para gravar este menu podemos utilizar qualquer software que grave som em formato Wav, porém, utilizaremos o próprio Asterisk para essa tarefa. Para isso, basta acrescentar uma extensão que chame a aplicação Record() no plano de discagem, como podemos observar na extensão 9000 do plano exibido na **figura 11**.

Vamos entender o que as quatro linhas de configuração da extensão 9000 significam:

- **exten => _9000.,1,Answer()**: indica que ao receber o número 9000 seguido de qualquer coisa, o PABX deve atender a ligação através da aplicação Answer();
- **exten => _9000.,n,Record(${EXTEN:4}.wav)**: após a execução da aplicação de prioridade 1, o PABX deve executar a aplicação Record(), que por sua vez gravará um arquivo Wav, cujo nome será obtido do número discado pelo usuário, com um offset de quatro



F12. Retorno da execução do comando dialplan reload.



F13. Interface do Twinkle.

dígitos para se retirar o número da extensão. Ou seja, ao discarmos a partir de um softphone para o "número" 9000Menu, a aplicação Record() gravará o som em um arquivo chamado Menu.wav. A gravação é finalizada pressionando-se a tecla #;

- **exten => _9000.,n,PlayBack(${EXTEN:4})**: após a execução das aplicações de prioridades 1 e 2, o PABX deve executar a aplicação PlayBack() que, por sua vez, reproduzirá o arquivo Wav gravado pela aplicação Record();
- **exten => _9000.,n,HangUp()**: após a execução das aplicações de prioridade 1, 2 e 3, o PABX deve executar a aplicação HangUp(), que desliga a chamada.

Uma vez configurado o plano de discagem, basta executarmos o comando dialplan reload na CLI (**figura 12**) para carregarmos as alterações. Feito isso, utilize o Twinkle para ligar para a extensão 9000Menu, por exemplo, e grave o áudio desejado (**figura 13**).

Configurando a URA

Com a mensagem já gravada, podemos seguir com a configuração. No nosso caso, vamos criar um novo contexto chamado "entrada" apenas para tratar as chamadas externas recebidas e, por esse motivo, configuramos anteriormente a opção context do arquivo digivoice.conf.

A execução de uma URA se resume principalmente à execução de uma única aplicação chamada Background(), que reproduz um arquivo de som e, enquanto isso, permite a captura das teclas pressionadas pela outra parte. Sendo assim, observe na **figura 14** como deve ficar a configuração de nossa URA.

Note que criamos três variáveis globais (seção globals) chamadas TELEFONISTA, DESENVOLVIMENTO e SUPORTE, contendo os valores de seus respectivos ramais para facilitar nossa configuração. Dentro do contexto entrada foram acrescentadas 7 linhas que detalhamos a seguir:

- **[entrada]**: define o contexto entrada;
- **exten => s,1,Answer()**: caso o Asterisk receba a extensão padrão (s), o PABX deve atender a ligação através da aplicação Answer(). O canal DIGIVOICE irá gerar (procurar por) uma extensão s no contexto entrada quando uma chamada chegar pela nossa linha analógica;
- **exten => s,2,Background(Menu)**: após a execução da aplicação de prioridade 1, o PABX deve executar a aplicação Background() que, por sua vez, reproduzirá o arquivo Wav chamado Menu enquanto aguarda que algum novo dígito seja recebido pelo PABX;
- **exten => s,3,WaitExten(2)**: após a execução das aplicações de prioridade 1 e 2, o PABX deve executar a aplicação WaitExten(), que aguarda algum dígito por determinado intervalo de tempo (no nosso caso, 2 segundos);
- **exten => t,1,Dial(${TELEFONISTA})**: caso o tempo da aplicação WaitExten() expire, o PABX deve discar para o ramal da telefonista. A extensão t indica timeout;
- **exten => i,1,Dial(${TELEFONISTA})**: caso o usuário utilize uma opção inválida em nossa URA, o PABX deve discar para o ramal da telefonista. A extensão i indica invalid;
- **exten => 1,1,Dial(${DESENVOLVIMENTO})**: caso o usuário utilize a tecla 1, o PABX deve discar para o ramal do desenvolvimento;
- **exten => 2,1,Dial(${SUPORTE})**: caso o usuário utilize a tecla 2, o PABX deve discar para o ramal do suporte.

Após configurar nossa URA, basta executar o comando dialplan reload na CLI (**figura 15**) e estamos prontos para receber chamadas.

```
flavio@ares: ~
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
[globals]
TELEFONISTA=SIP/7000
DESENVOLVIMENTO=SIP/7001
SUPORTE=SIP/7002

[default]
exten => 7000,1,Dial(SIP/7000,20,t)
exten => 7001,1,Dial(SIP/7001,20,t)
exten => 7002,1,Dial(SIP/7002,20,t)

exten => 6000,1,Answer()
exten => 6000,2,PlayBack(demo-thanks)
exten => 6000,3,HangUp()

exten => _9000.,1,Answer()
exten => _9000.,n,Record(${EXTEN:4}.wav)
exten => _9000.,n,PlayBack(${EXTEN:4})
exten => _9000.,n,HangUp()

exten => _0X.,1,Dial(DGV/G1/${EXTEN:1},40,Tt)

[entrada]
exten => s,1,Answer()
exten => s,2,Background(Menu)
exten => s,3,WaitExten(2)
exten => t,1,Dial(${TELEFONISTA})
exten => i,1,Dial(${TELEFONISTA})

exten => 1,1,Dial(${DESENVOLVIMENTO})
exten => 2,1,Dial(${SUPORTE})
<sk/extensions.conf" 30L, 689C written 21,0-1          All
```

F14. Configuração da URA.

```
flavio@ares: ~
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
hercules*CLI> dialplan reload
  == Parsing '/etc/asterisk/extensions.conf': Found
  == Setting global variable 'TELEFONISTA' to 'SIP/7000'
  == Setting global variable 'DESENVOLVIMENTO' to 'SIP/7001'
  == Setting global variable 'SUPORTE' to 'SIP/7002'
    -- Registered extension context 'default'
    -- Added extension '7000' priority 1 to default
    -- Added extension '7001' priority 1 to default
    -- Added extension '7002' priority 1 to default
    -- Added extension '6000' priority 1 to default
    -- Added extension '6000' priority 2 to default
    -- Added extension '6000' priority 3 to default
    -- Added extension '_9000.' priority 1 to default
    -- Added extension '_9000.' priority 2 to default
    -- Added extension '_9000.' priority 3 to default
    -- Added extension '_9000.' priority 4 to default
    -- Added extension '_0X.' priority 1 to default
    -- Registered extension context 'entrada'
    -- Added extension 's' priority 1 to entrada
    -- Added extension 's' priority 2 to entrada
    -- Added extension 's' priority 3 to entrada
    -- Added extension 't' priority 1 to entrada
    -- Added extension 'i' priority 1 to entrada
    -- Added extension '1' priority 1 to entrada
```

F15. Efetivando alterações a partir do comando dialplan reload.

Utilizando um provedor VoIP

Um problema que as pequenas empresas e escritórios enfrentam é que, muitas vezes, não podem negociar os vantajosos contratos que as grandes instituições realizam com as operadoras de telefonia. Felizmente hoje, existem diversos provedores VoIP que oferecem tarifas muito vantajosas e podem ser uma excelente alternativa. Além disso, outra boa notícia é que podemos configurar nosso Asterisk para utilizar um provedor para a realização de chamadas interurbanas e/ou internacionais, o que pode reduzir drasticamente o custo da conta telefônica.

No caso da nossa instituição, vamos utilizar o provedor JustVoip (**www.justvoip.com**), que no momento da produção dessa matéria estava oferecendo ligações gratuitas para o Brasil e para diversos outros países.

Para configurar, edite o arquivo /etc/asterisk/sip.conf e acrescente os dados para autenticação fornecidos pelo provedor, como na **figura 16**.

No arquivo /etc/asterisk/extensions.conf podemos, por exemplo, alterar a opção de discagem externa via linha analógica para exten => _00XXXXXXXX,1,Dial(DGV/G1/${EXTEN:2},40,Tt), que faria com que apenas ligações locais, com o número precedido de dois zeros, fossem realizadas via linha convencional. Além disso, poderíamos acrescentar ao plano de discagem a linha exten => _0Z.,1,Dial(SIP/${EXTEN:1}@PROVEDOR,90,Tt), que obrigaria que todas as ligações DDD e DDI saíssem via provedor (**figura 17**).

```
flavio@ares: ~
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
[general]
bindport=5060
bindaddr=192.168.1.102
context=default
disallow=all
allow=alaw,ulaw,gsm

[7000]
type=friend
secret=7000
dtmfmode=rfc2833
host=dynamic

[7001]
type=friend
secret=7001
dtmfmode=rfc2833
host=dynamic

[7002]
type=friend
secret=7002
dtmfmode=rfc2833
host=dynamic

[PROVEDOR]
type=friend
fromuser=meu_usuario
username=meu_usuario
secret=minha_senha
host=sip.justvoip.com
dtmfmode=rfc2833
</asterisk/sip.conf" 32L, 406C written 25,0-1          All
```

F16. Configuração do provedor.

```
flavio@ares: ~
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
[globals]
TELEFONISTA=SIP/7000
DESENVOLVIMENTO=SIP/7001
SUPORTE=SIP/7002

[default]
exten => 7000,1,Dial(SIP/7000,20,t)
exten => 7001,1,Dial(SIP/7001,20,t)
exten => 7002,1,Dial(SIP/7002,20,t)

exten => 6000,1,Answer()
exten => 6000,2,PlayBack(demo-thanks)
exten => 6000,3,HangUp()

exten => _9000.,1,Answer()
exten => _9000.,n,Record(${EXTEN:4}.wav)
exten => _9000.,n,PlayBack(${EXTEN:4})
exten => _9000.,n,HangUp()

exten => _00XXXXXXXX,1,Dial(DGV/G1/${EXTEN:2},40,Tt)
exten => _0Z.,1,Dial(SIP/${EXTEN:1}@PROVEDOR,90,Tt)

[entrada]
exten => s,1,Answer()
exten => s,2,Background(Menu)
exten => s,3,WaitExten(2)
exten => t,1,Dial(${TELEFONISTA})
exten => i,1,Dial(${TELEFONISTA})

exten => 1,1,Dial(${DESENVOLVIMENTO})
exten => 2,1,Dial(${SUPORTE})
<sk/extensions.conf" 31L, 748C written 19,0-1          All
```

F17. Grande flexibilidade para configurar plano de discagem.

Lembrando que, nesse caso, as ligações DDD e DDI devem conter o número internacional completo precedido de zero e sem operadora. Por exemplo, para ligar para a Editora Saber a partir de um ramal de nosso PABX seria necessário discar 0551120955333 e para realizar uma ligação local via linha analógica seria necessário discar 0020955333.

Após as alterações nos dois arquivos supracitados, é necessário recarregá-los no Asterisk, via CLI, com os comandos sip reload e dialplan reload.

Conclusões

Ao final dessa etapa, já podemos utilizar o Asterisk para, além de reduzir custos na aquisição de equipamentos, efetivamente trabalhar na redução dos custos da conta telefônica da instituição. Com a utilização de um provedor VoIP, é possível obter taxas de até R$0,04 por minuto nas ligações interurbanas, o que é muito vantajoso no momento de interligar seu PABX com a rede de telefonia convencional. Na próxima matéria, aprenderemos como integrar o Asterisk a um banco de dados e como configurar uma fila de atendimento. Até lá! **PC**

O baixo custo do acesso convencional à Internet é um grande apelo para a interligação de redes remotas através da segurança provida por configurações de rede virtual privada (VPN). Mas até pouco tempo, isso nem sempre era possível devido a problemas com servidores proxies e tradução de endereços IP.

A dupla Windows Vista SP1 e Server 2008 trazem uma nova realidade para as redes Microsoft. Nesta matéria você confere todos os detalhes para ter esse ambiente funcionando.



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.

Redes seguras com VPN

Quando falamos sobre tecnologias de acesso remoto logo pensamos, basicamente, em dois tipos de conexão: Rede Virtual Privada (VPN) e Conexão da Área de trabalho remota.

Para quem não conhece, a Conexão da Área de trabalho é uma tecnologia que permite ao usuário acessar remotamente a Área de trabalho do seu computador, utilizando o protocolo RDP. Quando uma conexão deste tipo é estabelecida de um computador na Internet para um computador dentro da rede interna, o número de máquinas nesta não se altera. Ou seja, se existirem 10 computadores antes da conexão, após o estabelecimento desta as mesmas 10 máquinas estarão presentes, visto que o acesso à área de trabalho de um sistema é limitado a apenas um usuário, independente deste estar local ou remotamente. Dessa forma, torna-se uma tecnologia de acesso útil para a realização de um diagnóstico remoto.

Já a VPN permite que um computador, localizado "atrás" da Internet, se conecte a uma rede remota da mesma forma que acontece quando isso é feito localmente. Seguindo o exemplo anterior, após uma conexão remota, via VPN, 11 computadores poderiam ser listados nesta rede. É como se existisse um cabo conectando o computador remoto ao switch da rede local.

A diferença está na velocidade da conexão, já que, enquanto a rede local estaria funcionando a 100 Mbps, a conexão VPN disponibilizaria algo em torno de 1 Mbps, por exemplo. Vale ressaltar que neste tipo de conexão os dados trafegados são protegidos por túneis criptografados, criados a partir de protocolos como o PPTP ou L2TP.

Pontos negativos

Os dois tipos de conexão citados são utilizados com freqüência, cada qual em situações específicas, porém, existem casos em que ambas não podem ser estabelecidas. Por exemplo, imagine uma empresa com sua matriz no Rio de Janeiro. O administrador da rede precisa ir à São Paulo para realizar um treinamento e ficará hospedado em um hotel que oferece aos seus hóspedes o serviço de acesso à Internet sem fio. Sendo assim, o administrador levará o seu notebook a fim de fazer uma conexão com a Área de Trabalho do servidor e, dessa forma, tentar solucionar possíveis problemas que surgirem. Ou então, estabelecer uma conexão VPN com o objetivo de executar ferramentas de diagnóstico remotamente.

Até aqui não falamos nada de novo, afinal de contas, este tipo de cenário é bastante comum. Porém, imagine que o acesso à Internet deste hotel seja oferecido através de um servidor Proxy e com um servidor DHCP devidamente configurado para fornecer um endereço IP e demais configurações ao notebook, tais como endereço de gateway e servidor DNS.

Apesar de parecer interessante, a Conexão da Área de trabalho remota permite que você trabalhe diretamente no servidor. Existem situações onde você pode precisar usar o seu próprio notebook como ferramenta de diagnóstico e, nesta situação, o referido tipo de conexão não ajuda muito. Sendo assim, a melhor opção seria mesmo a conexão VPN. O problema é que nem sempre elas poderão ser estabelecidas devido a restrições existentes na infra-estrutura da rede do hotel, como no nosso exemplo.

Como funciona uma conexão VPN?

Conforme dito anteriormente, conexões VPN podem ser estabelecidas através dos protocolos PPTP (*Point-to-Point Tunneling Protocol*), ou então o L2TP (*Layer 2 Tunneling Protocol*). Falando de conexões baseadas no protocolo PPTP, devemos entender que o mesmo é usado para criar um túnel pelo qual os dados serão transmitidos através da porta TCP 1723 e, numa segunda sessão, gerenciar o tráfego GRE (*Generic Routing Encapsulation*), que irá encapsular os dados. A criptografia das informações fica por conta do protocolo MPPE (no Windows Server 2003 a criptografia usa chaves de 128 bits) e o processo de compactação/descompactação dos dados, pelo protocolo MPPC. Apesar de ser relativamente simples de implementar (basta configurar o servidor e o cliente para usarem o PPTP, que os sistemas envolvidos se encarregam do resto), conexões VPN baseadas no PPTP são mais complicadas de serem gerenciadas pelos firewalls, pois duas sessões precisam ser liberadas. Por exemplo, se não for possível liberar o protocolo GRE através de um firewall, o túnel poderá ser criado, mas nenhum dado trafegará pelo mesmo. Além disso, se o notebook do referido técnico estiver atrás de um NAT (*Network Address Translation*), o mesmo deverá ser capaz de traduzir o tráfego GRE. Assim, o protocolo PPTP não trafega através de servidores Proxy.

No caso das VPNs baseadas no L2TP, o mesmo é responsável por criar o túnel que irá trafegar através da porta UDP 1701. O tráfego dos dados será feito através deste túnel e será criptografado pelo protocolo IPSec na porta UDP 500. Neste tipo de VPN, os problemas seriam basicamente os seguintes:

1) No caso dos firewalls, será necessário liberar as portas UDP 1701 e 500;

2) Se o cliente VPN estiver atrás de um NAT, tanto o servidor como o cliente VPN deverão ser capazes de suportar o NAT transversal (NAT-T), uma vez que o NAT não consegue traduzir adequadamente o tráfego IKE e os dados encapsulados pelo IPSec.

Além disso, assim como acontece com o tráfego da VPN PPTP, o tráfego da VPN L2TP não passa através de servidores Proxy. Soma-se a isso um considerável esforço administrativo para configurar a infra-estrutura de certificados digitais, necessária para suportar a tecnologia (configurar o servidor e o cliente VPN para confiarem na mesma autoridade de certificação; instalar os certificados IPSec nestes computadores, etc).

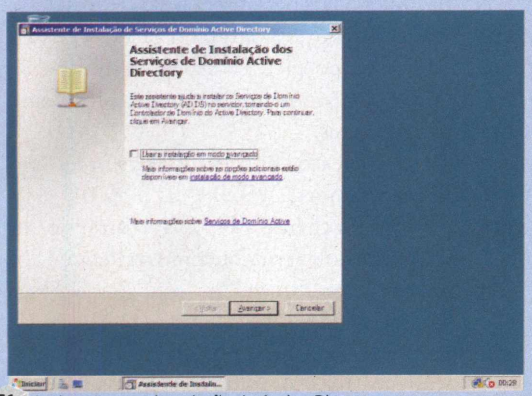
A solução - SSTP VPN

No mundo Microsoft, a solução para os problemas relacionados anteriormente atende pelo nome de *Secure Socket Tunneling Protocol*, ou simplesmente SSTP. Neste caso, trata-se de um tipo de túnel que protege o tráfego dos dados com o protocolo SSL. Isso significa que é possível estabelecer essa comunicação usando HTTPS. Isso mesmo! Estamos nos referindo ao mesmo tipo de comunicação, já bastante difundido, que permite a comunicação segura entre servidores e clientes através da Internet, na realização de operações comerciais. Sendo assim, o tráfego passa apenas pela porta TCP 443.

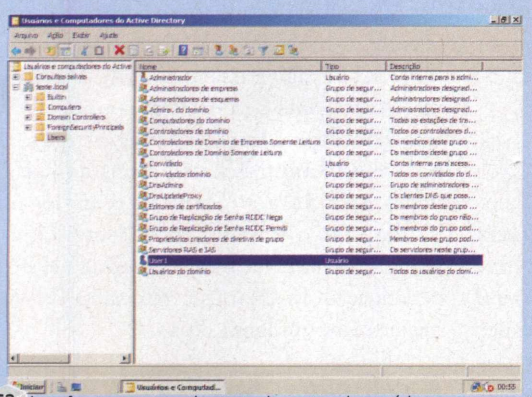
Se analisarmos com cuidado, veremos que a probabilidade de se encontrar problemas neste tipo de conexão é pequeno, pois o tráfego HTTPS é liberado na maioria dos

Atributos	PPTP	L2TP/IPSec	SSTP
Encapsulamento	GRE	L2TP sobre UDP	SSTP sobre TCP
Criptografia	MPPE com RC4	IPSec com 3DES ou AES.	SSL com RC4 AES
Protocolo de manutenção do túnel	PPTP	L2TP	SSTP
Quando a autenticação do usuário acontece?	Antes da criptografia iniciar	Depois que a sessão IPSec é estabelecida	Depois que a sessão SSL é estabelecida
Certificado necessário para estabelecer o túnel VPN	Nenhum	Certificado de computador tanto no servidor quanto no cliente	Certificado de computador no servidor VPN e o certificado da CA no cliente VPN

T1. Diferenças entre os protocolos PPTP, L2TP e SSTP.



F1. Assistente para instalação do Active Directory.



F2. Interface para gerenciamento de contas de usuários.

firewalls e permitido nos servidores Proxies existentes no mercado. Vale ressaltar ainda, que o uso deste novo tipo de VPN depende da presença de um servidor VPN baseado no Windows Server 2008 e do Windows Vista SP1 como cliente.

Funcionamento da conexão SSTP

1. O cliente SSTP estabelece uma conexão TCP com o servidor SSTP usando uma porta dinâmica no cliente e a porta 443 no servidor;
2. O cliente SSTP envia uma mensagem ao servidor indicando que deseja estabelecer uma conexão;
3. O servidor SSTP envia um certificado de computador para o cliente SSTP;
4. O cliente SSTP valida o certificado de computador enviado, determina o método de criptografia que será usado na sessão SSL, gera uma chave de sessão SSL e então criptografa a chave pública do certificado do servidor SSTP;
5. O cliente SSTP envia a chave de sessão SSL criptografada para o servidor SSTP;
6. O servidor SSTP descriptografa a chave SSL com a chave privada do certificado de computador. A partir disso, toda comunicação entre o servidor e o cliente será criptografada com o método negociado e com a chave de sessão SSL;
7. O cliente SSTP envia uma mensagem de requisição HTTPS para o servidor SSTP;
8. O cliente SSTP negocia um túnel SSTP com o servidor SSTP;
9. O cliente SSTP negocia uma conexão PPP com o servidor SSTP. Esta negociação inclui as credenciais do usuário autenticado com um método de autenticação PPP e estabelece as configurações necessárias para o tráfego IPv4 ou IPv6;
10. O cliente SSTP inicia o envio dos dados através do link PPP estabelecido.

Vamos testar?

Bem, depois de tanto falar sobre essa tecnologia, acreditamos que você esteja ansioso para testá-la, não é mesmo? Você não encontrará muitas dificuldades para acompanhar o teste, mas seria interessante que você já estivesse familiarizado com o processo de configuração de uma VPN PPTP/L2TP no Windows Server 2003.

Conforme dito anteriormente, para poder configurar uma VPN SSTP é necessário que o servidor VPN execute o Windows Server 2008 e o cliente, o Windows Vista SP1. Sendo assim, para executarmos o nosso teste precisaremos de duas máquinas rodando o Windows Server 2008. Uma desempenhará a função de Controlador de domínio e de servidor DNS, enquanto a outra executará o Serviço de Roteamento e Acesso Remoto (RRAS) e o Serviço de Informações da Internet (IIS 7), além de também servir como Autoridade de certificação, que emitirá os certificados que serão usados na configuração da VPN SSTP.

Preparando o DC

Para quem já está familiarizado com o processo de configuração da VPN no Windows Server 2003, podemos dizer que os conceitos aplicados são basicamente os mesmos, porém, a forma de implementar a tecnologia é um pouco diferente no Windows Server 2008.

Com relação à configuração do Controlador de domínio, o processo é até mais simples do que o utilizado no Windows Server 2003. Na verdade, o certo seria dizer que o processo agora é bem mais transparente para o administrador.

Para começar, configure uma máquina com o Windows Server 2008 com uma placa de rede que deverá ter o seu endereço IP ajustado para 192.168.0.1/24. Para quem nunca executou essa tarefa no referido sistema, o processo é o mesmo que usamos no Windows Vista, ou seja, uma das formas de fazê-lo seria usando a Central de Redes e Compartilhamento, que pode ser acessada através do Painel de Controle. Feito isso, basta clicar no menu Iniciar > Executar e digitar o comando DCPROMO. O sistema executará uma verificação para saber se os binários dos Serviços de Domínio do Active Directory (AD DS) estão instalados no computador. Caso não estejam instalados, isso será feito automaticamente pelo assistente.

Com o AD DS instalado, o Assistente de instalação do Active Directory irá apresentar a tela de boas vindas (**figura 1**). Clique em Avançar e siga as instruções do assistente, configurando o nome do domí-

nio como teste.local. Se você já configurou um DC anteriormente, as perguntas que o assistente fará serão respondidas com facilidade.

Finalizada essa etapa, aguarde o processo de configuração do sistema com a sua respectiva reinicialização. Feito isso, o servidor acabou de ser configurado como Controlador de domínio e como servidor DNS.

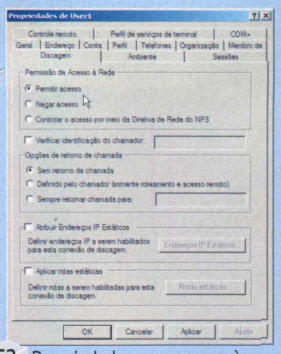
Depois que o servidor reinicializar, efetue o logon no sistema e abra o console Usuários e computadores do Active Directory (DSA.MSC). Com o mesmo aberto, crie uma conta de usuário chamada User1. Isso pode ser feito da mesma maneira como no Windows Server 2003, ou seja, abra o container Users, clique com o botão direito do mouse em uma área livre, no painel da direita, e clique em Novo > Usuário. Depois, basta seguir as instruções do assistente. Se você fez tudo certo até aqui, a conta do usuário será apresentada conforme mostra a **figura 2**.

A princípio, nenhuma conta criada no AD possui permissão para estabelecer conexões de acesso remoto, ou seja, conectar-se à rede através de uma VPN. Então teremos que habilitar isso para a conta do User1. Para isso clique com o botão direito sobre a mesma e selecione a opção Propriedades.

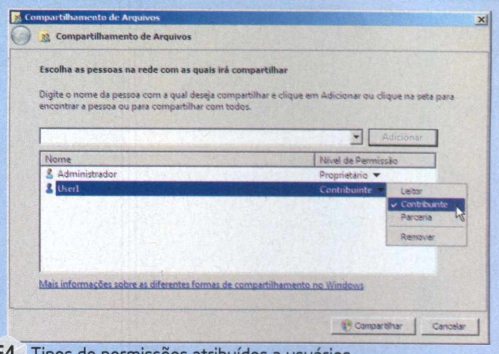
Na caixa de propriedades da conta, clique na guia Discagem (**figura 3**). Nela, você encontrará uma área chamada Permissão de Acesso à Rede, que possui três opções: Permitir acesso, Negar acesso e Controlar o acesso por meio da Diretiva de Rede do NPS.

As duas primeiras opções são auto-explicativas, já a opção "Controlar o acesso por meio da Diretiva de Rede do NPS" informa que o RRAS deverá verificar a existência de alguma diretiva de acesso configurada no Network Policy Server (NPS). Através dessas diretivas, poderíamos configurar, por exemplo, quais grupos teriam a permissão de acessar a rede a partir de uma VPN, informando inclusive o dia da semana e a hora de liberação do acesso.

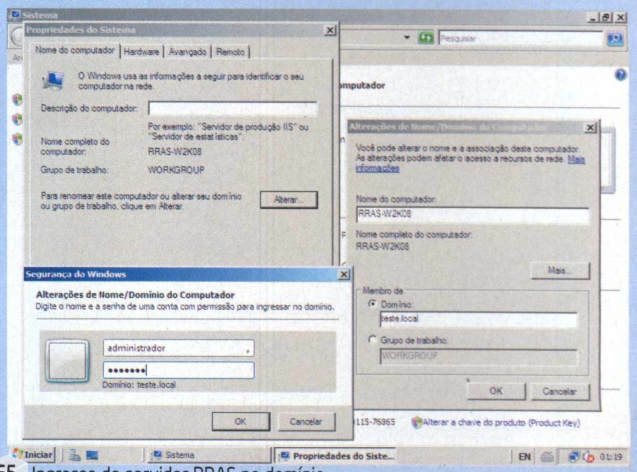
No Windows Server 2008, o NPS não vem com nenhuma diretiva configurada (como acontece com o Windows Server 2003). Sendo assim, iremos marcar a opção "Permitir acesso" para não aumentar mais a complexidade da configuração. Feito isso, basta clicar em OK.



F3. Propriedades para acesso à rede para a conta User1.



F4. Tipos de permissões atribuídos a usuários.



F5. Ingresso do servidor RRAS no domínio.

Para completar a configuração deste primeiro servidor, criaremos uma pasta para depois compartilhá-la. O objetivo aqui é criar um recurso que nos permita testar se o usuário que fará o acesso através da VPN realmente terá acesso aos recursos presentes na rede interna. Sendo assim, crie uma pasta na raiz da unidade C chamada Docs. Clique com o botão direito sobre a mesma e selecione a opção Compartilhar. Na caixa que aparece, a conta do administrador já está na lista de pessoas que devem ter acesso à pasta, e a permissão dele é de Proprietário. Para o nosso exemplo, adicione a conta do User1 e conceda a ele a permissão Contribuinte (**figura 4**).

Com o nosso DC pronto, agora vamos para o RRAS!

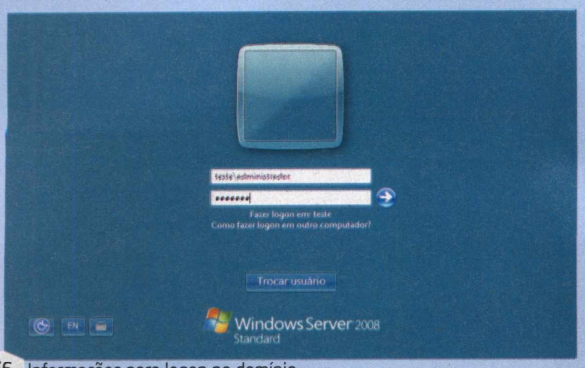
Configurando o RRAS

Inicie a segunda máquina com o Windows Server 2008. Vale ressaltar que este computador deve ter duas interfaces de rede, uma será usada na comunicação do servidor com a rede interna e a outra, na comunicação com a Internet.

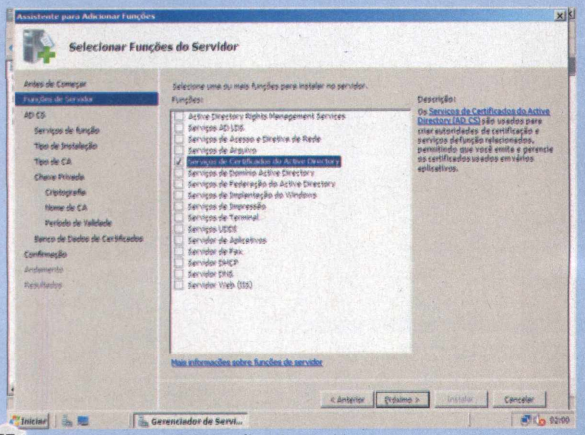
Comece renomeando para Rede Local a interface de rede que irá conectar o servidor à rede interna. Depois, configure o endereço IP da mesma para 192.168.0.2/24 e aponte o endereço do servidor DNS para 192.168.0.1, que é o endereço IP do primeiro servidor que preparamos e que também desempenha a função de servidor DNS, lembra?

A segunda interface deve ser renomeada para Internet e configurada com o endereço IP 200.200.200.1/24. Vale ressaltar que, no nosso exemplo, não é necessário configurar um endereço de gateway ou de outro servidor DNS.

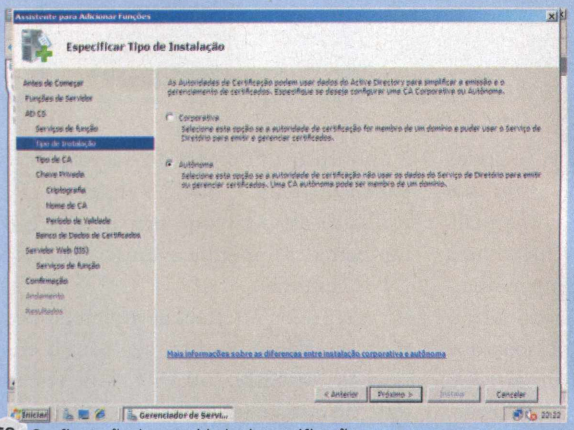
Feito isso, poderemos ingressar este servidor no domínio teste.local criado anteriormente. Para isso, use a combinação de teclas Windows + Pause para abrir as Propriedades do sistema. Na janela que aparece, clique no link Alterar Configurações para abrir a caixa de Propriedades do sistema. Na guia Nome do computador, clique no botão Alterar, informe o nome DNS do domínio e clique em OK. Uma caixa solicitando uma credencial válida no Active Directory será exibida (**figura 5**). Para o nosso exemplo, informaremos a conta do administrador com a sua res-



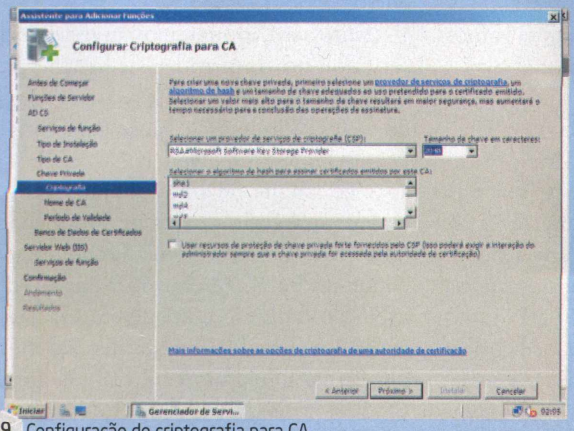
F6. Informações para logon no domínio.



F7. Assistente para definir funções do servidor.



F8. Configuração de autoridade de certificação.



F9. Configuração de criptografia para CA.

pectiva senha. Clique em OK e aguarde a caixa que confirma o ingresso do servidor no domínio.

O computador será reiniciado como parte do processo de ingresso no domínio. Quando a máquina voltar, para utilizar uma conta de domínio é necessário informá-la no formato NetBIOS-do-domínio\conta. No nosso caso, por exemplo, para efetuarmos logon usando a conta do administrador do domínio, devemos digitar o nome da conta da seguinte forma: TESTE\Administrador (**figura 6**).

Agora que o servidor está no domínio, iremos configurá-lo como uma Autoridade de certificação para o domínio teste.local. Para isso, devemos abrir o console Gerenciar servidor e clicar na opção Funções. Nesta janela, clique na opção Adicionar função para abrir o assistente correspondente. Com este aberto, selecione a opção Serviços de Certificado do Active Directory (AD CS) e clique em Próximo (**figura 7**).

Assim, o assistente iniciará o processo de configuração da CA. Clique em Próximo e, na tela seguinte, certifique-se de que as opções Autoridade de Certificação e Registro na Web de Autoridade de Certificação estejam marcadas. No caso, ao marcar a segunda opção citada, o assistente irá informar que funções adicionais (no caso, o IIS 7) são necessárias para que o recurso seja habilitado. Clique no botão Adicionar Serviços de Função Necessários e prossiga com o processo de configuração.

Na tela seguinte, o assistente pergunta se você deseja configurar uma autoridade de certificação corporativa ou uma autoridade de certificação autônoma. Como explicar a diferença entre estes dois tipos de CA foge ao escopo desta matéria, apenas marque a opção Autônoma e clique em Próximo (**figura 8**).

Agora você deve informar se deseja configurar uma CA Raiz ou uma CA Autônoma. Como esta é a primeira CA da rede, marque a opção CA Raiz e clique em Próximo.

Uma vez que iremos configurar uma CA Raiz, precisaremos determinar se uma nova chave privada será criada ou se iremos usar uma chave existente. Como não possuímos nenhuma chave, iremos marcar a opção Criar uma nova chave privada e, depois, clicar no botão Próximo .

Como uma nova chave privada será criada, é necessário informar qual deverá ser o provedor do serviço de criptografia (opção padrão, RSA), o algoritmo de hash que será usado (opção padrão SHA1) e o comprimento da chave (opção padrão, 2048 bits). Mantenha as opções padrão e clique em Próximo (**figura 9**).

Com estas informações, o assistente perguntará qual será o nome usado pela CA. Este será o nome exibido, por exemplo, no console de certificados na pasta Autoridades de certificação raiz confiáveis. Aceite o nome padrão e clique em Próximo. Nas próximas duas telas do assistente, você deverá informar o período de validade da chave privada (**figura 10**) e onde serão armazenados, respectivamente, o banco de dados e os logs do serviço de certificados.

Para a configuração da CA, estas informações são suficientes. Portanto, podemos prosseguir com a instalação. Porém, como o serviço do IIS também foi adicionado, será necessário configurá-lo como parte do processo de instalação da CA (nós usaremos uma página da web para solicitar os certificados nas máquinas envolvidas, como será visto mais adiante). A tela de configuração do IIS pode ser vista na **figura 11**.

Nas telas seguintes, basta utilizar as opções de configuração padrão. Como última etapa, basta clicar no botão Instalar.

Com o servidor configurado como CA, solicitaremos o certificado que permite fazer a autenticação do servidor perante o cliente de VPN SSTP. Essa tarefa será executada usando-se o site que o AD CS disponibilizou automaticamente através do processo de instalação executado anteriormente.

Para isso, abra o Internet Explorer e digite na barra de endereços **http://localhost/certsrv**, para acessar o site do serviço de certificados. Porém, assim como acontece com o Windows Server 2003, no Windows Server 2008 o Internet Explorer funciona de forma muito limitada para evitar que uma possível vulnerabilidade seja explorada, em caso de abertura de um site contendo código malicioso. Sendo assim, o site do serviço de certificados terá o seu funcionamento prejudicado, pois um controle Active X precisará ser executado como parte do processo de solicitação do certificado.

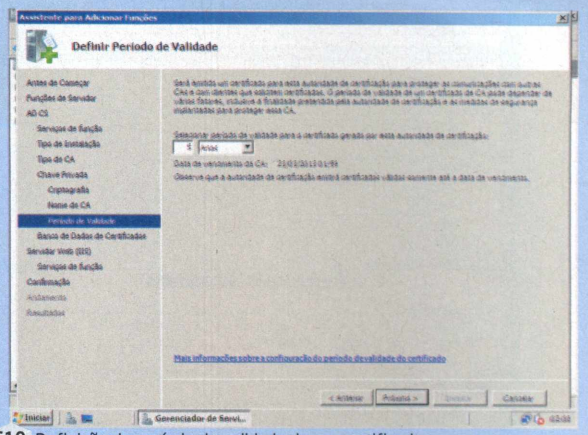
Visto o exposto, com a página inicial do site do serviço de certificados aberta, clique no menu Arquivo e aponte para a opção Adicionar site > Zona da Intranet Local (**figura 12**). Assim, o site será colocado na referida zona.

Agora, iremos reduzir o nível de segurança da zona Intranet Local, de forma que o site possa funcionar de maneira adequada. Uma das formas de executar esta tarefa é indo até o Painel de controle e abrindo as Opções da Internet, conforme mostra a **figura 13** (isso também poderia ser feito através do menu Ferramentas > Opções da Internet no Internet Explorer). Na janela que se abre, clique na guia Segurança e selecione a zona Intranet Local. Feito isso, reduza o nível de segurança para a opção Baixa e clique em OK.

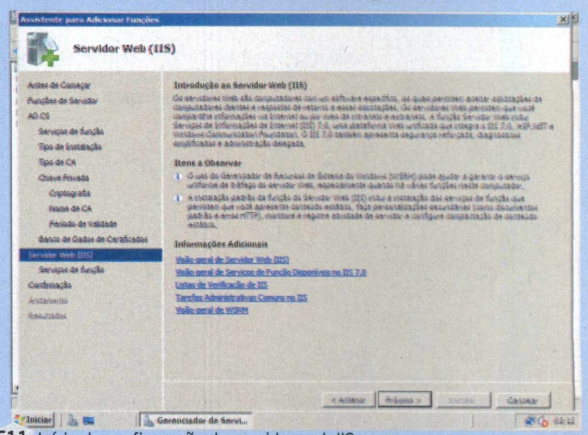
Com o site do serviço de certificados devidamente autorizado, na sua página inicial, clique no link Solicitar um certificado, o qual levará a uma página de mesmo nome (**figura 14**).

Como o certificado que precisamos não consta na lista (precisamos de um certificado que autentique o servidor), iremos clicar no link Solicitação avançada de certificado. Na página que será aberta, clique no link Criar e enviar uma solicitação para a autoridade de certificação.

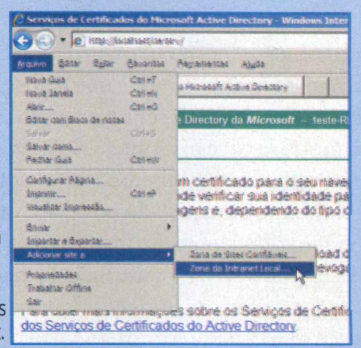
Na próxima página, você deve preencher o formulário de solicitação. Como o certificado é para um computador, basta preencher o campo Nome com o nome do computador. Aqui vale uma observação impor-

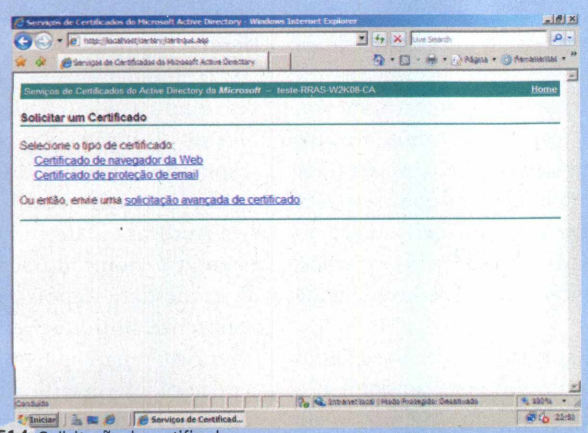


F10. Definição de período de validade de um certificado.

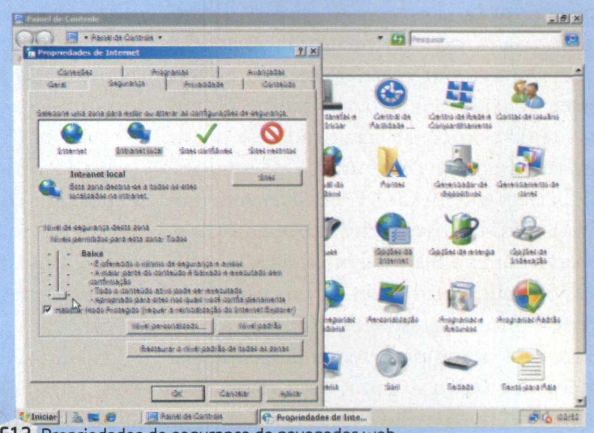


F11. Início da configuração do servidor web IIS.

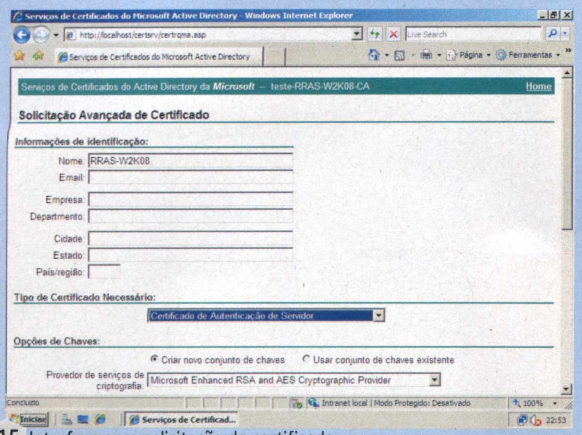

F12. Inclusão da página do serviço de certificados na intranet.



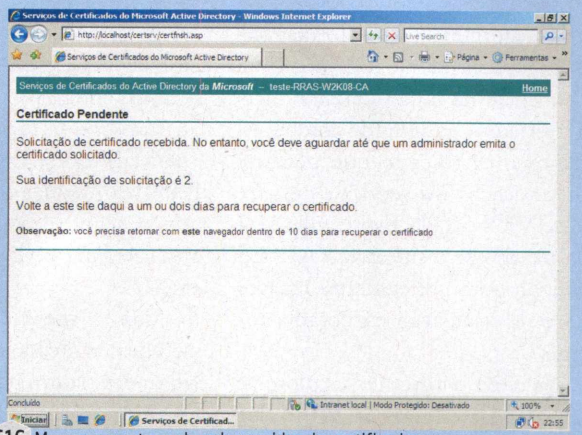
F14. Solicitação de certificado.



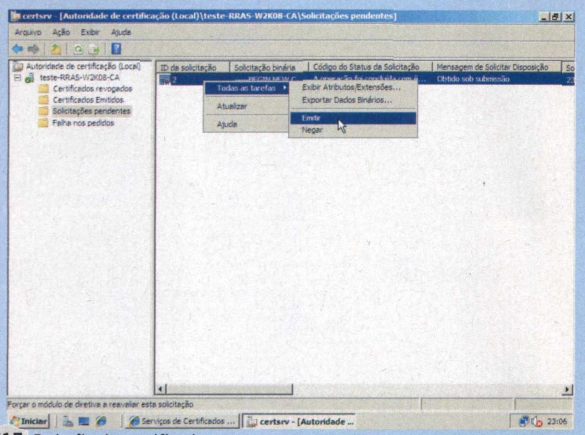
F13. Propriedades de segurança do navegador web.



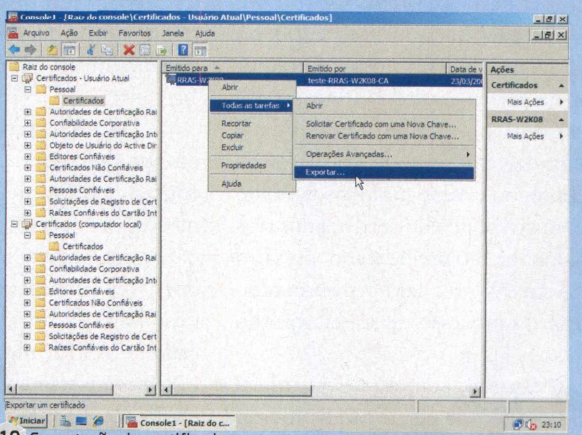
F15. Interface para solicitação de certificado.



F16. Mensagem retornada pelo servidor de certificados.



F17. Emissão do certificado.



F18. Exportação de certificado.

tantíssima: o nome que for digitado neste campo deverá ser o nome que será usado no cliente para estabelecer a comunicação. Por exemplo, se você informar o nome exemplo.teste.com como nome para o computador e, nas configurações da conexão VPN no computador cliente, fornecer o endereço IP do servidor RRAS (situação plenamente aceitável), uma mensagem de erro de conexão será exibida informando que o nome do servidor de destino não confere com o nome usado no certificado apresentado para fazer a autenticação do mesmo. Sendo assim, você deve inserir, no campo Nome do site do serviço de certificados, o nome que será usado no computador cliente para estabelecer a conexão. É possível solicitar vários certificados objetivando autenticar o servidor com nomes diferentes, ou seja, você poderia solicitar um certificado usando o nome vpnserver.teste.com (desde que, é claro, esse nome pudesse ser resolvido na Internet) e outro usando o seu respectivo endereço *IP* externo (200.200.200.1, por exemplo).

Pensando no que foi dito , informe o nome que será usado no certificado. Feito isso, no campo Tipo de Certificado Necessário, selecione a opção Certificado de Autenticação de Servidor (**figura 15**). Além disso, rolando a página você deverá marcar a opção Marcar as chaves como exportáveis. Isso deve ser feito porque quando o certificado for instalado no sistema, o mesmo será configurado como um certificado de usuário. Como o certificado deve ser instalado como um certificado de computador, posteriormente nós iremos exportá-lo para o referido armazenamento. Se esta opção não for marcada, a chave privada do certificado não poderá ser exportada com ele. Depois que as opções forem devidamente marcadas, clique no botão Enviar para poder enviar a solicitação do certificado para a Autoridade de certificação.

Como a Autoridade de certificação foi configurada como uma raiz autônoma, a sua configuração padrão de emissão de certificados determina que as solicitações de certificados devam ser configuradas como pendentes e só poderão ser emitidas manualmente por um administrador através do console de gerenciamento da CA. No caso de uma CA corporativa, a configuração padrão determina que a emissão de certificados deve ser feita de forma automática (isso pode ser alterado). Visto o exposto, o serviço de certificados informa que você deve aguardar até que o certificado seja emitido pelo administrador (**figura 16**).

Para poder emitir o certificado, uma vez que a CA está configurada neste mesmo computador, basta abrir seu respectivo console de gerenciamento em Ferramentas administrativas (console Autoridade de certificação). Agora, estenda o nome do servidor no painel da esquerda e depois faça o mesmo no recipiente Solicitações pendentes. Ao fazer isso, repare que no Painel da direita será exibido o certificado que foi solicitado através do site. Clique com o botão direito no mesmo, aponte para Todas as

tarefas e depois clique na opção Emitir (**figura 17**).

Feito isso, o certificado será emitido. Se achar necessário, isso pode ser conferido através da pasta Certificados emitidos, existente neste mesmo console. Agora, abra novamente o site do serviço de certificados e, na sua página inicial, clique no link Exibir o status de uma solicitação de certificado pendente. Ao fazer isso, você será levado para uma página, onde o serviço de certificados exibe os certificados emitidos, ou então, a informação de que o seu certificado ainda não foi emitido. Como nós já o fizemos, o certificado que solicitamos anteriormente aparece na lista de certificados que já estão disponíveis para instalação.

Sendo assim, clique no link do mesmo e siga as instruções para instalar o certificado. Note que o certificado terá sido instalado no local errado, ou seja, a instalação do certificado foi feita dentro do armazenamento de certificados pessoais de usuário. Nós precisamos deste certificado dentro do armazenamento de certificados pessoais do computador. Para isso, abra o MMC e adicione o snap-in de certificados de usuário e o snap-in de certificados de computador.

Com os dois sendo exibidos, abra o armazenamento de certificado pessoal dos certificados do usuário. Você encontrará o certificado que foi solicitado lá no site do serviço de certificados. Clique com o botão direito sobre o mesmo, selecione Todas as tarefas > exportar (**figura 18**).

Siga as instruções do assistente que será aberto, tomando o cuidado de marcar a opção que determina que a chave particular do certificado também deve ser exportada. As demais opções são autoexplicativas.

Com o processo de exportação concluído, devemos importar este certificado para o armazenamento de certificados pessoais do computador. Para isso, clique com o botão direito sobre a pasta Pessoal existente dentro do snap-in de certificados do computador e selecione Todas as tarefas > Importar (**figura 19**).

O assistente de importação será aberto. Na hora de localizar o certificado exportado anteriormente, atente para a seguinte situação: por padrão, o assistente tenta localizar certificados do tipo CER (Certificado X.509). Acontece que a chave privada do certificado também foi exportada e, sendo assim, o tipo do certificado passa a ser PFX (Troca de informações pessoais). Visto isso, ao encontrar o local onde você exportou o certificado, no campo Tipo de certificado, selecione a opção Troca de informações pessoais (*.pfx, *.p12), conforme exibido na figura 20. Localizado o certificado, basta seguir as instruções do assistente até concluir a operação. Com isso, o certificado passa a estar no local correto.

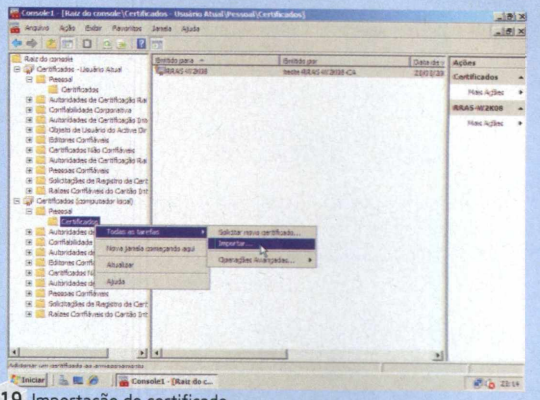
Em seguida, precisamos adicionar a função RRAS no servidor. Para isso, abra novamente o console Gerenciar servidor e clique em Adicionar função. No assistente que será aberto, selecione a função Serviços de Acesso e Diretiva de rede, e clique em Próximo.

Esta função de servidor permite configurá-lo, basicamente, como servidor RRAS/NAP. Para o nosso exemplo, precisaremos apenas da função de RRAS. Sendo assim, nesta segunda tela do assistente, selecione apenas a opção Serviços de Roteamento e Acesso Remoto e clique em Próximo. Depois, basta seguir as instruções do assistente até concluir o processo.

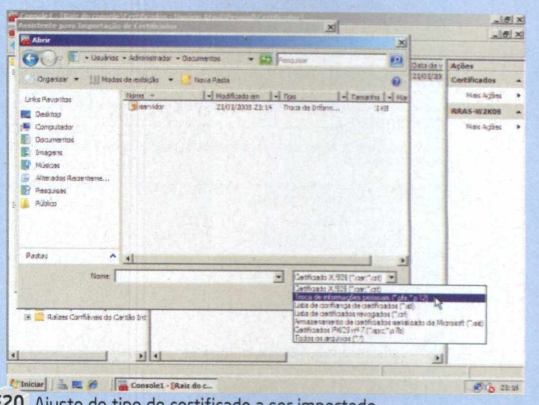
Com a função RRAS instalada, iremos configurar o sistema como um servidor de VPN. Abra o console de Roteamento e Acesso Remoto presente dentro de Ferramentas administrativas, clique com o botão direito sobre o nome do servidor e selecione a opção Configurar e Habilitar Roteamento e Acesso Remoto (**figura 21**).

Na primeira tela do assistente, devemos informar o serviço que será configurado. Como já existe uma opção pré-definida para o servidor de VPN, marque a opção Acesso remoto (dial-up ou rede virtual privada) e clique em Avançar.

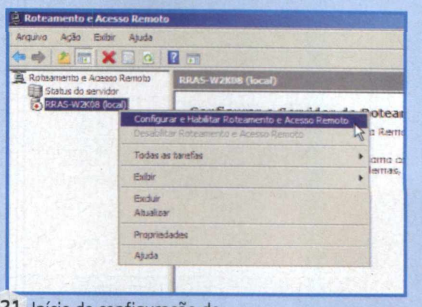
Feito isso, o assistente exibirá as opções referentes ao tipo de função selecionado anteriormente. Sendo assim, marque a opção VPN na próxima tela e clique em Avançar (**figura 22**).



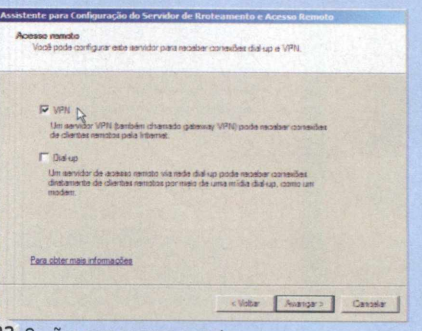
F19. Importação de certificado.



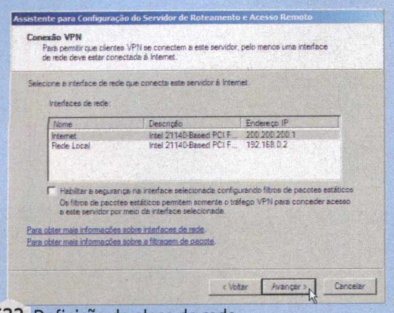
F20. Ajuste do tipo de certificado a ser importado.



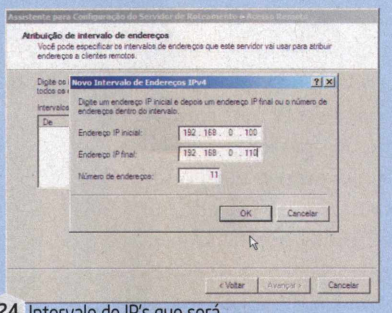
F21. Início de configuração do servidor para a função VPN.



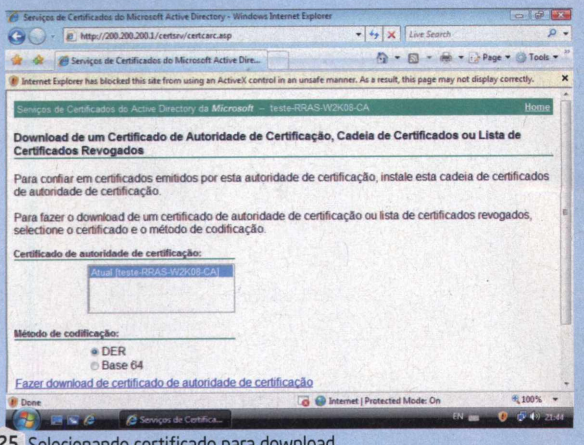
F22. Opções para acesso remoto.



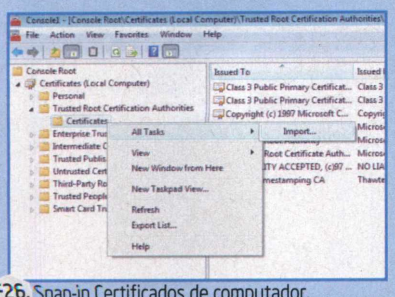
F23. Definição de placa de rede para acesso à Internet.



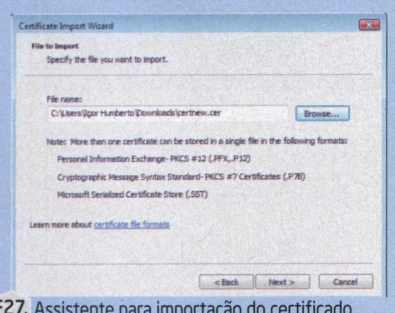
F24. Intervalo de IP's que será atribuído aos clientes.



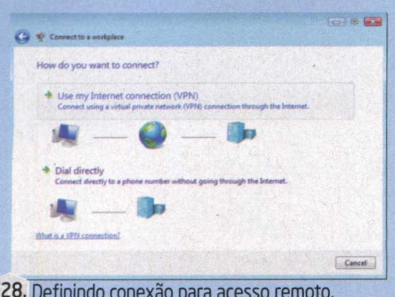
F25. Selecionando certificado para download.



F26. Snap-in Certificados de computador.



F27. Assistente para importação do certificado.



F28. Definindo conexão para acesso remoto.

Na tela seguinte, o assistente perguntará qual dos adaptadores de rede será usado para fazer a conexão com a Internet. Como os dois adaptadores foram renomeados no início do processo de configuração deste servidor, selecione o adaptador Internet, desmarque a opção "Habilitar a segurança na interface selecionada configurando filtros de pacotes estáticos" e clique em Avançar (**figura 23**).

Agora, o assistente pergunta como será feita a atribuição de endereços para os clientes da VPN. Como não temos um servidor DHCP configurado em nossa infra-estrutura, teremos que especificar um pool de endereços estáticos. Marque então a opção "De um intervalo de endereços especificado" e clique em Avançar.

Especifique o intervalo de endereços que será usado e clique em Avançar (**figura 24**). Na próxima etapa, o assistente lhe pergunta quem fará o processo de autenticação dos clientes da VPN. Você pode optar por usar o próprio RRAS, ou então, utilizar um servidor RADIUS. Como não temos um servidor RADIUS configurado, iremos selecionar a opção Não, usar o Roteamento e acesso remoto para autenticar pedidos de conexão. Feito isso, clique em Avançar.

Siga as últimas instruções do assistente até completá-lo. Feito isso, o servidor de acesso remoto para conexões VPN estará configurado.

Configurando o Windows Vista

Com a infra-estrutura adequadamente configurada, agora é hora de preparar o computador cliente. No caso, este cliente deve ser obrigatoriamente um computador configurado com o Windows Vista SP1, conforme já foi dito no início da matéria.

Nosso primeiro passo será o de fazer com que o cliente confie na CA que foi configurada dentro da nossa infra-estrutura. Isso será feito através do site do serviço de certificados configurado anteriormente.

Abra o navegador e digite **http://200.200.200.1/certsrv** na barra de endereços para abrir a página inicial do serviço de certificados. Clique no link Fazer o download de um certificado de autoridade de certificação, cadeia de certificados ou lista de certificados revogados. Isso o levará para uma outra página onde você deverá clicar no link Fazer o download de certificado de autoridade de certificação (**figura 25**). Salve o certificado em alguma pasta no computador.

Agora, abra o MMC e adicione o snap-in de certificados de computador. Expanda Trusted Root Certification Authorities (Autoridades de certificação raiz confiáveis), e clique com o botão direito em Certificates. Clique em All Tasks > Import (Todas as tarefas > Importar), como mostra a **figura 26**, e siga as instruções do assistente até concluir o processo (**figura 27**).

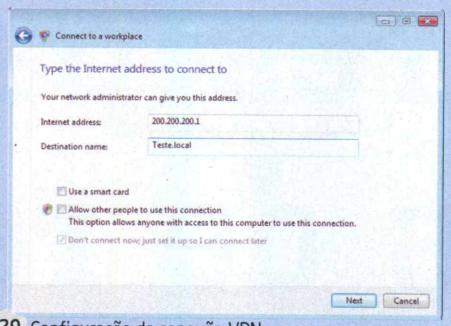
Com o computador cliente confiando na mesma CA que está sendo usada na rede corporativa, basta criar a conexão VPN. Para isso, abra a Central de redes e compartilhamento e clique no link que permite criar uma nova conexão. Isso abrirá o assistente Set up a connection or network (Configurar uma conexão ou rede). Neste, selecione a opção Connect to a workplace (Conectar ao meu local de trabalho) e clique em Next (Avançar).

Agora o assistente quer saber como será feita a conexão, se através de uma linha discada ou VPN. Marque a opção Use my Internet connection – VPN (Usar a minha conexão Internet – VPN), conforme mostra a **figura 28**.

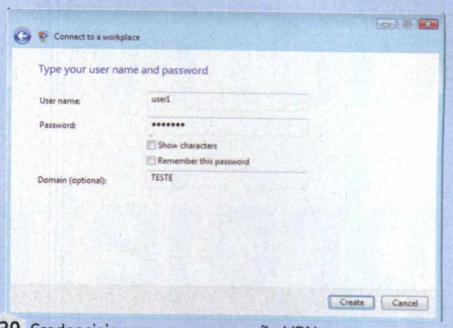
Na próxima tela, o assistente pergunta se você deseja configurar uma conexão com a Internet agora. Como a conexão já existe, basta clicar na opção I'll set up in a Internet connection later (Eu configurarei

uma conexão com a Internet mais tarde).

Nesta etapa, você deve informar o endereço que será usado para alcançar o servidor VPN. Lembre-se de que aqui você deve informar o mesmo nome que foi usado no momento em que o certificado para autenticação foi configurado no servidor VPN. Informe também um nome para a conexão. As outras opções podem ser mantidas com as suas respectivas opções padrão. Digite os dados e clique em Next (**figura 29**).



F29. Configuração da conexão VPN no cliente Windows Vista.



F30. Credenciais para uso na conexão VPN.

Forneça as credenciais que serão usadas para estabelecer a conexão e clique no botão Create para finalizar o assistente (**figura 30**). Pronto! A sua conexão está pronta.

Acabamos de preparar a conexão, porém, da mesma forma como acontece com as versões anteriores do Windows, o tipo de VPN é configurado como Automático. Ou seja, seguindo a lógica das versões anteriores, ao tentar estabelecer uma conexão, o sistema tentará se conectar primeiro por uma porta PPTP. Caso uma porta deste tipo não esteja disponível, o sistema tentará estabelecer uma conexão através de uma porta L2TP. Se, ainda assim, uma porta não estiver disponível, o sistema tentará se conectar através da porta SSTP (exclusiva dos sistemas Vista SP1 e Server 2008).

Para garantir que a conexão VPN será estabelecida através da porta SSTP, iremos alterar as propriedades da conexão VPN. Para isso, na Central de Redes e Compartilhamento, clique em Manage a network connection (Gerenciar conexões de rede) e, na janela que será aberta, clique com o botão direto sobre a conexão VPN criada anteriormente. No menu que aparece, selecione Properties para exibir as propriedades da conexão VPN. Agora, clique na guia Networking (Rede). No campo Type of VPN (Tipo de VPN), selecione a opção Secure Socket Tunneling Protocol (SSTP), conforme mostra a **figura 31**.

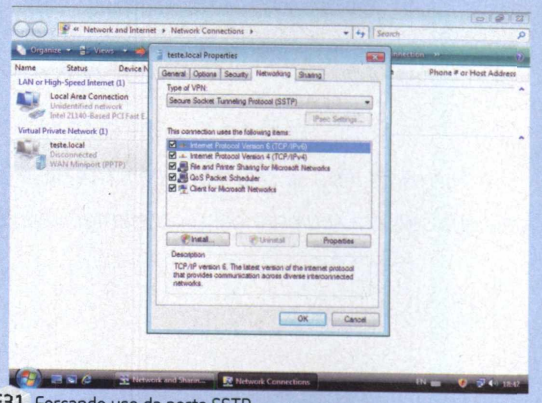
Agora é só realizar a conexão. O processo é o mesmo que é adotado com os outros tipos de VPN. A diferença está apenas no tipo de túnel criado, ou seja, sob o ponto de vista do usuário o processo é transparente. Para conferir se a conexão foi realizada com êxito, clique com o botão direito na conexão e selecione a opção Status. Se você fez tudo corretamente, deverá ver a **figura 32**.

Como agora você está conectado à rede, será possível abrir o compartilhamento Docs criado durante a preparação do DC. Para isso, clique no menu Iniciar e digite \\192.168.0.1\docs. Você deve conseguir abrir o compartilhamento (**figura 33**).

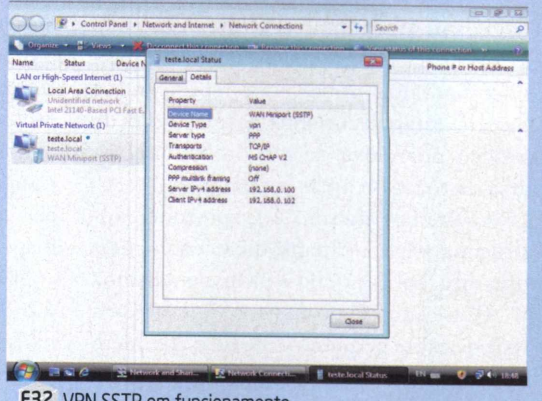
Conclusão

A conclusão que podemos tirar disso tudo é que agora não é mais necessário se preocupar com os firewalls que possam existir entre o cliente e o servidor de acesso remoto dentro da empresa, porque o tráfego HTTPS (TCP 443) normalmente é liberado em qualquer lugar, uma vez que muitos sites precisam dele. Além disso, o processo de configuração deste tipo de conexão não é tão simples quanto o de uma conexão VPN PPTP, mas também não é tão complexo quanto a configuração de uma conexão VPN L2TP. De qualquer forma, se surgirem dúvidas durante a configuração, sinta-se convidado a nos enviar um email (a.leitor.pcecia@editorasaber.com.br).

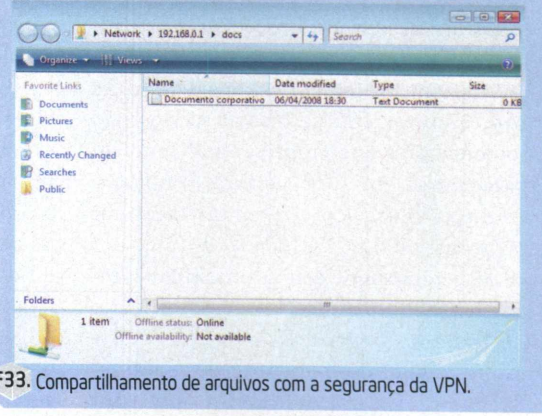
Até a próxima! **PC**



F31. Forçando uso da porta SSTP.



F32. VPN SSTP em funcionamento.



F33. Compartilhamento de arquivos com a segurança da VPN.

Softwares para projetos de redes



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.

O Microsoft Visio se saiu muito bem nos nossos testes. Como será que se sairá seu principal concorrente? Veja agora.

Software para projetos?

Vimos no artigo com o teste com o Microsoft Visio 2007 (PC&CIA 80) que um projeto mal acabado, mal feito e com documentação pobre pode representar o fim do estabelecimento da prestação de serviço por parte de um profissional da área de redes ou áreas correlatas.

O melhor mesmo é surpreender positivamente seu cliente oferecendo mais organização, capricho e profissionalismo.

Pense em um profissional que faz uma rede de porte pequeno a médio e que, além de fazer um bom serviço, ainda apresenta uma boa documentação, incluindo detalhes de lay-out da rede, ocupação dos armários de telecomunicações e organização de salas.

Certamente este profissional será muito bem visto e voltará a prestar serviço não somente para esta empresa, mas também para outras que, por ventura, venham a conhecer o serviço e queiram contratar tal profissional.

Queremos que este profissional competente e completo seja você. O mercado de trabalho nessa área não está fácil e existe um número absurdo de redes pequenas muito mal feitas. Não pode ser assim. É aí que você pode entrar e fazer a diferença.

Nós já abordamos vários assuntos sobre redes, cabeamento de redes, redes Wi-Fi, documentação de redes. Agora chegou o momento de apresentar a versão mais recente do software utilizado para desenhar projetos de redes de computadores e que ocupa o segundo lugar nas preferências dos profissionais pelo mundo afora, sejam elas cabeadas ou sem fio. Esse software está disponível para plataforma Windows.

O software que estamos testando agora é o Smart Draw em sua versão 2008, a mais recente (**www.smartdraw.com**). É possível fazer o download da versão de testes que permanece funcional por apenas sete dias, oficialmente, em w**ww.smartdraw.com/downloads/index.htm?WT.svl=left_text_download**.

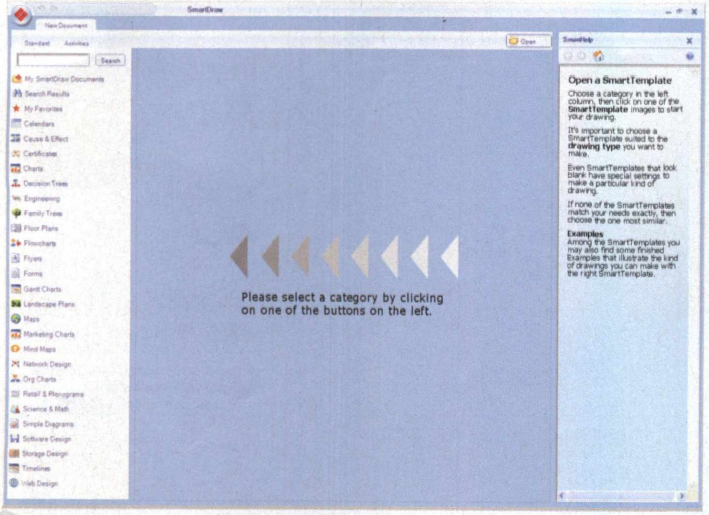
A primeira idéia que nos veio à mente quando começamos a testar o Smart Draw é que ele estaria à sombra do Microsoft Visio, o líder de mercado. Mas na realidade, o Smart Draw se destina a um segmento de mercado diferente daquele ocupado e liderado pelo MS Visio. Oficialmente falando, é claro.

Ao contrário do Visio, que se destina a um mercado mais profissional e corporativo, o Smart Draw quer mesmo é brigar pelo mercado das pequenas e médias empresas, por isso ele é muitíssimo mais barato. Uma licença do Smart Draw custa apenas U$ 197, aproximadamente R$ 345,00, contra os altos R$ 1.494,19 do Microsoft Visio.

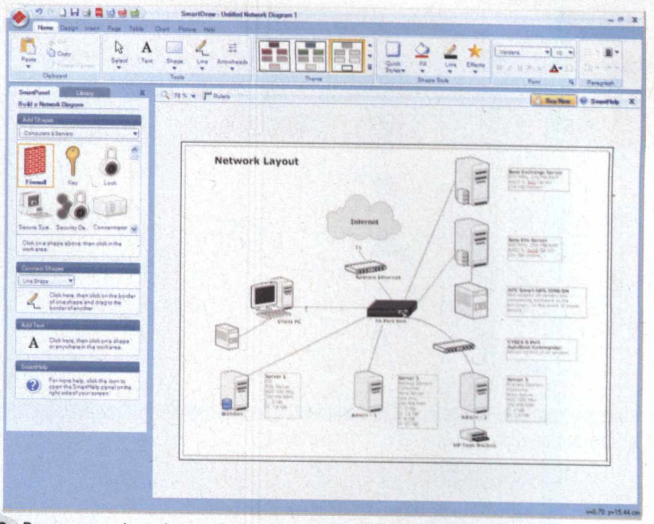
As novidades do Smart Draw 2008 podem ser conhecidas na página web inicial do produto. E por falar em página inicial, há muita coisa bem interessante no site oficial como, por exemplo, uma ampla coleção de diferentes soluções (**www.smartdraw.com/encyclopedia**), exatos 674 exemplos disponíveis para download em **www.smartdraw.com/exp/ste/examples/**, um centro de treinamento e aprendizado em **www.smartdraw.com/training/**, além da página de suporte técnico ao alcance de todos.

Como sabemos, a Microsoft vem fazendo um bom trabalho com o Visio 2007 e parece estar ainda mais empenhada em sua difusão após integrá-lo ao Office em sua versão mais completa. O Smart Draw é um solitário software da própria empresa com uma missão bem ingrata: conquistar usuários do MS Visio e ser melhor do que o Kivio, software semelhante para ambiente Linux **www.koffice.org/kivio/**, que está em sua versão 1.6.3.

Esses três softwares possuem características bem semelhantes. Além de fazerem fluxogramas, lay-outs, ilustrações e outros, eles também são muito úteis para



F1. Tela de abertura do Smart Draw 2008.



F2. Pronto para desenhar no Smart Draw 2008, já com um exemplo à nossa disposição.

quem trabalha com modelagem de dados e também quer dar aquela caprichada nos fluxogramas.

O Kivio é regido pela licença GPL mas ele não é totalmente gratuito, pois se precisarmos de mais de suas *templates*, chamadas de estêncil, precisaremos pagar até U$ 10. Não é muito e, além disso, nada impede que um usuário crie seu próprio estêncil e o disponibilize gratuitamente na Internet. Torçamos para que isso aconteça.

É possível achar estêncil gratuito para o Visio na Internet, como por exemplo no site **http://softwarestencils.com/uml/index.html#Visio2007**. A Microsoft também disponibiliza os seus gratuitamente em **http://office.microsoft.com/pt-br/templates/CT101527321046.aspx?av=ZVO**.

E, como já vimos, o site do Smart Draw é um legítimo portal do produto, onde podemos encontrar ajuda, consultas e respostas técnicas, exemplos, tutoriais, enfim, uma verdadeira enciclopédia à disposição do usuário do software.

Então, resumindo, se você nunca trabalhou com esse tipo de software, aproveite a oportunidade deste teste e trate de começar logo.

Usando o Smart Draw 2008

Pulamos a instalação? Sim, mas esta fase é extremamente fácil e tranqüila. Não há problema algum durante esse processo. Vale mencionar apenas que a instalação é feita on-line. O pequeno arquivo baixado serve somente para iniciar o procedimento de download e entrar no processo de instalação propriamente dito.

Ao se executar o Smart Draw 2008 pela primeira vez, o amigo leitor será lembrado de que só poderá utilizar a versão de testes por sete dias, após isso algumas poucas execuções do software serão permitidas. Em nossos testes, fomos remetidos a uma página que nos conferia um desconto de US$ 100,00! Está na página **www.smartdraw.com/offers/default/offer5.htm**, esperamos que ainda esteja funcionando quando o amigo leitor visitá-la.

Prosseguindo com a utilização do software, surgirá a tela inicial do programa (**figura 1**). Essa tela é dividida em três partes: uma coluna à esquerda com as áreas de interesse agrupadas, uma grande área central com um conjunto enorme de setas apontadas para a esquerda pedindo em letras generosas que selecionemos uma das categorias ao lado (esquerdo, óbvio) e, por fim, a coluna à direita, dedicada aos tópicos e links rápidos de ajuda.

Fora o que foi descrito agora, podemos notar pela figura 1 que "sobram" apenas um único botão, o de abrir arquivos do Smart Draw, e o menu "New Document", em inglês mesmo (por enquanto, não há Smart Draw em português). Este menu está subdividido em duas opções: "standard" e "activities".

Escolhemos "Network design" e depois, "Network Diagrams". Surgiu então a primeira tela na qual consta um exemplo do que selecionamos previamente. Resolvemos aproveitar esse exemplo (**figura 2**) e criar nossos desenhos a partir dele.

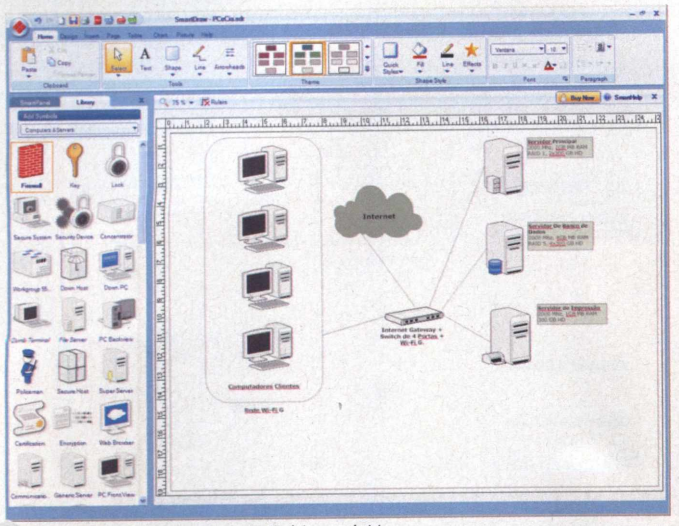
Os arquivos de documentos do Smart Draw são salvos com a extensão .sdr. Além dessa extensão, o Smart Draw é compatível com outras e também é capaz de salvar seus documentos como imagens, as quais obviamente não poderão mais ser editadas. Não é necessário exportar como uma imagem, pode-se salvar diretamente como um arquivo de imagem como no Visio. E por falar em Visio, infelizmente a tentativa de abrir um arquivo do Visio com extensão .vss não deu certo. Bom, nada é perfeito mesmo...

Quando for salvar um documento de desenho como uma imagem, preste atenção, porque ao contrário do Visio, que faz um recorte muito preciso limitando a imagem rigorosamente nas extremidades desenhadas, o Smart Draw deixa espaços como se fossem margens de um documento texto.

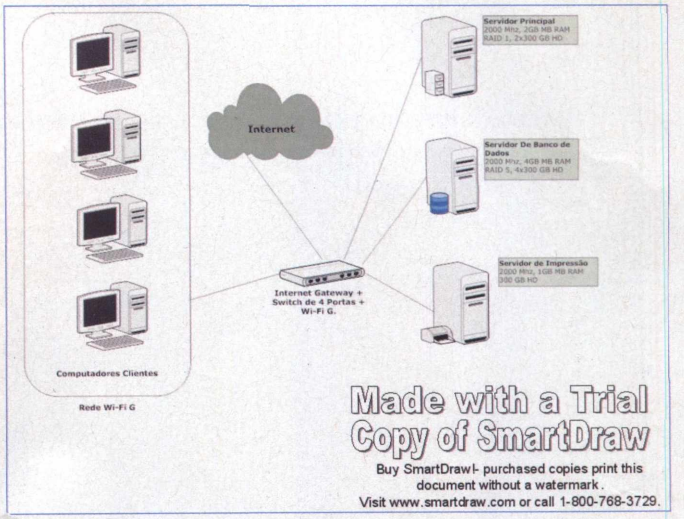
Tentamos trabalhar com as linhas de guia tal como fizemos no Visio, mas não conseguimos. O cursor do mouse levava uma linha sobre o desenho, mas esta nunca se fixava onde queríamos. No Visio isso é bem intuitivo e sempre funciona.

O Smart Draw oferece o mais simples dos inícios de um desenho. Basta selecionar a categoria à esquerda, o subtipo, se houver, e um exemplo já será criado. A partir disso, é só editar o exemplo ou até mesmo apagá-lo totalmente e criar um novo. Sinceramente, vale mais a pena partir pelo exemplo do que do zero.

Fizemos o desenho de um simples layout de rede (**figura 3**) em menos de seis minutos.



F3. Lay-out de uma pequena rede. Prático e rápido.



F4. Imagem exportada no padrão .jpg.

Experimente colocar um acesso à Internet com firewall, roteador e modem. Veja que também é possível aplicar um plano de fundo ou até mesmo um tema completo. Observe que duas guias surgirão no painel à esquerda: SmartPanel e Library. A primeira apresenta informações gerais, um breve resumo e o padrão de imagens que está sendo utilizado no momento. A segunda guia apresenta apenas a lista dos símbolos oferecidos ao padrão selecionado. É muito simples usar esses símbolos. Tal como no Visio, é só utilizar o recurso Drag and Drop (arrastar e soltar). Muito simples e intuitivo.

É bem verdade que os estêncils do Visio são mais completos, mas eles abrangem menos áreas de atuação se comparados aos modelos equivalentes do Smart Draw, que permite até a criação de modelos e documentos para área jurídica e médica. Os modelos de desenhos também são mais limpos se comparados diretamente aos do Visio. Um autêntico visual "clean".

Nos nossos testes, fizemos exportações de arquivos e objetos para os softwares Microsoft Word, Excel e Power Point sem maiores problemas, mas um pouco aquém da perfeição, exigindo um retoque nas formatações das imagens. E, por falar em imagens e exportações, esta versão de teste do Smart Draw aplica uma generosa estampa lembrando que a imagem gerada foi feita com uma versão de teste e que esta precisa ser registrada para que a marca d'água seja removida (**figura 4**).

Ao fazer um desenho, veja que o Smart Draw permite um controle de zoom e ainda oferece um controle de precisão de posicionamento de objetos quando se pressiona a tecla control e se desloca um objeto com as setas do teclado, preferencialmente. Aliás, o redimensionamento simultâneo de um conjunto de objetos é facilitado pela seleção coletiva. Para isso, basta clicar em uma área externa ao conjunto de objetos e arrastar até a extremidade oposta, como, por exemplo, do canto superior esquerdo para o inferior direito.

Há também uma ótima ferramenta que faz links entre diferentes objetos do desenho. No início, essa ferramenta oferece um pouco de dificuldade porque ninguém é capaz de saber qual exatamente será o percurso da linha do link, mas é possível mudá-la de posição e corrigir seu trajeto sem maiores esforços. Aliás, essa ferramenta se comporta melhor e de forma mais intuitiva do que no Visio.

Podemos observar que quando soltamos um objeto sobre a folha que estamos trabalhando, este apresenta as mesmas dimensões já utilizadas. Curiosamente, mas positivo, os objetos são arrastados e soltos na mesma escala. Isso facilita muito a vida de quem estiver fazendo um desenho arquitetônico ou de engenharia.

Os pontos de redimensionamento são os quadrados, enquanto que a pequena estrela de seis pontas representa o ponto para rotação do objeto. Os fluxogramas do Visio são ótimos e completíssimos. Excelentes para os estudantes de algoritmos.

Podemos configurar detalhadamente a página utilizada no menu Page e em seguida configurá-la sem maiores problemas. É possível detalhar as dimensões do papel, grade de medidas e escala também. Opte pela escala com centímetros ou milímetros. Lembre-se de que o Smart Draw ainda não apresenta uma versão feita especificamente para o mercado brasileiro, por isso, tenha em mente que alguns ajustes na configuração de página podem ser necessários.

Ao contrário do Visio, que apresenta algumas maluquices, o Smart Draw tem um comportamento funcional mais íntegro. E já que falamos em integridade, o Smart Draw apresentou um único evento de travamento, mas este deve ser atribuído às temporizações de memória, que ao retornar aos valores recomendados, manteve a total estabilidade do sistema.

Conclusão

O Smart Draw é um excelente software. Possui muitos recursos e ainda é incrivelmente simples de ser utilizado por qualquer um que tenha intimidade com o PowerPoint, por exemplo. Quem já domina o Visio, vai adorar o Smart Draw.

Experimente fazer um desenho de uma rede e você ficará surpreso com a aparência profissional do mesmo. Os novos desenhos de objetos em um 3D simples e "clean" nos convidam a fazer ainda mais desenhos.

Indicamos o uso do Smart Draw 2008 sem a "ressalva" aplicada ao Microsoft Visio, que custa aproximadamente R$ 1.494,19 para cada licença do produto novo e completo. Já o Smart Draw custa quase 25% desse valor e ainda há a possibilidade de maiores descontos financeiros. Com uma única licença do Visio, é possível adquirir três do Smart Draw. O Visio completo novo custa somente um pouco menos do que o Windows Server 2008.

Se o amigo leitor desejar um teste com outros utilitários de desenho de engenharia e fluxogramas, por favor mande-nos um e-mail. O próximo a ser testado será o Kivio para plataforma Linux. E se o amigo leitor também conhecer outros softwares desse nível, por favor sinta-se à vontade para entrar em contato.

Até a próxima. **PC**

Proteja sua rede com um IPS

Saiba como proteger sua rede com um sistema de prevenção contra intrusos (IPS) e a simular um ataque para ver a sua eficiência.

São muitos os usuários que imaginam estarem seguros por ter implementado um firewall com o "iptables" na empresa. O problema é que se esquecem ou não sabem que qualquer firewall só dá segurança no que diz respeito às portas de acesso de origem e destino. Até existem alguns *patches* que podem ser aplicados ao kernel e ao binário do iptables para se ter um firewall mais robusto, que opere na camada 7 do modelo OSI. Contudo, ainda assim o firewall será incapaz de detectar uma possível invasão ou até mesmo uma anomalia no tráfego de rede. Para ter essa funcionalidade na rede, é necessário contar com um sistema de tratamento contra intrusão, o que sob o ponto de vista técnico pode ser feito a partir de um IDS ou de um IPS.

O IDS (Intrusion Detection System) é um software que detecta e loga todo o tráfego que ele julga ser malicioso, sem nenhum tratamento sobre o que fazer. Logo surgiu o conceito de IDS reativo, o qual, ao detectar o tráfego malicioso, enviava um sinal de reset para ambos os lados da conexão (atacante e atacado). No entanto, quando esse sinal era enviado, pelo menos um pacote malicioso já havia passado ao seu destinatário e, conseqüentemente, o método não era 100% seguro. Afinal, não é muito legal deixar um pacote passar, uma vez que poderia se tratar de um exploit tentando derrubar o seu servidor web (apache), por exemplo.

O tempo passou e outras alternativas surgiram para proteger a rede, sendo que uma delas é o IPS (Intrusion Prevention System), um sistema que atua de modo in-line (transparente) na topologia e é capaz de detectar e tratar anomalias de tráfego com um nível maior de segurança e eficiência. Nesta matéria demonstraremos a instalação, configuração e o uso desta ferramenta. Além disso, simularemos um ataque a um determinado serviço para que você possa realmente vê-lo funcionando.



Renato Kopke
Há 16 anos no mercado de TI, atualmente é responsável por projetos na plataforma Linux e análise de risco em redes, na Detection, empresa do grupo M.Cury, no RJ.

Projeto HLBR

O projeto HLBR começou em 2005, quando um grupo formado por brasileiros pegou o desenvolvimento de um antigo projeto de IPS denominado Hogwash (baseado no Snort). Além de melhorar os bugs existentes, esse grupo implementou novos recursos para a detecção de anomalias na rede. É um projeto realmente maravilhoso que já suporta até expressões regulares para personalização e melhora das regras de detecção de ataques à rede.

Onde colocar o HLBR

Considerando o sentido de comunicação da Internet para a rede local, o HLBR deve ser colocado antes do seu firewall e depois do seu roteador da Internet. Desse modo, ele será capaz de analisar e possivelmente bloquear, ou logar, todo o tráfego que passe por ele, caso as regras configuradas e habilitadas considerem-no como um ataque (**figura 1**).

Instalação e configuração do HLBR

A equipe de desenvolvimento do HLBR está de parabéns por ter sido capaz de simplificar ao máximo a instalação e a configuração do software. Você dificilmente terá dificuldade para manipulá-lo. Além disso, todos os arquivos de configuração estão em português, o que facilita ainda mais o processo de configuração. No site **http://hlbr.sourceforge.net/**, você encontrará muitos detalhes a esse respeito. Agora vamos à prática.

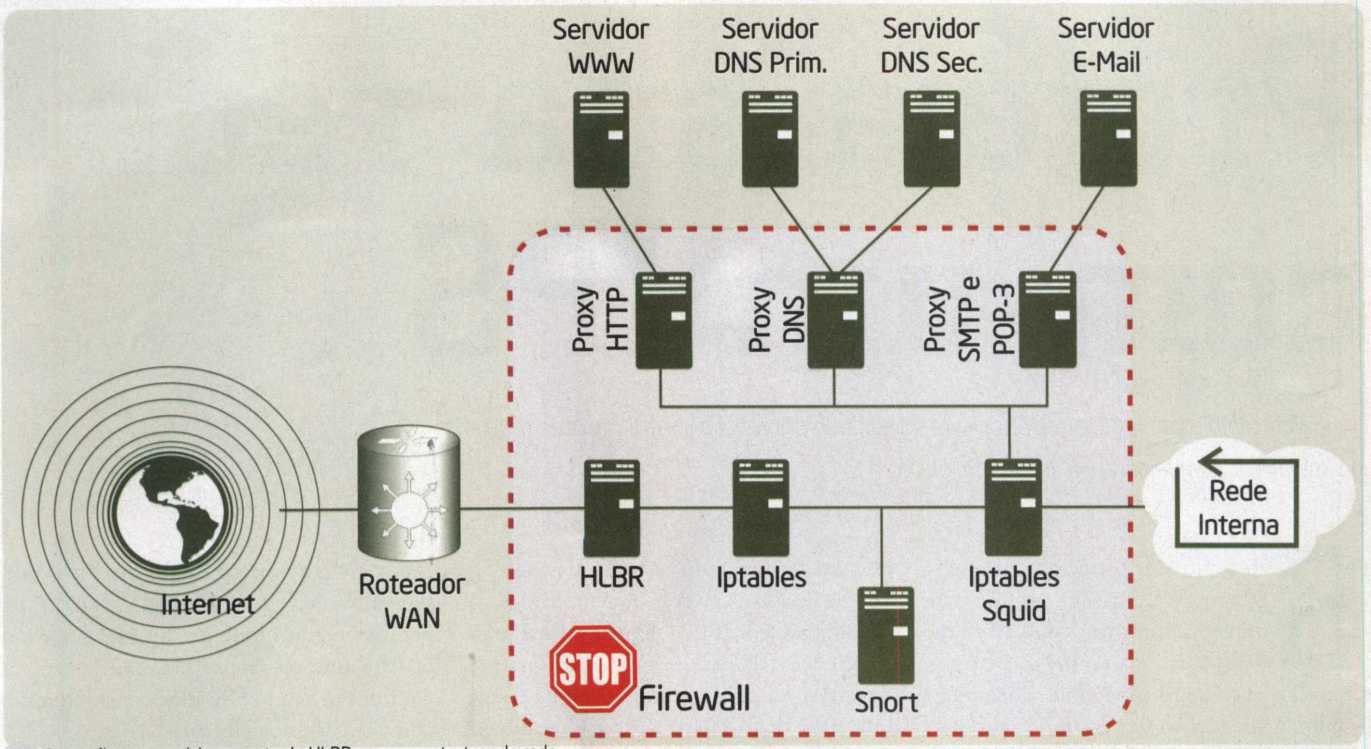
Qual distribuição utilizar? Apesar de termos escolhido o Debian, o amigo leitor pode se sentir à vontade para utilizar qualquer distribuição, uma vez que usaremos o programa no formato código-fonte. Então basta fazer o download do site do projeto e compilá-lo. Nossos testes foram feitos com a revisão de kernel 2.6.18.

O primeiro passo *será irmos até o site* acima e fazer o download do software (**figura 2**), no caso do arquivo hlbr-1.1.tar.gz:

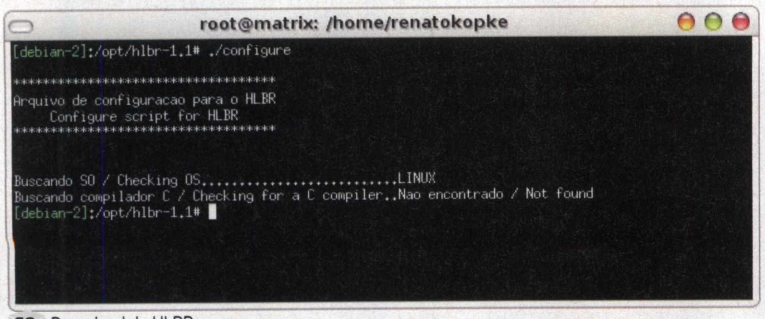
```
# tar zxvf hlbr-1.1.tar.gz -C /opt
# cd /opt/hlbr-1.1
#./configure
```

Se tentarmos compilar o HLBR sem as ferramentas de compilação (gcc), provavelmente receberemos a mensagem de erro da **figura 2**. Então vamos instalar o gcc:

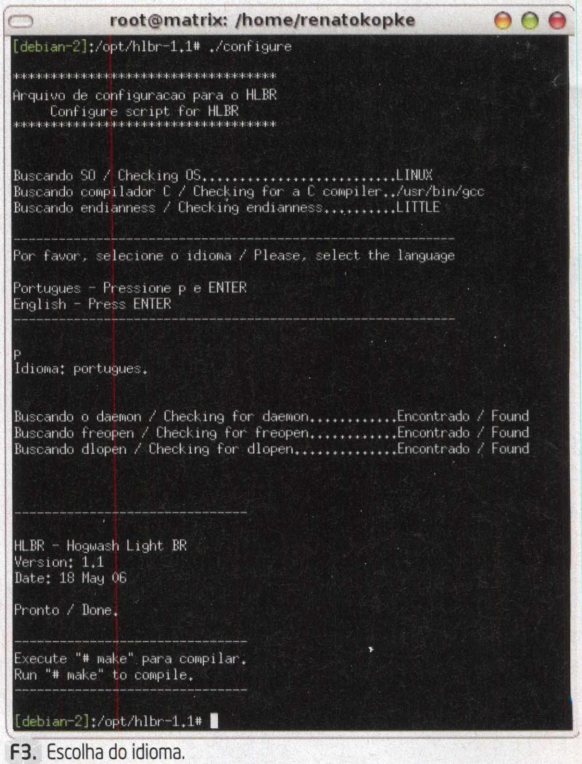
```
#apt-get install gcc g++ make libc6-dev
```



F1. Sugestão para posicionamento do HLBR em uma estrutura de rede.



F2. Download do HLBR.



F3. Escolha do idioma.

Agora sim podemos executar o processo de instalação e muito provavelmente teremos sucesso:

```
#./configure
```

Durante o processo será solicitado o idioma, pressione a letra **p** para português e, a seguir, **enter** (**figura 3**).

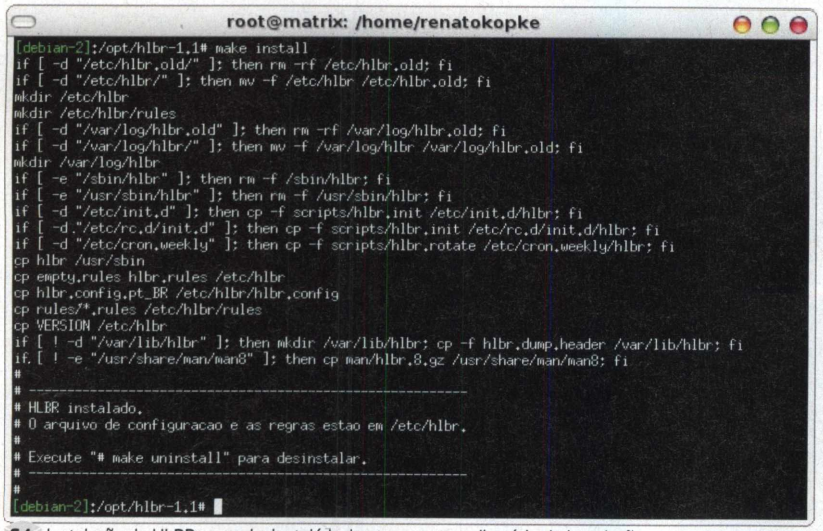
Após executar o ./configure, ele preparará o HLBR para ser instalado no seu sistema. O próximo passo é executar o *comando* **make**, o qual serve para compilar todos os binários do hlbr:

```
#make
```

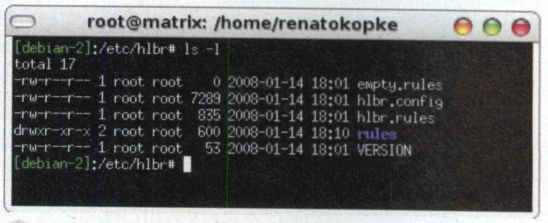
Agora vamos executar o comando **make install** para instalar os arquivos de configuração e binários nos devidos diretórios (**figura 4**). Por padrão, o HLBR fica instalado no diretório **/etc/hlbr/**.

O próximo passo será configurar as interfaces de rede do nosso sistema para que o HLBR inicie o monitoramento do tráfego da rede. Vale lembrar que devido ao fato de o software trabalhar na camada 2 do modelo OSI, não precisaremos configurar os IP's das interfaces de rede. Você pode até mesmo modificar o seu kernel para que ele não trabalhe na camada de rede, de modo a deixar o IPS ainda mais seguro uma vez que o atacante não teria como detectar e nem saber de sua existência na rede. O "problema" é que isso exige um processo ainda mais complexo, que é pegar um kernel novo e compilá-lo sem o suporte à rede. No nosso caso não faremos isso por questões de simplificação e facilidade. Quer dizer então que nosso servidor ficará vulnerável? Não necessariamente.

A solução para esse problema é simples, basta configurar a interface de rede



F4. Instalação do HLBR; para desinstalá-lo, basta acessar o diretório de instalação e executar o comando "**make uninstall**".



F5. Listagem dos arquivos do diretório /etc/hlbr.

%sip	ip de origem	%dip	ip de destino
%sp	porta de origem	%dp	porta de destino
%f	dia	%m	mês
%y	ano	%h	hora
%min	minuto	%s	segundos
%usec	microssegundo	%pn	seqüência do pacote
%ac	número de alerta - começa em 1 sempre que o HLBR é reiniciado.		

T1. Lista das possíveis variáveis que podem ser utilizadas no tratamento de logs.

eth0 com o IP 127.0.0.10 e a eth1 com o 127.0.0.20 (uma placa para a rede externa e a outra, para a interna). Pronto, seu IPS não estará visível na rede e com isto você poderá utilizar o "tcpdump", entre outras ferramentas que trabalham na camada de rede, para analisar os logs gerados pelo HLBR. Lembre-se de que "127.0.0.1" é utilizado para *loopback* e qualquer IP como 127.0.0.10 e 127.0.0.20 não será roteado por pertencer a uma classe "127". Então, quem analisa os pacotes na camada de rede? O HLBR. Vamos aos comandos:

```
# ifconfig eth0 127.0.0.10
# ifconfig  eth1  127.0.0.20
```

Agora acesse o diretório do HLBR (#cd /etc/hlbr)e digite ls-l para listar o conteúdo do diretório (**figura 5**). Vamos analisar o que cada arquivo faz:

- **empty.rules**: este arquivo vem em branco;
- **hlbr.config**: Arquivo de configuração do HLBR, nele configuramos os IPs e redes protegidas pelo software;
- **hlbr.rules**: Neste arquivo especificamos quais módulos de proteção devem ser habilitados. Estes módulos estão no diretório "/etc/hlbr/rules", você pode criar seus próprios mecanismos de análises para melhorar ainda mais a segurança da sua rede;
- **VERSION**: versão do HLBR.

Os próximos passos serão analisar e configurar esses arquivos, começando pelo hlbr.config. Ao abri-lo (#vi /etc/hlbr/hlbr.config), encontramos a seguinte entrada logo no começo:

```
<system>
Name=HLBR_1
ID=1
Threads=1
AlertHeader=%ac%d/%m/%y%h:%min:%s ▸
▸%sip:%sp->%dip:%dp
</system>
```

Onde:

- **Name**= Define um nome para este servidor como HLBR_1 e HLBR_2
- **ID**= Apenas um ID para o seu sistema IPS
- **Threads**= Número de threads, 0 diz que ele deve executar apenas uma e 1 seria (n+1), onde N representa o número de placas de rede.
- **Alertheader** = Como os logs serão apresentados (**tabela 1**).

```
<interface eth0>
Type=linux_raw
Proto=Ethernet
</interface>

<interface eth1>
Type=linux_raw
Proto=Ethernet
</interface>
```

Em interfaces definiremos quais interfaces de rede serão utilizadas, o que no nosso caso é eth0 e eth1:

Em IPList definiremos sobre quais IPs e redes queremos que as regras (rules) detectem possíveis ataques. Troque o 200.xxx.yyy.195 e 196 pelo IP do servidor ou da rede que você vai monitorar.

```
<IPList www>
        192.168.1.230
        #192.168.1.0/24
</list>
```

Onde:

- **<IPList www>** = O nome www está associado às regras que serão utilizadas para a análise. Elas estão prontas em /etc/hlbr/rules;
- **192.168.1.230** = Coloque o IP ou rede que você deseja monitorar. O "IPList www" vai associar www ao IP (192.168.1.230) que está

indicando o servidor que possui o serviço web (Apache) instalado. Nesse caso utilizamos o IP do servidor, mas poderíamos ter definido toda uma rede, como por exemplo a "192.168.1.0/24";

- **</list>** = Fim do bloco de código do IPList.

Dica

No arquivo /etc/hlbr/hlbr.config você encontrará várias linhas com IPList definidas como exemplo. Procure comentar as linhas que você não for utilizar, a exemplo das que trazem IPList com os serviços "www, dns, email, firewall, network, others". Supondo que você precise proteger somente os servidores Web e DNS desta máquina, então utilize o IPList do "www e dns" e comente todo o restante. Após, é só configurar o www e o dns com o IP do servidor.

Em <IPList servers>, definiremos quais IPList serão analisados:

```
<IPList servers>
        www
        dns
</list>
```

Você também encontrará uma sessão chamada *action*, onde definimos o tipo de ação que nossas regras devem tomar ao detectar uma anomalia na rede ou servidor:

```
<action action1>
response=alert file(/var/log/hlbr/hlbr.log)
response=dump packet(/var/log/hlbr/hlbr.dump)
response=drop
</action>

<action action2>
response=alert file(/var/log/hlbr/hlbr-2.log)
response=dump packet(/var/log/hlbr/hlbr-2.dump)
</action>

<action virus>
response=alert file(/var/log/hlbr/virus.log)
response=dump  packet(/var/log/hlbr/virus.dump)
response=drop
</action>
```

É claro que o amigo leitor pode criar outras ações ou modificar as existentes. Vamos entender cada uma delas:

- **action1** = Diz que ele deve logar em hlbr.log e criar um arquivo *dump*, o qual pode ser analisado com o tcpdump; além disso, diz que o resultado para essa ação será negar o acesso;
- **action2** = É basicamente o mesmo de *action1*, só que ele somente vai logar as tentativas e não executará nenhuma ação ao computador de origem;
- **action3** = Faz a mesma coisa que o *action1* (logar e negar o acesso ao serviço), mas cria um arquivo de log chamado virus.*.

Na sessão *routing*, criamos nossa *bridge* entre as interfaces que o software irá monitorar. Observe que essa sessão só admite o uso de 2 interfaces:

```
<routing>
SBridge(eth0, eth1)
</routing>
```

Agora vamos analisar o arquivo que define quais módulos de análise de rede devem ser habilitados:

```
#vi /etc/hlbr/hlbr.rules

<include rules/awstats.rules>
<include rules/bufferoverflow1.rules>
<include rules/bufferoverflow2.rules>
<include rules/bufferoverflow3.rules>
<include rules/codered-nimda.rules>
<include rules/coppermine.rules>
<include rules/dnsattacks.rules>
#<include rules/mailvirus.rules>
#<include rules/mambo-phpnuke.rules>
<include rules/passwd.rules>
<include rules/shell.rules>
<include rules/webattacks.rules>

# As regras dos arquivos abaixo deverão ▸
▸ ser analisadas antes de serem utilizadas.
# Isso porque elas poderão interromper ▸
▸ parte do tráfego legítimo da rede.

#<include rules/http.rules>
#<include rules/php.rules>
#<include rules/sql-xss.rules>
#<include rules/www.rules>
```

Para habilitar os módulos basta acrescentar uma linha <include caminho das rules>.

Dica: conforme já foi dito, deve-se estudar quais regras você deseja habilitar para que seja realizada uma análise mais precisa. Não tem lógica habilitar um módulo de email se você não tem um serviço de email ativo naquele servidor que foi configurado em <IPList>.

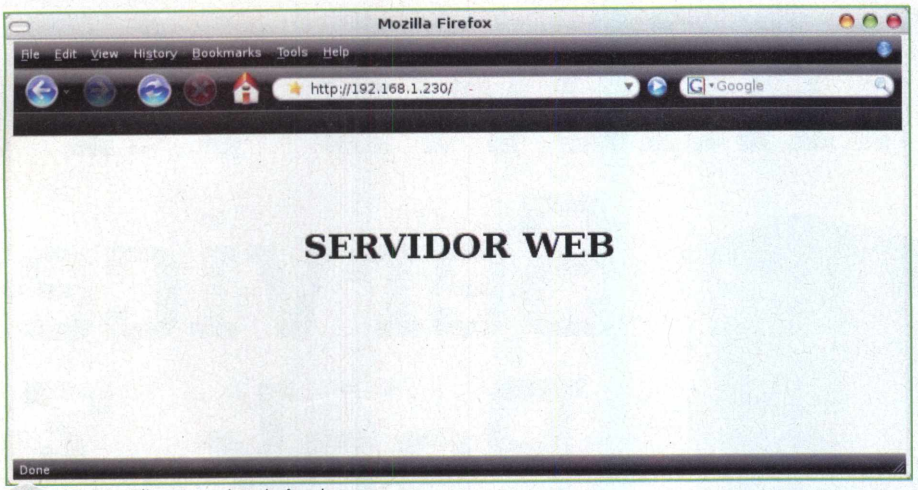
Caso você crie novas regras (rules) ou queira acrescentar novos módulos, basta olhar os módulos em "/etc/hlbr/rules" e acrescentar neste arquivo com <include caminho/rules>.

Aproveitando que estamos analisando os arquivos, que tal olharmos uma regra que será utilizada para analisar um possível ataque nosso para fins de teste, e tentar entender o seu funcionamento básico?

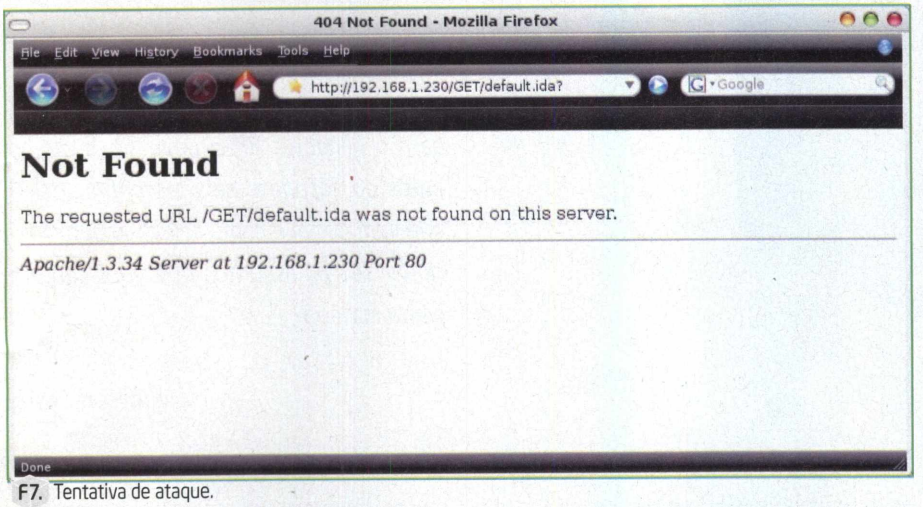
```
# cd /etc/hlbr/rules
# vi codered-nimda.rules
<rule>
ip dst(www)
tcp dst(80)
tcp regex((root|cmd|explorer)\.exe)
message=(codered-nimda-2-re) ▸
▸ (root|cmd|explorer) request
action=action1
<rule>
```

Este módulo foi habilitado em hlbr.rules com a diretiva <include ...>. Ele é responsável por analisar uma estação que tenha como IP de destino "www" (definido na diretiva "<IPList www>, em hlbr.config, com o IP do nosso servidor") e porta de destino 80 (será analisada no datagrama). Ao abrir o datagrama, o HLBR verificará a existência de uma expressão que descreva uma tentativa de acesso ao servidor com o seguinte comando "root/cmd/explore". Se ele encontrar, executará uma ação *"action1"* que foi definida no arquivo hlbr.config, a qual, só para relembrar, diz que ele deve logar a tentativa de acesso e negar o acesso a este servidor no exato momento. Que ótimo! Veja o significado do quadro acima, linha a linha:

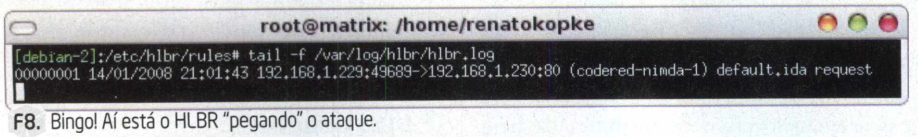
- **ip dst(www)** = Assume como referência o IPList com a rede ou IP do servidor a ser protegido;
- **tcp dst(80)** = Define a porta que ele analisará no datagrama. 80 é servidor web;
- **tcp regex()** = Expressão que ele utilizará para analisar o datagrama, à procura de uma tentativa de acesso;
- **message** = Qual mensagem ele utilizará para logar em hlbr.log;



F6. Página padrão retornada pelo Apache.



F7. Tentativa de ataque.



F8. Bingo! Aí está o HLBR "pegando" o ataque.

- **action** = Nome da ação que ele chamará em hlbr.config para executar um determinado processo.

Feito tudo isto, basta agora executar o *daemon* do HLBR parra colocá-lo em ação em sua rede:

```
#/etc/init.d/hlbr start
```

Se o serviço não subir, verifique o processo de configuração que apresentamos e tente executá-lo novamente.

Para monitorar o log do HLBR a fim de procurar possíveis ataques, digite o seguinte comando:

```
#tail -f /var/log/hlbr/hlbr.log
```

Simulação de ataque

Assumindo que todo o processo de instalação e configuração foi executado com sucesso, vamos partir para a parte bacana que é ver o HLBR monitorando e executando ações no host do atacante.

A simulação do ataque será bem simples. Basicamente, tentaremos simular um vírus CodRed tentando passar pelo nosso HLBR, o qual, na verdade, atacava uma vulnerabilidade do servidor web IIS da Microsoft, causando um Buffer Overflow. Na figura 6 vemos um servidor web Apache em operação após a instalação padrão.

Abra um browser (de preferência o Firefox) e execute a seguinte linha na barra de endereço: **http://192.168.1.230/GET/default.ida?** (**figura 7**).

Você notará que o Apache, diferentemente do IIS, não sofreu com o ataque. Mas na verdade a intenção é fazer o HLBR detectar o ataque, logar a tentativa e ainda executar uma ação previamente configurada pelo administrador. Vamos analisar o log do /var/log/hlbr/hlbr.log e ver se ele logou a tentativa de ataque (**figura 8**):

```
# tail -f /var/log/hlbr/hlbr.log
```

Veja que o HLBR pegou e logou a tentativa do CodRed de atacar nosso servidor web. E com isto foi executado uma ação "action1", a qual loga e também nega o acesso ao atacante. Observe que o detalhamento do log também apresenta o IP de origem do atacante, além da hora e data da tentativa do ataque. Apenas como experiência, tente executar outros ataques como o de explorar o shell da máquina Windows, que tinha como característica o vírus Ninda:

http://192.168.1.230/system/cmd.exe?dir+c:

Caso o amigo leitor queira analisar os arquivos com extensão .dump, utilize o *tcpdump* (pode ser que seja necessário instalá-lo antes em seu sistema):

```
# tcpdump -vvv -tttt -X -s 1500 -r  hlbr.dump
```

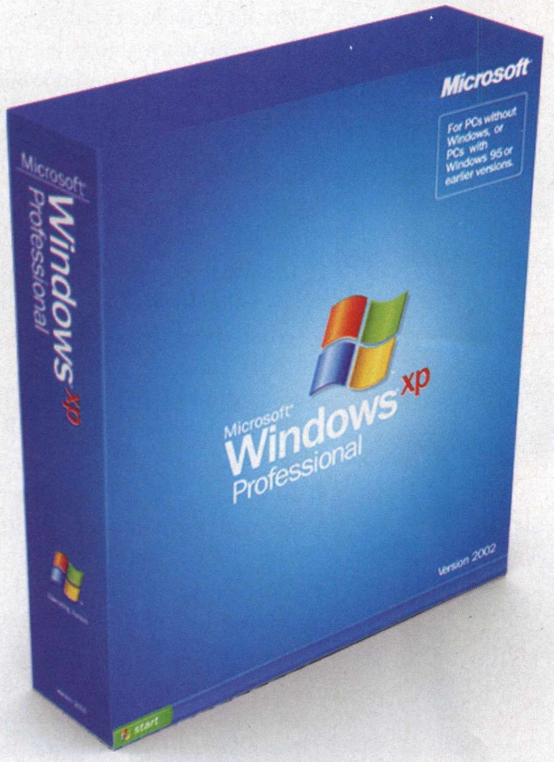
Onde:

- **vvv** = Em modo detalhado
- **tttt** = Modo de tempo detalhado (hora e data)
- **X** = Modo hexadecimal
- **r** = Ler um arquivo de entrada no formado tcpdump
- **s** = Tamanho da MTU

Conclusão

Vimos neste artigo como um IPS *open-source* pode ser aplicado em nossas redes para garantir ainda mais a segurança de nossos servidores. Além disso, de modo a deixá-lo invisível para o atacante, apresentamos uma forma para colocá-lo em operação como uma *bridge*, ou seja, na camada 2 do modelo OSI, onde nenhuma modificação é feita ao cabeçalho dos pacotes que por ele passam. Se tiver dúvidas, fique à vontade para entrar em contato conosco através do email **a.leitor.pcecia@editorasaber.com.br**. **PC**

Windows XP Service Pack 3



Um novo pacote de atualização chega para o Windows XP e deve ser o último antes do software ser descontinuado. O que vem por aí e como colocá-lo para funcionar são os assuntos que você confere nesta matéria.

Igor Humberto

Apesar de sabermos que, na maioria das vezes, o profissional de infra-estrutura não costuma desenvolver código, sabemos que todo código está sujeito a bugs, os famosos erros de programação.

À medida que o software vai sendo utilizado pelos usuários, esses erros vão aparecendo e, conforme a possibilidade, são repassados para a equipe de desenvolvimento que o criou a fim de que trabalhem na disponibilização de correções.

Dependendo do tamanho do produto, nenhum ou apenas alguns erros podem ser encontrados no software (às vezes o erro até existe, mas a condição necessária para que o mesmo se manifeste nunca é satisfeita). Mas quando falamos de um sistema operacional a situação é bem diferente, pois se trata de um produto muito mais complexo e, desta forma, a possibilidade de encontrar problemas se torna muito maior.

No mundo Microsoft, apesar dos produtos sempre passarem por um processo de desenvolvimento, no qual o programa é muitas vezes colocado em produção internamente (o conjunto Windows Server 2008 + IIS 7, por exemplo, já estava em produção na Microsoft antes mesmo do lançamento oficial do mesmo), além de passarem pelo crivo de milhares de beta testers espalhados pelo mundo (**http://connect.microsoft.com**) que podem testar o produto, existem situações que somente um legítimo usuário pode reproduzir (é incrível como os usuários são criativos!).

Sendo assim, independente dos esforços de qualquer empresa de desenvolvimento de software (considerando software proprietário ou não), os bugs sempre existirão. E isso se torna verdadeiro, principalmente, quando falamos de um produto complexo como um sistema operacional.

Visto o exposto, por mais que sejam procurados, os bugs sempre existirão em qualquer sistema operacional. É claro que o uso de técnicas de desenvolvimento profissionais (refiro-me aos profissionais que realmente estudam como desenvolver de forma segura e responsável) contribui consideravelmente para reduzir as probabilidades de ocorrência desses problemas, mas ainda assim não as eliminam.

O que podemos chamar de bugs do SO?

Existem diversas categorias de bugs que podem afetar um sistema operacional, mas normalmente três elementos são afetados quando um bug existe: segurança, estabilidade e desempenho. Sendo assim, um SO atualizado estará menos vulnerável a estes três tipos de problemas e é por isso que o uso do Windows Update torna-se extremamente importante. Com isto, você garante que o seu sistema está com os bugs conhecidos corrigidos (às vezes são liberadas atualizações para uma atualização lançada, mas isso é outra história).

Desde o seu lançamento em 2001, o Windows XP recebeu milhares de atualizações. Já pensou em como seria

complicado implantar o sistema? Sim, porque você precisaria instalar o sistema, fazer a instalação dos dispositivos, acessar o Windows Update e baixar as atualizações existentes ali. Como a quantidade de atualizações é grande, seria necessário ficar um bom tempo na etapa de atualização do sistema. Isso sem contar que, para fazer uma atualização de BIOS e/ou instalar um determinado driver, muitas vezes é necessário ter uma atualização do sistema em execução. Ou seja, você teria que voltar diversas vezes ao site do Windows Update até completar o processo de instalação do sistema.

Além dos problemas citados anteriormente, devemos considerar também que, conforme o tempo passa, o sistema operacional vai ganhando novas necessidades tecnológicas que o usuário precisará (o suporte para a tecnologia Bluetooth não existia no Windows XP RTM, por exemplo). Pensando nisso, a Microsoft passou a distribuir o que ela chama de Service Pack (SP).

Um Service Pack do Windows, ou pacote de serviços, nada mais é do que um pacotão contendo todas as atualizações do sistema lançadas até um determinado momento. A implantação do sistema fica mais simples porque basta instalar o Windows e, posteriormente, instalar um SP específico para que o sistema esteja atualizado. Além disso, se uma determinada atualização for necessária para a instalação de um driver específico, basta informar ao usuário que um determinado SP precisa existir no sistema, e não que será necessário instalar 25 atualizações específicas. Além disso, também seria possível acrescentar as atualizações tecnológicas necessárias para que o sistema ofereça suporte ao que houver de novo no mundo.

Um bom exemplo de como um Service Pack pode transformar a cara de um SO foi o SP2 do Windows XP. Além de corrigir os diversos bugs presentes no sistema até então, ele trouxe diversos novos recursos, tais como: o Firewall do Windows (substituindo o ICF), Data Execution Prevention (DEP), Internet Explorer com gerenciador de complementos, etc.

Apesar de parecer interessante, muitas pessoas hesitavam em instalar um SP logo depois do seu lançamento. Isso acontecia porque, muitas vezes, alguma atualização poderia impedir que uma aplicação específica, usada internamente dentro da empresa, funcionasse corretamente depois que a mesma fosse aplicada. Sendo assim, o computador ficava sem aquelas centenas de atualizações, além de também ficar sem todos os novos recursos embutidos no SP. Isso tudo por causa de uma atualização específica presente no SP. O efeito disso foi que muitas pessoas relutaram em instalar o SP2 do Windows XP. O problema em questão agora é que além de deixar os sistemas vulneráveis até que as adaptações fossem desenvolvidas para as aplicações internas usadas nas empresas, os administradores deixavam para trás, também, os novos recursos que serviriam para deixar o usuário mais protegido.

Pensando nisso, a Microsoft adotou a seguinte filosofia: um Service Pack deve conter apenas atualizações do sistema. Nada de novos recursos. Isso só deve acontecer se o recurso em questão for muito importante mesmo. Assim, novas funcionalidades só seriam lançadas em um pacote separado, sem atualizações de sistema, o qual poderia ser aplicado sem atrapalhar o funcionamento das aplicações existentes. Estas atualizações especiais seriam lançadas depois de dois anos do lançamento do produto.

O Windows Server 2003 foi o primeiro sistema operacional da Microsoft a ser afetado por esta iniciativa. Depois de dois anos do seu lançamento, a Microsoft lançou o que eles chamaram de R2. Esta atualização não oferecia correção de bugs, somente adicionava novos recursos no sistema. A experiência que a Microsoft teve foi boa e serviu de base para que, daqui pra frente, dois tipos de atualizações estejam disponíveis para os administradores: O Service Pack, com as correções de bugs, e a versão R2, que oferecerá apenas os novos recursos e é lançada depois de dois anos do lançamento do produto. Sendo assim, pelo menos em teoria, em 2009 a Microsoft deve lançar algo como o R2 para o Windows Vista (em 2009 o Windows Vista fará dois anos).

O que o SP3 do Windows XP trás de novo?

Tendo abordado as observações feitas até aqui, podemos concluir que o SP3 do Windows XP só entregará mesmo correções do sistema com um pequeno punhado de novidades, mas que não irão causar o mesmo impacto produzido pelo SP2.

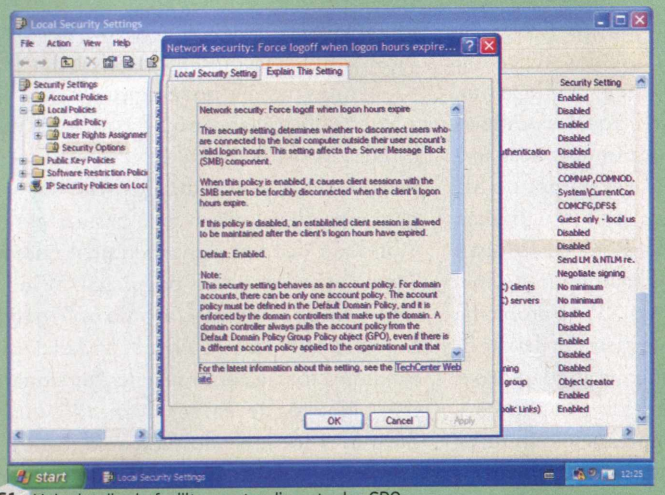
Muitas pessoas nos perguntam por que a Microsoft irá lançar o SP3, uma vez que o referido sistema será descontinuado em meados deste ano (ainda existirá suporte para o produto, mas o foco passará para o Windows Vista exclusivamente). A questão é que muitas empresas possuem o Windows XP no seu ambiente. Como o Windows Server 2008 trás muitas novidades que mudam a forma como as redes funcionam, dois objetivos devem ser alcançados quando o SP3 for lançado: lançar um último pacote de atualizações contendo todas as correções lançadas até então, e adaptar o Windows XP às mudanças encontradas no Windows Server 2008.

Vale ressaltar que muitas dessas atualizações podem ser obtidas diretamente do site de downloads da Microsoft (www.microsoft.com/downloads) e que outras só estarão disponíveis se o SP3 for aplicado no sistema. Além disso, assim como aconteceu com todos os outros SPs, o SP3 é cumulativo, ou seja, você pode aplicá-lo em um sistema que esteja executando o Windows XP RTM (Release To Market) e todas as novidades presentes no SP1 e SP2 também serão aplicadas.

Atualizações obtidas de forma independente

Na lista abaixo, apresentamos as atualizações que você pode instalar no Windows XP sem precisar instalar o SP3:

- MMC 3.0: é a interface de gerenciamento que surgiu com o Windows 2000. Essa nova versão contém, além de melhorias, algumas novidades.
- MSXML6: Esta atualização oferece maior confiabilidade e segurança para o padrão XML existente de acordo com as recomendações do W3C.
- Windows Installer 3.1 v2: o Windows Installer é a opção da Microsoft de engine de sistema de instalação de aplicativos. Além de ser uma opção para os desenvolvedores de aplicativos, ele também confere ao sistema operacional maior controle e segurança nos processos de instalação de aplicativos que se valem de suas facilidades.



F1. Help detalhado facilita o entendimento das GPOs.

- BITS 2.5: BITS é a sigla para Background Intelligent Transfer Service. Com esta tecnologia, é possível realizar transferências de forma mais confiável e flexível.
- IPSec: Através do IPSec é possível fazer o isolamento de redes e de domínios, além de oferecer segurança na comunicação devido à possibilidade de autenticar e criptografar o tráfego entre computadores e dispositivos. A atualização que estamos destacando aqui simplifica a criação de diretivas IPSec no sistema, tanto no Windows Server 2003 quanto no Windows XP.
- DIMS: Esta é a sigla para Digital Identity Management Services, um serviço que permite a utilização de um conceito batizado pela Microsoft de credenciais móveis (Credential Roaming). Basicamente, ela especifica o funcionamento do mecanismo que permite que os certificados do usuário utilizados no EFS, por exemplo, sejam transportados. Não confunda com exportação de certificados, pois o recurso aqui é diferente.
- PNRP 2.1: Esta é a sigla para Peer Name Resolution Protocol, um protocolo que foi desenvolvido especialmente para facilitar o funcionamento de aplicações P2P. Esta atualização permite que programas desenvolvidos para trabalharem com esta tecnologia no Windows Vista também possam se comunicar com programas desta categoria no Windows XP. Vale ressaltar que esta versão do protocolo não possui compatibilidade retroativa, ou seja, não será possível "falar" com programas que usem versões mais antigas deste protocolo.
- Suporte para WPA2: O WPA2 (Wi-Fi Protected Access 2) é o nome da mais recente solução de segurança para comunicação em redes sem fio. Trata-se de uma tecnologia derivada do padrão IEEE 802.11i. Podemos dizer que esta tecnologia substitui com maior robustez o protocolo WEP.

Atualizações "casadas" com o SP3

Ao contrário da lista anterior, existem atualizações que só estarão disponíveis se o SP3 for instalado. São elas:

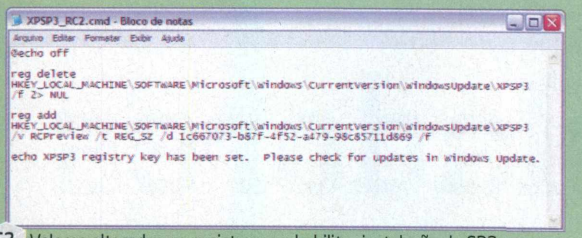
- Detecção de roteadores black hole: Dada a complexidade, foge ao escopo dessa matéria explicar o que seriam estes roteadores, mas podemos dizer que a detecção deste tipo de roteador resulta em menos erros nas transferências e, portanto, melhora a confiabilidade das transmissões. Isso pode ser feito automaticamente pelo Windows Vista e pelo Windows Server 2008 e agora também no Windows XP com SP3. Caso contrário, algumas alterações precisam ser feitas manualmente no sistema para evitar o problema.
- Cliente NAP: Com este recurso o Windows XP poderá ser usado em redes baseadas no Windows Server 2008 que estejam usando o Network Access Protection. Conforme abordado na PC&CIA 70, esta tecnologia é capaz de avaliar a "saúde" do sistema que tenta se conectar a uma rede e, se for o caso, bloquear o ingresso da máquina se ela não atender a um determinado perfil configurado por você. O Windows Vista possui o cliente NAP nativamente, mas no Windows XP essa funcionalidade só será adicionada depois que o SP3 for instalado.
- Descrição de algumas diretivas de segurança: Quem trabalha com a implementação de GPOs (Políticas de Grupo) já deve ter percebido que, ao abrir um item de configuração presente em qualquer modelo administrativo, existe uma guia especial chamada Explicação que fornece mais informações sobre como configurar o item selecionado. Depois que o SP3 do Windows XP for aplicado, esta funcionalidade se estende às diretivas de segurança, de forma que o administrador do sistema tenha maior controle sobre o que está sendo feito. Vale ressaltar que no Windows Server 2003 este comportamento já pode ser observado desde que o sistema esteja atualizado. Você encontra um exemplo desta funcionalidade na **figura 1**.
- Avanços de segurança especiais: Ao aplicar o SP3, o System Essentials for Windows XP SP3 também será instalado, permitindo que avanços nas diretivas de segurança sejam aplicados;
- Avanços na criptografia: Com o SP3, será instalado também o Microsoft Kernel Mode Cryptografic Module (Fips.sys), um software aderente ao padrão FIPS 140-1 que adiciona um módulo criptográfico que funciona no nível do kernel do sistema.

Como instalar o SP3?

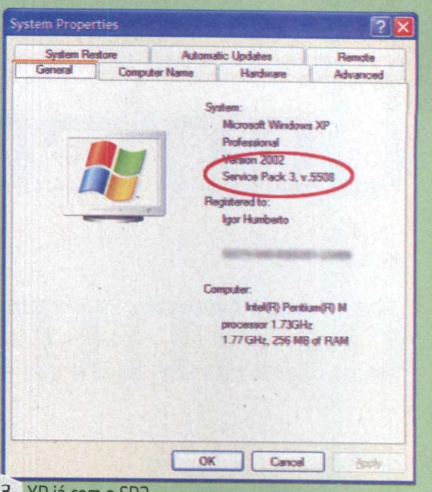
Enquanto trabalhávamos nesta matéria, a única versão do SP3 disponível no site de downloads da Microsoft era a RC2 (Release Candidate 2), nos idiomas Alemão, Japonês e Inglês – nossa escolhida.

Há duas maneiras de se instalar o SP3. Considerando que a versão em inglês do

Windows XP esteja instalada, você pode optar por fazer o download do arquivo de instalação (link no site da revista) ou então, permitir a detecção automática do mesmo através do Windows Update. Neste link citado acima existe um aplicativo que, ao ser instalado, modifica algumas linhas do registro do sistema de forma a permitir que o Microsoft Update reconheça a necessidade pela instalação do SP3 (**figura 2**).



F2. Valores alterados no registro para habilitar instalação do SP3.



F3. XP já com o SP3.

O processo de instalação é similar ao dos outros SPs, ou seja, basta seguir as instruções para concluir a instalação. Você só deve considerar que por se tratar de uma versão RC, ainda pode conter bugs e, como tal, deve ser usada em um ambiente de testes para evitar problemas.

Depois de instalado, nenhuma diferença na aparência é percebida em função das informações passadas anteriormente. Para saber que o SP3 realmente foi instalado, podemos utilizar a janela de Propriedades do sistema (**figura 3**).

Conclusão

Quem espera que o SP3 do Windows XP cause o mesmo impacto das versões anteriores do pacote, ficará decepcionado. Podemos dizer que 90% do SP3 é composto por atualizações do sistema e poucas foram as funcionalidades adicionadas. Vale ressaltar que esta, provavelmente, será a última grande atualização que o sistema receberá antes de ser descontinuado. Podemos concluir também que, com o SP3, será possível fazer com que o Windows XP trabalhe com um dos grandes atrativos do Windows Server 2008, o NAP. Durante nossos testes, não percebemos quaisquer problemas de compatibilidade com o software existente. No site da revista, estão os links para as atualizações independentes e casadas do SP3.

A versão de 64 bits, por se tratar de uma versão diferente do Windows XP (ela é baseada no Windows Server 2003), não poderá ser atualizada pelo SP3. Neste caso, o SP2 do Windows Server 2003 é que deverá ser aplicado.

Até a próxima!

Comandos Windows Server 2003

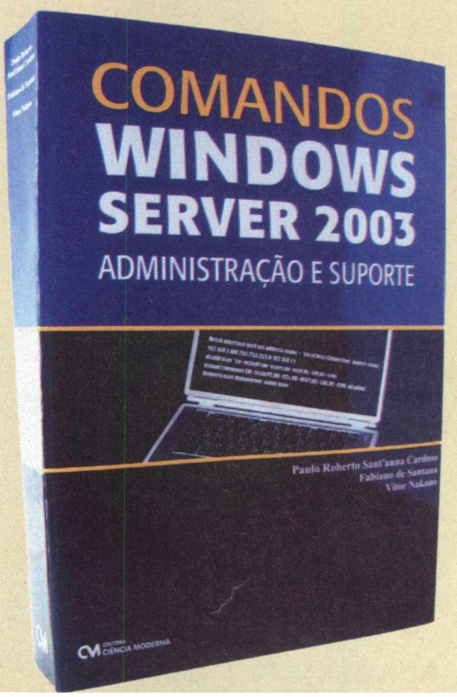
O uso de ferramentas e a execução de tarefas tornam-se bem mais simples quando podemos observar todas as opções em uma interface gráfica, ao alcance de alguns cliques. Contudo, imagine o trabalho maçante que seria adicionar dezenas de novos usuários na rede através da interface "User Manager". Não seria muito melhor se pudéssemos criar um script que lesse um arquivo de parâmetros chamado Usuários.txt, por exemplo, e automatizasse essa tarefa? A partir de então, sempre que a realização desse trabalho fosse necessária, bastaria criar um arquivo texto contendo os nomes dos novos usuários e proceder com a execução do script para, instantes após, ter o trabalho concluído.

Embora não aborde o processo de criação de scripts, o livro "Comandos Windows Server 2003 Administração e Suporte", publicado pela Editora Ciência Moderna, consiste em um guia de referência rápida dos comandos que podem não apenas serem utilizados em scripts, como também para rapidamente conduzir-nos à resolução de problemas de configuração da rede e administração de servidores baseados no Windows Server 2003.

Tendo como autores Fabiano de Santana, Vitor Nakano e nosso colega de redação, Paulo Roberto Sant'anna Cardoso, o livro apresenta 374 opções de comandos ao longo dos seguintes capítulos: Comandos para Administração e Manutenção do servidor, discos e arquivos; Comandos de Rede; Comandos para Administração do Active Directory (AD) e DNS; Comandos para Administração de Políticas de Grupo (GPOs); Comandos para Administração dos serviços de Terminal (Terminal Services); Comandos para o WSUS.

O capítulo 7, Console de Recuperação, e mais três apêndices, complementam esta obra que recomendamos aos profissionais desejosos de terem maior controle e produtividade no dia-a-dia com servidores Windows. E aos analistas e administradores de redes mais resistentes ao uso da interface de linha de comando, é simplesmente leitura obrigatória.

Comandos Windows Server 2003
ISBN: 978-85-7393-647-6
Páginas: 588, 1ª Edição 2008
Preço: 95,20 - www.lcm.com.br/index.php?Escolha=13



Controladores de domínio Windows Server 2008

PARTE 1

Aprenda nesta matéria o que será necessário fazer para integrar os novos controladores de domínio, baseados no Windows Server 2008, às redes Microsoft já existentes.

Igor Humberto

O Windows Server 2008 deve chegar em março deste ano trazendo diversas novas tecnologias, dentre as quais podemos destacar a possibilidade de trabalhar com uma nova função de servidor, denominada Read Only Domain Controller (RODC). A proposta é diferente da adotada pelo BDC (Backup Domain Controller) na época do Windows NT. Este mantinha uma cópia do banco de dados do domínio completo disponível para leitura, o qual era útil para garantir a disponibilidade das informações para as máquinas clientes, em casos de queda do PDC (Primary Domain Controller). Já o RODC irá se comportar na rede de uma forma um pouco diferente, conforme veremos a seguir.

Quando usar um RODC?

Se a empresa possui um cenário de filiais, o administrador de TI deverá considerar os seguintes fatores:

- Numa filial, geralmente é difícil encontrar um profissional de TI devidamente capacitado para administrar uma rede;
- Neste tipo de cenário, segurança da informação não é o principal foco e, conseqüentemente, o controlador de domínio (DC) fica ainda mais vulnerável;
- Normalmente o link com a matriz é mais lento e caro do que o usado na rede local;
- Em alguns casos, a máquina que desempenha o papel de DC possui também o software que é usado na linha de negócios da empresa, o que exige que alguém nessa filial (não precisa ser necessariamente um administrador de redes, apenas uma pessoa com conhecimento sobre o software em questão) receba credenciais administrativas no sistema.

Visto o exposto, devemos avaliar que a infra-estrutura normalmente usada nas empresas que possuem filiais é aquela onde em cada unidade existe um DC para tornar o processo de autenticação dos usuários o mais

eficiente possível. Já pensou como seria o *desempenho* dos sistemas clientes se todos os usuários de uma determinada filial tivessem que se autenticar na matriz em São Paulo, através de um link de apenas 256 kbps a partir do Rio de Janeiro? Como esses computadores (DCs) possuem uma cópia integral da base de dados do Active Directory no modo leitura/gravação, os seguintes pontos podem ser destacados como negativos:

- Se o DC da filial for roubado, o ladrão terá nas mãos toda a base de contas do domínio;
- Como o administrador do software usado na linha de negócios da empresa possui mais privilégios do que o necessário neste sistema, acidentalmente ou não diversos tipos de estragos poderiam ser produzidos;
- Tráfego de replicação do Active Directory, entre os sites, sendo feito através do link lento existente na filial.
- Neste tipo de cenário, o ideal é usar o RODC pelas seguintes razões:
- Ao contrário do que acontece com um DC gravável, o RODC possui todos os objetos do AD, porém as senhas dos usuários, incluindo as credenciais das contas dos computadores, não são armazenadas. Sendo assim, se um ladrão roubar o servidor, ele não terá acesso às informações completas das contas;
- Pensando na idéia de que a aplicação usada na linha de negócios da empresa possa estar instalada no RODC, devemos considerar que é possível configurar o sistema de forma que a conta com privilégios administrativos seja usada apenas para administrar um determinado RODC, sem comprometer, portanto, os demais DCs da rede. Numa rede baseada no Windows Server 2003, se a pessoa que estiver em um DC possuir privilégios administrativos, esta será capaz de realizar alterações em qualquer DC do domínio;
- Como o RODC possui apenas alguns objetos do AD, menos informações precisam ser replicadas entre ele e os DCs comuns.

Como funciona um RODC?

Se alguma aplicação precisar fazer a leitura da base de dados do AD, esta operação poderá ser executada normalmente no RODC. Porém, se alguma operação demandar a alteração desta base de dados, a aplicação receberá como resposta do RODC um caminho LDAP que irá referenciar um DC gravável e, assim, a operação poderá ser concluída. Depois que isso acontece, o DC gravável envia ao RODC as alterações feitas.

Outro detalhe a se destacar é a diminuição da replicação entre os DCs, pois considerando que no RODC não é possível fazer alterações no AD, os DCs graváveis não precisam sincronizar atualizações provenientes do RODC. Assim, a tarefa de replicação passa a ser unidirecional, ou seja, somente dos DCs graváveis para os RODCs, nunca no sentido contrário. Além de ajudar a reduzir o tráfego de dados, essa característica também auxilia aos administradores, visto que são menos servidores para monitorar a replicação de dados.

Para compreender outra funcionalidade do RODC é necessário que você entenda primeiro o funcionamento do processo de autenticação normal, ou seja, quando se trabalha com DCs comuns, baseados no Windows Server 2003. Quando uma solicitação de autenticação é feita, através das informações existentes nos registros do servidor DNS (registros SRV) a estação irá estabelecer uma conexão com o DC do seu respectivo site, ou seja, quando tudo está configurado adequadamente, aquele que se encontra mais próximo. Este DC entregará ao cliente que está tentando fazer logon um ticket que determina tudo o que o usuário, por exemplo, poderá fazer naquela rede. Essa tarefa é executada pelo Kerberos (mais informações em **http://pt.wikipedia.org/wiki/Kerberos**). Com o ticket, o cliente prossegue com o processo de autenticação. Vale ressaltar que não são apenas usuários que solicitam autenticação. Computadores e serviços também o fazem dentro de uma rede baseada no Active Directory. Agora que você já tem uma visão geral de como o processo normalmente funciona, vamos entender como o RODC trabalha dentro da rede.

Como já foi dito, por padrão o RODC não armazena as credenciais das contas do AD (contas de usuários e de computadores). As únicas exceções são duas contas: A conta de computador do próprio RODC e uma conta especial, denominada krbtgt, que será usada para executar a emissão dos tickets do Kerberos. Dentro do site onde o RODC se encontra, este é anunciado como KDC (Centro de distribuição de chaves) e, conseqüentemente, será visto como um servidor capaz de emitir os tickets.

Para ilustrar a situação, quando um usuário tenta se autenticar em uma estação pela primeira vez, o RODC envia a solicitação para algum DC gravável no site do hub, que deve executar o Windows Server 2008. Se a autenticação ocorrer, o DC assina e criptografa a solicitação usando aquilo que chamamos de TGT (Ticket-Granting Ticket, ou algo como Ticket de acesso). Após essa etapa, o RODC aproveita para "perguntar" se as credenciais podem ser enviadas para que seja feito o armazenamento em cache. Como a solicitação foi feita por um RODC, o DC gravável verifica a diretiva de replicação apropriada e determina se isso poderá, ou não, ser feito. Através da referida diretiva o DC verifica se é possível enviar as credenciais para o RODC. Caso positivo, as mesmas serão enviadas e armazenadas em cache, no referido servidor.

De forma sintetizada, o que foi dito anteriormente pode ser traduzido no seguinte diálogo:

RODC: DC, eu tenho um usuário com as seguintes credenciais tentando se autenticar aqui. Você poderia, por favor, verificar se elas são autênticas?

DC: Um minuto, por favor. Sim, elas são autênticas.

RODC: OK, obrigado. Se não for pedir muito, você poderia me passar essas credenciais para que de uma próxima vez eu não precise lhe incomodar novamente com esta questão?

DC: Por favor, aguarde um instante que eu verei se o administrador me permite liberar esta informação para você. Ok, pelo que vi aqui, posso lhe passar essa informação sim. Pegue!

RODC: Obrigado!

Quando um usuário tentar se autenticar novamente, o RODC verificará quem assinou o ticket (TGT) que foi usado da última vez. Se a assinatura foi feita por um DC gravável, o RODC irá iniciar novamente aquele "bate-papo" com o

referido servidor. Se a assinatura foi feita usando a conta krbtgt do próprio RODC, este entende que as credenciais estão armazenadas em cache e que não é necessário conversar com outro servidor.

Por padrão, o RODC não armazena em cache as credenciais de nenhum usuário e nem de nenhuma conta de computador. Porém, esta pode não ser a melhor forma de trabalhar, pois, desse jeito, a todo instante o RODC terá de falar com outros DCs. Considerando isso, talvez fosse interessante armazenar em cache apenas as credenciais dos funcionários comuns da filial. As credenciais das contas com um nível de privilégio mais alto (contas dos administradores, por exemplo) poderiam ser configuradas para não terem essa informação armazenada no cache do RODC. Agora vamos a um exemplo prático para explorar melhor o que foi dito até aqui.

Implementando um RODC

Quando o Windows Server 2008 for lançado, a maioria das empresas irá implementar o referido sistema na infra-estrutura existente, ou seja, pensando que no ambiente possa existir uma infra-estrutura do Active Directory em funcionamento. Devemos considerar, então, que DCs baseados no Windows 2000 Server e Windows Server 2003 estarão em execução. Somente as empresas que estiverem iniciando o seu processo de informatização, e estas não serão a maioria das empresas, começarão este processo usando diretamente servidores baseados no Windows Server 2008.

Sendo assim, pensando no que será visto na maioria das vezes, vamos demonstrar a implementação do RODC em um ambiente baseado no Windows Server 2003 pré-existente.

Preparando o ambiente

Como o Windows Server 2008 realizará muitas alterações no Active Directory que o Windows Server 2003 não conhece, será necessário, antes de qualquer coisa, preparar o domínio e a floresta para receber este novo tipo de DC na rede (o DC 2008 + RODC).

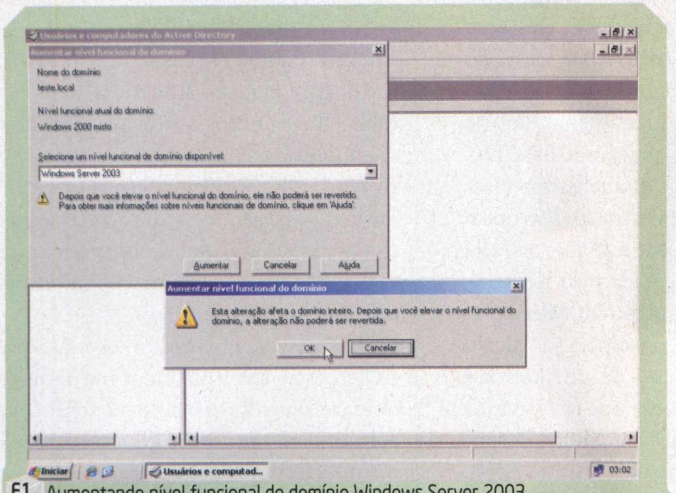
O ambiente que será configurado é um domínio baseado no Active Directory chamado teste.local. Neste domínio existe apenas um DC, denominado DC2003, o qual além de possuir a função de armazenar a base de dados do AD, também possui a função de servidor DNS do domínio. Sendo assim, se você quiser reproduzir nosso exemplo, configure um servidor Windows Server 2003 com o IP 192.168.100.1/24. Feito isso, faça a configuração deste servidor para que o mesmo assuma a função de DC, ou seja, execute o Assistente de instalação do Active Directory (DCPROMO.EXE). Através do assistente, configure o domínio com o nome teste.local e configure o servidor para ser o servidor DNS do domínio.

Vale ressaltar que alguns dos procedimentos que serão exibidos aqui não são reversíveis, ou seja, se você executá-los no seu ambiente, sem ter a certeza do que está fazendo, não será capaz de reverter essas ações. Se esta for a sua situação, execute os procedimentos em um laboratório de testes, ou em máquinas virtuais.

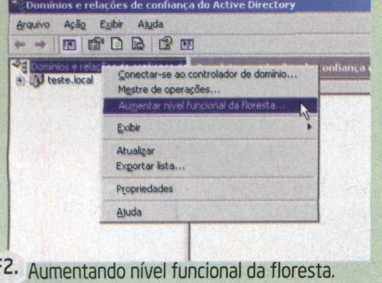
O nosso objetivo será configurar um RODC neste domínio, porém, um RODC não irá se comunicar de forma adequada com um DC baseado no Windows Server 2003. A razão é simples: o 2003 não compreenderá a lógica de funcionamento do RODC, ou seja, o sistema de cache de credenciais. Um RODC só irá se comunicar com um DC baseado no Windows Server 2008 gravável existente na rede. Sendo assim, a nossa segunda tarefa será a de implementar um DC adicional baseado no referido sistema.

Antes de prosseguir com esta tarefa, devemos nos certificar de que o nível funcional da floresta é Windows Server 2003. Para fazermos esta configuração, primeiro será necessário elevar o nível funcional do domínio para Windows Server 2003 (o nível funcional padrão do domínio é Windows 2000 misto e o nível funcional padrão da floresta é Windows 2000).

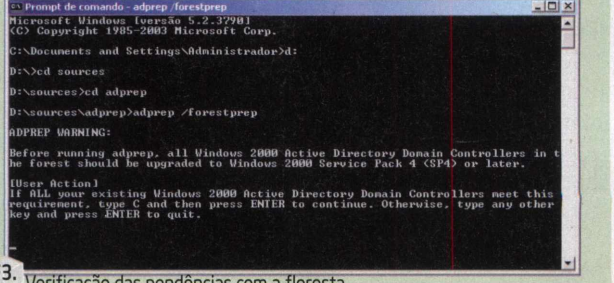
Para executar essa tarefa, no Windows Server 2003 abra o console Usuários e computadores do Active Directory (DSA.MSC) e clique com o botão direito sobre o nome do domínio. No menu que aparece, selecione a opção Aumentar nível funcional do domínio. Na caixa que se abre, selecione a opção Windows Server 2003 e depois clique no botão Aumentar (**figura 1**). Vale ressaltar que esta operação só poderá ser executada se todos os DCs do domínio estiverem executando o Windows Server 2003. Além disso, é importante enfatizar que esse procedimento não é reversível, ou seja, não existe uma opção para rebaixar o nível funcional do domínio. Conforme diz a caixa de informação que é exibida depois que o procedimento é concluído, esta operação será replicada para todos os demais DCs da rede. O tempo que essa operação



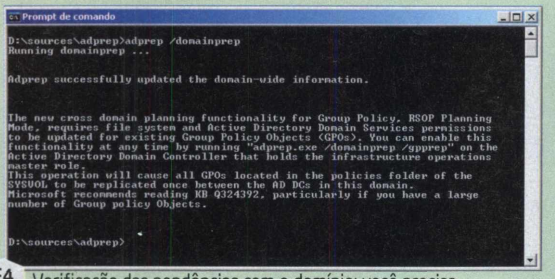
F1. Aumentando nível funcional de domínio Windows Server 2003.



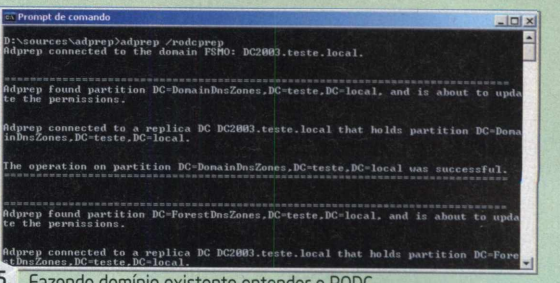
F2. Aumentando nível funcional da floresta.



F3. Verificação das pendências com a floresta.



F4. Verificação das pendências com o domínio: você precisa executar este comando no DC que possui a função de mestre de infra-estrutura.



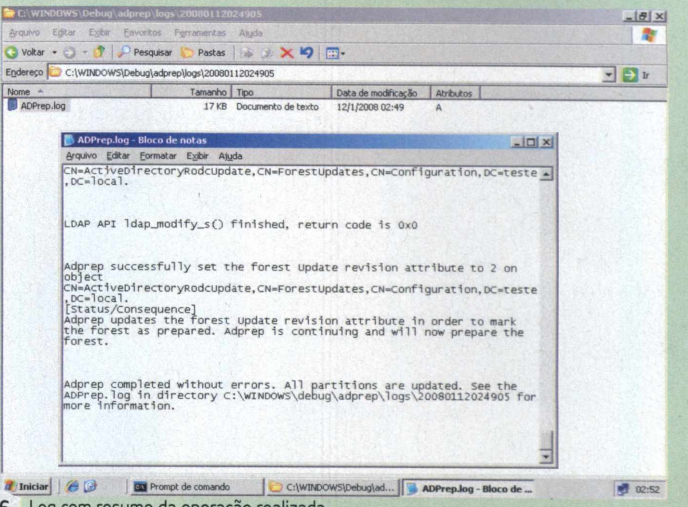
F5. Fazendo domínio existente entender o RODC.

levará depende de como foi configurada a topologia de duplicação no domínio, lembrando que é possível forçar esta operação através do console Serviços e sites do Active Directory (DSSITE.MSC).

Agora que o nível funcional do domínio foi elevado para Windows Server 2003, o pré-requisito para elevarmos o nível funcional da floresta, também para Windows Server 2003, foi estabelecido. Para isso, abra o console Domínios e relações de confiança do Active Directory (DOMAIN.MSC). Agora clique com o botão direito em Domínios e relações de confiança do Active Directory e selecione a opção Aumentar nível funcional da floresta (**figura 2**). Na caixa que será aberta, selecione a opção Windows Server 2003 e clique no botão Aumentar. Vale ressaltar que para executar essa tarefa, o nível funcional de todos os domínios existentes na floresta deve ser Windows Server 2003. Da mesma forma que aconteceu quando o nível funcional do domínio foi aumentado, se existirem outros DCs na rede, o processo de duplicação dessa nova informação para esses outros servidores dependerá de como foi configurada a topologia de duplicação. Além disso, esse procedimento não é reversível, ok?

Agora que os níveis funcionais do domínio e da floresta foram devidamente elevados, devemos preparar a floresta e o domínio para receber um DC baseado no Windows Server 2008 (não necessariamente um RODC). Isso se faz necessário em função dos novos atributos e classes que são necessários no Esquema do Active Directory.

Para executar essa tarefa, insira a mídia de instalação do Windows Server 2008 no computador que estiver executando o Windows Server 2003 como DC. Vale ressaltar que este DC deve ser o primeiro que foi promovido na rede.



F6. Log com resumo da operação realizada.

Abra o prompt de comandos e siga para o caminho X:\SOURCES\ADPREP, onde "x" representa a letra da sua unidade de DVD. Agora execute a seguinte linha de comando: ADPREP /FORESTPREP <ENTER> (**figura 3**).

Repare a observação que é feita antes de prosseguir com o procedimento. A aplicação diz que caso exista algum DC executando Windows 2000 Server, será necessário garantir que este servidor possua pelo menos o Service Pack 4 instalado para garantir a compatibilidade. Se não for o caso, não prossiga! Como não é esta a nossa situação, basta teclar "c" e depois <ENTER>. Este procedimento pode demorar alguns minutos.

Com a floresta pronta, iremos preparar o domínio. Para isso, execute o comando ADPREP /DOMAINPREP <ENTER>. Você perceberá que este comando será executado mais rapidamente que o anterior (**figura 4**). Além disso, a aplicação fala sobre o comando ADPREP /DOMAINPREP /GPPREP <ENTER>. De forma resumida, este comando adapta o Active Directory para que ele possa trabalhar de maneira mais adequada com as diretivas de grupo, pois o Windows Server 2008 faz algumas alterações no tratamento destes objetos. Este comando poderá ser executado posteriormente; a não execução dele agora não irá nos atrapalhar.

Floresta preparada, domínio preparado. Para colocar um DC com Windows Server 2008 na infra-estrutura da rede existente, já seria suficiente. Porém, como o objetivo é o de colocar também um RODC na rede, além desses comandos será necessário preparar o domínio para compreender o funcionamento do RODC. Para isso execute o comando ADPREP /RODCPREP <ENTER>, conforme mostra a **figura 5**.

Este procedimento também não deve demorar. Depois que o comando for concluído, você receberá a informação de que um log, com o registro da operação, foi criado automaticamente em %WINDIR%\Debug\adprep\logs\número (**figura 6**).

Na próxima edição continuaremos com a implantação e configuração dos servidores Windows Server 2008. Até lá! **PC**

Certificação Microsoft MCTS

FINAL



Neste décimo e último artigo da série preparatória para o exame 70-620, apresentaremos um conjunto de ferramentas internas do Windows Vista para diagnóstico de problemas, as configurações do sistema em Tablet PCs e como conectar máquinas com Vista em redes wireless.

Igor Humberto e Paulo Sant´anna

Um dos grandes atrativos no Windows Vista está nas novas ferramentas de diagnóstico que foram acrescentadas no sistema. Antes disso, seria necessário utilizar ferramentas de terceiros se você quisesse fazer uma análise do funcionamento da máquina. Como profissional MCTS, é evidente que você deve conhecê-las para poder diagnosticar adequadamente os problemas que surgirem no sistema.

WDI (Windows Diagnostic Infrastructure) é o nome do conjunto de ferramentas que o sistema oferece para não somente diagnosticar problemas no sistema mas, também, para evitar que os mesmos aconteçam. Isso é feito mediante o envio, ao administrador, de informações que possam alertá-lo de que algo não anda bem. Mais adiante, você aprenderá a usar essas ferramentas a seu favor.

Diagnosticando problemas de memória

Este é um dos problemas mais comuns com os computadores atuais. Normalmente, o defeito no módulo de memória é causado durante o manuseio ou processo de estocagem. O fato é que, na maioria dos casos, não podemos contar com um vendedor técnico capacitado para lidar com o equipamento. Por isso, é comum ver o manuseio incorre-

to expondo os módulos a problemas com descargas eletrostáticas (ESD).

Os problemas podem se manifestar de diversas formas: o computador pode não iniciar, ou seja, ficar na tela preta sem informar absolutamente nada para o usuário; pode ocasionar as famosas telas azuis, etc.

A questão aqui é que não surge nenhuma caixinha informando ao usuário que o problema está com a memória e, nestes casos, o técnico acaba trabalhando com o computador tal como um pediatra lida com uma criança. Em outras palavras, como a mesma não sabe dizer corretamente o que está sentindo, o médico precisa coletar evidências que o conduzam a um diagnóstico correto.

No caso do computador, a falta de um equipamento de diagnóstico adequado somada à falta de informação técnica, faz com que o problema persista no sistema durante bastante tempo.

Quando nos referimos ao equipamento de diagnóstico, uma placa do tipo POST pode ser de grande utilidade quando o computador não inicia e se limita a apresentar uma tela preta antes mesmo de começar a carga do sistema operacional. O defeito com os módulos seria "pego" através dos displays da placa.

Já em relação à falta de conhecimento técnico, estamos falando de profissionais que não estudam o produto a fundo e, assim, fazem os seus trabalhos de diagnóstico baseando-se em "achismos". Poucos sabem, por exemplo, que para cada sistema operacional lançado pela Microsoft há um respectivo Resource Kit, em cujo material é possível, por exemplo, encontrar a descrição de cada tela azul que o sistema pode retornar. Conseqüentemente, o técnico pode entender exatamente o que está ocorrendo com o computador.

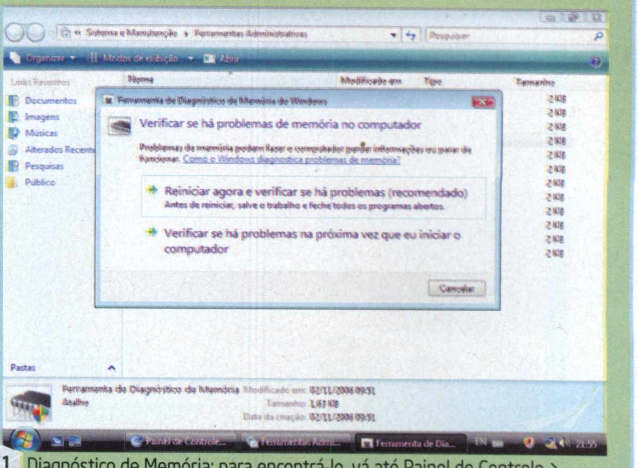
Além disso, a falta de conhecimento técnico também se traduz na ignorância quanto às ferramentas de software adequadas para a realização de diagnósticos precisos da saúde do sistema. Diante desse cenário, nem precisaria dizer que este conjunto de fatores resulta na demora para a resolução de problemas, principalmente quando se trata de falhas causadas por defeito na memória.

Pensando nisso, a Microsoft incluiu no Windows Vista a Ferramenta de Diagnóstico de Memória, a qual basicamente testa a memória repetidamente, gravando dados na mesma e depois lendo-os para saber se não foram alterados. Se isso ocorrer, o erro será relatado e a área da memória correspondente será evitada pelo sistema a partir deste momento. Vale ressaltar que problemas na memória podem ser intermitentes, ou seja, mesmo quando esta ferramenta informar que não existem problemas estes podem perfeitamente existir. Sendo assim, é importante executar o teste estendido com um bom número de repetições para poder aumentar sua confiabilidade.

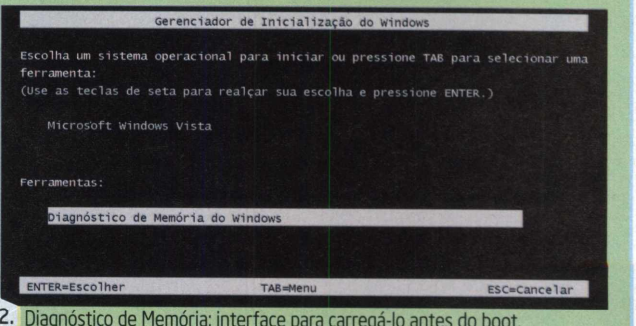
Normalmente, você não precisa se preocupar em executar esta ferramenta periodicamente porque o próprio sistema, ao detectar uma falha que possa ter relação com a memória, irá sugerir que o teste seja feito (**figura 1**).

Outra forma de executar essa ferramenta é a partir do Gerenciador de boot do Windows Vista. Para isso, reinicie o sistema certificando-se de que não há nenhuma mídia inicializável inserida em outra unidade de disco (DVD-ROM, por exemplo). Depois que o POST terminar, pressione repetidamente a tecla Espaço a fim de abrir o Gerenciador de Inicialização do Windows (**figura 2**). Em seguida, pressione a tecla TAB e selecione a opção Diagnóstico de Memória do Windows.

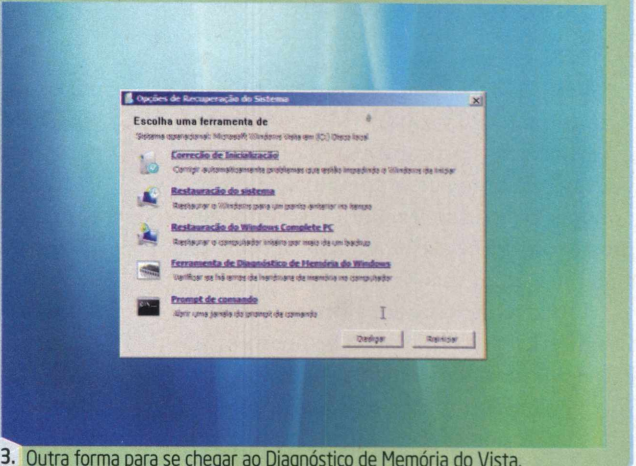
Além disso, a ferramenta de Diagnóstico de Memória pode ser acessada através do DVD de instalação do Windows Vista. Para isso, inicie o computador com o DVD de instalação no drive óptico, configure as opções regionais da forma que achar mais apropriada e clique em Avançar. Na tela seguinte, clique na opção Reparar o computador. Agora você deve selecionar qual instalação do Windows deseja reparar e depois, mais uma vez, clique em Avançar. Na próxima etapa, a *janela* Opções de Recuperação do Sistema irá apresentar a opção de iniciar a Ferramenta de Diagnóstico de Memória do Windows (**figura 3**).



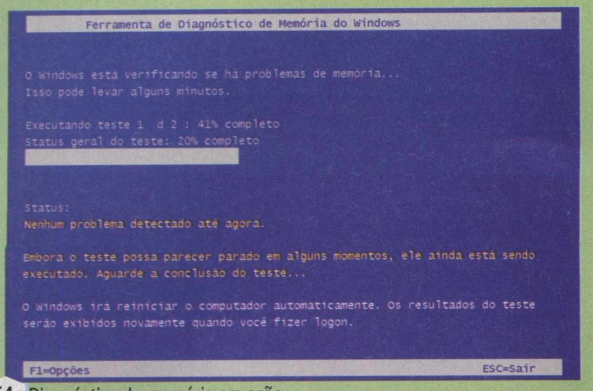
F1. Diagnóstico de Memória: para encontrá-lo, vá até Painel de Controle > Sistema e Manutenção > Ferramentas Administrativas.



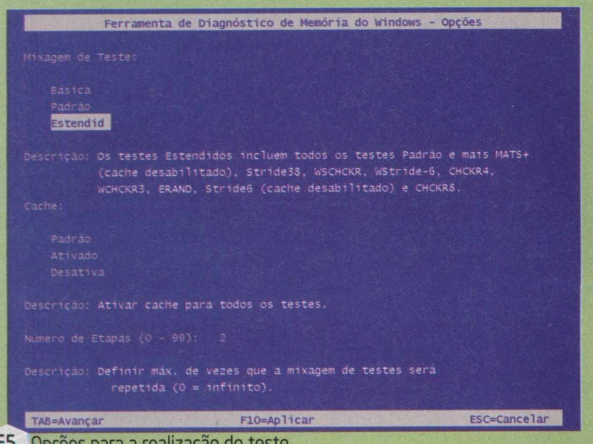
F2. Diagnóstico de Memória: interface para carregá-lo antes do boot.



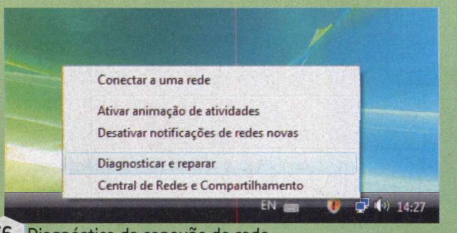
F3. Outra forma para se chegar ao Diagnóstico de Memória do Vista.



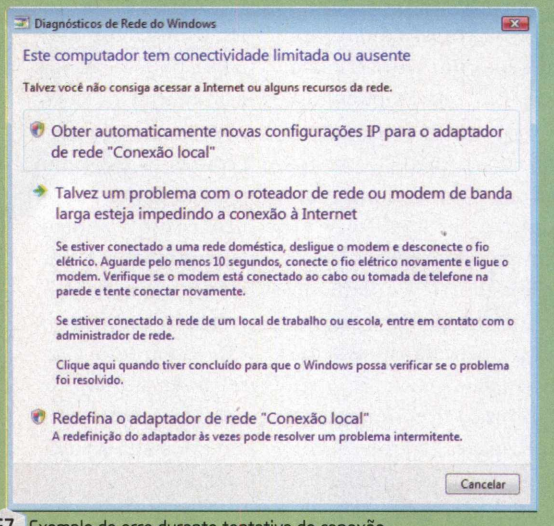
F4. Diagnóstico de memória em ação.



F5. Opções para a realização do teste.



F6. Diagnóstico da conexão de rede.



F7. Exemplo de erro durante tentativa de conexão.

Nesta janela você verá duas opções: Reiniciar agora e verificar se há problemas e Verificar se há problemas na próxima vez que eu reiniciar o computador. Nós optamos pela primeira. Portanto, antes de prosseguir, feche os programas abertos e aguarde o computador reiniciar.

Ao ser reinicializado, a Ferramenta de Diagnóstico de Memória do Windows será executada automaticamente (**figura 4**). Se você não quiser intervir, o teste será executado com as configurações padrão. Se você julgar necessário, pressione a tecla F1 para exibir as opções avançadas do teste.

As opções disponíveis são:

- Mixagem de teste: Onde é possível escolher entre diversos níveis de testes pré-definidos que poderão ser executados. Você pode optar pelas configurações de teste Básico, Padrão ou Estendido. Para cada uma das opções selecionadas, uma breve descrição informa que tipos de testes serão executados;
- Cache: Aqui você escolhe como o sistema irá lidar com o cache mediante a execução dos testes, ou seja, se ele será ativado ou não. Você pode optar por utilizar as opções Padrão, Ativado ou Desativado;
- Número de etapas: Esta opção permite que você defina a quantidade de vezes que o teste será realizado. A opção "0" informa que o teste seja executado indefinidamente.

Na **figura 5**, você pode ver a tela com as opções disponíveis para o teste. Tendo feito a escolha, pressione F10 para executar o teste. Você será levado novamente à tela inicial da ferramenta e o teste será reiniciado com as configurações feitas por você. Durante a execução do mesmo, a ferramenta informará se erros foram encontrados. Depois de concluído, o computador será reiniciado automaticamente. Chegando novamente à Área de trabalho, o sistema fornecerá informações sobre o teste. Além disso, informações mais detalhadas são armazenadas no log de eventos do sistema com a fonte MemoryDiagnosticsResults, sob o código 1201.

Dado que problemas nos módulos de memória não podem ser facilmente reparados, via de regra será necessário substituí-los para solucionar o problema. Se você tiver vários módulos de memória instalados no sistema, será complicado identificar o defeituoso e pode ser necessário substituir os módulos um a um, intercalando este processo com uma nova execução da Ferramenta de Diagnóstico de Memória. Você precisará fazer isso até que os testes não apresentem mais erros. Apesar disso, você deve considerar que a memória poderá apresentar mau funcionamento em função de aquecimento excessivo dentro do gabinete e/ou interferências elétricas e que problemas na placa-mãe ou no processador também podem desencadear um mau funcionamento da memória.

Diagnosticando problemas de conectividade

Outro problema comum de ocorrer com os usuários é o de conectividade com a rede. Nesta categoria de problemas podemos incluir aqueles que impedem a

conexão do sistema a outros computadores presentes na rede interna (ambiente corporativo) ou apenas um problema de conexão com a Internet (ambiente doméstico).

Independente do tipo de problema, o usuário ficará algum tempo sem acesso às informações da rede e, claro, isso o deixará insatisfeito. Como existem algumas causas comuns que podem impedir o computador de se comunicar com outros na rede, a Microsoft incluiu no Windows Vista uma ferramenta que retorna ao usuário mais informações do que um simples "cabo de rede desconectado" (na melhor das hipóteses, porque se o problema for com o roteador, por exemplo, nenhuma mensagem é retornada).

Sendo assim, caso existam problemas de conectividade, basta clicar com o botão direito do mouse sobre o ícone da conexão de rede, que se encontra na bandeja de sistema, e selecionar Diagnosticar e reparar (**figura 6**). Vale ressaltar que esta ferramenta também pode ser aberta através do Centro de Rede e Compartilhamento.

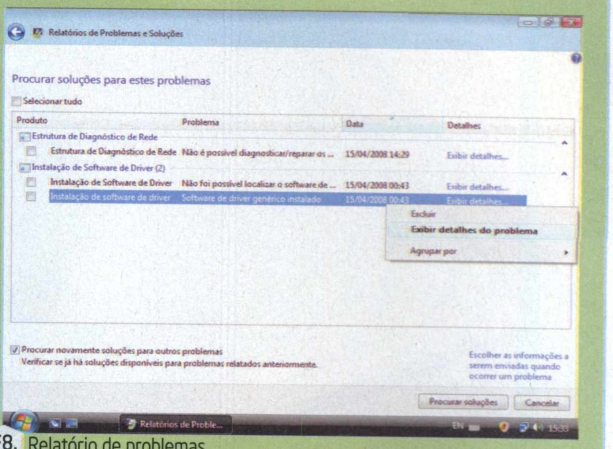
O sistema fará uma breve análise das configurações da rede a fim de determinar a causa do problema. Quando chegar a alguma conclusão, uma caixa será exibida para o usuário informando as possíveis causas do problema. Na **figura 7** você pode ver um exemplo desta caixa. No caso, o adaptador de rede está configurado para usar um endereço IP dinâmico e não existe um servidor DHCP disponível. Repare que a linguagem usada pelo sistema é bem simples e de fácil entendimento.

Além disso, através da Ferramenta de Diagnóstico de Rede, o sistema é capaz de resolver sozinho alguns problemas mais simples. Por exemplo, naqueles casos em que um "restart" do adaptador de rede é suficiente.

Relatórios de Problemas e Soluções

Esta ferramenta trabalha em conjunto com o Serviço de Relatório de Erros do Windows, ou seja, aquele que é executado automaticamente quando algum problema com uma aplicação, por exemplo, é detectado e sugere o envio dos dados coletados para a Microsoft, através da Internet. Se existir alguma solução, um link é exibido para o usuário com informações que visam a ajudá-lo a resolver o problema.

Se você estiver se perguntando onde a Ferramenta Relatórios de Problemas e Soluções entra nessa história toda, saiba que com ela você será capaz de criar uma linha de investigação que o ajudará a descobrir a causa e a solução para o problema. Para executar esta ferramenta, clique em Iniciar > Todos os programas > Manutenção.



F8. Relatório de problemas.

Com a mesma aberta, você poderá escolher uma dentre as seguintes opções:

- Procurar por novas soluções: a ferramenta tentará descobrir uma solução para os problemas existentes;
- Consultar problemas para verificar: a ferramenta listará os problemas atuais para que você tente encontrar uma solução;
- Exibir histórico de problemas: opção auto-explicativa;
- Alterar configurações: definir como o sistema se comportará diante de um problema. A configuração padrão determina que o mesmo tente resolver o problema automaticamente, o que é adequado para a maioria dos casos;
- Limpar histórico de soluções e problemas: opção auto-explicativa.

No sistema que estamos usando como exemplo, ao clicarmos em Consultar problemas para verificar pudemos observar alguns problemas pendentes. Ao clicar com o botão direito sobre alguma opção disponível, é possível obter mais informações sobre o problema específico (**figura 8**).

Ferramentas de reparação da inicialização

Até o Windows Server 2003, a Microsoft disponibilizava um conjunto de ferramentas que permitiam que o técnico tentasse diagnosticar possíveis problemas de inicialização do sistema. Tal conjunto está disponível através do Console de recuperação, que poderia ser iniciado, por exemplo, através da inicialização do sistema com o CD de instalação do produto.

Apesar de eficiente, alguns problemas ainda não poderiam ser resolvidos somente com o auxílio do Console de recuperação, sendo necessárias ferramentas de terceiros para colocar o sistema no ar novamente.

No Windows Vista, um novo conjunto de ferramentas foi disponibilizado para ajudar nessa tarefa. Para ter acesso às mesmas, basta iniciar o sistema usando o DVD de instalação do Windows Vista, selecionar as configurações de idioma e layout do teclado apropriadas para o seu computador e depois clicar na opção Reparar o computador. Você será levado para a caixa Opções de Recuperação do Sistema exibida na figura 3.

Você poderá usar esta ferramenta para detectar e/ou corrigir, basicamente, os seguintes problemas: incompatibilidade de drivers, configurações de sistema perdidas, inadequadas ou corrompidas, problemas no disco e problemas de memória.

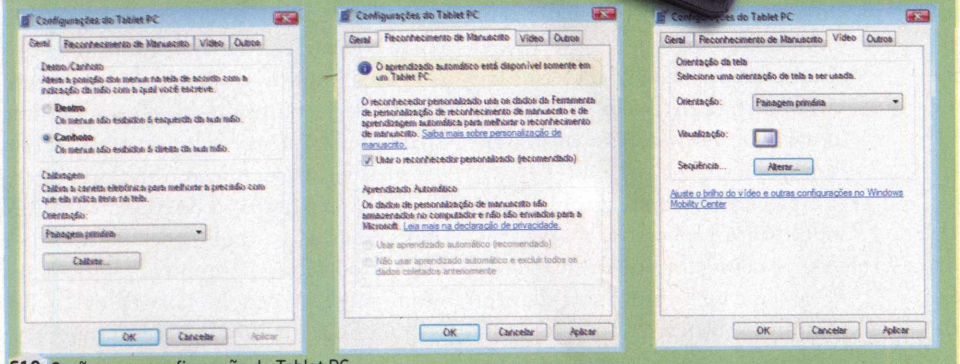
Windows Vista em Tablet PCs

Podemos utilizar o Windows Vista em computadores portáteis como Notebooks e Tablet PCs. Estes são computadores portáteis que suportam as operações através do toque de uma caneta especial na tela, ou seja, sendo possível escrever diretamente na tela, assim como é feito nos Handhelds, Pocket PCs e Palms. Para tal, são usadas ferramentas disponíveis no sistema para reconhecimento da escrita e mapeamento dos comandos e ações do usuário.

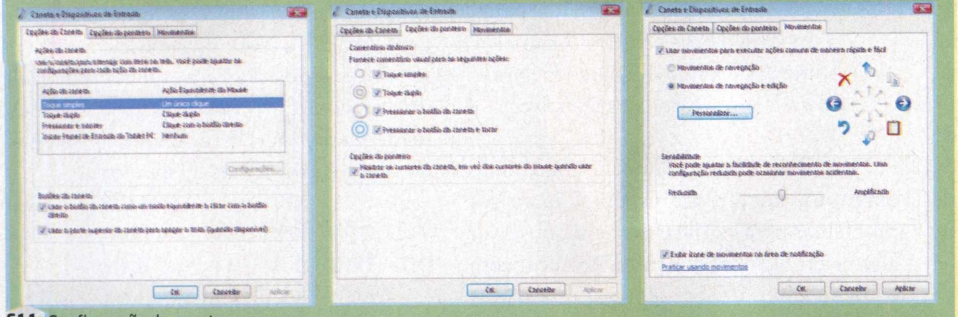
Um Tablet PC tem mais ou menos o tamanho de um caderno ou uma prancheta, e é bem mais leve que um notebook con-



F9. Exemplo de Tablet PC tipo Mesa com Windows Vista instalado.



F10. Opções para configuração de Tablet PC.



F11. Configuração da caneta.

vencional devido à falta de portas e à menor quantidade de componentes internos. Não se trata de um equipamento que possamos chamar de popular, mas pode ser utilizado em alguns nichos de mercado, como por exemplo, no ramo hospitalar ou no acadêmico. Esses são chamados de Tablet PCs do tipo Mesa (**figura 9**) e não possuem teclado e mouse, o que não impede que sejam utilizados através de conexão USB.

Notebooks com a tecnologia Touch Screen e que permitem rotação da tela em 180 graus são chamados de Tablet PCs do tipo conversíveis.

Anteriormente existia uma versão especial do Windows XP destinada à utilização em dispositivos do gênero, porém no Windows Vista o suporte a Tablet PCs é nativo. Ou seja, trata-se do mesmo sistema operacional instalado em um desktop ou notebook, não havendo uma versão do Windows Vista especial para Tablet PCs. Aliás, podem ser instaladas as versões Home Premium, Business, Enterprise e Ultimate.

Configurando Tablet PC

A configuração do Windows Vista em Tablet PCs é cobrada no exame 70-620, portanto vamos conhecer as opções disponíveis. Para isso, devemos acessar as Configurações do Tablet PC no Painel de Controle. Essas configurações estão disponíveis e podem ser visualizadas no Windows Vista mesmo que o sistema não esteja sendo executado em um Tablet PC.

Na Guia Geral (**figura 10**), podemos definir a posição dos menus exibidos na tela de acordo com a indicação da mão (Destro/Canhoto) que será utilizada para escrever e também fazer a Calibragem da caneta utilizada para tocar a tela Touch Screen.

Na guia Reconhecimento de Manuscrito, temos um dos recursos mais interessantes disponíveis no Windows Vista com relação à utilização de Tablet PCs, pois o sistema procura reconhecer a forma de escrever do usuário a fim de adaptar-se ao mesmo e facilitar o uso, além de promover melhoras na produtividade. Para utilizar o recurso, mantenha marcada a opção Usar o reconhecedor personalizado (recomendado) e, em Aprendizado Automático, marque a opção Usar aprendizado automático. Nós mesmos também podemos configurar as opções de escrita no Tablet. Para isso basta desabilitar as opções comentadas acima.

Na guia Video, podemos definir a orientação (Horizontal/Vertical ou Paisagem/Retrato) da tela que será utilizada. Vale citar que alguns modelos de Tablet PCs possuem botões para rotação da orientação da tela e esta opção nos permite definir a ordem de alteração da Orientação da tela quando o botão for acionado.

Na guia Outros, podemos acionar a Configuração da Caneta utilizada no Tablet PC ao clicar em Ir para Caneta e Dispositivos de Entrada, cujas definições veremos a seguir.

Configurando a Caneta e Dispositivos de Entrada

A ferramenta para configuração da Caneta e Dispositivos de Entrada está disponível no Painel de Controle do Windows Vista. Na guia Opções de Caneta (**figura 11**), definimos as ações que poderão ser realizadas com a caneta e ao lado podemos ver a ação equivalente à realizada pelo Mouse. Por exemplo, toque duplo da caneta na tela corresponde ao duplo clique do Mouse.

Na guia Opções do ponteiro, podemos definir Comentários visuais para determinadas ações realizadas pelo usuário ao utilizar a caneta. Trata-se de uma forma de confirmação de que o sistema operacional reconheceu a ação realizada com a caneta.

Na guia Movimentos, podemos fazer um mapeamento das ações mais comuns realizadas pelo usuário, como copiar, colar, excluir, entre outras. O nível de Sensibilidade do toque também pode ser definido nesta guia. A opção Exibir ícone de movimentos na área de notificação já vem marcada por padrão. Clicando em Praticar usando movimentos, podemos exercitar o uso da caneta.

Em Personalizar Movimentos, podemos editar as ações para cada movimento de acordo com a necessidade.

Windows Vista em Redes Wireless (WLAN)

Que técnico já não se deparou com aquelas redes onde o cabeamento mais parece com um "ninho de cobras"? Nestas situações, quem nunca pensou em não mexer nas configurações para evitar que as coisas parassem de funcionar? Bem, para resolver situações deste tipo, a melhor solução é a implementação de redes sem fio, ou seja, uma WLAN.

Além do aspecto mais limpo, usar uma infra-estrutura de rede sem fios ajuda, por exemplo, na hora em que for necessário mover uma estação de trabalho para outro lugar dentro da empresa.

Apesar disso, vale ressaltar que redes deste tipo também apresentam os seus problemas. Elas são, por exemplo, muito mais suscetíveis a interferências do que as redes cabeadas. Além disso, você terá que se preocupar um pouco mais com a segurança dos dados que trafegam pela rede, uma vez que o meio de comunicação usado será o ar. O que queremos dizer é que qualquer pessoa que possa captar o sinal da sua rede pode, potencialmente, visualizar os seus dados.

Como funciona uma WLAN?

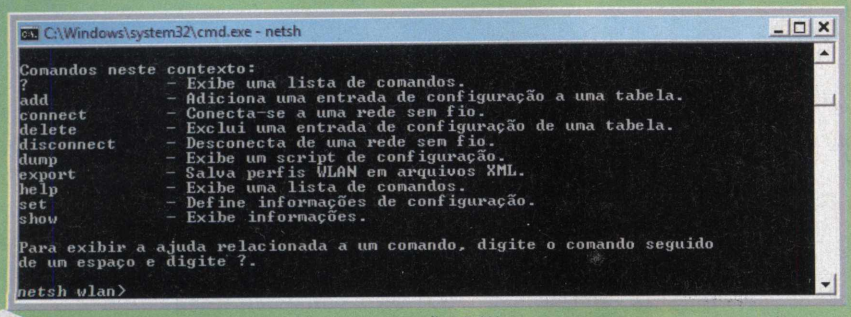
Antes de mostrarmos a configuração do Windows Vista para trabalhar com este tipo específico de rede, é necessário relembrar alguns termos técnicos e padrões relacionados a esta tecnologia. Primeiro, as redes WLAN podem funcionar em dois modos:

- AD Hoc: Comparando com uma rede cabeada, este modo se assemelha à conexão entre dois computadores através de um cabo cross-over. A diferença está na quantidade de computadores que podem se comunicar neste modo, que aqui são mais de dois. Neste tipo de rede não existe um dispositivo concentrador responsável por sustentar a infra-estrutura. No caso, os computadores colaboram uns com os outros para viabilizar a comunicação entre eles. Para ter acesso à Internet, é necessário que um dos computadores envolvidos na rede possa atuar como um roteador;
- Infra-estrutura: Neste modo, um dispositivo concentrador será usado. Este pode ser um Access Point (AP) ou um roteador sem fio. Normalmente, estes dispositivos permitem que a rede sem fio se comunique com os computadores que estão na rede cabeada. Quando este modo de operação está ativo, um identificador especial, denominado Service Set Identifier (ou simplesmente SSID), é usado para permitir que os computadores sem fio encontrem a rede.
- Agora vamos conhecer os três principais padrões tecnológicos que uma rede sem fio pode usar:
- IEEE 802.11a: Esta tecnologia é pouco usada atualmente. Apesar da velocidade de 54 Mbps, o alcance deste padrão é pequeno;
- IEEE 802.11b: Apesar de apresentar baixa velocidade (11 Mbps), este padrão é muito usado em aeroportos e cybercafés (para acessar a Internet não é necessário ter mais que 10 Mbps). Uma das razões para a adoção do padrão está em sua maior área de alcance;
- IEEE 802.11g: Este padrão vem sendo cada vez mais adotado por suportar uma velocidade maior (54 Mbps), permitir uma quantidade maior de usuários conectados simultaneamente e ainda oferecer compatibilidade com o padrão IEEE 802.11b.

Vale ressaltar que as velocidades citadas anteriormente dependem de outros fatores, tais como driver dos adaptadores de rede sem fio, qualidade dos APs envolvidos na solução, agentes que podem causar interferência no sinal, etc. Sendo assim, lembre-se de que estes são valores teóricos.

Depois de conhecer os modos de operação e os padrões tecnológicos, chegou a hora de analisarmos rapidamente os métodos de proteção disponíveis:

- WEP: Esta é a sigla para Wired Equivalent Privacy, um método de proteção que se baseia no uso de uma chave pré-compartilhada para autenticar o cliente. Todos os dispositivos envolvidos devem estar configurados com a mesma chave WEP. A proteção dos dados é feita através da criptografia RC4. Os níveis disponíveis são 40, 128, 154 ou 256 bits, os quais dependem da implementação feita por cada fabricante;
- WPA: Esta é a sigla para Wi-Fi Protected Access. Trata-se de uma evolução do WEP, pois permite autenticar tanto o computador quanto o usuário. Além disso, essa tecnologia suporta o uso de uma chave de criptografia mais complexa do que a utilizada pelo WEP. Sendo assim, conexões wireless protegidas com o WPA são bem mais seguras e difíceis de quebrar. Existem dois tipos de WPA. O WPA padrão, que utiliza criptografia RC4 da mesma maneira que o WEP. Porém, a diferença está no fato de que o WPA adiciona 48 bits no vetor de inicialização para aumentar o comprimento da criptografia. O outro tipo é o WPA2, que usa o CCMP para criptografar o conteúdo dos pacotes de autenticação e é considerado mais seguro que o WPA padrão.



F12. Interface de linha de comando para configurar conexão WLAN.

Independente do tipo de WPA utilizado (WPA padrão ou WPA2), você poderá usá-los de duas formas: WPA Enterprise ou WPA2-Enterprise, onde um servidor de autenticação 802.1x distribui chaves individuais WPA ou WPA2 para usuários que serão identificados como Usuários sem fio, ou no modo WPA-Personal ou WPA2-Personal, que também é conhecido como chave pré-compartilhada (PSK). Neste modo, cada usuário deverá fornecer a senha estabelecida pelo administrador da infra-estrutura de rede.

Autenticação 802.1x

Apesar da possibilidade de proteger os dados que irão trafegar pela rede sem fio, o ideal seria que apenas os clientes devidamente autorizados tivessem acesso à mesma. A tecnologia que permite isso se baseia no protocolo 802.1x. Como ela trabalha na camada 2 do modelo OSI, ou seja, na camada de enlace (link de dados), se não existir autorização de acesso o cliente não terá como acessar nenhum recurso da rede, mesmo que este tenha um nome de usuário e senha para autenticação. Sendo assim, o bloqueio passa a ser feito diretamente no dispositivo.

O princípio de funcionamento é simples. O computador que irá estabelecer a comunicação através do adaptador de rede sem fio deve possuir um certificado digital que o autentique. Ao tentar se comunicar com um AP compatível com esta tecnologia, o cliente fornecerá o certificado de computador instalado. O AP, por sua vez, irá utilizar autenticação RADIUS para validar o certificado do computador (no Windows Server 2003 isso pode ser feito através do Serviço de Autenticação da Internet – IAS). Uma vez validado, o computador poderá iniciar a conversa com os outros dispositivos da rede. Caso contrário, como a comunicação terá sido bloqueada na camada 2, não será possível falar com nenhum outro dispositivo da rede.

Configurando a rede

O processo de configuração de uma rede sem fio pode ser resumido em duas etapas:

1. Configurar o roteador wireless ou AP da forma mais segura possível, de acordo com a documentação do produto. Lembre-se também de que os métodos de proteção escolhidos devem ser suportados pelos demais dispositivos que farão parte da rede sem fio. Aqui vale uma dica importante: apesar de estarmos trabalhando com padrões, já vimos casos em que apenas os dispositivos de um determinado fabricante funcionavam juntos. Sendo assim, procure trabalhar com dispositivos de uma marca específica para evitar surpresas desagradáveis;

2. No computador cliente executando o Windows Vista, você precisará de um adaptador de rede sem fio. Normalmente os notebooks já possuem um, mas se você quiser conectar um computador desktop, precisará obter um adaptador avulso. Existem soluções USB, inclusive. Com o dispositivo instalado fisicamente, você deve fazer a instalação do driver que acompanha o mesmo. Aqui vai outra dica: procure baixar os drivers mais atualizados do site do fabricante do dispositivo. Muitos problemas de conectividade do Windows Vista em redes sem fio, são provenientes de drivers que não funcionam adequadamente. Estando tudo funcionando, basta abrir o assistente de configuração, que pode ser acessado de diversas formas. Basicamente, as maneiras de fazer essa configuração são: através do assistente que pode ser iniciado clicando-se em Iniciar > Conectar a, através da ferramenta de linha de comando NETSH WLAN (**figura 12**), ou ainda através de GPOs que podem ser configuradas de forma centralizada em um ambiente baseado no Active Directory.

Além disso, é importante realizar testes antes de instalar redes sem fio. Principalmente para verificar a qualidade do sinal que será fornecido para as máquinas. Não existe uma receita pronta, é necessário fazer o teste. Se a qualidade do sinal for boa, a tecnologia poderá ser implementada com sucesso.

Conclusão

Chegamos ao final da série de artigos preparatórios para o exame 70-620 – Configuring Windows Vista e acreditamos ter atingido o nosso propósito inicial de abordar todos os tópicos cobrados no mesmo.

Além do conhecimento teórico, recomendamos que o candidato procure conhecer bem o sistema, e fazer o maior número de experiências, a fim de se familiarizar com as novidades inerentes ao Vista, da sua interface mais amigável e sofisticada, o ambiente com segurança melhorada e as ferramentas oferecidas no pacote.

A realização de experiências hoje em dia, com o recurso das máquinas virtuais e várias ferramentas do tipo disponíveis, é bem mais fácil, pois montar laboratórios e fazer simulações através delas é extremamente prático, pois ao criar uma máquina virtual de referência, ou seja, com uma instalação do Windows Vista, podemos ter várias estações rapidamente e em rede. A necessidade de ter mais de um micro, a infra-estrutura (mesmo que simplificada, é coisa do passado, bem como as diversas vezes onde se fazia necessário formatar o HD e reinstalar o sistema, onde boa parte do tempo era consumida sem nenhum ganho.

Ter uma boa experiência com o Vista, suas configurações, novos recursos e ferramentas, sem dúvida pode garantir uma aprovação mais tranqüila no exame. Com as ferramentas de virtualização, ficou mais fácil. Além disso, existe bastante material sobre o sistema disponível no site da Microsoft. Fique atento, pois em breve apresentaremos novidades com relação à preparação para o exame. Bons estudos!

PC

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.sabereletronica.com.br

COOLER MASTER®

Expand Your Imagination

Com Cooler Master você sempre vence!

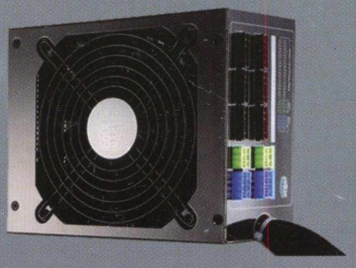
Silêncio, Performance, Refrigeração



Arme-se com o melhor



+



Real Power Pro 850W

+



Hyper 212

COSMOS

www.coolermaster.com.br