

Access Point para redes WiFi em crescimento

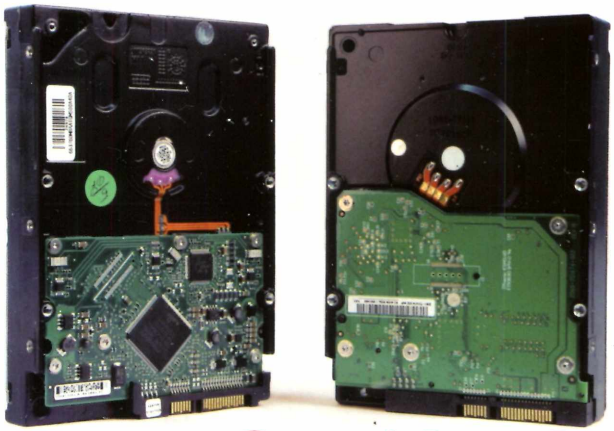
IDF
Os novos chips e tecnologias da Intel

Memórias DDR3
Conheça as especificações



www.revistapcecia.com.br

PC &CIA



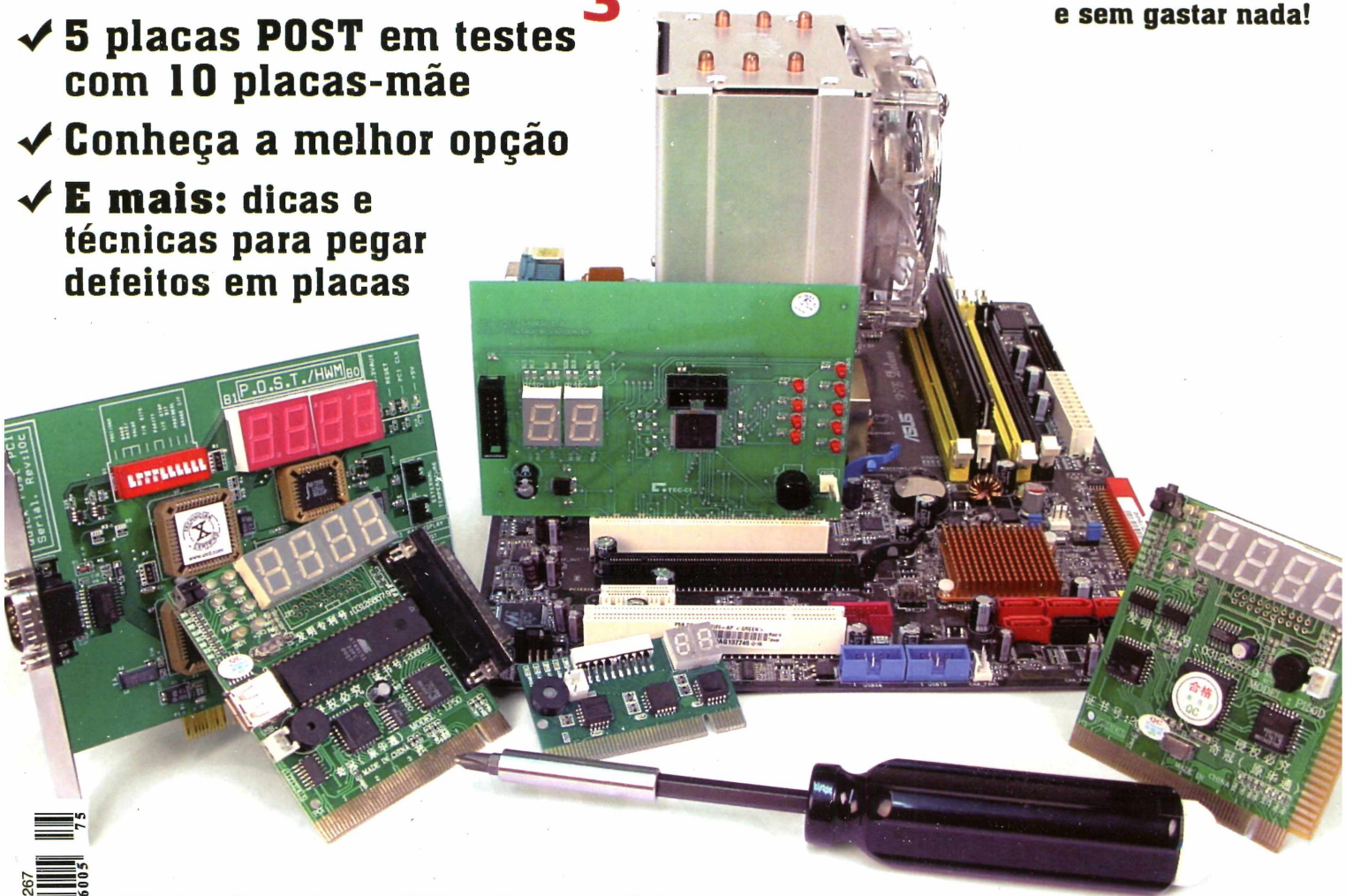
Servidor de Backup em HDs

Aprenda a configurar na prática Para redes Windows e Linux e sem gastar nada!

ANO 7 - Nº 75 - Outubro / 2007 Europa €4,30 - Brasil R$12,90

Manutenção

- ✔ **5 placas POST em testes com 10 placas-mãe**
- ✔ **Conheça a melhor opção**
- ✔ **E mais: dicas e técnicas para pegar defeitos em placas**



Tela Azul no Windows XP

Por que reinstalar o sistema se você pode resolver o problema!?

Gerenciamento de documentos

Solução gratuita para ter os arquivos sempre à mão

ISSN 1519-5267

E se você pudesse ter uma nova alternativa para ferramentas de desenvolvimento ?



Buscando oferecer uma altenativa às placas de avaliação importadas, a **NXP** desenvolveu parcerias locais visando expandir ainda mais a acessibilidade às ferramentas de desenvolvimento de produtos com os **microcontroladores LPC2000**.

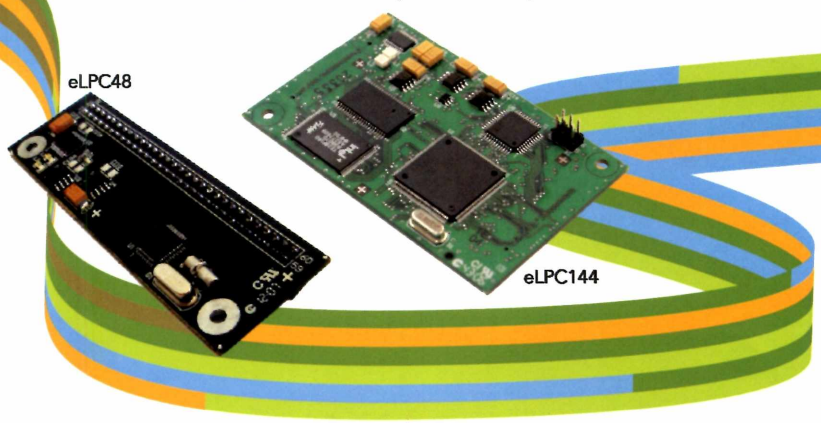
Conheça agora as ferramentas desenvolvidas pela eSystech e LabTools (grupo Mosaico): eLPCs* e McBoard ARM7.1.

Principais características das eLPCs:

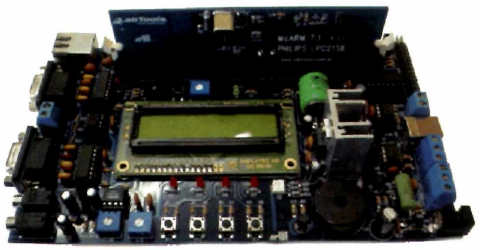
- Aplicam o conceito de SOM (System-on-Module) aos microcontroladores LPC2000.
- Sistema completo de processamento, contendo o LPC2000, cristais de CPU e RTC, reguladores de alimentação e quando for o caso, memórias Flash e RAM externas.
- Placa-mãe com conectores seriais, conexões para fonte de alimentação, conector MICTOR para funções de Trace, JTAG (20 pinos), JTAG DB-25 para conexão com porta paralela, bateria de Lítio.
- Acompanha CD contendo um pacote de softwares (Sistema operacional da eSysTech - X Real-Time Kernel; Versão demo do compilador IAR; Conjunto completo de ferramentas GNU GCC; Datasheets de todos os componentes do módulo SOM; User Guide e esquemático da placa-mãe).

Principais vantagens das eLPCs:

- Pode ser aplicado em projetos desenvolvidos pelo próprio cliente utilizando o conceito de módulo.
- Conexão com placa-mãe através de conectores denso ou barra de pinos.
- Flexibilidade para desenvolver com extrema rapidez protótipos de validação de aplicação muito requisitados em produtos de licitação e demonstração em feiras.



McBoard ARM7.1



Principais características da McBoard ARM7.1:

- Composta de uma placa-filha, ou CPU, baseada no CI LPC2138.
- Na placa-mãe residem os conectores para todas as principais interfaces seriais e analógicas.
- Display LCD alfanumérico.
- SuperCAP para manutenção do relógio RTC.
- Alto falante tipo Buzzer.
- Memória e sensor de temperatura controlados por barramento I²C.
- Porta para conexão de emulador JTAG.

Principais vantagens da McBoard ARM7.1:

- Livro de teoria e prática sobre a utilização da placa ("Microcontroladores ARM7 - O Poder dos 32 bits" - Ed. Érica).
- A partir desta placa de avaliação o projetista tem à disposição todos os principais recursos da linha LPC2000 podendo inclusive validar uma série de funcionalidades na fase inicial de projeto antes iniciar o protótipo.

Para cotações e disponibilidade da família de microcontroladores LPC2000, consulte nossos distribuidores autorizados.

Distribuidores:

ARROW BRASIL S/A (11) 3613-9300

AVNET do Brasil (11) 5079-2150

KARIMEX (11) 5189-1900

FUTURE ELECTRONICS (19) 3737-4100

Parceiros:

eSysTech Embedded Systems Technologies (41) 3029-2960

LabTools Mosaico Didactic Division (11) 4992-8775

www.nxp.com

* As placas eLPCs estarão disponíveis para compra a partir da 2a. quinzena de Mai/07.

FCP Publicidade

Editora Saber Ltda.

Diretores
Hélio Fittipaldi
Thereza Mozzato Ciampi Fittipaldi

PC &CIA

www.revistapcecia.com.br

Editor e Diretor Responsável
Hélio Fittipaldi

Editor de Tecnologia
Fernando Ramos da Silva

Conselho Editorial
Newton C. Braga, Orlando Gomes Ferreira

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

Auxiliar de Redação
Claudia Tozetto
Fabieli de Paula

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

Produção
Yassari Gonçalo

VENDAS DE PUBLICIDADE

André Zanferrari, Carla de Castro Assis,
Ricardo Nunes Souza

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

Impressão
Prol Editora Gráfica Ltda.

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

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

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

Associada da:

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

anatec 20 anos
www.anatec.org.br
Associação Nacional das Editoras de Publicações Técnicas, Dirigidas e Especializadas.

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

Oportunidade para empreendedores



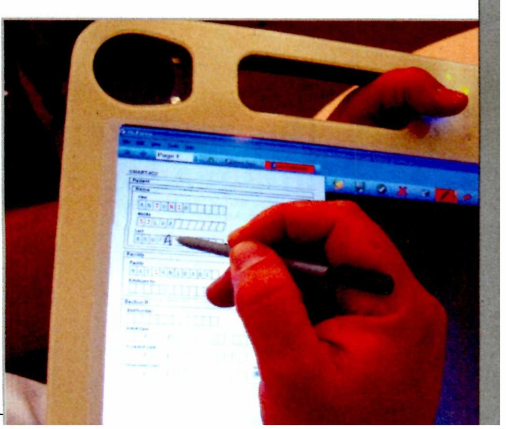
Dias atrás levei um susto ao ver uma senhora de idade avançada caindo no chão devido a um choque provocado por um motorista desatento que dava ré em seu carro para sair. Graças a Deus, nada de pior ocorreu e a simpática senhora, embora um pouco abatida, não precisou sequer ser levada ao hospital. Confesso que na hora os pensamentos mais diversos passaram pela cabeça e você já vai entender o porquê.

Se ela requeresse cuidado médico urgente, será que trazia consigo alguma informação referente ao médico da família, histórico de saúde ou, quem sabe, o telefone de algum familiar junto ao qual essas informações pudessem ser obtidas? E mesmo que encontrássemos o telefone, será que o filho, por exemplo, conseguiria respondê-las de imediato? Agora pense no apuro que médicos e enfermeiros passam e como a falta de informações aparentemente simples pode, na melhor das hipóteses, retardar um atendimento e por conta disso acarretar em alguma sequela. Por que não pensarmos num conceito de cartão digital de saúde que, a exemplo do cartão do banco, possa ser convenientemente levado conosco para onde formos? Indo um pouco além, a equipe de resgate poderia ter um leitor de cartões e ali mesmo, no próprio veículo, já saber quais as providências iniciais a serem tomadas e simultaneamente transmitir as informações ao hospital ao qual o paciente será encaminhada, via link de satélite, GPRS ou, por que não, WiMAX. Ao chegar ao hospital, tanto a equipe médica quanto as acomodações já estariam prontas e seguramente ela estaria em melhores condições para um final feliz.

Felizmente, isso não é totalmente sonho, na verdade já funciona dessa maneira em alguns hospitais mundo afora e aos poucos começa a ser cogitado em hospitais de primeira classe aqui no Brasil. O fato a ser destacado é que sob o ponto de vista tecnológico não há nada de absurdo, ou seja, estamos falando de tecnologias amplamente disponíveis. O que precisa é desenvolver a inteligência do negócio e fazer um trabalho de consultoria. Com um pouco de criatividade, é possível desenvolver acessórios médicos muito interessantes, a exemplo de um *tablet* com reconhecimento de escrita operando sobre formulários que alimentam servidores de banco de dados e, conseqüentemente, toda a cadeia de produção dentro de um hospital, por exemplo. Tive a oportunidade de ver um *tablet* desses baseado na arquitetura de referência MCA (Medical Clinical Assistance) da Intel, e fiquei surpreso com os trabalhos que estão sendo desenvolvidos nesta área (mais detalhes em **www.intel.com/healthcare/ps/mca/index.htm**).

Achei oportuno relatar o caso aqui para reforçar uma vez mais as oportunidades que o acelerado progresso tecnológico em nossa área têm aberto. Se você pesquisar, verá que esse mercado ainda é pouquíssimo explorado e que há um grande potencial para o desenvolvimento de soluções. Milhões de dólares são desperdiçados todo ano com remédios e exames que poderiam ser evitados devido a consultas realizadas sem prontuário, por exemplo (25% hoje, segundo um estudo apresentado pela Intel).

Mas o complicado mesmo no Brasil é encontrar os empreendedores. Em nossa última pesquisa veiculada no newsletter, apenas 9,3% disseram que a principal motivação para fazer uma faculdade era montar negócio próprio. Para a maioria, ainda o fazem para "constar no currículo para obter um emprego".



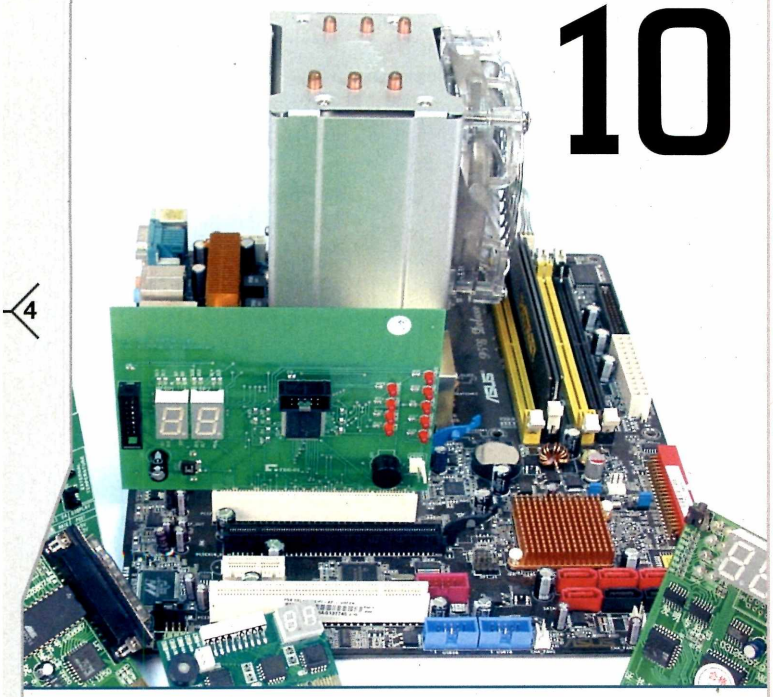
De nossa parte, a linha editorial continuará focando em desenvolvimento. Semelhantemente a outros projetos já publicados aqui, nesta edição estamos apresentando uma placa POST, uma ferramenta que faz parte do kit básico de todo profissional da área de suporte. Através dela pretendemos explorar alguns conceitos mais técnicos sobre hardware e você, mais uma vez, está convidado a participar com seus comentários.

Fernando Ramos da Silva
fernando@editorasaber.com.br

HARDWARE

7 Mercado de Workstations

Manutenção em placas-mãe 10



Manutenção de PCs 14

Memórias DDR3 24

26 Desenvolvendo soluções integradas - Parte 2

TESTES

HDs de 750 GB 30

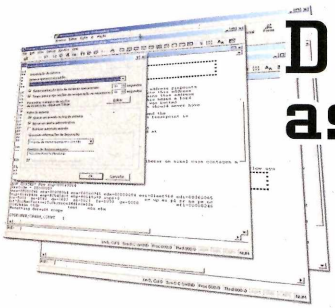


REDES

Access Point com função Roaming 34



SISTEMAS OPERACIONAIS



Decifrando as BSOD 36

42 Pack de ferramentas Windows

44 Gerenciamento de documentos com software livre - Parte 1

Certificação Microsoft MCTS - Parte 3 52

56 Servidor de Terminais com segurança

5 Segurança High-Tech: Procura-se um profissional de segurança da informação

6 A vez do leitor

Procura-se um profissional de segurança da informação

Parte 2



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

A importância que a área de segurança da informação vem ganhando nos últimos tempos deve-se, entre outros aspectos, ao fato de que o uso de ferramentas de software e hardware conectados por meio de tecnologias de rede estão presentes como infra-estrutura fundamental de parte considerável dos ambientes corporativos. Vírus, *worms*, *pishing*, *firewalls*, *proxy*, *trojan horse* (ou cavalo de tróia), DMZ e *spam* são alguns dos termos que extrapolaram os meios técnicos e hoje transitam livremente nas conversas de gerentes, de coordenadores e até mesmo de usuários domésticos.

Não é raro encontrar empresas, seja da iniciativa pública ou privada, cujo maior bem não se encontra num depósito ou estoque, mas em servidores. Daí a preocupação em manter os dados armazenados disponíveis, íntegros e confidenciais, quando necessário. Diante dessa realidade, as perguntas do mês anterior persistem: onde encontrar bons profissionais de segurança? Por que existem tantos profissionais de computação alheios às questões de segurança?

A discussão parece ter início já no ambiente acadêmico dos cursos de computação. Parcela considerável dos problemas de segurança são oriundos de falhas encontradas em softwares que são, local ou remotamente, exploradas pelos atacantes. É certo que se faz necessário reafirmar uma realidade que muitas vezes parece ser ignorada: a de que não existe software perfeito, 100% seguro e livre de problemas e falhas. E a lógica parece ser muito simples.

Quem produz software são pessoas que por sua vez não são perfeitas. Soma-se a isso o fato de que o nível de sofisticação dos softwares e o número de recursos vêm aumentando consideravelmente, o que significa elevar a probabilidade de erros a serem posteriormente explorados por malfeitores digitais.

Embora seja utópico pensar na produção de softwares livres de falhas, muitas medidas, técnicas e recursos podem ser empregados para minimizar o número de *bugs*. Em um primeiro momento, para que um software tenha um bom nível de segurança é necessário que esse quesito seja considerado desde o momento de sua concepção.

Um caso interessante a ser citado nesse sentido é o dos servidores de email Sendmail e Postfix. O primeiro, sistema padrão para a configuração desse tipo de serviço em muitos ambientes Unix há alguns anos, veio perdendo espaço com o passar do tempo por um motivo simples: tinha muitos problemas de segurança e sempre estava no topo das listas de vulnerabilidades, produzidas por instituições como o CERT (*Computer Emergency Response Team*). Por outro lado, o Postfix, sistema que vem tornando-se cada vez mais popular, foi projetado levando em consideração rígidos requisitos de segurança. Outro aspecto interessante é que existem inúmeras ferramentas para gerar códigos executáveis livres de problemas comuns. Entretanto, são raros os cursos onde esse aprendizado faz parte das ementas das disciplinas técnicas de análise de sistemas, linguagens de programação, bancos de dados, dentre outros. É dada ênfase em como resolver problemas, mas nunca em como resolvê-los de maneira segura.

Quando se consegue vencer toda aí vem a última dificuldade: os poucos profissionais competentes na área de segurança são disputados a peso de ouro por médias e grandes empresas que já tomaram ciência que é preciso ter uma equipe de qualidade para proteger suas informações e infra-estruturas computacionais.

Existem várias técnicas conhecidas para a solidificação da prática de programação segura. Entretanto, novamente, é um item que anda às margens no processo de formação profissional. Sendo essa a realidade da maioria das instituições de ensino superior, o que dizer dos "cursinhos de esquina" que ensinam fundamentos de programação?

Existem treinamentos de segurança fora das universidades. Entretanto, aqueles que são de qualidade ainda requerem um alto investimento financeiro, por conta dos custos que podem aumentar significativamente quando se pretende fazer algum treinamento fora do País. No Brasil, como em qualquer outro lugar, é preciso estar atento aos treinamentos que limitam-se a mostrar a utilização pura e simples de ferramentas de ataque e defesa como se essa fosse a solução definitiva para formar bons profissionais. Além das ferramentas, um profissional de segurança necessita ter sólidos conhecimentos a respeito de protocolos, criptografia, normas de segurança, redes de computadores e muitos outros assuntos os quais não podem ser resumidos em poucas horas de sala de aula, sob pena de formar profissionais cuja capacidade não vai além do que o adestramento nas ferramentas lhe permite.

Quando se consegue vencer tudo isso aí vem a última dificuldade: os poucos profissionais competentes na área de segurança são disputados a peso de ouro por médias e grandes empresas que já tomaram ciência que é preciso ter uma equipe de qualidade para proteger suas informações e infra-estruturas computacionais. Resumidamente, levar a segurança a sério requer um investimento compatível.

Até a próxima! **PC**

Placas de Vídeo DirectX 10

Constantemente acompanho os testes publicados na PC&CIA, que ao meu ver é a melhor revista de hardware da atualidade. Gostei do teste sobre as VGA's publicado na edição 74, mas gostaria de saber por que não foi usado um driver mais recente para as placas da ATI/AMD. Imagino que isto deve ter sido decisivo para o desempenho fraco e pelo fato do 3DMark 2006 não rodar. Sugiro também que vocês explorem o potencial de aceleração de vídeo via hardware das placas ATI, que codifica os formatos MPEG-2, MPEG-4, DivX, WMV9, VC-1 e H.264. Creio ser este o principal atrativo da série HD 2000.

Ironildo Joabe

Agradecemos seu contato e comentários sobre a revista. Na época dos testes, as suítes de drivers disponíveis eram realmente o Catalyst 7.6 e o Forceware 158.24. Ocorre que entre o fechamento da matéria e o lançamento da revista, há um intervalo de tempo de pelo menos 15 dias. Além disso, é impressionante o ritmo em que os fabricantes de GPUs estão lançando novos drivers de vídeo. É preciso ficar atento a isso e, de nossa parte, publicar novos testes em breve. Aliás, pretendemos fazer isso em relação à decodificação acelerada pela GPU e nos mais diversos formatos de vídeo. Conforme você bem comentou, este é um nicho interessante para essa nova safra de placas DX10 porque reduz o consumo de energia e abre um precedente também para economizar na compra do processador.



Placas-mãe para Core 2 Duo

Não consegui entender por que as placas da Asus, tidas como uma das melhores para Core 2 Duo, não foram testadas nesta reportagem. Qual o motivo do preconceito?

David Vieira
Belo Horizonte – MG

Elas não foram testadas desta vez porque não chegaram a tempo. Mas, tal como fizemos em matérias comparativas publicadas anteriormente, elas deverão entrar nos próximos testes.

Consumo de energia

Primeiramente, parabéns pela revista. Sem sombra de dúvida, a melhor no mercado de PCs no Brasil. A minha pergunta é simples: gostaria de saber qual seria o consumo de energia num computador. Se a soma dos componentes do computador é de 300W, por exemplo, tanto faz se eu tiver uma fonte de 400W ou uma de 600W?

Walter Müller Junior
São Caetano do Sul - SP

O consumo da máquina é dado em função da potência consumida por cada componente mais a ineficiência da fonte, que durante sua operação desperdiça parte da energia consumida sob a forma de calor, principalmente. Por exemplo, se o consumo é de 300W e a fonte tem um rendimento de 80%, isso significa que o consumo na rede elétrica será de 300 / 0,8, ou 375W. Em relação à potência da fonte, o exemplo dado, embora coerente, não é válido porque cada fabricante de fonte é livre para desenhá-la segundo o perfil de potência que bem entender. Devido ao fato da fonte atuar sobre várias saídas de tensões, pode acontecer inclusive do modelo de 400W atender à necessidade de um PC, enquanto a de 600W, não. Por quê? Simples, vamos considerar um Pentium D operando em overclock e demandando 22A da saída 12V2 da fonte, que é a responsável pela alimentação neste caso. Enquanto a de 400W pode estar baseada em um projeto capaz de fornecer toda a potência em uma saída, independente das demais, e nesse caso suportar este processador, a de 600W pode ter um projeto com várias saídas de +12V, limitada a 20A no 12V2 e que não prevê a possibilidade de aproveitar a energia não usada nas demais saídas para uma em especial que esteja consumindo mais. O que, aliás, é o caso mais comum. Por último, supondo que essas duas fontes citadas tenham projetos idênticos, a de 600W, apesar de provavelmente mais cara, deve ser escolhida por duas razões: primeiro, porque é recomendável garantir uma reserva de potência de 30% para comportar futuras expansões e também em função do menor estresse sobre os componentes internos; segundo, porque trabalhando com uma folga maior o rendimento da fonte tende a ser maior e, conseqüentemente, seu dinheiro retornará sob a forma de menores gastos com conta de luz.

Servidores e Workstations Reais

Gostaria de saber se os chipsets de placas-mãe para desktops LGA775, que suportam os processadores Core 2 Duo e Quad, também suportam os Xeon das séries 3000 e X3200 (Dual e Quad-Core). Se sim, poderia citar alguns chipsets compatíveis?

Marcelo A A Prado
Administrador de Empresas
Uberândia-MG

Os Xeon Dual-Core da série 3000 possuem as mesmas especificações dos Core 2 Duo da série E6000, e os Quad-Core da série X3200, por sua vez, também o são em relação aos Core 2 Quad Q6000. Todos são mecanicamente compatíveis com o socket LGA775 e vários modelos possuem a mesma cotação. Em resumo, as atuais placas de desktop devem suportar os Xeon sem maiores problemas, porém, isto depende de revisão de BIOS. Até o momento desconhecemos um fabricante que tenha liberado uma versão que os suporte.

O posicionamento de mercado desses Xeon, na visão da Intel, é para os servidores de entrada de linha, monoprocessados (1 socket na placa-mãe). Como tal, a empresa recomenda os chipsets 3000 e 3010, os quais trazem como diferenciais, em relação aos modelos para desktop, alguns recursos extra dentro do conceito de indústria denominado RASUM (Reliability, Availability, Serviceability, Usability e Manageability). Em resumo, significa que esses chipset provêem as condições ideais para uma maior confiabilidade, disponibilidade, capacidade de receber manutenção, usabilidade e facilidade de gerenciamento do servidor. Continuaremos pesquisando sobre este assunto para, em breve, publicaremos as descobertas e, quem sabe, um teste.

Mercado de Workstations

Para falar sobre o assunto, conversamos com Antonio Julio, Diretor para o Grupo de Workstations da Dell. Ele é responsável pelo desenvolvimento de negócios a nível mundial, atuando na identificação das necessidades de clientes e na determinação dos *roadmaps* que as contemple.

Fernando Ramos

PC&CIA: Qual é a participação da Dell no mercado atual de workstations?

Antonio: *Segundo o IDC, foram comercializadas cerca de 666 mil unidades no último trimestre fechado em Junho (Q2), o que representa um crescimento de 19,3% sobre igual período de 2006. Desse total, a Dell participou com 45,6%.*

PC&CIA: Há alguns anos, esse mercado era caracterizado por máquinas de arquitetura RISC e custo elevado. Como está hoje?

Antonio: *Vemos uma acelerada migração para hardware x86 com processadores Xeon e Opteron (PWS – Personal Workstations). De 1,5 bilhão de dólares faturado em Q2, as TWS, como são conhecidas as tradicionais workstations Unix com processadores RISC ou Itanium, foram responsáveis por apenas 2,8%, com um total de 10746 máquinas.*

PC&CIA: Opteron ou Xeon?

Antonio: *96% das máquinas x86 vendidas foram com Xeon. A AMD teve a oportunidade para se consolidar com uma plataforma boa, que consome pouca energia e gera menos calor, aspectos estes fundamentais nos data centers. Mas a partir de Q2 de 2006 a empresa praticamente não se mexeu para responder ao lançamento dos Xeon Dual-Core Woodcrest, e depois novamente em Novembro, diante da chegada do primeiro Xeon Quad-Core (série 5300). É importante destacar que estamos considerando máquinas two-way, isto é, com até dois processadores na placa-mãe. Até porque ainda há muitas aplicações nessa área que são tipicamente single threading, a exemplo de Autocad, Pro Engineer e Catia.*

A plataforma Windows continua sendo mais usada, sobretudo em aplicações de engenharia, DCC (criação de conteúdo digital) e no setor financeiro, com uma penetração de 85%. Os Unix e derivados se concentram em aplicações científicas e geofísica, por exemplo.

PC&CIA: Quais são os principais mercados para as workstations?

Antonio: *Primeiro, vem o de engenharia, com programas do tipo CAD e CAM respondendo por 39%. Na seqüência, vem o de DCC com ilhas de criação de filmes e renderização. Outros segmentos que estão crescendo são os de aplicações científicas e geofísica. Munidas de GPS instalados em brocas e workstations fazendo análise geofísica em tempo real, empresas como a Petrobrás conseguem reduzir significativamente o tempo para encontrar uma nova jazida de petróleo. Na área médica, o cirurgião pode ter uma visão 3D do cérebro e fazer as simulações necessárias antes de realizar uma cirurgia. Reduz-se o tempo e a precisão é maior.*

PC&CIA: O poder computacional da plataforma x86 permitiu às PWS substituírem as TWS, mas abriu espaço para novos competidores. Com componentes custando cada vez menos e ampla disponibilidade no mercado local de distribuição, até mesmo um pequeno integrador pode lançar suas workstations. Como competir neste cenário?

Antonio: *Apesar do hardware base, como processador e placa de vídeo, ser o mesmo, é preciso entender que há diferenças significativas. Não desenhamos uma máquina genérica e tentamos promovê-la a diferentes nichos de mercado. Todo o projeto, desde o chipset da placa-mãe até a vazão de dados nos barramentos de I/O, é otimizado para entregar a performance requerida pela aplicação do cliente. Temos placas-mãe que suportam até 64GB de RAM, por exemplo. Além disso, as placas de vídeo utilizadas em nossas máquinas vão com drivers próprios, otimizados, e não com os drivers padrão do fabricante do processador gráfico (nVidia e ATI).*

Outra diferença fundamental diz respeito às aplicações. Quando entregamos uma workstation, temos compromisso com todo o conjunto, não apenas com o hardware. Nossos equipamentos são certificados para operar com as aplicações dos ISV (desenvolvedores de software). Realizamos algo em torno de 400 a 450 certificações por ano. Se a PTC faz uma modificação no Pro/ENGINEER, a Dell submete o equipamento a uma nova certificação. Se um cliente nos liga e relata um problema com este software, o técnico da Dell tem condições de oferecer um resultado melhor no pós-venda porque conhece ambos, hardware e software. Em resumo, esforçamo-nos para vender uma solução que permita ao cliente trabalhar e ter a tranqüilidade de uma estrutura por trás que o ampare, quando necessário.

PC&CIA: Qual é o principal desafio da Dell?

Antonio: *A educação. Hoje, a plataforma x86 ocupa uma posição consolidada, é padrão de mercado e tem custo acessível. Se no passado o desafio era migrar grandes clientes para x86, a discussão atual é entre x86 profissional e PCs. A época de domínio das TWS fez com que muitos usuários se vissem restritos aos PCs por não terem poder de compra. O problema é que muitos desses usuários de pequenas empresas ainda não reveram esse conceito e, conseqüentemente, estão aquém de seu potencial ao rodarem um Autocad ou 3ds Max, por exemplo, em um PC. Embora seja difícil quantificar a penetração dos chamados white box e equipamentos oriundos do mercado cinza, há margem para dobrar o mercado atual das PWS.*

Especial Intel Developer Forum

Roberto Luiz R. Cunha

Entre os dias 18 e 20 de Setembro, a Intel realizou sua edição do IDF em San Francisco, nos EUA, e estivemos lá conferindo os detalhes dos próximos lançamentos. Confira aqui uma prévia da cobertura.

Microarquitetura 45nm Nehalem

Para 2008 a Intel anunciou uma nova microarquitetura denominada Nehalem, a qual será dinâmica e escalável (figura 1). A proposta é permitir a obtenção tanto de desempenho sob demanda quanto uma ótima relação entre preço/desempenho/eficiência energética para cada tipo de plataforma. Ela pretende atender a esses requisitos através de:

- Gerenciamento dinâmico de núcleos, *threads*, memória cache, interfaces e consumo de energia;
- Tecnologia que permite o processamento de quatro instruções por ciclo de clock;
- Multi-Threading simultâneo, é o retorno da tecnologia HT (Hyper-Threading) do Pentium 4;
- Utilização de instruções SSE4 mais um conjunto de instruções ATA;
- Controladora de memória integrada e cache compartilhado entre os núcleos;
- Desempenho escalável entre uma e dezesseis (ou mais) *threads* e entre um e oito (ou mais) núcleos.



F1. Apresentação do wafer Nehalem, de tecnologia 45 nm, feita por Pat Gelsinger (à esquerda), vice-presidente e gerente geral do Digital Enterprise Group, e Jim Brayton, gerente do projeto Nehalem

Centrino Montevina

A plataforma Montevina representa a quinta geração da família Centrino. Composta pelo chipset de codinome "Cantiga", mais o Southbridge ICH9M, ela irá suportar os processadores Core 2 de 45nm e as memórias DDR3-800, que possuem uma eficiência energética superior às memórias DDR2-800. Está previsto para essa plataforma a adoção da solução combo wireless, integrando tanto uma interface Wi-Fi quanto uma interface WIMAX.

Intel Threading Building Blocks

O objetivo do Intel Threading Building Blocks consiste em simplificar a programação voltada para processadores Multi-Core.

Apresenta uma biblioteca C++ cuja função é abstrair e esconder a complexidade do gerenciamento de *threads* quando vários núcleos estão disponíveis. Dessa forma, o programador especifica tarefas concorrentes e a biblioteca as mapeia entre as *threads*, buscando obter a melhor eficiência no uso da memória cache e balanceamento de carga entre os núcleos disponíveis. Essa biblioteca pode ser utilizada junto com outros pacotes de gerenciamento de *threads*, a exemplo do OpenMP.

A biblioteca Intel Threading Building Blocks faz parte dos pacotes Intel Compilers 10.0 Professional Edition, os quais apresentam a Intel Integrated Performance Primitives (C++), que por sua vez inclui funções de natureza *thread-safe* para multimídia, comunicações e processamento de dados. Além disso, há a Intel Math kernel Library (C++ e Fortran), cujo objetivo é acelerar aplicações de computação intensiva com funções matemáticas paralelizáveis e altamente otimizadas. Os desenvolvedores podem baixar versões de avaliação desses softwares no site **www.intel.com/cd/software/products/asmona/eng/219690.htm**.

Virtualização do hardware

Aproveitamos o evento para conhecer um pouco mais do lançamento feito recentemente da tecnologia vPro, que tecnicamente responde pela sigla AMT (Tecnologia de Gerenciamento Ativo) e agora chegou à versão 3.0. Desta vez a sigla introduzida foi a VT-d, que permite que os periféricos sejam diretamente atribuídos às máquinas virtuais (figura 2). Até então, com o VT-x, apenas o processador facilitava a operação dos softwares gerenciadores de virtualização, a exemplo do Xen e VMware Server.

Para isso, os processadores receberam um novo conjunto de instruções específicas para virtualização, conhecido como TXT (Trusted Execution Tecnology, ou Tecnologia de Execução Confiável). Até o momento, apenas três modelos de Core 2 Duo com suporte ao TXT foram lançados: E6550 (2.33 GHz), E6750 (2.66 GHz) e E6850 (3 GHz). Do lado da placa-mãe, para seu sistema ser compatível com o VT-d ele deverá ter o chipset Q35 na combinação com o Southbridge (Ponte Sul) ICH9-DO e controlador de rede Gigabit 82566DM. Uma placa-mãe que já atende a esses requisitos é a Intel DQ35JO (**http://download.intel.com/support/motherboards/desktop/dq35jo/sb/d9003701_en.pdf**), que no exterior pode ser encontrada por aproximadamente US$ 150.

USB 3.0 ou Superspeed USB

O padrão anunciado USB 3.0 representa uma evolução do atual padrão USB, devendo portanto apresentar compatibilidade com os dispositivos USB 2.0, ao mesmo tempo que deverá atingir um aumento de, pelo menos, 10x no desempenho da interface atual. Será possível atingir 5 Gbps, aproximadamente!

Além disso, deve apresentar um aumento na eficiência energética para todas as plataformas e suportar virtualização de dispositivos.

Alguns requisitos esperados são rápida sincronização quando conectado, o que reduzirá o tempo de espera do usuário. O sistema deve permitir o download de um filme em alta definição, de 27 GB, em 70 segundos.

Para otimizar o consumo de energia, os dispositivos devem apresentar menor consumo em estado ativo e em espera, além do que serão eliminadas as consultas periódicas entre os dispositivos conectados (*device polling*). Um dispositivo somente será ativado quando ele for transmitir ou receber dados válidos. Na figura 3 podemos ver os dispositivos que irão se valer da maior velocidade do padrão USB 3.0.

Silicon Photonics

A Intel se empenha em pesquisas na área de fotônica visando o desenvolvimento das tecnologias que irão formar os processadores do futuro.

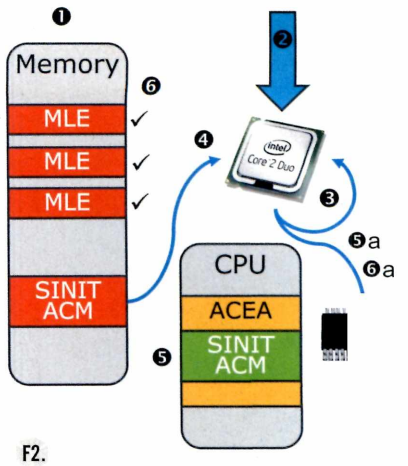
Os processadores da era Pentium eram otimizados para velocidade bruta com execução de uma única *thread* por vez e fora de ordem. Esse processo leva a uma baixa eficiência energética, já que a operação a altas freqüências força o consumo de elevadas potências e alta geração de calor.

Os chips atuais utilizam diversos núcleos que promovem um balanço no desempenho, seja processando uma *thread* simples ou múltiplas *threads*. Esse processo permite ganhos de eficiência porque o núcleo opera a freqüências mais baixas e, conseqüentemente, consome menos energia e gera menos calor. Além disso, utiliza técnicas mais avançadas de redução de consumo.

Segundo estimativas da empresa, dentro de um prazo entre 5 a 10 anos os processadores utilizarão dezenas ou centenas de núcleos conectados em rede. Isso mostra a migração de uma filosofia otimizada para velocidade para outra com enfoque na relação desempenho/watt.

Fotônica é a tecnologia de emissão, transmissão, controle e detecção de luz (fótons), também conhecida como opto-eletrônica.

Hoje, a maioria dos dispositivos opto-eletrônicos é feita de materiais raros, cujo processamento apresenta custo elevado e necessitam de encapsulamentos complexos. Para a Intel a pesquisa em fotônica visa desenvolver dispositivos utilizando silício e técnicas padronizadas de produção em larga escala existentes nas fábricas atuais.

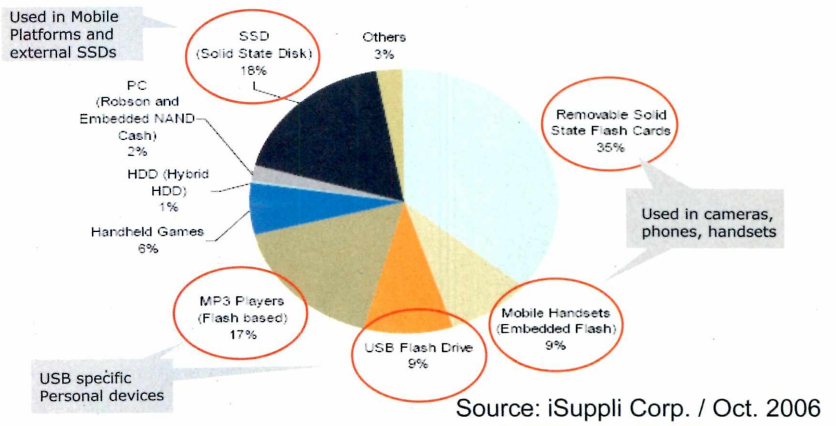


F2. Com apoio do chip TPM na placa-mãe, somente sessões autenticadas de software terão acesso à RAM. Será o fim dos *malwares*? Testes já podem ser feitos com Xen.

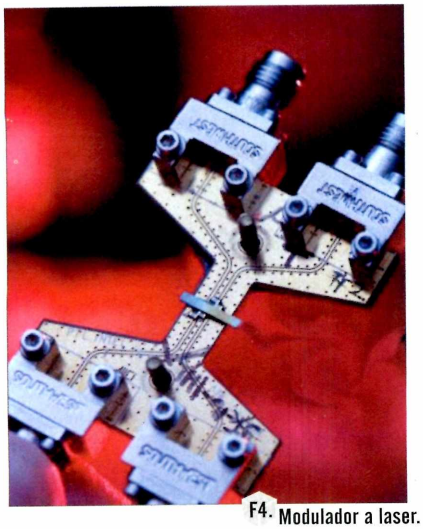
Durante o IDF, a empresa apresentou um modulador a laser feito de silício, com capacidade de transmissão de dados a 40 Gb/s. Trata-se do modulador laser a silício mais rápido atualmente (figura 4).

Um dispositivo como esse poderá vir a ser utilizado como I/O em futuras máquinas com desempenho de supercomputadores (figura 5).

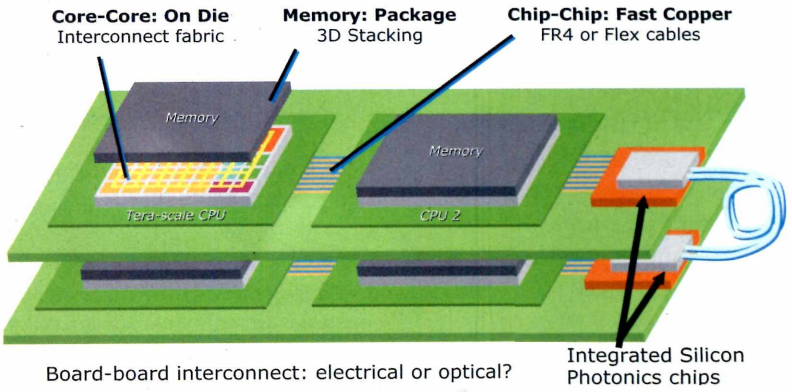
PC



F3. Imagine os novos HDs de estado sólido (SSD) com interface USB 3.0. Será verdadeiramente um fôlego novo para as máquinas.



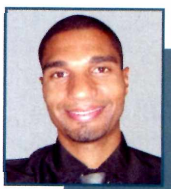
F4. Modulador a laser.



F5. Arquitetura pretendida para os futuros processadores.



Manutenção em placas-mãe



Vanderson Nascimento
Formado em eletrônica, possui 7 anos de experiência com manutenção de placas e já atuou em grandes fabricantes da indústria local.

A placa-mãe é o principal componente de um computador, é nela que todos os demais dispositivos estão conectados. Muitos de nós possuímos alguma placa-mãe que parou de funcionar e só não foi jogada fora ainda porque ficamos com dó ou alimentamos esperanças de que um dia ela volte a funcionar. De um dia para outro simplesmente ligamos o computador e a imagem não aparece mais no monitor, ou o sistema não é carregado corretamente, trava, enfim, muitas são as possibilidades de problemas. Nesta matéria, apresentaremos algumas dicas para evitar ou reparar prováveis defeitos com a placa-mãe.

Ao ser chamado para uma entrevista de emprego descobri que era uma empresa onde além de fabricar, também consertava placas-mãe de computador. Surpreso, perguntei à pessoa que me entrevistava: Mas é possível consertar uma placa-mãe? No Brasil? Sim, ele me respondeu. Sei que hoje esta pergunta seria ridícula, mas apesar do conserto de placas-mãe ser muito comum em outras partes do mundo, no Brasil ainda era algo muito raro e pouquíssimas empresas prestavam este serviço.

Além disso, as empresas sempre foram muito limitadas, não sendo capazes, por exemplo, de realizar a troca de um chipset devido ao fato deste usar um encapsulamento do tipo BGA (Ball Grid Array) e a máquina para tal ser muito cara para o mercado brasileiro. Além da falta da máquina extratora e soldadora de chips BGA, quem disse que era fácil conseguir um chip para substituição? Sempre foi difícil realizar esta compra por conta do preço, disponibilidade, taxas de importação, etc.

O intuito desta matéria não é o de ensinar a retirar e soldar chips BGA, mas o de apresentar algumas técnicas aprendidas na prática, que podem auxiliá-lo a analisar uma placa-mãe com defeito mesmo que você não disponha de equipamentos sofisticados. Além disso, acreditamos que ela servirá para derrubar alguns mitos do tipo "não compre uma placa-mãe onboard, pois se algum dispositivo queimar você perderá toda a placa". Veremos que atualmente esta e outras questões são facilmente contornadas e sem a necessidade de comprar uma placa nova. Na pior das hipóteses, esta placa poderá ser encaminhada a algum RMA Center e provavelmente terá conserto.

Primeiro Passo

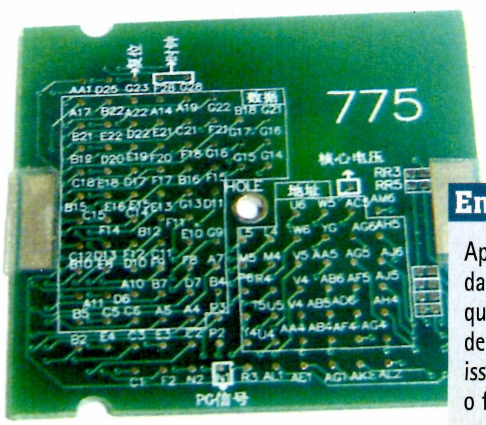
Antes de partir efetivamente para a análise de placa-mãe, temos que ter em mente que

ela não funciona por si só. Para o bom funcionamento de todo seu sistema, é necessário que o conjunto esteja funcionando bem, a começar pela fonte de alimentação. Uma fonte de má qualidade interfere diretamente no funcionamento de todo seu computador. Sinais elétricos irregulares e com altas e constantes variações podem danificar a placa-mãe, processador, memória ou outro dispositivo conectado a ela. Além disso, pode gerar instabilidade e travamentos no sistema, como, por exemplo, danificar as portas de comunicação (serial, paralela, etc).

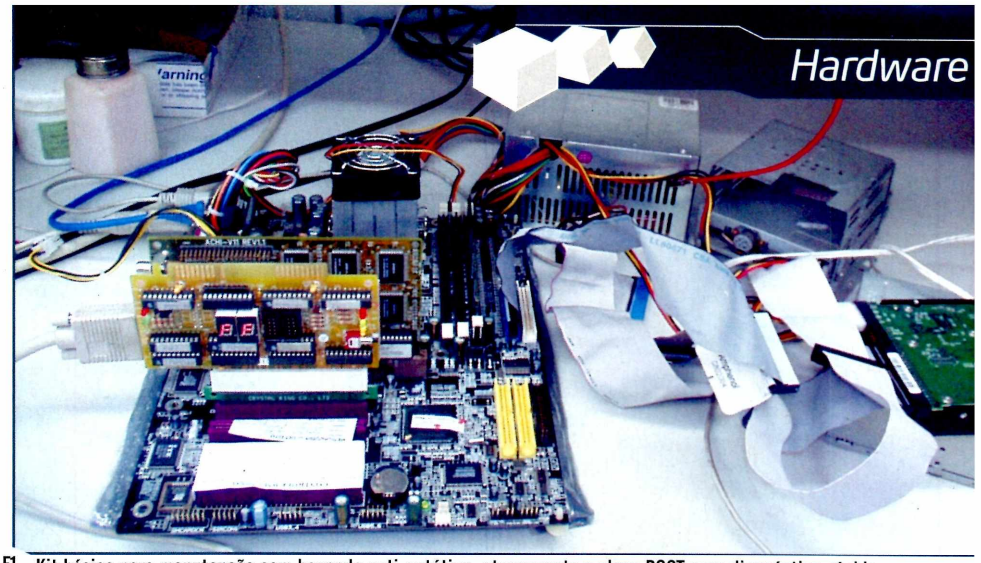
Procure fazer uma boa escolha na hora de comprar uma fonte, a fim de evitar problemas futuros ao seu computador. Dê preferência a uma fonte com potência Real, as quais normalmente não acompanham gabinete e custam pelo menos R$ 200 hoje, no mercado local.

Segundo Passo

Procure retirar todas as placas de dentro do gabinete e monte novamente a máquina em uma bancada. É extremamente importante utilizar bancadas com sistema de aterramento para evitar danos ao equipamento por descarga de eletricidade estática (ESD). Vale destacar também que não precisa ser uma bancada comprada pronta, o que nos faz pensar em preços inviáveis para um usuário doméstico ou técnico que não tenha muito trabalho de manutenção. Você mesmo pode construir uma bancada, com itens facilmente encontrados no mercado e que no final das contas será igualmente eficiente contra eletricidade estática, além de ter um custo muito inferior. A construção passo-a-passo pode ser encontrada no livro "Guia de Sobrevivência do Integrador de PCs", publicado pela Editora Saber e disponível em nosso site **www.sabermarketing.com.br**.



Alguns emuladores de processador (CPU Emulator) usados por fabricantes e, no detalhe, um para o socket LGA775. Observe a presença dos pontos chave para medição dos sinais vitais.



F1. Kit básico para manutenção com bancada anti-estática, aterramento e placa POST para diagnóstico rápido.

Terceiro Passo

Certifique-se que todos os seus dispositivos estão funcionando corretamente. A regra prática mais seguida é testá-los em outro computador que esteja operando normalmente, porém ao fazer isso é importante estar ciente de alguns conceitos. Se por um lado periféricos como monitor, teclado, mouse e impressoras conectadas às portas serial, paralela e USB podem ser facilmente avaliados em outra máquina, os componentes internos requerem maior atenção.

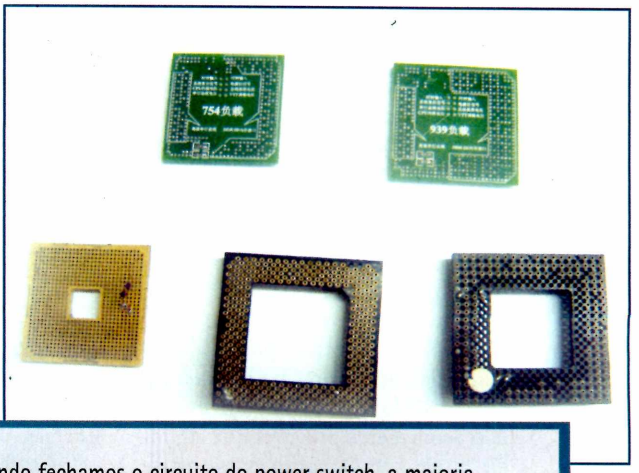
Imagine que seu computador não apresenta imagem no monitor. Seria um problema com o processador, memória ou com a placa de vídeo offboard? Agora, imagine que a placa de vídeo está em curto e ao levá-la para a outra máquina acaba queimando algum componente desta placa-mãe. Embora difícil de acontecer, o fato é que há o risco. Além disso, se sua instalação não atende ao segundo passo descrito acima, até mesmo um simples teste de memória pode ser arriscado, porque exporá os chips do módulo aos efeitos da ESD.

O ideal, portanto, é estar munido das ferramentas básicas para isolar o maior número de possibilidades de diagnóstico na própria máquina. Ter um multímetro e conhecer o básico da técnica de soldagem, por exemplo, para avaliar o estado dos componentes do circuito regulador de tensão da placa-mãe; ter uma placa POST para pelo menos ter uma idéia de onde está o problema e assim evitar um troca-troca de peças desnecessário que poderia acarretar na queima de algum componente durante um diagnóstico feito dessa maneira; por último, ter um testador de fontes ATX que nos permita avaliá-la fora da máquina (figura 2). Esse, aliás, deve ser nosso primeiro teste quando a placa-mãe sequer ligar.

11

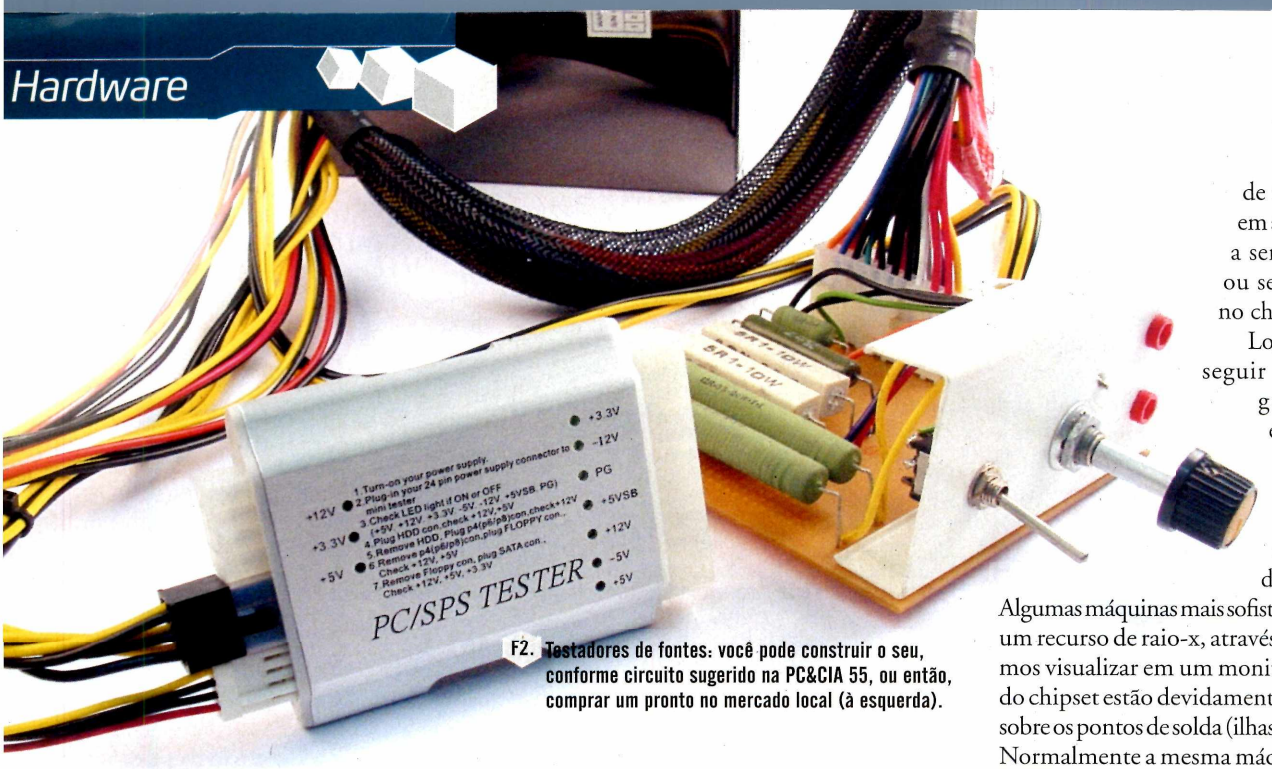
Dicas

As dicas a seguir são para quaisquer placas-mãe, independente da plataforma



Emuladores

Apesar de acionarem a fonte quando fechamos o circuito do power switch, a maioria das placas-mãe existentes no mercado hoje só funciona com todas as tensões liberadas quando existe uma carga no soquete do processador. Porém, quando se fala em conserto de placa-mãe, é difícil saber qual é o defeito dela antes de ligá-la e é muito arriscado fazer isso com um processador. Se ela fornecer uma alimentação muito acima do necessário para o funcionamento do processador (1,5V, em média), ele irá queimar. Para evitar este inconveniente, é utilizado um "emulador" que simula a presença do processador, criando uma carga e acionando os pontos necessários do circuito. Vale observar que já vi muitos casos em que um processador queimado (pelo menos sob o ponto de vista do usuário) funcionou perfeitamente tal como um emulador. Na verdade, o circuito presente na maioria dos emuladores é bem simples, contendo alguns resistores ligados entre os pinos.



F2. Testadores de fontes: você pode construir o seu, conforme circuito sugerido na PC&CIA 55, ou então, comprar um pronto no mercado local (à esquerda).

ou fabricante, pois são regras básicas para detecção de defeitos. Partiremos do princípio que não há imagem no monitor, ou seja, na linguagem popular é o famoso "não dá vídeo":

1) Faça uma inspeção visual na placa, tentando localizar componentes quebrados ou amassados, trilhas rompidas ou em curto por pingos de solda, fio, terminal de componentes, etc. Se notar alguma anormalidade, acredite que o problema poderá estar ali. Se localizar trilhas rompidas, estas poderão ser religadas utilizando pedaços de fio de cobre estanhados para fazer a "ponte" da seguinte forma: raspe cuidadosamente ambos os lados da trilha rompida a fim de eliminar o esmalte protetor, estanhe-os tal como o fio de cobre e solde cuidadosamente. É importante atentar-se para que não haja curto-circuito entre as trilhas ao lado. Após religar as trilhas, teste novamente a placa.

2) Se a placa-mãe não liga, ou seja, se nem ao menos aciona a fonte de alimentação, verifique se os MOSFETs estão em curto, testando suas pinagens (figura 3). Você também pode conectar apenas o cabo principal da fonte (o do ATX12 fica fora) e ver se os MOSFETs esquentam muito. Se isso acontecer, é provável que algum esteja queimado. A confirmação pode vir se você conseguir ligar a placa apenas com esse cabo conectado.

3) Ao ligar a placa-mãe, coloque os dedos sobre os chips dos principais componentes, tais como North e South Bridge do chipset (Ponte Norte e Sul, respectivamente), som, rede e controlador RAID. Se houver dissipadores sobre eles, retire momentaneamente. Verifique se estes chips estão muito quentes, a ponto de queimar os dedos. É verdade que os chipsets mais novos (principalmente) já superaquecem naturalmente por trabalharem em freqüências elevadíssimas, mas isso conforme a utilização e demanda de processamento solicitada pelo usuário. Já o aquecimento a que nos referimos aqui é típico de chips queimados, ou seja, eles superaquecem imediatamente, ao ligar o sistema. É importante inclusive ficar atento para não queimar os dedos. Se isso acontecer, será necessário trocá-los por novos e, neste caso, somente em uma assistência técnica especializada.

Em se tratando de um chip com encapsulamento BGA, uma série de procedimentos devem ser respeitados e seguidos. O chip danificado é retirado em uma máquina extratora de BGA. Esta máquina aquecerá a área onde o chip está instalado a uma temperatura próxima a 300 °C, e através de uma ventosa o chip é preso e retirado por sucção.

Para limpar os resíduos de solda que ficam na placa-mãe, utiliza-se uma malha de cobre e um ferro de solda de boa qualidade. É preferível que seja uma estação de solda, pois ao entrar em contato com a malha de cobre um ferro de solda comum perde muito calor pelo fato da malha funcionar como dissipador. É perigoso o ferro "esfriar" no meio de uma limpeza e a malha ficar grudada nos pontos onde as esferas do chip novo serão soldadas e, ao puxar a malha, estes pontos podem ser arrancados da placa. Para facilitar o deslizamento da malha, utiliza-se fluxo de solda em pasta. Com os pontos da placa limpos e homogêneos, aplica-se uma fina camada de fluxo de solda em ambos os lados a serem soldados, ou seja, na placa e no chipset.

Logo após, basta seguir as guias serigrafadas para enquadrá-lo corretamente e posicionar a placa na máquina soldadora de BGA. Algumas máquinas mais sofisticadas possuem um recurso de raio-x, através do qual podemos visualizar em um monitor se as esferas do chipset estão devidamente posicionadas sobre os pontos de solda (ilhas) da placa-mãe. Normalmente a mesma máquina extratora é também a soldadora. Dentre os principais fabricantes destes equipamentos, podemos citar a Fonton.

Após a soldagem a placa deverá passar por uma nova bateria de testes e ainda assim o problema pode persistir devido a três motivos básicos:

- O chip foi mal soldado, o que significa dizer que alguma esfera não foi bem soldada à placa-mãe. Pressionando o chip com os dedos contra a placa conseguimos fazê-la funcionar, pois induziremos manualmente o contato que deveria ser feito através da soldagem. Deve-se refazer a solda do chip;
- Ao manusearmos o chip, devemos ter todo o cuidado, pois é muito comum ele queimar por eletricidade estática;
– Pode acontecer do problema não ser do chip substituído. Neste caso, o chip novo soldado não é perdido, porque existe uma máquina justamente para recuperar as esferas dos chips dessoldados que estejam em bom estado de funcionamento (figura 4). Esta máquina é conhecida como *Reballing*. O procedimento é parecido ao da soldagem na placa-mãe. Deve-se limpar o chip e posicionar sobre ele uma espécie de molde que é perfurado em todos os pontos onde existem esferas. Após passar o fluxo gelatinoso no chip e posicionar o molde, "joga-se" as esferas que ficarão coladas pelo fluxo e esta máquina aquecerá o chip até que as esferas fiquem presas pela própria solda. Este chip está pronto para ser reutilizado.

4) Outra dica importante diz respeito à bateria que atua na manutenção dos dados gravados na memória CMOS. Algumas placas-mãe simplesmente não

ligam quando estão sem bateria ou com baixa carga. Verifique se a bateria está carregada com 3V, considerando uma tolerância de 10%.

5) Outro ponto imprescindível para o funcionamento da máquina são as memórias. Quando existe algum problema com elas, normalmente as placas emitem um beep alertando o defeito, mas isto não é uma regra. Procure limpar bem os contatos do módulo com uma borracha branca macia e também os contatos do soquete de memória soldados à placa, a fim de eliminar oxidação e sujeira que provocam mau contato.

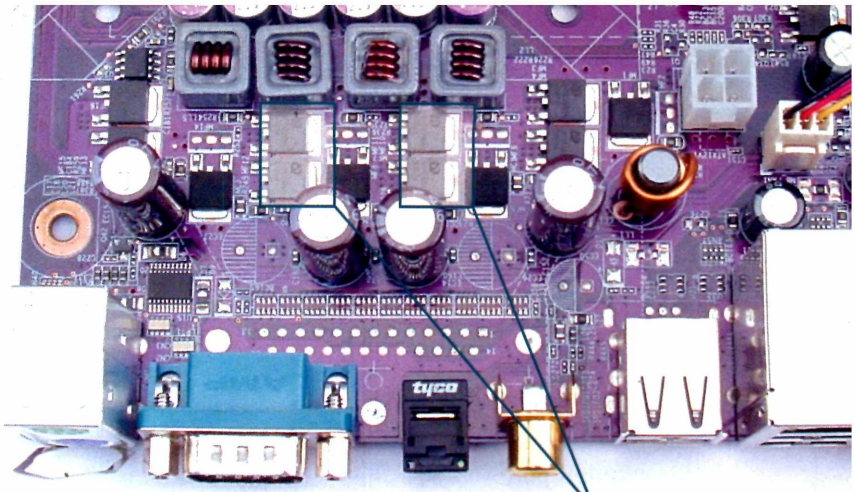
6) Estando tudo aparentemente normal, passamos então para outra dica importantíssima, o BIOS. O chip onde ele está instalado também possui rotinas de software para controle do POST e o programa Setup, mas aqui nos ateremos apenas ao software básico de inicialização e testes com o hardware, que é o tão conhecido BIOS.

Muitas vezes a causa do não funcionamento, ou até mesmo do mau funcionamento da placa, se dá por conta de um BIOS corrompido ou com uma revisão incompatível com algum componente de hardware. Aqui entra em cena a atualização do BIOS. É importante sempre mantê-lo atualizado, basta ir ao site do fabricante da placa e fazer o download. Veja que a atualização também pode ser útil em situações de lentidão e instabilidades do sistema, e não apenas quando a máquina deixa de ligar após um upgrade de processador, por exemplo.

Se o BIOS estiver corrompido, é possível reprogramar o chip Flash ROM onde ele está gravado. Isso pode ser feito através de um equipamento conhecido como reprogramador de flash (testes na PC&CIA 32), ou então utilizar uma placa idêntica boa para fazer uma atualização "a quente". Após ligar a máquina "estepe" em modo MS-DOS, remova cuidadosamente o chip Flash da placa, atentando-se para não curto-circuitar os pinos, e em seguida encaixe o Flash da placa morta. A partir daqui basta seguir os passos básicos para a atualização, descritos no site do fabricante da placa. No passado, era possível realizar este procedimento entre placas diferentes, bastando atentar-se ao modelo do chip para evitar queimas devido a uma incompatibilidade elétrica (tensão de alimentação diferente). Hoje, isso não é possível porque os softwares usados na reprogramação normalmente checam se o arquivo do BIOS é de fato o utilizado na placa-mãe.

Um último detalhe: se o chip Flash estiver soldado diretamente na placa-mãe, o procedimento será o mesmo em relação ao descrito acima, mas será mais complicado porque será preciso removê-lo e ressoldá-lo. O que evidentemente demandará equipamentos especiais e prática com soldagem.

7) Se o problema ainda persistir, ao ligar a placa na bancada use o polegar para pressionar os chips Ponte Norte e Sul. Faça isso pelo menos três vezes e de maneira alternada, pressionando em pontos diferentes e especialmente no centro do chip. Com o passar do tempo, muitas vezes estes chips perdem o contato entre suas esferas e a base da placa por conta de solda fria. Principalmente em placas de baixa qualidade. Ao pressionar o chip, estas esferas voltam a ter contato com a placa e então funcionam normalmente naquele momento. Este chip deverá ser ressoldado ou até mesmo trocado por um novo. O North Bridge é o mais importante neste sentido, aliás, esta dica vale também para problemas com memória. Se sua placa emitir beeps de defeito, ou a POST indicar um código relacionado com memória, faça também este teste.

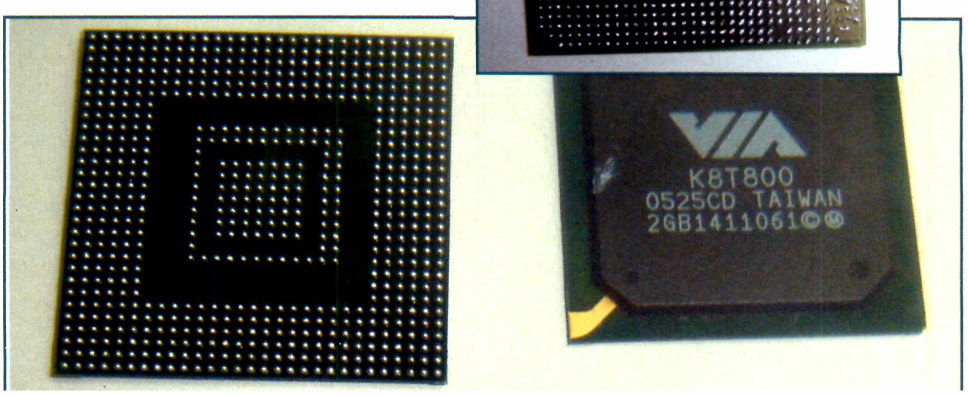


F3. Região do circuito regulador de tensão do processador e destaque nos MOSFETs.

Conclusão

Além de apresentar a rotina de diagnóstico normalmente seguida pelos RMA Centers mundo afora, procuramos apresentar nesta matéria alguns procedimentos simples e rápidos que você mesmo pode usar com eficácia para evitar e diagnosticar muitos defeitos em placas-mãe. Em muitas vezes, o que faz diferença não é nem mesmo o dar nova vida a uma placa, mas sim chegar com rapidez ao diagnóstico e evitar perda de tempo e prejuízos bobos que normalmente ocorrem quando simplesmente ficamos trocando peças sem nenhum critério técnico. De posse dessas dicas e de tantas outras apresentadas em edições anteriores da revista, se você não conseguir resolver o problema, pelo menos agora já sabe que mesmo placas-mãe podem ser consertadas aqui no Brasil. **PC**

F4. Ponte Norte de chipset em estado original e com pontos de solda derretida após remoção da placa.



Manutenção de PCs

Fernando Ramos da Silva

Boa apresentação pessoal, ética e conhecimento técnico, esses itens são essenciais a todo profissional que se preze. O de manutenção, em particular, também requer um bom conjunto de ferramentas, caso contrário acaba desperdiçando tempo, colocando peças em risco à toa, trabalhando muito para ganhar pouco e ainda corre o risco de passar vergonha no cliente. Esta matéria traz um teste com cinco placas POST, considerada a ferramenta mínima para os profissionais dessa área.

O básico

POST, boot e BIOS são as siglas que descrevem em linhas gerais o funcionamento básico de todo microcomputador durante o início de sua operação. Lembrado por muitos usuários como sendo um item de hardware, por estar contido num chip de memória de tecnologia Flash ROM integrado na placa-mãe, na verdade o "BIOS" é composto pelo seguinte conjunto de softwares:

- **Setup**: conjunto de interfaces onde estão os itens configuráveis do BIOS. Normalmente acessível após pressionarmos a tecla Del durante a inicialização da máquina, é ali que definimos quais periféricos integrados serão utilizados, a freqüência de operação do processador, etc;
- **BIOS**: um programa escrito normalmente em linguagem *assembly*, o qual descreve os testes que serão realizados com o hardware antes da tentativa de carregar um sistema operacional. Aqui também estão os drivers de controle de periféricos mínimos à inicialização, tais como teclado, floppy, disco rígido, portas serial e paralela. Periféricos que possuem memórias ROM, como placa de vídeo e controladora SCSI ou SATA PCI, por exemplo, também são lidas pelo BIOS e carregadas na memória RAM;
- **POST**: sigla para Power On Self Test, é o teste realizado automaticamente pelo BIOS sobre o hardware, todas as vezes que a máquina é ligada. A saída desse teste é normalmente apresentada através de mensagens enviadas para o monitor de vídeo (contagem de memória, por exemplo), padrões sonoros (beeps) para a saída de alto-falante (Speaker) no conjunto de pinos do painel frontal da placa-mãe, e também a partir de códigos enviados para o endereço de I/O 80h (o "h" é de notação hexadecimal, um sistema de numeração que possui os números de 0 a 9, além das letras a, b, c, d, e, f);
- **Boot**: nome dado ao processo de busca por um sistema operacional, que pode estar localmente em uma unidade de disco, ou remoto, acessível a partir de uma placa de rede. Só é realizado quando os testes de POST são concluídos com sucesso.

Placas de diagnóstico

Antes mesmo de surgir imagem no monitor de vídeo, uma série de testes é realizado no computador. Processador, chipset, memória RAM e outros circuitos básicos em uma placa-mãe, tais como temporizadores e o próprio BIOS, são inicializados e tem sua integridade verificada. Esse conjunto de testes está contido num segmento do BIOS conhecido como *boot block*, o qual é automaticamente buscado pelo processador quando a máquina é ligada (endereço FFFF0h ou 1048560 em decimal).

Na verdade, ele já vem programado para fazer isso, justamente no espaço de endereçamento reservado para a memória Flash ROM. Repare que este endereço está contido no primeiro megabyte inicial de memória, pois o processador inicia seu funcionamento em modo real e operando com 16 bits. Após essa bateria inicial de testes, o código do BIOS é carregado para a RAM, o vídeo é inicializado e os demais testes são realizados.

Dito isso, já sabemos que se o micro apresentar um problema antes do vídeo estar disponível, ficaremos literalmente no escuro, sem saber onde está o problema. É verdade que nesse caso os beeps poderiam nos ajudar. Porém, além da implementação dos beeps ser normalmente simples e não contemplar uma correspondência para cada teste realizado, de uns tempos para cá os fabricantes de placas-mãe têm relaxado um pouco em relação a isso e deixado de implementar os beeps. Imagine uma estrutura condicional do tipo If-Then-Else, na ocorrência de uma falha deveria existir no código assembly uma instrução para gerar o padrão sonoro referente ao erro. Mas não há em vários casos, conforme tivemos a oportunidade de detectar durante nossos testes (detalhes a seguir).

Agora vamos às placas de diagnóstico. As do tipo POST são mais simples. Eletricamente elas são classificadas como passivas, pois só pegam os códigos POST enviados pelo BIOS

para o endereço 80h (antigamente num slot ISA, hoje num PCI) e os demonstram em um display (figura 1). Quando nada falha durante o POST, os códigos vão passando um a um, de 00 a FF, por exemplo, embora não necessariamente nesta seqüência. Se ocorrer da RAM não passar no teste, automaticamente seu código de teste fica congelado no display e o usuário pode então, através de uma correspondência destacada no manual que acompanha a placa, encontrar o responsável pela falha.

Existem no mercado placas mais sofisticadas que não apenas lêem os códigos POST, como também são capazes de programar os registradores do chipset a fim de ter controle total da máquina. A partir daí, elas podem por em execução suas rotinas de testes que a acompanham no próprio hardware, isto é, estão contidas em ROM da própria placa e rodam a partir da RAM que elas também possuem. Maiores detalhes sobre a operação delas podem ser vistos na PC&CIA 45.

Placas POST na prática

Após desligar a máquina normalmente ontem, você liga hoje e a máquina trava durante o POST. O código demonstrado, 6F, tem relação com o floppy, porém a máquina sequer tem um drive de disquete. E detalhe: a máquina não tem duas semanas de operação e está rodando com tudo original, sem qualquer overclock que poderia induzir o hardware a um comportamento errôneo não documentado pelo fabricante.

Será que o processador está sobreaquecendo, ou é a configuração de floppy que ficou habilitada no Setup? Mas o que fazer se a máquina está travada e o teclado não responde? Claro, um ClearCMOS (CCMOS)! O problema é que nem ele resolveu. E agora, qual será o problema desta placa Abit AW8-Max?

Com uma placa POST e diante de um código esdrúxulo como esse, sem qualquer relação com o funcionamento da máquina, fica a "quase certeza" de que o sistema está sofrendo de algum transiente ou descarga eletrostática (ESD) corrompendo o valor de algum registrador do hardware, e que o procedimento padrão de CCMOS não está sendo suficiente para "zerar" a configuração. E de fato, após desconectar a fonte da alimentação elétrica, retirar a bateria e deixar o sistema de "molho" durante a noite, no dia seguinte lá estava o sistema bom novamente, pronto para funcionar!

É verdade que falando desse jeito até parece que tudo é muito simples e que a solução foi descoberta em alguns minutos, mas o que gostaríamos de destacar aqui é a **IMPORTÂNCIA** do descarte de uma linha de raciocínio.

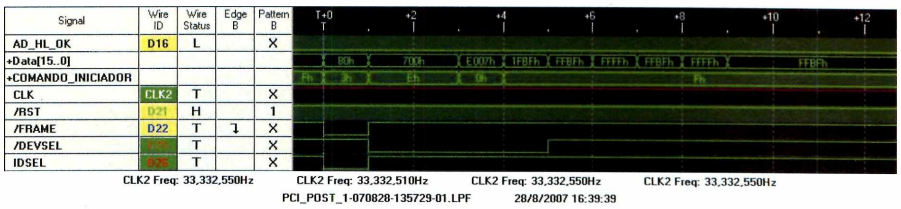
Quem trabalha com manutenção sabe bem o que é isso. Sem ver o tal código esdrúxulo, poderíamos desconfiar de tudo o mais na máquina e antes do CCMOS: processador, memória e até da placa-mãe. Agora se imagine pegando uma trilha de diagnóstico errada e fazendo tudo isso em uma instalação sem aterramento e qualquer cuidado com ESD. Ao invés de resolver um problema, estaríamos criando outro, e com prejuízos!

É impressionante como ainda são muitos os ditos profissionais afirmando que cuidados com ESD e necessidade de aterramento é assunto teórico de colégio (figura 2). É verdade que de uns anos para cá os fabricantes conseguiram enrobustecer a tolerância dos chips aos efeitos da ESD. Porém, o que poucos usuários sabem é que apesar do chip não queimar após várias vezes de sujeição indevida em relação à ESD, o componente está gradativamente perdendo confiabilidade e desempenho (depois não sabe porque seu overclock não funciona, né?).

Poderíamos discorrer várias páginas de matéria relatando problemas como esse, ou seja, de defeitos misteriosos que na escuridão da falta de ferramentas pode se transformar num verdadeiro pesadelo, mas por ora vamos às placas.

QuickPOST PCI Serial Rev.10c

Esta é mais uma placa da Ultra-X que recebemos para testes e nos impressionou (figura 3). É verdade que o custo de R$ 1780 (cotação no site **www.uxdiag.com.br**) é considerado proibitivo para muitos técnicos, até por que



F1. Leitura de alguns sinais no barramento PCI com um analisador lógico. Junto com osciloscópio ampara o desenvolvimento da placa POST.

Important Notification about Power Issue

NForce chipset is very sensitive to ESD (Electrostatic Discharge), therefore this issue mostly happens while the users intensively swap memory modules under S5 (power-off) states, and the power code is plugged while installing modules. Due to several pins are very sensitive to ESD, so this kind of memory-replacement actions might cause system chipset unable to boot. Please follow the following solution to avoid this situation.

Unplug the AC power cable (shown in figure 1) or unplug the power connectors (shown in figure 2 & figure 3) before the 1st installation or during system upgrade procedure.

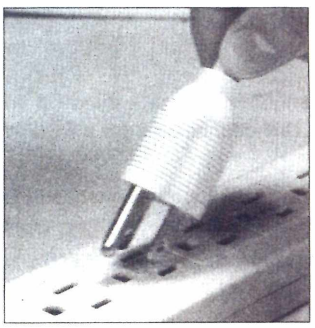


Figure 1:
Unplug the AC power cable

F2. Teoria ou prática? Manual de uma placa-mãe atual (modelo P6N SLI, da MSI) alertando sobre riscos de ESD durante manipulação de memória.

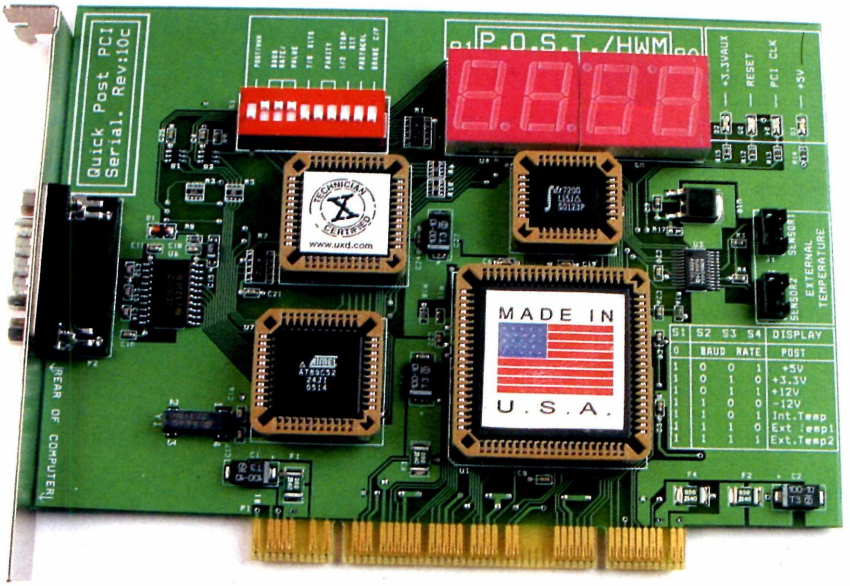
não se trata apenas de uma placa POST!? A resposta é não. Além dos códigos POST da porta 80h enviados para dois de seus displays, dispostos à direita, essa placa assume grande importância no mercado brasileiro por ser a opção de entrada, mais acessível, que pode ser usada para efetivamente testar uma fonte ATX na prática. Ou seja, ligada com a máquina em pleno funcionamento.

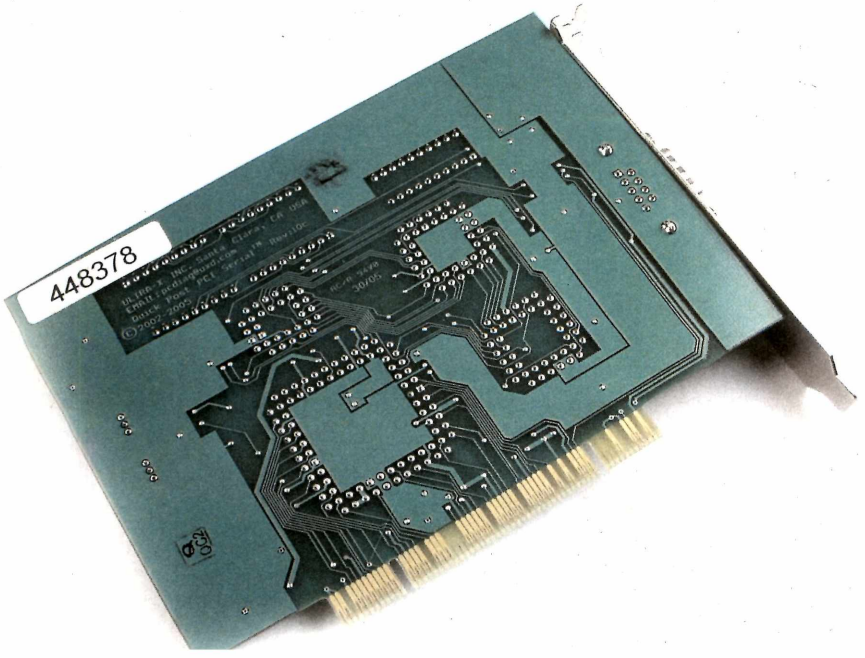
Note que ao lado dos quatro displays há um dip switch com 10 micro-chaves. Pois bem, é nele que configuramos se os displays exibirão códigos POST, ou então, uma das tensões (3,3 / 5 / 12 / -12V). As demais chaves configuram os parâmetros utilizados no protocolo de comunicação serial, a fim de que a placa envie os dados lidos para um outro computador conectado à sua interface serial DB-9. Ou seja, ao invés de ter de ficar olhando os displays para ver se alguma tensão da fonte excede os limites descritos na norma, você pode deixar a placa instalada na máquina do cliente e voltar no dia seguinte para tomar uma conclusão sobre o funcionamento da fonte (figura 4).

Além disso, a placa também é capaz de monitorar três temperaturas, sendo uma interna (o manual não descreve onde está o sensor, apenas diz "sistema" e com faixa de leitura entre 0 e 127 °C) e duas externas, a partir de sensores opcionais que podem ser convenientemente dispostos para analisar o comportamento de uma placa de vídeo ou HD, por exemplo. A faixa de leitura, nesse caso, vai de 0 a 85°C. E com isso chegamos a uma ferramenta que vai muito além de uma simples POST e pode ser usada inclusive para homologação de uma nova máquina ou manutenção realizada.

Um detalhe interessante diz respeito à eletrônica da placa. Dona de uma apresentação invejável, os chips empregados são atuais e alguns, como o conversor analógico-digital (A/D), esbanja sofisticação no 10 ou 12 bits para fazer a amostragem de tensões? Que nada, o Analog Devices ADM9240 possui 14 bits de resolução e suporta uma taxa de amostragem de 10MSPS (dez milhões de amostras por segundo). Sinceramente não dá para desconfiar da precisão das leituras. O manual diz que há uma tolerância de +-2% para a placa reportar uma falha com alguma das tensões.

Ademais, a placa possui dois displays adicionais para a leitura da porta 81h, que pode ser usada por desenvolvedores de software em seus *checkpoints* (pontos de verificação para auxiliar no debug do programa), quatro leds em montagem SMD (3,3 e 5V, presença do reset e do clock no barramento PCI). O esmero do projeto também contempla uma boa área de "pega" nas duas laterais superiores da placa, ou seja, o usuário poderá manuseá-la tranqüilamente dentro da máquina sem tocar em nenhum componente eletrônico.





Mini debug card

Esta placa possui apenas o trivial para a leitura dos códigos POST na porta 80h. O circuito principal é baseado em três chips idênticos do tipo PAL (Programmable Array Logic), nos quais são configuradas as portas lógicas usadas para construir a máquina de estado que lê o barramento PCI.

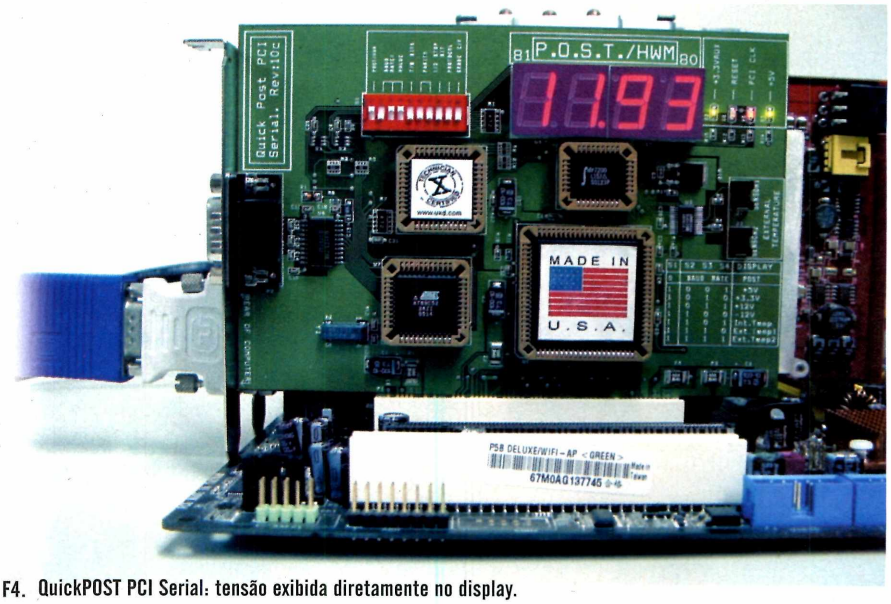
Como muitas placas-mãe e gabinetes já não trazem mais um alto-falante, essa placa tem seu próprio alto-falante e um conector para trazer a conexão do painel frontal da placa-mãe (cabo é fornecido no kit). Além disso, estão presentes cinco leds SMD (3,3 e 5V, e sinais Frame, Reset e IRDY) e dois displays de sete segmentos duplicados. Os montados paralelamente à placa facilitam a leitura dos códigos, o que é particularmente interessante quando instalada nos slots PCI inferiores e com a placa montada no gabinete (figura 5).

Ultimate Diagnostic Card

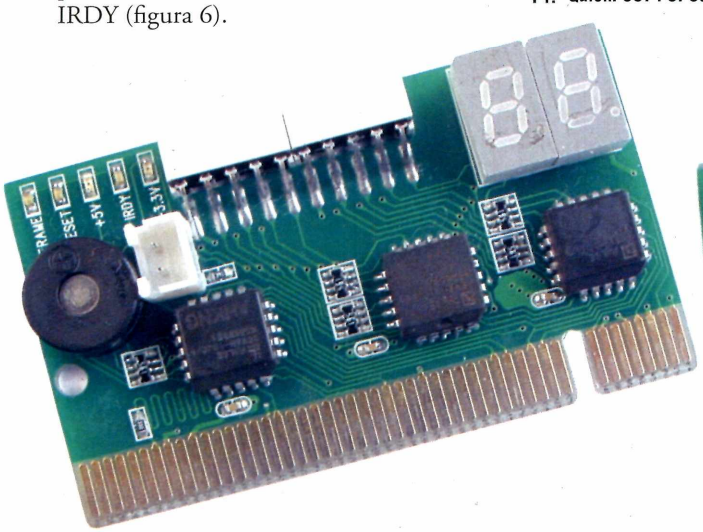
Outra POST da categoria mais simples, esta placa apresenta como diferencial a possibilidade de leitura em notebooks, através

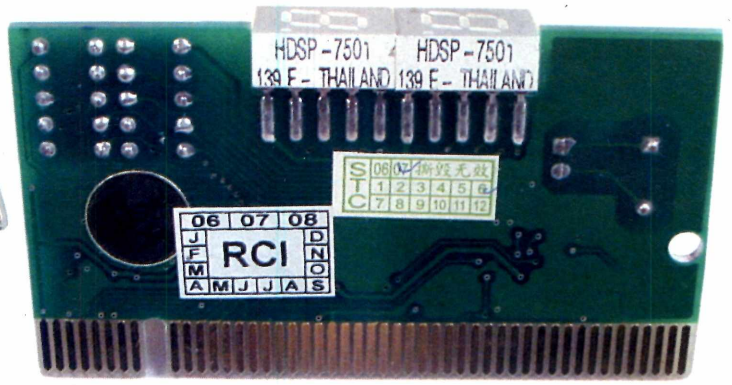
de uma porta paralela. O kit também vem com um cabo USB, usado para a alimentação elétrica da placa durante este uso.

Dos displays, dois são usados para a leitura do código atual lido na porta 80h, enquanto os demais ficam como função memória, retendo o código anterior. Assim como a placa anterior, há a leitura das tensões de 3,3 e 5V, além de +12 e -12V, mas não se trata de uma leitura precisa, já que não há processamento e nem conversão A/D. O sinal é simplesmente "levantado" dos pinos do slot PCI para os leds, portanto, apenas atestam que existe tensão, e não que está dentro ou fora de limites. Outros leds presentes são o de Reset, Clock, Frame e IRDY (figura 6).

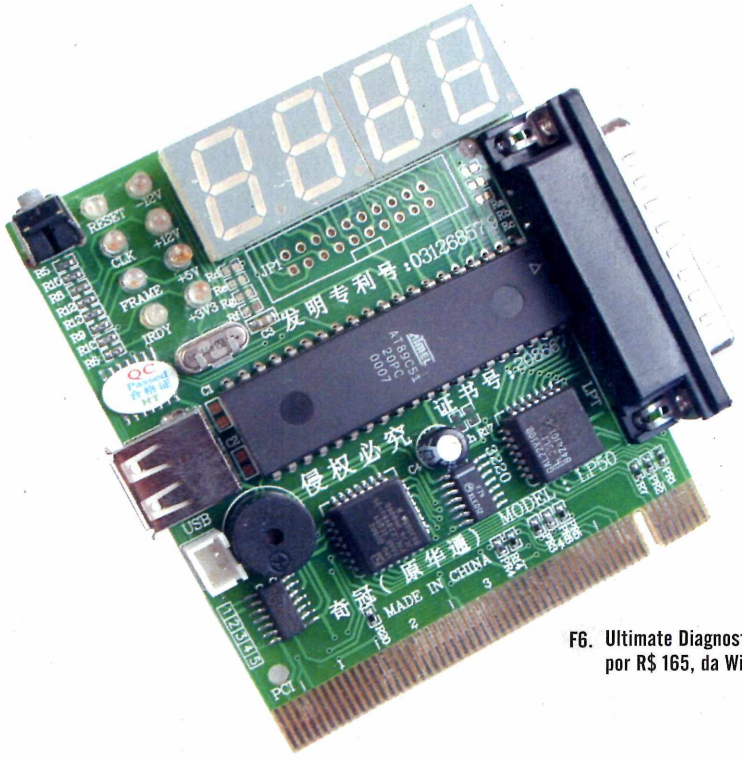


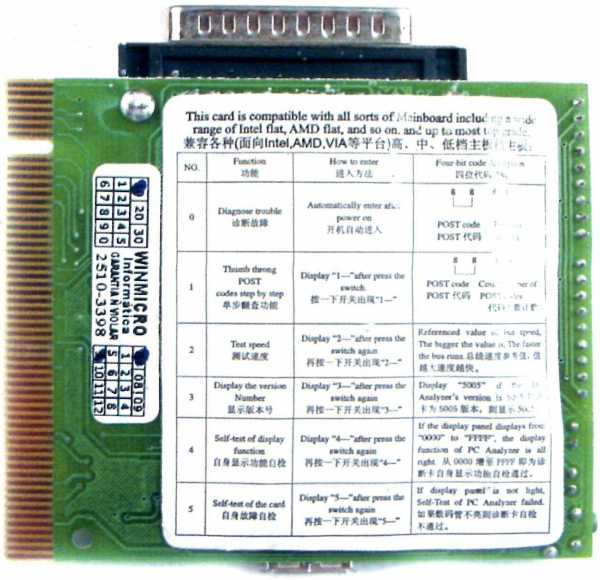
F4. QuickPOST PCI Serial: tensão exibida diretamente no display.





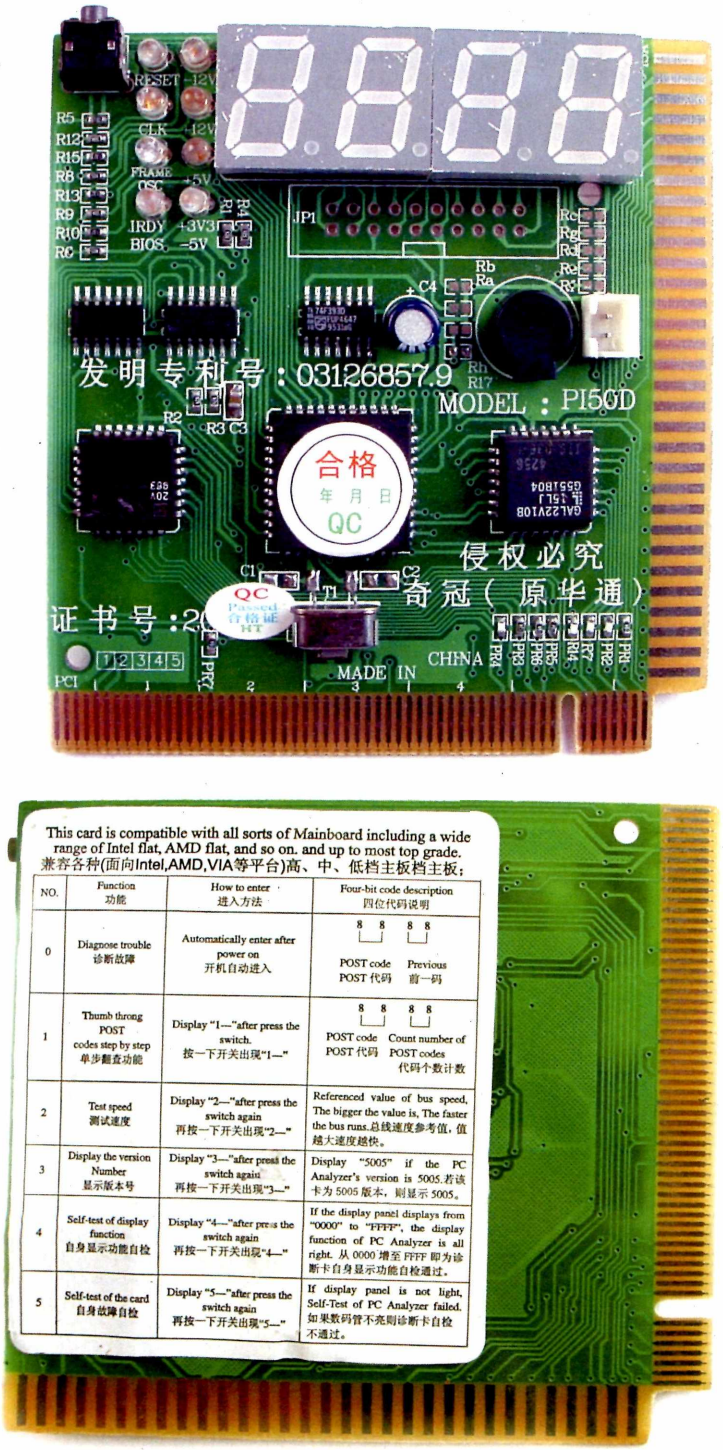
F5. Projeto é tão enxuto que é impossível instalar ou remover a placa sem tocar em algum componente ou terminal. Comprada no site Mercado Livre por R$ 80.





F6. Ultimate Diagnostic Card (UDC): disposição dos leds não permite uma boa leitura. Comprada por R$ 165, da WinMicro Informática.

Ao lado dos leds há uma chave que aciona uma rotina de teste da placa e de seus displays, podendo ser realizado com a máquina energizada. A eletrônica de leitura de barramento da placa é baseada em dois chips PAL. Além disso, existe um circuito oscilador interno que pode ser o responsável pelo fato da placa só ter funcionado em placas-mãe antigas, de geração Pentium III para trás. Neste caso, as possibilidades de diagnóstico da placa ficam limitadas aos beeps da placa-mãe, que podem ser trazidos para seu conector de dois pinos e soados através de seu pequeno alto-falante.



F7. PC Analyzer: praticamente uma cópia da anterior e conector ISA que não funcionou em nenhuma placa-mãe. Adquirida por R$ 110 no site Mercado Livre.

PC Analyzer

Contando com um projeto similar ao da placa anterior, esta POST só poderia se comportar de modo semelhante, tendo seu funcionamento restrito às placas-mãe Pentium III e anteriores. Não há a possibilidade de teste em notebooks, no lugar do conector da porta paralela está montado o conector para slot ISA (figura 7).

PCI POST Saber 1.0

Essa placa é a primeira revisão da POST que há algum tempo estávamos desenvolvendo em nosso laboratório. A exemplo de outros projetos já publicados na revista, como o MediaPC, PC&Cia Linux e Display Case Multifuncional, o objetivo é fomentar entre nossos leitores o grande potencial que há por trás do desenvolvimento de soluções.

Como tal, ela não estará à venda, será distribuída gratuitamente aos novos assinantes, que poderão inclusive entender melhor o funcionamento do barramento PCI e também se relacionar conosco para a resolução de problemas. Neste sentido, a placa traz os leds apenas indicativos da presença de tensão no barramento (3,3 / 5 / 12V), além de todos os sinais envolvidos desde o momento que o iniciador PCI (o controlador integrado no Southbridge) manifesta a intenção de colocar um dado no endereço 80h e sinaliza com o comando de escrita em I/O (3h), até o target (alvo, no caso a placa POST) dizer ao iniciador que esse dado é para ele e realizar a leitura do barramento. São eles: Frame (usado pelo controlador PCI para indicar o início e a duração de um acesso), IRDY (Initiator Ready – iniciador ou controlador PCI pronto), DevSel (indica o dispositivo que decodificou o endereço em resposta ao sinal de frame, ou seja, é o alvo se anunciando ao controlador PCI), TRDY (Target Ready – alvo ou periférico pronto), clock e reset. Você verá que a cada código POST os quatro primeiros leds piscam (figura 8).

A eletrônica da placa é baseada em apenas um chip principal, um CPLD da Altera operando em 3,3V LVTTL (baixa tensão de nível TTL). A fim de garantir a compatibilidade com placas-mãe antigas, que como as PCChips não levam a tensão de 3,3V aos slots PCI, foi colocado um regulador de tensão na placa que pega os 12V do barramento e dali alimenta o CPLD.

Se de um lado os circuitos PAL das placas anteriores permitem ao desenvolvedor implementar uma lógica mais complexa a partir de simples portas lógicas do tipo OR, por outro elas não podem ser usadas para

compor circuitos *schmitt-trigger* e, conseqüentemente, podem ter sua estabilidade prejudicada. Na prática, pode haver as chamadas indeterminações dos sinais.

Vale dizer também que a placa foi projetada para ler os endereços 80 e 84h (alguns BIOS mais antigos jogam a saída para esse endereço), e está amarrada ao clock do barramento PCI, suportando inclusive freqüências superiores ao padrão de 33 MHz. Isso pode ser útil em sistemas overclocados baseados em chipsets antigos, os quais são incapazes de travar a freqüência do PCI de modo independente à freqüência do barramento FSB.

Além do alto-falante e seu conector, a placa possui ainda outros dois conectores. Um deles é usado como uma espécie de extensão para o display, ou seja, dali sairá um cabo que irá até uma placa opcional contendo outros dois displays para facilitar a visualização. Já o outro é reservado para atualizações da máquina de estado. Ou seja, após o desenvolvimento de uma nova versão de hardware, que aqui é codificado através de um programa, poderemos receber as placas e fazer uma atualização com o objetivo de aumentar sua compatibilidade com uma futura geração de placas-mãe, por exemplo. Ou então, até mesmo aumentar a funcionalidade da placa, através de um conjunto extra que atue como tradutor de códigos. Ele lerá o último código POST, consultará uma tabela de códigos gravada em uma memória interna e demonstrará a falha em um display na forma de texto, e em bom português.

Testes

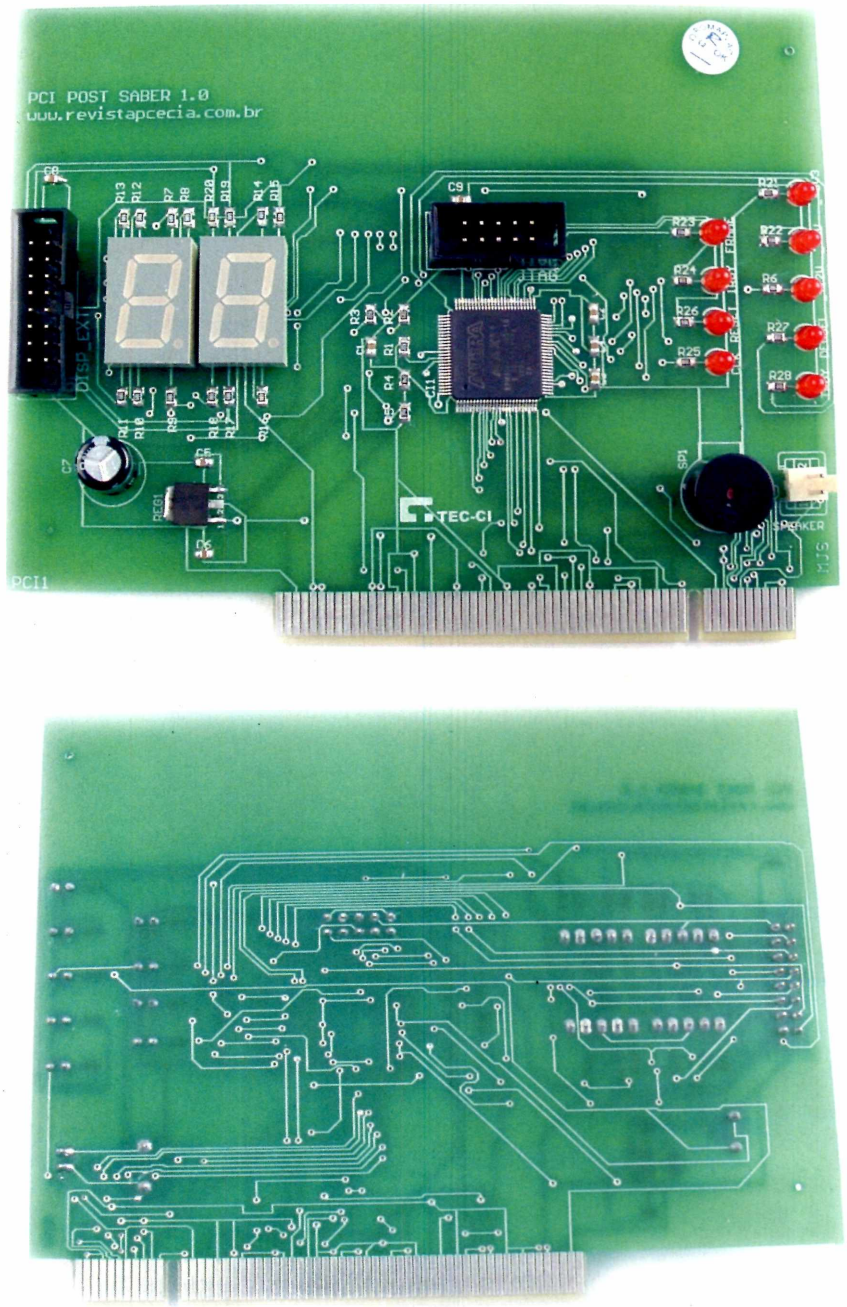
Considerando que o barramento PCI está solidificado sobre uma proposta de padrão aberto da indústria e, como tal, de especificação de domínio público, somos levados a pensar que basta seguir a documentação que tudo funcionará. Mas prova de que isso não é tão simples assim são os inúmeros casos de periféricos que não instalam em determinado modelo de placa-mãe e outros que sofrem com compartilhamento de interrupções no barramento PCI. Vários manuais de placas POST inclusive alertam quanto a isso. Além da qualidade do projeto eletrônico da placa-mãe fazer toda a diferença, haja vista a operação em elevadas freqüências e questões relacionadas, como o casamento de impedância no barramento, o que fazer em placas-mãe atuais? Afinal, por implementarem o barramento PCI-Express e conseqüentemente não "levantarem" todos os 6 slots PCI normalmente suportados pelo chipset, como se livrar dos slots compartilhados e garantir o funcionamento da POST? É por isso que optamos por, a seguir, apresentar um breve relato dos testes que fizemos com cada placa-mãe, ao invés de simplesmente dizer se a placa POST X é compatível com a revisão de barramento PCI Y.

A7N8X-VM/400

Esta placa da Asus é um modelo baseado no chipset nForce2 com vídeo integrado, destinada à plataforma dos processadores socket A, a exemplo do Athlon XP 2500+ instalado. O desenvolvimento do BIOS vem da Amibios 2003, com binário de revisão 1003 beta 2.

Ela possui um slot AGP e 3 PCI compatíveis com a revisão de barramento 2.2.

As POST UDC e Analyzer não funcionaram em nenhum slot, quando a máquina era ligada os displays só demonstravam os códigos FF. Como ambas responderam bem ao auto-teste e não há qualquer jumper para ajustar o endereço do barramento a ser lido,



F8. POST Saber: apenas 8 bits do barramento de endereços são coletados para a placa funcionar. Espaço na parte superior para evitar contato com trilhas e/ou componentes.

isso significa que não funcionaram porque são limitadas.

É curioso notar que o manual delas não faz qualquer referência a uma suposta lista de compatibilidade com placas-mãe e/ou com revisão de barramento PCI. Dessa forma, a atuação de ambas fica limitada aos beeps, como por exemplo um problema de memória RAM, que provoca a seqüência de beeps um longo e dois curtos.

Já as outras POST funcionaram a contento. Sem RAM instalada, os displays de todas congelavam no código EE, ainda dentro da rotina do *boot block* do BIOS. Importante destacar que, ao contrário do que possamos imaginar, a seqüência de códigos não vai do código 00 até FF seqüencialmente. Primeiro, há uma contagem inicial do *boot block*, etapa na qual não há imagem no monitor, e depois outra contagem é iniciada e vai até 00, código este que, segundo o manual da Amibios, é o indicativo de boot.

SL-75FRN2-RL

Outra placa-mãe com chipset nForce2, desta vez da Soltek e com BIOS de versão 6.00PG desenvolvido pela Award. Projetada para overclock, ela possui vários parâmetros no BIOS para ajuste de tensão e freqüências dos barramentos, permitindo inclusive a operação assíncrona entre o barramento de memória e o do processador (FSB). Há ainda um jumper na placa-mãe que força a operação do FSB em 133 ou 166 MHz. Com várias opções e processadores de diferentes FSB (desde um Duron de 100 MHz até um Athlon XP operando em overclock para 200 MHz), era comum a máquina ficar sem responder e sem exibir imagem no monitor.

Com as POST, o overclock é facilitado. Quando a memória não suportar a freqüência definida no Setup, por exemplo, o código nos displays é o EF. Se o problema é com o processador, em algumas POST o display não é inicializado (QuickPOST e MiniDebug) ou exibe um código baixo (04, na Saber). Em relação à compatibilidade, somente essas três POST funcionaram normalmente, as outras duas não inicializavam a exibição dos códigos.

5DTX-TC

Esta placa utiliza o chipset Intel 430TX com Southbridge (Ponte Sul) PIIX4 compatível com a revisão de barramento PCI 2.1. O BIOS instalado é da revisão 4.51PG da Award, uma versão clássica que termina os códigos POST em FF. O teste foi feito com um Pentium MMX 233 MHz e um módulo de memórias SDRAM rodando a 66 MHz.

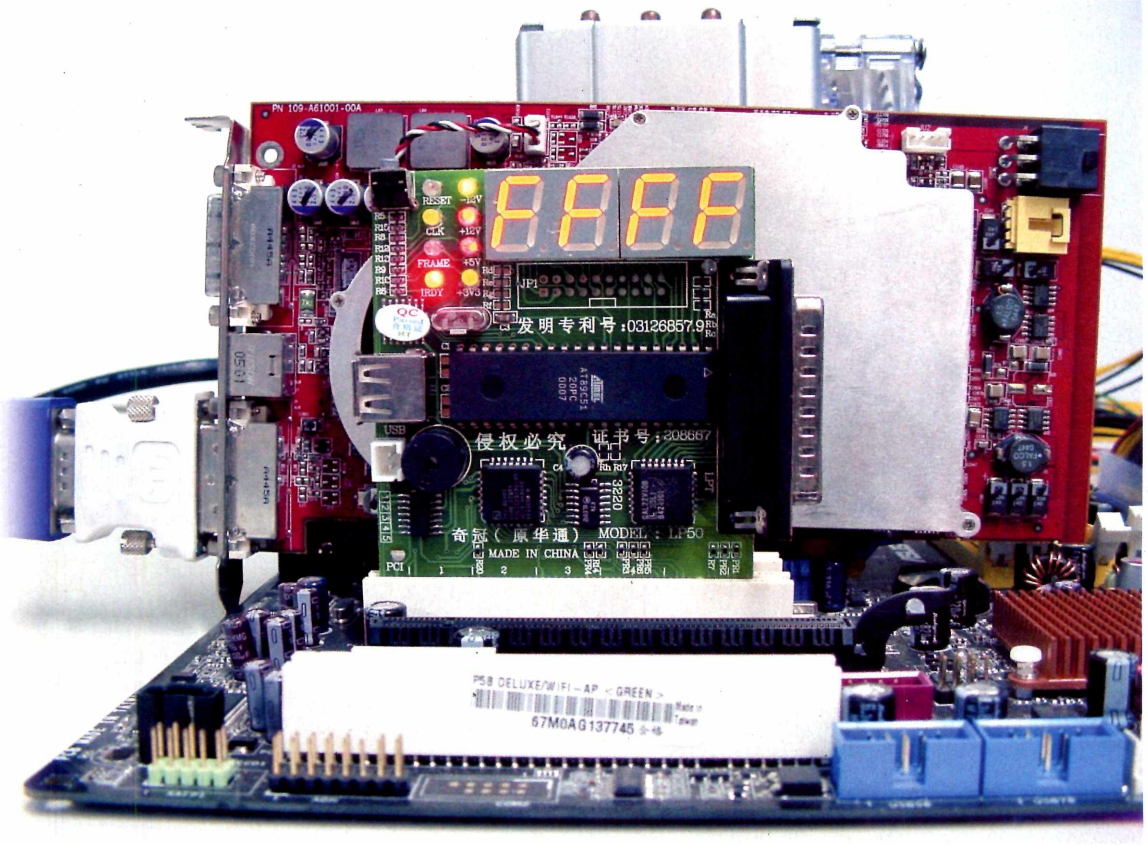
Todas as POST inicializaram normalmente, com exceção da Saber, que mesmo depois de habilitarmos o parâmetro "PCI 2.1 Compliance" no Setup não saiu do FF. A MiniDebug demonstrou-se instáveis em alguns momentos, com seus displays caindo para 00 durante a contagem de memória, por exemplo.

Ficou a dúvida em relação à qualidade do projeto da placa-mãe, uma vez que ambas as POST são compatíveis com esta revisão de PCI.

Já as três POST restantes comportaram-se bem, a Quick POST inclusive foi usada para condenar a fonte AT dessa máquina. A tensão de 12V apresentava picos de 12,74V.

M585LMR

Junto com os processadores AMD K6-2, esta placa-mãe da PCChips foi muita comercializada no Brasil. Seu chipset VIA Apollo MVP4 com vídeo integrado traz também o Ponte Sul 82C686A, compatível com a revisão PCI 2.2. O BIOS utilizado é da versão 4.51PG da Award. No único slot PCI implementado, todas as placas POST funcionaram normalmente, sem quaisquer instabilidades.



F9 Placa UDC travada durante o POST, código FF direto

P5B Deluxe

Com BIOS de revisão 1215 e desenvolvimento da Amibios, esta placa da Asus rodou com um processador Core 2 Duo E6300, 1 GB de memórias DDR2-800 e placa de vídeo Radeon X800XL. O Ponte Sul ICH8R é compatível com o PCI 2.3.

Aqui, as POST UDC e a Analyzer se demonstraram inúteis, porque esse BIOS não possui instruções para jogar os beeps na saída de alto-falante (figura 9). Após a contagem de memória, a Saber travava a máquina durante a inicialização das controladoras USB, exibindo o código 20h. Descobrimos um problema de compartilhamento de interrupção com

uma interface de rede integrada, também conectada ao barramento PCI. Ao desabilitá-la no Setup, a placa conseguia acompanhar o POST até o final. Já as demais, QuickPOST e MiniDebug, funcionaram normalmente mesmo com a interface de rede PCI habilitada.

M748MR-H

Outra placa-mãe da PCChips, da época em que a empresa tinha boa aceitação em nosso mercado. Seu chipset é o SiS620 com Ponte Sul 5595, compatível com o PCI 2.1. Com o projeto de BIOS da Amibios 1996, o teste foi feito com um Pentium III 450 MHz slot 1, um módulo de 128 MB SDRAM e placa de vídeo PCI *offboard*, da S3.

Esse BIOS também não envia beeps para o alto-falante e se destacou por ser um dos poucos que ainda interrompem o POST quando a placa de vídeo está queimada ou não está instalada, por exemplo. O display congela no código F9.

Todas as POST inicializaram normalmente com esta placa-mãe, porém, só a Saber pegava o código referente à ausência da memória RAM, que é o 01, logo após d3. As demais apresentaram um comportamento errático, exibindo os códigos seqüencialmente, um a um, e a uma velocidade inferior em relação ao processamento normal do POST. Além disso, o sistema travava, sequer respondendo aos comandos de teclado.

A8N-SLI Premium

Esta placa da Asus utiliza o chipset nForce 4 com projeto de BIOS da Phoenix-Award, versão 6.00PG. O teste foi feito com um Athlon 64 3000+, Radeon X800XL e dois módulos de 512 MB DDR400.

Foi com ela que as POST mais sofreram de problemas de compatibilidade. Enquanto a UDC e a Analyzer ficam travadas no FF, porque só vão até o PCI 2.2 (e isso apenas com alguns modelos), a Minidebug e até QuickPost travavam já no início do POST.

O display inicializava a exibição, mas após alguns códigos travava no 50. Elas se demonstraram incapazes inclusive de reportar uma falha de memória, uma vez que o código correspondente, C1, vem depois do 50. Já a Saber conseguia acompanhar o POST normalmente até o final, com o código de boot FF, mas por alguma razão travava a máquina se apertássemos Del durante o POST para entrar no Setup. O código do display mudava para 60, sinalizando que a placa entendeu o comando do teclado, mas o monitor não exibia o Setup.

GA 965QM-DS2

Também empregando um chipset com controlador PCI 2.3, este modelo da Gigabyte implementa um BIOS da Award, revisão 6.00PG, e foi avaliada com um Core 2 Quad Q6600, vídeo integrado e 2 GB de memórias DDR2-800.

As POST Saber e Minidebug foram até o mesmo ponto, travando no código 26, um pouco antes da inicialização do controlador de vídeo. É o suficiente para pegar erros com os componentes avaliados pelo segmento *boot block*, como chipset, processador e RAM. Desta vez, a QuickPost foi a única capaz de acompanhar o POST até o código final FF.

P5W DH Deluxe

Esta placa da Asus utiliza o Southbridge Intel ICH7R (PCI 2.3) e BIOS da Amibios 2006, e foi avaliada com um Core 2 Duo E6300, 1 GB de memórias DDR2-800 e Radeon X800XL.

As três POST compatíveis com o PCI 2.3 funcionaram normalmente com esta placa, indo até o final com a exibição do código de boot, 00. No teste sem RAM, todas congelaram no código E0 e o BIOS desta placa também sinaliza falha de memória com beeps. Aliás, foi devido a um beep emitido quando o POST passava pelo código 2A, durante o teste sem placa de vídeo, que conseguimos descobrir uma forma de pegar uma falha com a placa de vídeo, já que os BIOS, via de regra, não travam mais quando isso ocorre.

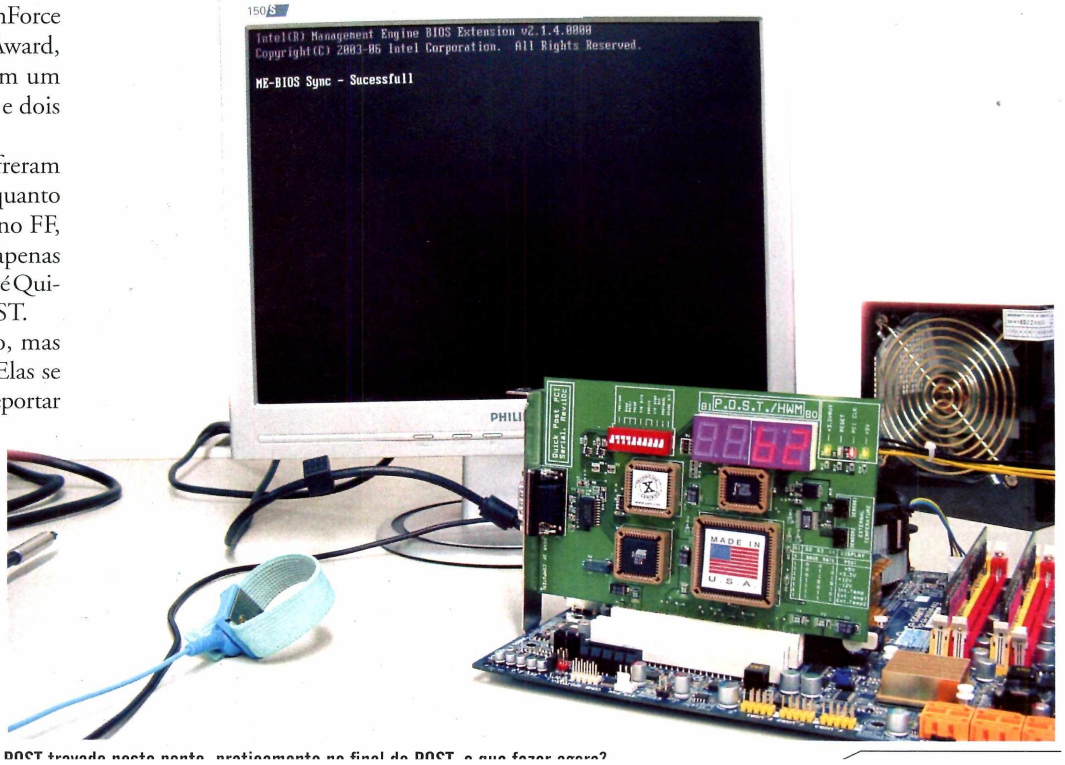
Notamos que quando tudo está normal, o POST executa uma seqüência de testes extra relacionada com o controlador de vídeo, passando por 2C, 31, 33, etc; caso contrário, ele simplesmente salta do 2A para o 38.

915P NEO-V

Outra placa baseada em um chipset Intel, desta vez no Southbridge ICH6, o qual também é compatível com o PCI 2.3. O projeto deste modelo da MSI emprega o BIOS da Phoenix-Award, versão 6.00PG. O sistema base usado nos testes tinha um Pentium 4 HT de 3 GHz, 1 GB de memórias DDR-400 e Radeon X800XL. Semelhantemente ao teste anterior, as três POST se saíram bem com esta placa-mãe.

Conclusão

Cinco placas POST e testes em 10 placas-mãe de diferentes gerações, indo desde um simples Pentium MMX, que hoje já está praticamente encostado, até modelos sofisticados operando com um Core 2 Quad. A primeira constatação é que mesmo as placas de diagnóstico mais simples continuam sendo indispensáveis para quem lida com manutenção. Embora seja possível, não é nada conveniente trabalhar no "escuro", ainda mais se for diante de um cliente.



F10 - POST travado neste ponto, praticamente no final do POST, o que fazer agora?

Por outro lado, é necessário tomar cuidado com alguns projetos de placas POST que, a exemplo de duas avaliadas aqui (UDC e Analyzer), são projetos antigos que apresentam problemas de compatibilidade para funcionarem até com placas de revisão PCI 2.2 e sequer mencionam isso em seus manuais. A atuação delas é ainda mais restrita porque muitas placas-mãe recentes não enviam mais os beeps para o alto-falante.

Além disso, convém ressaltar que mesmo no caso da melhor POST avaliada aqui, a QuickPost da Ultra-X, não é possível ter 100% de certeza quanto à compatibilidade com as placas-mãe disponíveis no mercado, como foi o caso da Asus A8N-SLI. A limitação neste caso pode ter se dado tanto devido à placa-mãe, quanto ao projeto do chipset. O que é fato, e que poucos usuários se dão conta disso, é que muitos detalhes contidos nas especificações de padrões abertos como PCI, ATX, etc, são recomendações, não imposições.

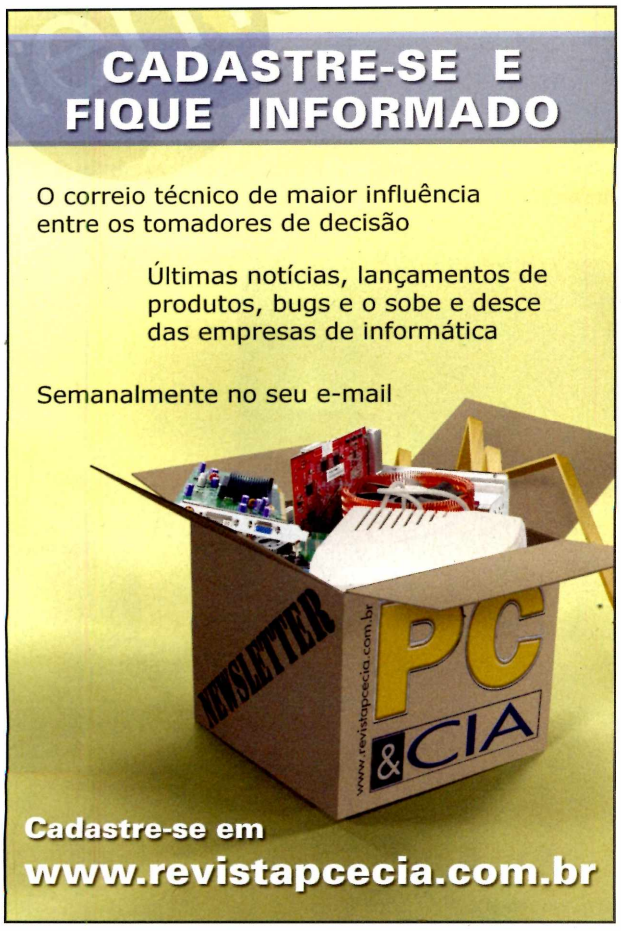
E também não há nenhuma entidade que homologue projetos de placas e chipsets e libere o fabricante para estampar um selo do tipo "PCI ou ATX compliance". Portanto, quem deve fazer isso é o próprio usuário, ou no caso aqui, o fabricante que estiver por trás da placa POST.

Outro detalhe importante diz respeito aos códigos POST. Primeiro, vale ressaltar que são poucas as tabelas a serem consultadas. Veja que varremos um amplo espectro de placas-mãe e ao final chegamos à conclusão que só precisamos de duas tabelas da Award, uma referente ao BIOS 4.51PG e outra para 6.00PG (isso também vale para Award-Phoenix), e uma da Amibios. São tabelas genéricas que apresentam os códigos padrão colocados nos BIOS por esses dois fabricantes, cujos sites atuais são **www.phoenix.com e www.ami.com**, respectivamente. Porém, a versão final de cada BIOS depende exclusivamente do fabricante de placa-mãe. Afinal, é ele quem define o projeto da placa e sabe se haverá uma rotina de inicialização durante o POST para tratar do BIOS de uma controladora RAID SATA *onboard*, ou do BIOS referente à tecnologia de gerenciamento ativo da Intel (vPro), que está integrada na placa GA 965QM-DS2 da Gigabyte, por exemplo (figura 10).

O travamento reportado na figura aconteceu após a contagem e teste de RAM, vídeo e barramentos, praticamente antes do início do boot. Com a placa POST podemos ter pelo menos uma trilha do defeito, já que o display, neste caso, ficou congelado em 62. Porém, ao ir à tabela da Award encontramos apenas o significado "Reserved", isto é, de implementação específica do fabricante, que neste caso é a Gigabyte. Nenhum manual de placa POST apresentou o significado e nem seus respectivos sites de suporte, que conforme estamos fazendo questão de frisar aqui, exercem um papel fundamental. Resultado: estamos aguardando uma posição da Gigabyte, e depois de muita tentativas, neste caso no "escuro", descobrimos que o causador do problema é a controladora IDE. É só desconectar o HD IDE (um Samsung SP2514N) da controladora que a máquina conclui o POST e faz o boot a partir de um HD SATA ou LiveCD, por exemplo. E o HD Samsung foi testado em outra máquina e respondeu bem.

Portanto, é indiscutível que uma boa placa POST ajuda e muito durante o diagnóstico, mas por outro lado é preciso ter em mente que ela não é a salvação da lavoura. Em relação aos sites de suporte das placas avaliadas aqui, segue a lista: QuickPOST (**www.uxd.com.br**), Ultimate Diagnostic Card (**www.winmicrorio.com.br**) e Saber (**www.revistapcecia.com.br/placapost**).

PC



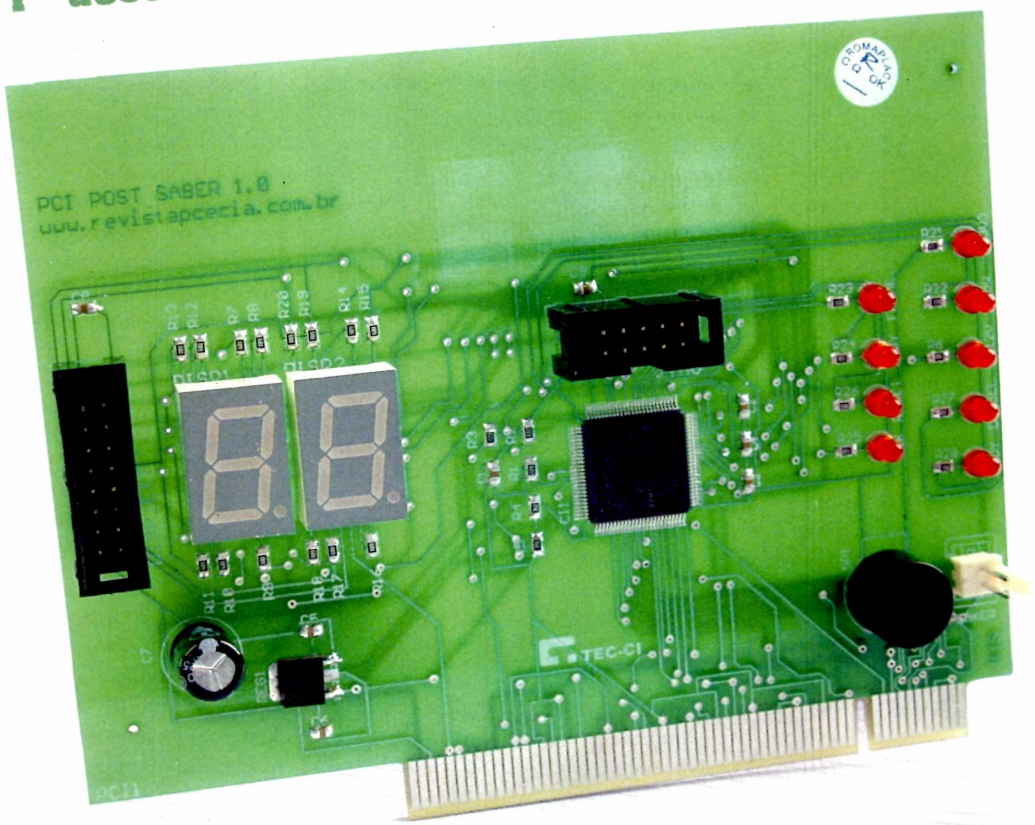


Mais de 30 milhões
de micros que podem precisar de manutenção

A única revista brasileira capacitada tecnicamente para ajudar você, projetou uma placa POST exclusiva para um diagnóstico mais rápido e preciso.

Afinal um micro não pode ficar parado!

A 1ª desenvolvida no Brasil e com suporte local!



Esta placa pode ser sua!
Acesse www.revistapcecia.com.br/placapost
e saiba como obtê-la.

SABER



Memórias DDR3

Conheça aqui as memórias DDR3 e saiba como elas podem te ajudar.

Marcus Brandão de Moura

Mais um novo tipo de memória

Não é de hoje que o desempenho das memórias RAM fica abaixo do desempenho dos microprocessadores. A última vez em que eles estiveram equiparados foi na geração dos 80386 de 40 MHz. Nessa ocasião tínhamos os pentes de memória SIMM de 30 vias e 8 bits, com tecnologia Fast Page Mode, funcionando a 16, 33 e até 40 MHz. Essas memórias não eram acessadas diretamente pelo microprocessador. Isso só era feito através da memória cache de 128 KB, que era externa, para ciclos de escrita. Mas essas memórias já estavam no limite e quando surgiram os 80486 não havia como equiparar o desempenho das memórias RAM com o dos microprocessadores.

Nesse período "histórico" surgiu o conceito do FSB e dos multiplicadores, que estão presentes até hoje. De lá para cá já tivemos memórias FPM, EDO, SDRAM, RDRAM, DDR-SDRAM e DDR2. As memórias DDR3 já estão no mercado, porém há quem diga que as FB-DIMM poderão causar "problemas" às ambições comerciais daqueles que estão por trás das DDR3. Principalmente nas plataformas de servidores. À exceção das memórias RDRAM, por enquanto, todas as outras marcaram época e se consolidaram.

O fato é que de alguma maneira os 80386 deixam saudades, não só por ter sido a geração de microprocessadores que mais tempo ficou no mercado, com incríveis sete anos, mas também porque foi a última vez na história em que o desempenho das memórias se equiparava ao desempenho dos microprocessadores.

Assim surgiram as memórias DDR-SDRAM, DDR2 e agora as DDR3, que seguem uma mesma linha tecnológica, mas com avanços significativos a cada nova geração.

Memórias DDR

Quando as memórias DDR-SDRAM surgiram, trouxeram como principal característica a capacidade de transferir duas vezes mais informações do que as SDR-SDRAM de mesma freqüência. Isso ocorre porque as memórias DDR conseguem transferir dois bits por ciclo de clock, contra apenas um das SDR-SDRAM. Essa é a principal diferença.

Além dessa diferença, aos poucos as memórias DDR passaram a trabalhar em uma freqüência real mais elevada, o que melhorava o desempenho. De início, a latência das memórias SDR-SDRAM era mais agressiva do que a das DDR, entretanto com o avanço constante da tecnologia, a diferença entre as latências foi diminuindo, abrindo ampla vantagem para as DDR-SDRAM sobre as SDR-SDRAM.

As memórias DDR2 trouxeram uma capacidade de operação a freqüências reais mais altas e um novo processo construtivo dos chips de memória que oferecia melhor dissipação térmica e maior proteção para os contatos elétricos. Isso acaba refletindo na menor vulnerabilidade dos chips de memória aos efeitos da energia eletrostática.

As memórias DDR3 seguem a mesma receita bem sucedida de evolução tecnológica e comercial. Mais uma vez, como sempre houve entre as DDRs, o encaixe físico do pente de memória é diferente de suas gerações anteriores, isso evita encaixes errados feitos por falta de atenção.

A tabela 1 mostra uma comparação entre as memórias DDR, DDR2 e DDR3.

Assim como as memórias DDR2, as DDR3 também têm 240 pinos em seus pentes convencionais de 64 bits e 72 bits para os pentes com ECC ou registrados.

Os principais módulos de memória DDR3 terão as características descritas na tabela 2.

As únicas diferenças físicas nos pentes de memória DDR3 em relação aos DDR2 são o posicionamento da fenda de encaixe entre os contatos e a existência de dois pontos de trava mecânica em cada extremidade lateral do módulo de memória. Fora isso, são quase iguais.

Já no atual estágio de desenvolvimento do projeto das memórias DDR3, notamos que elas podem ser até duas vezes mais rápidas do que as memórias DDR2.

As diferenças mais destacadas entre as memórias DDR2 e as DDR3 são a redução de tensão de alimentação de +1,8VCC (+

ou – 0,1) para +1,5VCC (+ ou – 0,075), freqüências reais mais altas, alterações de geometrias de circuitos internos e a possibilidade da inclusão de sensores para leitura de temperatura. Esta é uma ótima idéia, porque em breve será necessário.

As melhorias relacionadas à dissipação térmica ficam em torno de 16% se comparadas às memórias DDR2, com isso, as DDR3 podem oferecer o dobro da dissipação térmica por Watt. Além disso, um sistema de refresh seletivo permite que as memórias DDR3 consumam ainda menos energia elétrica e ainda ofereçam um acréscimo de desempenho.

As latências das memórias DDR3 estarão em declínio constante. O novo arranjo de oito bancos de memória internos contra apenas quatro das DDR2 vai ocasionar um incremento do prefetch e com isso as latências tendem a diminuir, assim como também deve diminuir o tempo que o computador, através do BIOS, leva para configurar as memórias instaladas.

Com o uso de freqüências mais altas, o desempenho tende a aumentar, mas a comunicação de dados no interior dos chips e também no módulo inteiro tende a ficar mais crítica. Para evitar problemas de integridade de dados, um novo caminho de transmissão foi estabelecido (figura 1), por onde trafegam comandos e endereços. Esse caminho é chamado de "fly-by" e o caminho usado nas DDR2 era conhecido como "T branches". Cada memória DDR3 possui um circuito de calibração e memorização desse caminho. Essa calibração é feita automaticamente toda vez que se liga um computador equipado com memórias DDR3.

Tanto o controlador de memória quanto os módulos precisam de uma área do núcleo (die) dos chips para abrigar essas novas funções. Certamente isso resultará em um maior custo, mas tal custo será diluído com o aumento da demanda.

Os módulos de memórias DDR3 registrados possuem dois caminhos "fly-by" individuais, um para cada metade dos chips de memória. Isso gera uma dificuldade técnica para se manter ambos os caminhos perfeitamente sincronizados entre si, porém otimiza o desempenho.

A melhor maneira de se aproveitar todo o potencial das DDR3 é usá-las em um sistema cujo FSB seja o mesmo da freqüência real de operação das memórias, preferencialmente em dual channel.

Os problemas de se estabelecer freqüências mais altas para comunicação de dados é que a integridade da comunicação fica cada vez menos precisa. Comece a se acostumar a ler termos empregados em comunicação sem fio de dados, como *strip line*, *micro strip*, impedância de terminação e perda de retorno, associados às memórias DDR3.

Os pentes de memória DDR3 de até 1.333 MHz podem trabalhar em controladoras dual channel, entretanto os pentes com freqüências a partir de 1.600 MHz só são capazes de trabalhar em controladoras single channel. Pelo menos por enquanto.

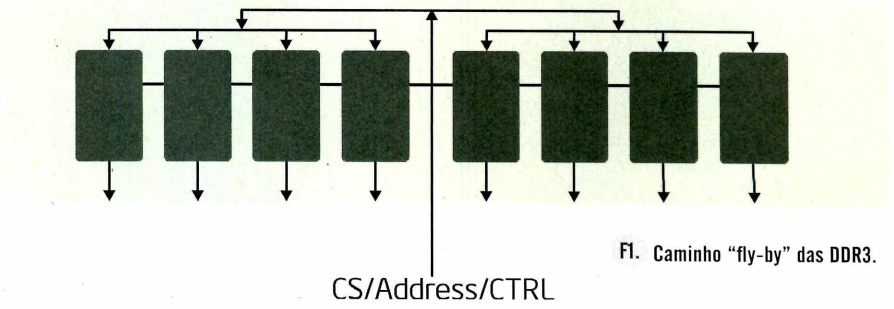
Os chips de memória DDR3 serão fabricados em larga escala com densidades de armazenamento de 512 Mbit a 8 Gbit e densidade de produção dos circuitos da ordem de 60 a 50 nanômetros. Os módulos de memória terão entre 256 MB e 8 GB. Por enquanto, os preços das DDR3 são razoavelmente mais altos, mas há uma expectativa de que no segundo quadrimestre de 2008 os preços das DDR2 e das DDR3 sejam equiparados. No momento, dois pentes de memórias DDR3 de 1GB e 1.333 MHz custam pouco menos de R$ 2 mil, enquanto que dois pentes de memória DDR2 de 1GB e 1.066 MHz custam R$ 1.100. Mas dois pentes de memória DDR2 de 1GB e 1.250 MHz custam elevados R$ 2.450. Espera-se que em 2009 a participação das DDR3 no mercado seja de aproximadamente 65%.

	DDR	DDR2	DDR3
Taxa de transmissão	De 200 a 400 Mbps	De 400 a 800 Mbps	De 800 a 1600 Mbps
Tensão de alimentação	2,5VCC +/- 0,2VCC	1,8VCC +/- 0,1VCC	1,5VCC +/- 0,075VCC
Interface	SSTL_2	SSTL_18	SSTL_15
Encapsulamento	66 TSOP2, 60 BGA	60 BGA para x4/x8 84 BGA para x16	78 BGA para x4/x8 96 BGA para x16
Transmissão em modo burst	2, 4, 8 com 2 bits de prefetch	4, 8 com 4 bits de prefetch	4, 8 com 8 bits de prefetch
Número de bancos	4 bancos	512Mb: 4 bancos 1024Mb: 8 bancos	512 e 1024Mb: 8
CL/tRCD/tRP	~ 15/15/15 ns	~ 15/15/15 ns	~12/12/12 ns
Reset	Não	Não	Sim
Calibração de driver	Não	Calibração fora do chip	Autocalibração pelo pino ZQ

T1. Comparação de características técnicas dos chips de memória DDR-SDRAM, DDR2 e DDR3.

Padrão	Tipo	Freqüência real	Transferência de dados (freqüência comercial)	Taxa de transferência
PC3-6400	DDR3-800	400 MHz	800	6400 MB/seg
PC3-8500	DDR3-1066	533 MHz	1066	8530 MB/seg
PC3-10667	DDR3-1333	667 MHz	1333	10660 MB/seg
PC3-12800	DDR3-1600	800 MHz	1600	12800 MB/seg
PC3-14900	DDR3-1866	933 MHz	1866	14930 MB/seg

T2. Características dos principais módulos de memória DDR3 comercializados.



F1. Caminho "fly-by" das DDR3.

Conclusão

As memórias DDR3 representam mais um avanço para tentar minimizar a diferença de desempenho entre os microprocessadores e as memórias DRAM e assim assegurar um maior desempenho ao sistema como um todo.

Acreditamos que antes de 2009 os problemas técnicos que eventualmente atrapalhem um pouco esta nova tecnologia de memórias possam estar totalmente resolvidos.

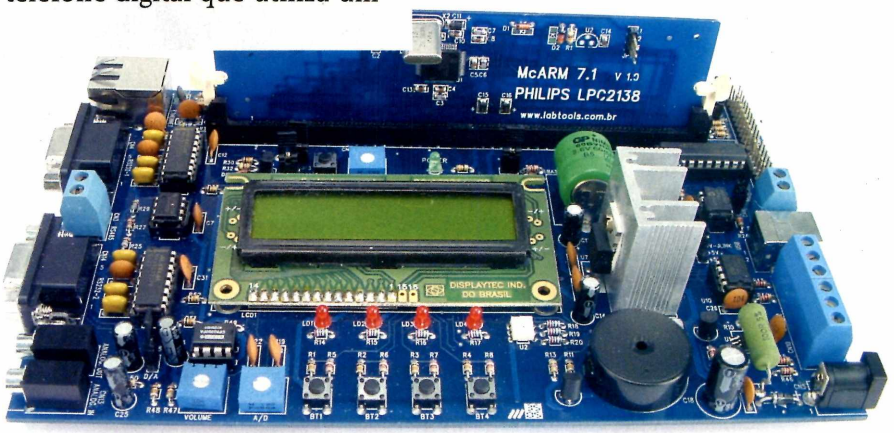
Definitivamente teremos um melhor desempenho com menor consumo de energia elétrica e menor aquecimento com as memórias DDR3, se comparadas às DDR2.

É esperar um pouco e comprar! Até a próxima. **PC**

Desenvolvendo

Parte 2

Assim como dissemos no artigo anterior, o desenvolvimento de soluções integradas será uma grande fonte de projetos nos próximos anos, principalmente por se tratar, na maioria dos casos, de sistemas de processamento em tempo real. Que tal conciliar seus conhecimentos em hardware com os de programação para explorar mais um nicho de mercado? Nesta matéria você encontrará as instruções sobre a plataforma RISC e as formas de compilação e debug dos programas, tendo em vista a construção de um telefone digital que utiliza um ARM7 de 32 bits.





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

Desde o início a arquitetura ARM teve a iniciativa de manter o hardware simples, por este motivo os processadores ARM se transformaram em líderes de mercado no segmento de sistemas embarcados. Além de se adaptarem muito facilmente às necessidades de cada aplicação, eles têm custo muito reduzido se comparado ao de outras arquiteturas.

Podemos encontrar processadores em telefones celulares, máquinas fotográficas digitais, aparelhos de som, impressoras, máquinas de lavar, fornos de microondas, automóveis e em uma série de outros equipamentos. Os sistemas embarcados exigem que os fabricantes utilizem recursos limitados se comparados à computação mais tradicional. A redução cada vez maior do custo, melhor utilização da memória e o consumo de energia tornam-se ainda mais fundamentais, uma vez que muitos sistemas embarcados utilizam baterias, as quais devem propiciar uma autonomia suficiente para mais atividades a cada dia.

Tomaremos como base para este artigo a plataforma ARM7 de 32 bits, empregada no microprocessador LPC2138, e a placa de desenvolvimento MCBoard, ambos da NXP (**www.nxp.com**). Essa placa facilita muito o desenvolvimento de aplicações para diversos segmentos (automação e sensoriamento, por exemplo) porque já vem com uma série de recursos, periféricos e conectores que agilizam o processo de programação: LCD alfanumérico, teclas e leds (quatro leds convencionais e 1 RGB), buzzer, memória serial EEPROM 24WC256 (protocolo I²C), sensor de temperatura LM75A (protocolo I²C), aquecedor, interfaces seriais RS232 (x2) e RS485, conversor A/D, dois conectores de expansão com 40 I/O cada, conector com 16 saídas bufferizadas, conector para utilização do depurador J-Link, entrada e saída de áudio, botão de reset manual, gravação in-circuit compatível com o programa Flash Utility 2.2.2 (via RS232-1), além de comunicação I²C (x2), SPI, CAN, USB e Ethernet.

Falando do nosso projeto, utilizaremos essencialmente os recursos de conversão ADC (analógico-digital), DAC (digital-analógica), a entrada/saída de áudio, a interface Ethernet, além de botões e leds para controle.

Processamento de dados em ARM

Iniciaremos nosso projeto entendendo melhor como podemos trabalhar com o processamento de dados. Uma vez que iremos tratar de um telefone digital, isto significa essencialmente que teremos um conversor Analógico-Digital para realizar a amostragem da voz e transformá-la em uma seqüência de bits. Por este motivo, é essencial conhecermos a estrutura de registradores e memória que utilizaremos neste processo. Tal como ocorre na maioria dos processadores RISC, o ARM utiliza uma arquitetura load-store, ou seja, as instruções processam apenas informações disponíveis em registradores e sempre armazena seus resultados também em um registrador.

No ARM 7, existem 15 registradores de propósito geral em modo aberto (r0-r14) e o PC (program counter, ou contador de programa (r15)). No modo protegido, existem outros vinte registradores com funções específicas. Outras características do ARM7 são:

luções Integradas

- Uniformidade e tamanho fixo dos campos das instruções para simplificar a sua decodificação;
- Execução condicional;
- Auto-incremento e decremento dos endereços das instruções;
- Instruções de múltiplos loads / stores para melhorar o desempenho;
- Controle sobre a ALU (unidade lógica e aritmética) e o shifter (deslocador) em todas as instruções de processamento de dados.

Além disso, a arquitetura possui mais um registrador de controle CPSR capaz de armazenar quatro *flags* de condição, os quais gravam resultados de comparações ou características específicas da última operação. Os quatro *flags* de condição são:

- *Negative:* Será 1 se a última operação da ULA que alterou os *flags* produziu um resultado negativo;
- *Zero*: Será 1 se a última operação da ULA que alterou os *flags* produziu zero como resultado;
- *Carry*: Será 1 se a última operação da ULA que alterou os *flags* produziu um *carry-out* ("vai um" ao dígito de ordem mais alta);
- *Overflow*: Será 1 se a última operação da ULA que alterou os *flags* produziu um descarregamento de pilha no bit de sinal.

O *pipeline* da arquitetura apresenta oito estágios com algumas características básicas:

- Todas as instruções ocupam o *datapath* (barramento de dados) por um ou mais ciclos de *clock* adjacentes;
- Sempre que uma instrução ocupa o datapath em determinado ciclo, a mesma instrução necessariamente ocupou a unidade de decodificação e controle no ciclo imediatamente anterior;
- Durante seu primeiro ciclo no datapath, a instrução deve executar a busca da próxima instrução mais uma;
- As instruções de branch (desvio) esvaziam o pipeline e voltam a preenchê-lo com as instruções apropriadas.

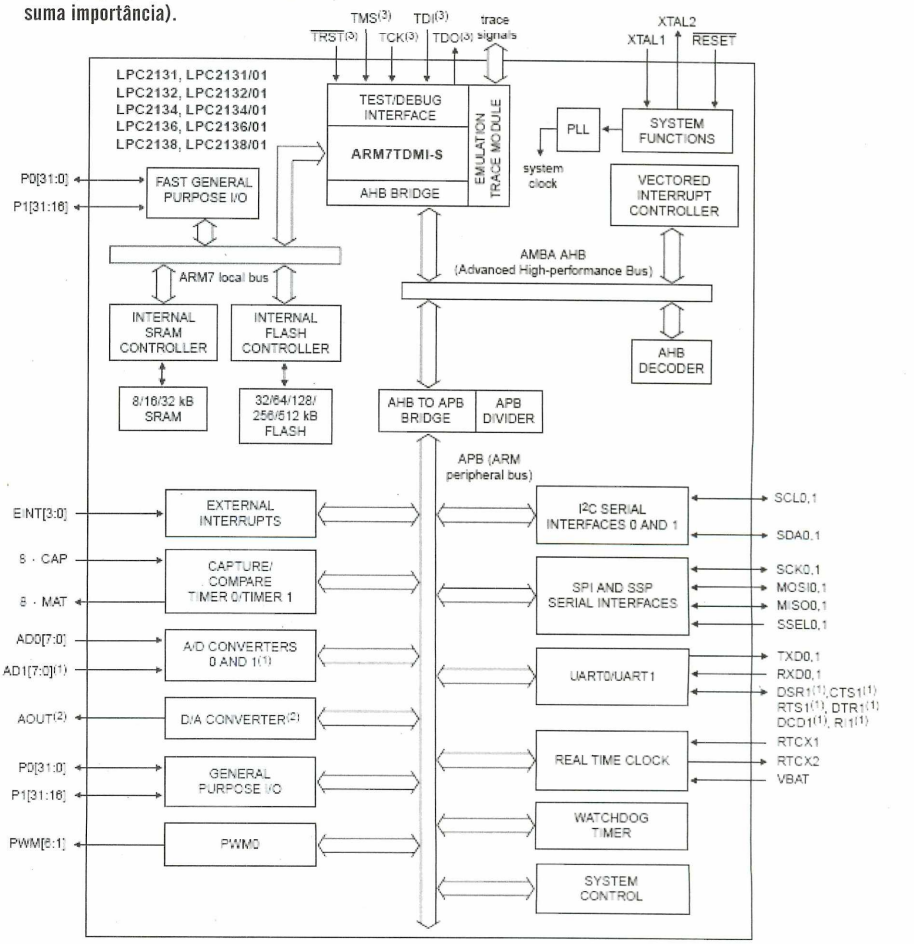
Este comportamento do pipeline sugere que no estágio de execução o PC (R15) deve conter sempre o valor da instrução corrente mais oito, uma vez que o endereçamento é baseado em bytes e as instruções são todas de 32 bits (4 bytes). Isto de fato acontece, e deve-se atentar para este fato no caso de se alterar o valor de PC ao escrever diretamente no registrador R15, embora o assembler ou o compilador acertem esse tipo de detalhe na maioria dos casos (figura 1).

Além do diagrama de blocos, você pode encontrar o esquema de pinos e suas respectivas funções. Esse diagrama pode ser muito útil no momento de diagramar a placa ou mesmo durante os testes em protoboard, se você não estiver utilizando um kit de desenvolvimento específico.

Manipulação da Memória

Por serem encontrados em diversos tipos de aplicação, os requisitos de memória dos processadores ARM variam conforme a finalidade de utilização, tendo-se como base os seguintes recursos: múltiplos tipos de memória, caches, buffers de escrita, memória virtual e outras técnicas de mapeamento. O CP15, também conhecido como co-processador de Controle de Sistema, é responsável por realizar o controle do sistema de memória padrão do ARM e suas facilidades. Ele pode conter até 16 registradores primários, com 32 bits cada um. E para alguns destes registradores, existem bits adicionais usados para identificar uma versão específica do registrador e/ou o tipo de acesso específico do registrador.

F1. Montagem interna do LPC2138 demonstrando a distribuição das funções e periféricos na arquitetura ARM (para os próximos passos de nosso projeto, o ADC e o DAC serão de suma importância).



Os processadores foram projetados para serem conectados a uma memória endereçada por byte, ou seja, cada endereço da memória corresponde a um byte. Dessa forma, para ter acesso a uma *word* (palavra) os dois bits menos significativos são ignorados, e caso se queira ter acesso a uma *half word* (meia-palavra), apenas o bit menos significativo é ignorado. Vale ressaltar que o formato dos dados de um processador ARM é igual ao formato do sistema de memória comumente encontrado nos PCs, por exemplo, com a memória usada para armazenar os programas estando dividida em Memória Principal (RAM) e Memória ROM.

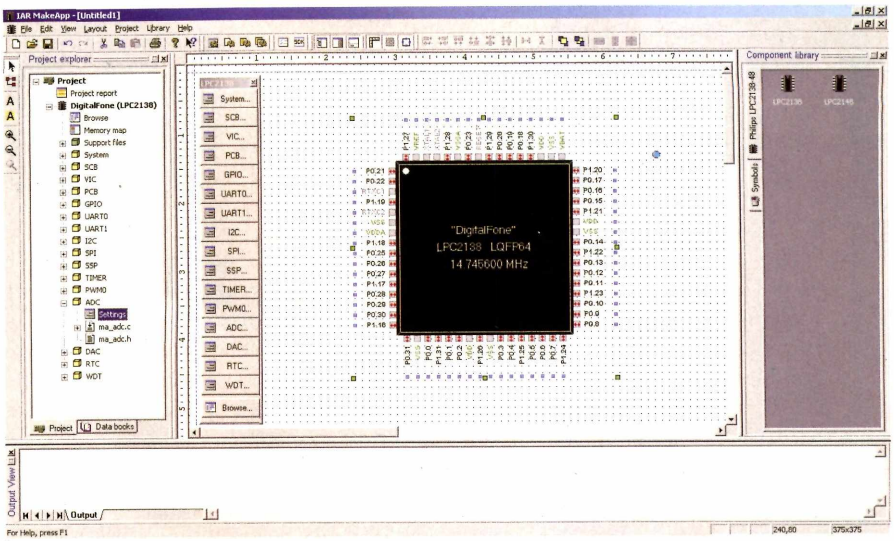
O sistema de memória de primeiro nível é composto por cache de instrução e dados separados, áreas separadas de memória para instruções e dados, sistema DMA (Direct Memory Access – acesso direto à memória) para acessar a memória, buffer de escrita e duas micro-TLBs.

Cada local de memória na cache é conhecido como linha de cache. A cache no ARM é full associative, o que significa dizer que ela é associativa por conjunto de N vias, sendo N o número total de linhas de cache. Assim, qualquer busca na cache precisa checar cada linha de cache.

A cache é também mapeada diretamente, ou seja, a cache é associativa por conjunto de N vias, com um conjunto de N blocos e uma entrada podendo residir em qualquer bloco dentro desse conjunto. O tamanho das linhas de cache é sempre uma potência de dois e tipicamente são de 16 bytes (4 words) ou de 32 bytes (8 words). A política de substituição utilizada pela cache dos processadores ARM pode ser pseudo-randômica. Quanto ao tamanho, o sistema de memória ARM permite diferentes tamanhos de cache, dependendo da importância de desempenho no próprio dispositivo.

Os processadores ARM dividem sua cache em duas partes: uma cache exclusiva para dados e outra para instruções, podendo acelerar o processo de execução, já que são permitidas instruções de leitura e escrita num mesmo ciclo de clock. E o tamanho da cache de dados pode diferir do tamanho da cache de instrução.

Para cada cache existe uma área da memória RAM dedicada também separadamente, uma para dados e outra para instruções. Essas áreas são chamadas de TCM. A TCM foi desenvolvida com o objetivo de fornecer uma memória mais estável que as caches, e ao mesmo tempo com baixa latência. Assim, elas são utilizadas para conter rotinas críticas.



F2. Tela inicial de um projeto com o componente LPC2138 adicionado.

Compiladores e Debugers

Existem muitos compiladores diferentes para ARM. Alguns deles são gratuitos, com destaque para o GCC (Gnu Compiler Collection), que nos permite utilizar as bibliotecas C/C++ e assembler, cujas bibliografias estão disponíveis para consulta na Internet. O GCC é poderoso e possivelmente seja uma das soluções de compilação mais usadas no planeta. Com ele você faz código seguro, robusto, veloz e eficiente usando linguagem de alto nível, além de também compilar códigos desenvolvidos na linguagem assembly.

Para construir aplicações sobre o ARM, você pode encontrar uma grande quantidade de códigos abertos para as mais diversas finalidades, inclusive com drivers de dispositivos, como é o caso de codificadores e decodificadores de áudio (MP3, por exemplo), GSM, bibliotecas de criptografia, compactadores, drivers de LCDs gráficos, players de vídeos, drivers de controle da serial, drivers para controle USB, drivers TCP/IP, servidores web, emuladores e linguagens de script, bibliotecas para comunicação GPRS e com GPS, etc.

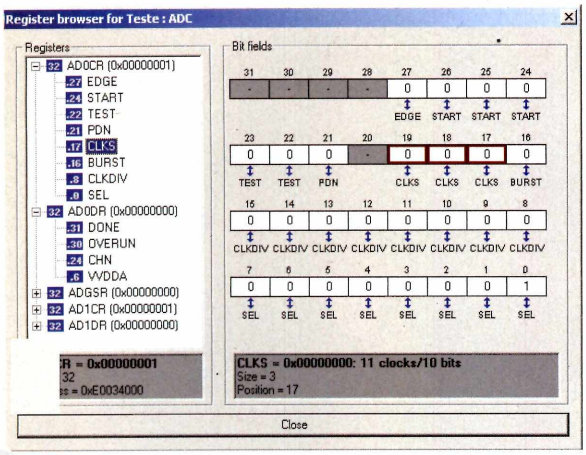
No caso específico da placa McBoard, o kit enviado conta com outros dois programas desenvolvidos pela IAR que serão muito úteis no desenvolvimento. Um deles é o IAR MakeAPP, uma espécie de gerador de código C, cuja configuração é realizada pelo próprio usuário, o que facilita bastante a criação e organização de novos projetos baseados na configuração inicial do componente (figura 2).

Para inserir o componente basta iniciar um novo projeto, abrir o menu *Component Library* e arrastar o LPC2138 para a área de trabalho do aplicativo. Após, clique duas vezes no componente e configure sua freqüência de operação, que neste caso será de 20 MHz. Note que, uma vez realizada esta operação, a janela de periféricos aparecerá automaticamente e nela você poderá configurar e programar todas as funções sem muito esforço de programação. Navegando por suas funcionalidades, você poderá configurar e programar os registradores de uma forma gráfica e amigável, conforme mostrado na figura 3.

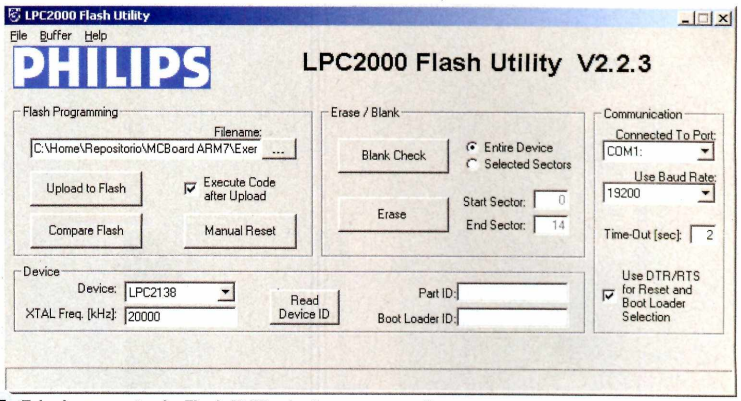
Além do *MakeApp*, a IAR disponibiliza o IAR *Embedded Workbench*, o compilador/debugger dos códigos C gerados a partir do *MakeApp*, por exemplo. Este é o editor de códigos C em sua essência, aqui você poderá alterar os códigos, compilar os programas e depurá-los. É essencial que configuremos qual dispositivo está sendo utilizado neste ambiente. Para isto, acesse o menu *Project > Options*, clique em *General Options* e depois escolha o modelo Philips:LPC2138 na caixa *Device*. Isto fará com que todas as bibliotecas sejam reconhecidas e inseridas no projeto.

Na figura 4 é possível visualizar um código C sendo editado. Além da linguagem C, o editor também reconhece e compila códigos assembly. Depois de configurado, basta acessar o botão *Make* para gerar o arquivo binário que será usado para a gravação do microprocessador.

Por último, existe o utilitário *Flash Utility* fornecido pela própria Philips. Esta ferramenta é responsável pelo processo de gravação do microprocessador. Para isso configure a porta do computador na qual a placa de gravação está conectada, além da velocidade de comunicação, que geralmente é configurada em 19200bps. Depois



F3. Tela de programação dos registradores.



F5. Tela de operação do *Flash Utility*, junto com as configurações necessárias para se gravar o ARM LPC2138.

de configurado, você deve acessar o botão *Erase* para apagar o conteúdo do processador e somente depois clicar em *Upload to Flash*. Para realizar esta operação, você deve selecionar previamente na caixa *Filename* o arquivo binário gerado na compilação mencionada anteriormente. Depois de realizada esta operação, seu processador já estará disponível para utilização com o novo programa carregado (figura 5).

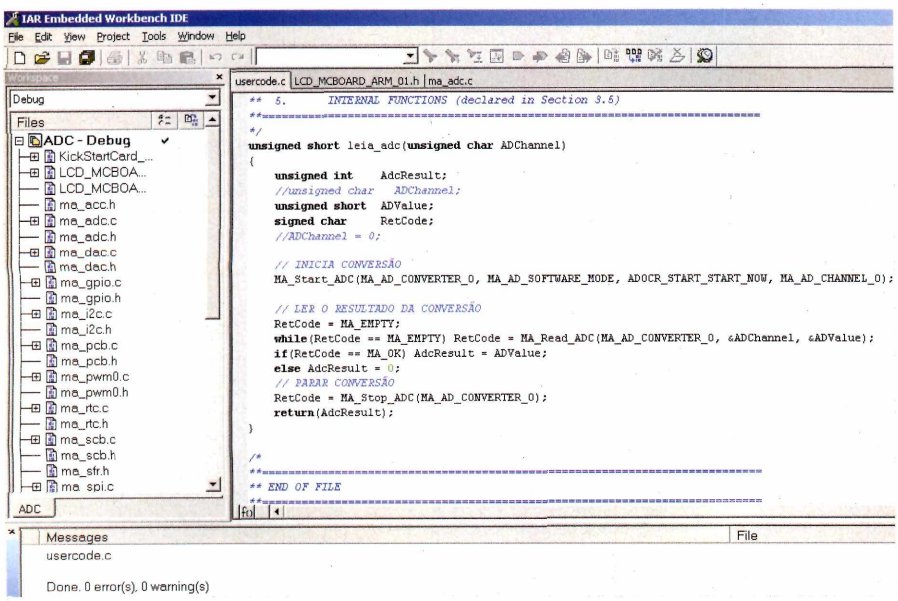
Conclusão

A arquitetura ARM é implementada em grande parte dos processadores de 32 bits atuais, principalmente devido à sua versatilidade de uso em diversas aplicações práticas, pelo bom desempenho que apresenta e pela constante atualização de novas versões que são lançadas pela ARM. Esse sucesso pode ser atribuído à dedicação exclusiva no desenvolvimento de projetos dos processadores, sem se preocupar com questões mercadológicas do produto final. Mas apesar de muito utilizados, os processadores ARM são muito pouco conhecidos, principalmente pelos usuários finais.

Como dissemos anteriormente, os processadores ARM são principalmente utilizados em dispositivos móveis, como PDAs, Smartphones e equipamentos de rede, sendo que a grande expansão desse mercado é um fator determinante que promete manter por muito tempo o uso dessa arquitetura.

No próximo artigo entraremos a fundo nos códigos C para a construção de um Codec de voz utilizando-se do LPC2138, assim como outras informações importantes para o aproveitamento deste poderoso microprocessador.

PC



F4. Editor, compilador e debugger de código escrito em linguagem C.





HDs de 750GB

Enquanto a nova safra de HDs SSD (Solid-State Disk – Disco de estado sólido) não chega ao mercado, confira nesta matéria um comparativo entre dois discos rígidos que vão na direção de necessidades por armazenamento cada vez maiores.



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

Capacidade ou desempenho?

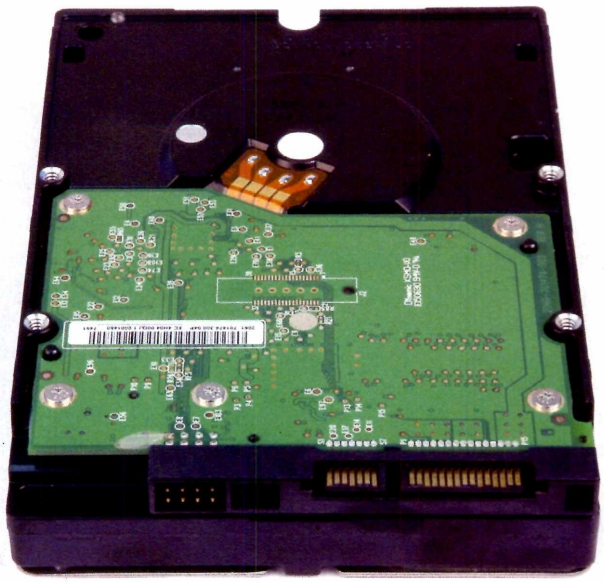
Seja em um ambiente doméstico ou corporativo, é o subsistema de disco que poderá, ou não, fazer toda diferença na usabilidade de uma aplicação ou serviço disponível na máquina. A capacidade de armazenamento e o custo são aspectos importantes, mas não fundamentais. O desempenho e a confiabilidade devem estar em pé de igualdade, ou melhor, condizentes com a carga de trabalho que os HDs deverão exercer. Dentre os diversos cenários onde essa afirmação é verdadeira, podemos citar a virtualização. O crescimento de servidores virtuais (de arquivos, Web ou banco de dados, por exemplo) dentro das empresas tem realçado a importância do desempenho dos discos rígidos. Principalmente quando as máquinas virtuais são criadas para promover recursos de armazenamento de dados na rede. Nesses ambientes virtuais, a carga de I/O gerada nos discos rígidos é algo constante. Quanto menor forem os tempos médio de leitura e escrita, melhor. É claro que outros fatores, como velocidade rotacional e o suporte ao enfileiramento de requisições (NCQ - Native Command Queuing), também são relevantes. Agora resta-nos saber se além de "gigantes" os novos HDs andam em sintonia com o aspecto desempenho.

WD Caviar SE16

Dentro da categoria *mainstream*, ou intermediária, a família de discos rígidos Caviar SE16 (**www.wdc.com/pt/products/Products.asp?DriveID=311**) é hoje a opção de maior performance dentro da Western Digital. Está disponível em modelos de 200GB, 250GB, 320GB, 400GB, 500GB e 750GB, com opções de interface SATA II de 300MB/s e Ultra ATA de 100MB/s. Aliás, a única diferença entre os modelos SATA II e UATA é em relação ao tamanho dos discos rígidos (apenas 320, 400 e 500GB no UATA). Ou seja, independente da interface de comunicação, toda linha Caviar SE16 apresenta as mesmas especificações técnicas para todos os HDs, a exemplo da velocidade rotacional de 7200 RPM, do buffer de memória de 16MB, e de tempos médios para leitura e escrita de 8,9ms e 10,9ms, respectivamente. A taxa média para o pior caso, quando o mecanismo atuador percorre a maior distância (mais conhecido como full-stroke) sobre a superfície do disco é de 21ms (figura 1).



F1. Caviar SE16 (código WD7500AAKS): 750GB distribuídos através de 4 discos. Cotado a US$ 190 no exterior, no site de referência www.newegg.com.



Um diferencial dos Caviar SE16 é o denominado Intelligent Seek, um recurso que visa a otimizar o tempo gasto pelo mecanismo atuador para localizar determinados setores do disco (ver box).

Outros recursos presentes são a tecnologia de gravação perpendicular dos dados – utilizada atualmente no processo de fabricação dos discos para alcançar maiores densidades - e o NCQ. A documentação da empresa apresenta 60ºC como temperatura limite para a operação deste disco. O consumo de energia típico declarado é de 8,77 Watts, divididos em um consumo de 460mA e 650mA nas linhas de 12V e 5V, respectivamente.

Barracuda 7200.10

Depois de ser muito bem avaliado na edição 65, novamente tivemos acesso a um modelo da família Barracuda 7200.10, desta vez um de 750GB, o topo de linha (figura 2). Ele só deixou de ser a solução da Seagate (**www.seagate.com.br**) de maior capacidade de armazenamento para os desktops, porque a empresa já oferece ao mercado os modelos da nova família 7200.11 – indo até 1TB.



F2. Barracuda ST3750640AS: 7200.10 com 750GB, são 4 discos e 8 cabeças para leitura/gravação, além de também possuir jumper para definir operação como SATA I. Cotado a US$ 210 em www.newegg.com.

Apenas para recapitular, as unidades disponíveis na família 7200.10 são de 80GB, 160GB, 250GB, 320GB, 400GB, 500GB e 750GB, tanto em interface SATA II de 300MB/s como Ultra ATA/100. A quantidade de memória buffer varia conforme o modelo, sendo que no modelo de 750GB é de 16MB. Em relação aos indicadores de performance durante escritas e leituras, o 7200.10 ostenta bons valores médios de 10ms e 8,5ms, respectivamente.



Gravação perpendicular de dados na mídia magnética e o NCQ também são recursos presentes neste disco. Sua temperatura limite durante operação é de 55°C, e para o consumo elétrico a Seagate se limita a mencionar um pico de 2,8A na linha de +12V durante a inicialização. Veja que é o valor máximo, e não o consumo típico, tal como declara a Western Digital.

Testes

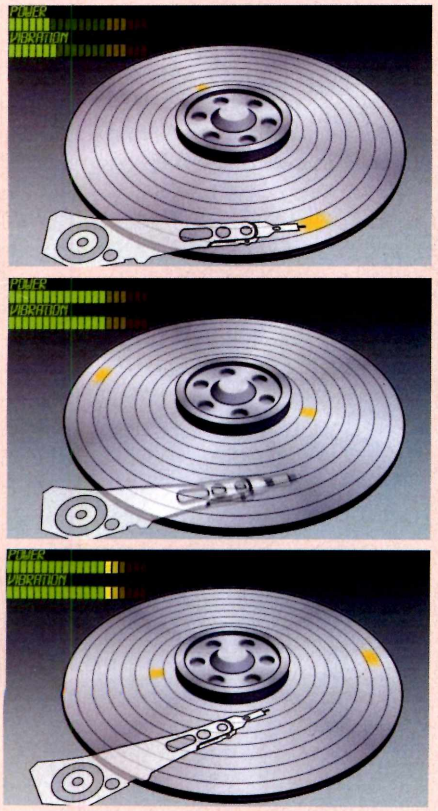
Os programas utilizados foram o HD Tach 3.0.1.0 (**www.simplisoftware.com**) para a varredura na superfície, o IOMeter 2004.07.30 (**www.iometer.org**) simulando aplicações de servidor (empregamos a carga típica de "File Server" sugerida pela Intel na documentação do programa) e por último o PCMark04 (**www.futuremark.com**) reproduzindo cenários de uso comuns a usuários de desktops.

A configuração base da máquina tinha uma placa-mãe P5B Deluxe WiFi-AP com processador Core 2 Duo E6300 rodando em overclock para 3.0GHz, 2GB de memórias DDR2-9200 (1150MHz) da Patriot, placa de vídeo Radeon X800 e HD Raptor X de 150GB como o disco de sistema, no qual instalamos o Windows XP SP2 e demais programas. Portanto, nenhuma atividade, além dos testes de benchmark, foi executada sobre os HDs em avaliação (ambos rodaram normalmente como SATA II na controladora do Ponte Sul ICH8R da Intel). Aliás, vale mencionar que no caso dos dois primeiros benchmarks os discos sequer precisam receber formatação e, conseqüentemente, um sistema de arquivos. Ou seja, tanto o HD Tach quanto o Iometer conseguem acessar os discos fisicamente, sem precisar de chamada ao sistema operacional. Para os testes com o PCMark04, utilizamos o sistema de arquivos NTFS. Além dos testes de benchmarks, avaliamos a temperatura dos discos com um termômetro digital (medição sobre a PCB, placa) e a partir do relatório de SMART, via programa HD Tune, e também o ruído com um decibelímetro. Todos os testes foram feitos na bancada a uma temperatura ambiente de 27ºC.

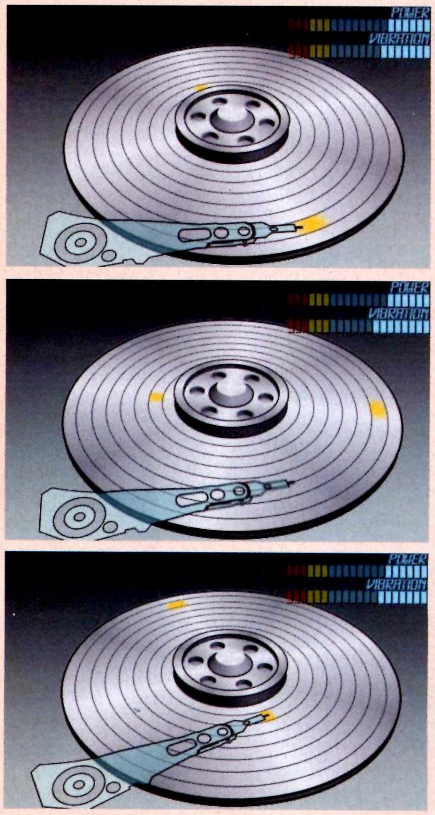
Intelligent Seek (Busca inteligente)

Para que as operações nos discos rígidos sejam executadas do modo mais otimizado (ou rápido) possível, a velocidade do mecanismo atuador (braço) que movimenta a cabeça de leitura e escrita é sempre alta e, dependendo da operação, constante. Porém, esse mecanismo não implica em menores valores de latências. Por exemplo, quando o braço está posicionado no cilindro mais externo do HD e recebe um comando de gravação ou leitura na parte mais interna, ele deve se movimentar rapidamente para a região determinada. Contudo, antes de realmente realizar a operação, a cabeça de leitura/escrita terá de aguardar o posicionamento rotacional do disco. Ou seja, não existe um sincronismo entre a velocidade do braço e a do disco (figura abaixo). De forma resumida, sempre que o braço realizada um deslocamento em sua posição, ele chega "atrasado" e tem de esperar um giro do disco para, daí então, ler ou gravar um dado.

Através do recurso Intelligent Seek, antes do braço se deslocar de um cilindro a outro, um circuito implementado no Caviar SE16 realiza alguns cálculos entre a posição atual e de destino da cabeça de leitura/escrita. O resultado determinará a velocidade do braço durante o deslocamento a ser realizado, e o objetivo é garantir que a cabeça chegue ao setor desejado no momento em que o disco estiver passando naquela região. Comparado aos discos rígidos anteriores, sem o Intelligent Seek, o braço movimenta-se mais lentamente. Entretanto, isso é algo proposital, uma vez que diminui o consumo elétrico, a vibração e o barulho gerado pelo disco.



Da cima para baixo: operação de leitura/escrita no disco (ponto em amarelo); após receber um comando da controladora, o braço se desloca para outro ponto em amarelo, mais interno; por último, apesar de estar preparada, a cabeça deverá esperar o posicionamento rotacional do disco. Ou seja, somente quando o ponto amarelo estiver na posição correta é que será feita a leitura ou gravação dos dados.



Da cima para baixo: operação de leitura/escrita no disco, deslocamento do braço na direção do cilindro mais interno, e chegada simultânea do braço ao cilindro do qual o setor será lido (ou gravado).

Resultados

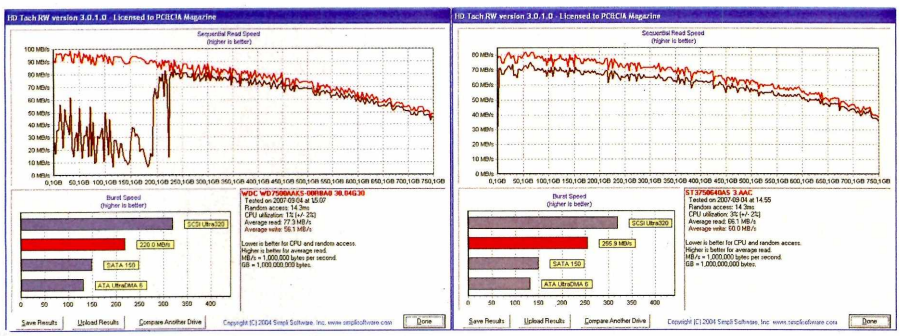
No HD Tach, os discos apresentaram resultados próximos e com algumas particularidades (figura 3). Enquanto o Barracuda 7200.10 demonstrou maior eficiência na transferência média de gravação, o Caviar SE16 foi melhor na transferência média de leitura, e na menor utilização de CPU (1% ante 3% do Barracuda).

Reproduzindo a carga de servidor de arquivos, vimos uma ligeira superioridade do Caviar SE16 em um dos principais indicadores de desempenho retornados pelo programa, que é a quantidade de I/O´s processados por segundo em um ambiente no qual a fila de requisições simultâneas oscila entre 1 e 256 (figura 4).

Aproveitamos a flexibilidade do Iometer para medir o ruído produzido pelos discos no pior caso, isto é, quando o mecanismo atuador é configurado para se deslocar continuamente através de regiões totalmente aleatórias (randômicas) do disco, em acessos de apenas 512 bytes. Ou seja, mal ele chegou na posição e terminou de ler um único setor, já tem de se deslocar para outro setor distante. Esse comportamento pode ser facilmente configurado no Iometer. O Caviar SE16 se deu bem melhor, saindo do estado de repouso, com ruído de 60dbA, para 65dbA. Já o 7200.10 foi de 61dbA para 73dbA. As medições foram feitas a aproximadamente 10mm do centro do disco. A fim de dar um valor prático a esses resultados, vale dizer que, se colocados dentro de um gabinete, ambos os discos passariam imperceptíveis quanto ao ruído, porém, na bancada, era fácil identificar o 7200.10 pelo ruído.

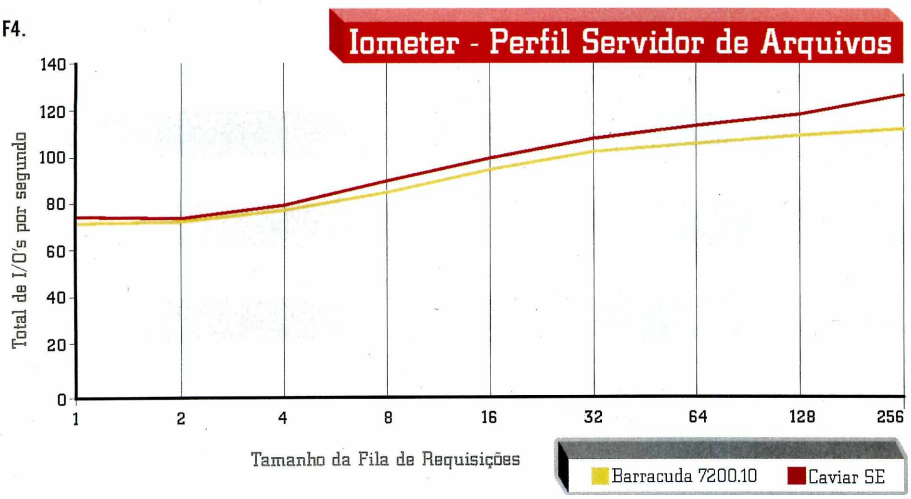
Por fim, vieram os testes com o PCMark04, onde o Caviar SE 16 ganhou em dois testes e o Barracuda 7200.10 imprimiu uma vantagem expressiva em um deles, o de cópia de arquivo.

Na avaliação das temperaturas, ambos tiveram resultados positivos. O Caviar SE16 iniciou os testes do PCMark04 a 36°C e finalizou em 39°C, enquanto o Barracuda 7200.10 começou a 40°C e finalizou a 43°C. Vale lembrar que este benchmark tem duração de cinco minutos.

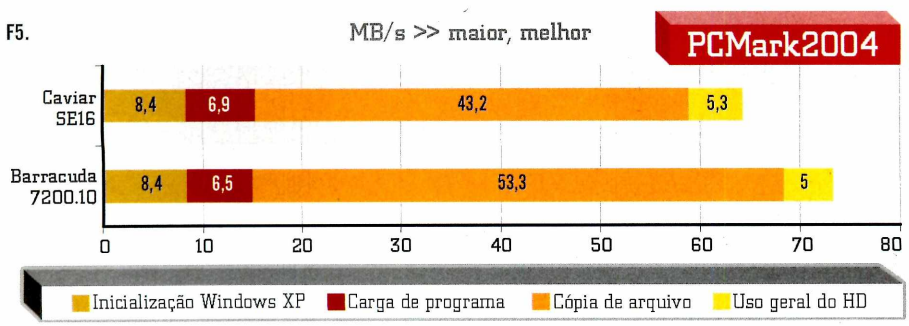


F3. Barracuda 7200.10 e WD Caviar SE16, à esquerda. Teste com configuração "Long bench – 32mb zone"

F4.



F5.



Conclusão

Conhecemos nesta matéria a performance de dois discos de grande capacidade, são nada menos que 750GB e por um preço que fica a cada dia mais convidativo. Impressionante! Diante dos resultados demonstrados, você estará em melhores condições para tomar sua decisão. No geral, o Caviar SE 16 foi superior, mas vale lembrar que a Seagate continua se destacando por oferecer 5 anos de garantia, ao passo que a Western Digital, 3. Além disso, se você busca máxima performance em discos "grandões", vale a pena considerar o Barracuda 7200.11, este sim o atual concorrente do Caviar SE 16. Em breve, traremos novos testes.

PC

Access Point com função Roaming

O que fazer para evitar a perda de conexão em áreas de transição entre Access Point diferentes? Veja alguns casos e sugestões aqui.



F1. Linksys WAP 200 com função *roaming*.

Wi-Fi em ambiente público, residencial e corporativo

As redes wireless já são populares e estão cada vez mais ao alcance de todos, principalmente em ambientes públicos como aeroportos e shoppings, e ambientes privados que envolvem escritórios, depósitos e muito mais.

Nos shoppings e nos aeroportos, essas redes estão presentes para proverem acesso à Internet, mas não costumam ser muito seguras e nem apresentam grandes funcionalidades adicionais. Nessas circunstâncias, quem acessa esse tipo de rede tende a ficar parado com um laptop sobre uma mesa ou algo parecido.

Em ambiente doméstico, as redes Wi-Fi estão se popularizando rapidamente, porque o custo dos Internet Gateway ("Roteadores") para acesso via banda larga está caindo muito. Esses equipamentos estão cada vez mais completos, práticos e seguros. Atualmente, mesmo que não se tenha qualquer dispositivo de rede Wi-Fi em casa, é preferível adquirir um Internet Gateway que agrega rede Wi-Fi compatível com o padrão IEEE 802.11g. Certamente ele será útil em um futuro não muito distante.

Mas nos ambientes corporativos a história é outra...

Concordamos que em um pequeno escritório que necessite de apenas um Access Point e que possua menos de oito computadores em sua rede Wi-Fi, não se tem maiores problemas, mesmo considerando que cada um dos oito computadores ligados à rede via Wi-Fi ficará com apenas 6,75 Mbps. Isso parece ruim, mas não é tão ruim assim, basta usar um Internet Gateway que também tenha quatro portas de switch e ligar pelo menos dois computadores na rede cabeada. Feito isso, cada um dos seis computadores remanescentes terá uma taxa nominal de 9 Mbps, enquanto que os outros dois da rede cabeada funcionarão a 100 Mbps. De fato, trata-se de um cenário simples.

Mas em um ambiente corporativo com dois ou mais Access Points, que juntos precisem cobrir a totalidade de uma área, com certeza teremos problemas de desempenho. Esses problemas de desempenho piorarão razoavelmente se o equipamento utilizador da rede Wi-Fi, seja ele um laptop, coletor de dados ou handheld, precisar se deslocar fisicamente e com isso sair da área de atuação de um Access Point e entrar na área de outro.

Vamos piorar um pouco esse cenário com a necessidade de uso de VoWiFi (VoIP sobre Wi-Fi). Agora precisamos nos deslocar fisicamente pelos diferentes ambientes da empresa, percorrendo áreas de abrangências de diferentes Access Points, portando smartphones que utilizam VoIP sobre a rede Wi-Fi. E agora?

O que acontece é que no momento de transição entre diferentes Access Points há uma interrupção significativa na transferência de dados. Como resolver ou minimizar isso?



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

Função roaming

No momento em que um dispositivo utilizador Wi-Fi sai da área de cobertura de um Access Point e entra em outra área, a transição não é tão resumidamente pacífica.

Inicialmente sabemos da necessidade de haver uma pequena sobreposição das áreas de abrangência dos Access Points, de forma a manter uma boa distribuição do sinal e também visando reduzir ao máximo a atenuação natural do sinal e das áreas cegas.

Sendo assim, um utilizador Wi-Fi "entra" na área de outro Access Point antes mesmo de ter deixado a sua. Em condições tradicionais, a passagem de fato para o próximo Access Point só ocorre quando o sinal deste passa a ser mais forte do que o sinal do anterior. Nesta ocasião, o utilizador Wi-Fi deve iniciar os procedimentos de negociação com o Access Point a fim de passar a ser seu "cliente". Isso é rápido, mas não o bastante para evitar problemas na transmissão e recepção de dados, principalmente em se tratando de VoWi-Fi.

Durante o evento de mudança da área de cobertura de diferentes Access Points, ocorre o *handoff*, que é caracterizado a partir do momento em que a perda de pacotes atinge 1,0% e a latência chega a 200ms. Nessas condições é comum haver perda de comunicação, embora o sinal eletromagnético esteja normalmente presente.

Mas já é possível minimizar significativamente esses problemas com o uso de Access Points compatíveis com a função roaming (IEEE 802.11f), que fazem uso do protocolo IAPP (Inter-Access Point Protocol).

Esses equipamentos suportam processos de transição mais amigáveis, minimizando o *handoff* e eliminando uma perda mais significativa de dados em trânsito (figura 1).

Utilizando a função roaming, somente uma única identificação de rede (SSID) será aplicada a todo o conjunto de Access Points configurados. Além disso, os canais Wi-Fi utilizados e também as configurações de segurança serão replicados. Tudo isso ajuda a reduzir as latências e garante uma melhor qualidade nas conexões dos dispositivos móveis.

O *handoff* será bastante minimizado, mas não será definitivamente eliminado, até porque ele acaba sendo "ajudado" pelo próprio protocolo IAPP (Inter-Access Point Protocol). Ele especifica que somente os dispositivos utilizadores móveis terão de realizar todos os procedimentos de migração entre diferentes Access Points, sem a ajuda destes. Esses procedimentos compreendem quatro fases distintas: escaneamento do novo Access Point, autenticação neste, associação e reassociação. Futuramente o padrão IEEE 802.11r reduzirá os tempos de *handoff*.

A função roaming não será útil somente aos dispositivos utilizadores móveis. Tomemos como exemplo um escritório de vendas de uma grande empresa que ocupa um imóvel único, como um galpão. Neste ambiente, podemos ter quatro Access Points para atender todos os cinqüenta computadores da empresa, por exemplo. Todo dia no início do expediente, ao se ligar os Access Points, serão montadas quatro redes Wi-Fi, cada uma com um SSID (Service Set Identifier) distinto. Os computadores que estiverem em áreas de transição de cobertura levarão mais tempo para entrarem na rede.

Entretanto, se trocarmos esses equipamentos por versões mais modernas, com função roaming, somente uma única rede Wi-Fi será montada no início do expediente, com um único SSID aplicado aos 4 Access Points. Além disso, os canais Wi-Fi utilizados serão os mesmos e as configurações de segurança, também.

Outra boa característica conseqüente da função roaming é a facilidade e praticidade de administração da rede Wi-Fi, que ainda costuma pregar peças em alguns administradores de rede.

Conclusão

A função roaming sozinha não vai resolver todos os problemas das redes Wi-Fi, porém elimina alguns dos problemas mais irritantes e limitadores de novas aplicações para essas redes.

Com o uso de Access Points com função roaming, a possibilidade de utilização de VoWi-Fi passa a ser uma tentação para algumas empresas, o que acabará representando uma economia a médio prazo em função da diminuição das chamadas telefônicas.

A facilidade de administração de uma rede Wi-Fi com alguns Access Points passa a representar uma ótima característica a ser levada em conta no momento de se projetar uma nova rede wireless.

Até a próxima! **PC**

PC POWER TESTER

T&C

A T&C Ltda. apresenta o único wattímetro do mercado brasileiro portátil, de custo acessível e confiável para medições da rede elétrica e testes de consumo de equipamentos eletro-eletrônicos. Agora você pode fazer seu overclock e manutenção com maior tranqüilidade.

Realiza as seguintes medições:
Freqüência da rede elétrica (Hz)
Tensão da rede elétrica (Volts RMS)
Corrente (Amperes RMS)
Consumo do equipamento (Watts)
Potência do equipamento (VA)
Consumo Horário (KWH)
Fator de Potência (PF)
Tempo de Operação (Horas, Minutos)
P/ redes de 110/127 VAC - 50/60 Hz
Potência máxima : 15A
LCD, 4 dígitos, 12 mm
Peso: 135 gramas
Dimensões (Alt/Larg/Prof): 13/6/3 (cm)
Precisão: melhor que 0,2%
Manual de operação em português
Garantia Total de 1 (um) ano



Por apenas R$ 320,00

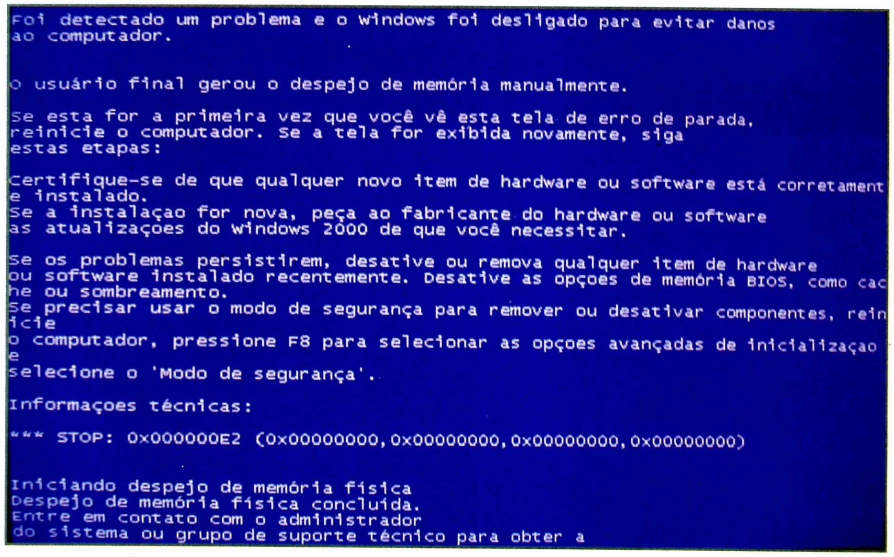
Para mais informações e pedidos, acesse:
www.telecommunications.com.br

Ou envie um e-mail para:
comercial@telecommunications.com.b

Rua Barão de Tatuí, 555 – SP – SP
Tel/Fax (+5511) 6886-9858/8409-6949

Decifrando as BSOD

BSOD é a sigla em inglês de *Blue Screen of Death*, algo que aqui no Brasil é mais conhecido simplesmente por tela azul, o supremo indicativo de problemas no Windows e que muitas vezes leva usuários a reinstalar todo o sistema. Nesta matéria apresentamos um roteiro para decifrá-la. Após a leitura, o medo das BSOD será coisa do passado.



Todo sistema operacional, ou melhor, qualquer software e também hardware, pode apresentar erros durante a operação. Quando há um certo nível de qualidade, eles recebem algum tratamento a partir de mensagens que relatam as condições de erros e mecanismos co-relacionados, como logs e códigos de erros. A tela azul faz parte desse mecanismo do Windows, junto com os erros de GPL, se bem que esses são mais comuns na série Windows 9x e anteriores.

A tela azul é utilizada desde os primórdios do Windows, mas foi popularizada com o advento do Windows NT, com o famoso IRQL_NOT_LESS_OR_EQUAL, que ocorria tipicamente quando havia algum problema com dispositivos de armazenamento, ou especificamente quando o driver da interface de disco não era instalado ou se esquecia de formatar o HD em FAT16 ou NTFS. Claro que esse erro também tinha diversas outras origens. Não podemos esquecer dos erros que ocorriam quando ia se instalar uma interface Plug and Play qualquer, acionar uma nova interface SCSI ou mesmo configurar o vídeo.

Independente de ser tela azul, sinais sonoros ou qualquer outra forma de indicação de erros, a grande questão é a documentação sobre eles, bem como se há alguma ferramenta para auxiliar no processo de resolução. Documentação existe, mas nem sempre é tão simples achá-la e mesmo com a Internet à disposição. Dependendo do caso, é como procurar uma agulha num palheiro.

Assim como numa entrevista de emprego, onde o postulante não leva uma lista de problemas e defeitos, mas sim um conjunto de qualidades e virtudes, o mesmo ocorre com qualquer produto, apenas as qualidades são listadas. A seção FAQ costuma ser a última em qualquer manual, por vezes quase que escondida. A seção de problemas e soluções então é mais simples e óbvia ainda. Não raros são os casos em que todos os problemas são endereçados a algo do tipo "contate o fabricante".

Com o Windows isso também ocorre: quem nunca ficou irritado com as respostas contidas na ajuda e com a teimosia do assistente em prestar auxílio, muitas vezes inútil? O portal do Technet possui uma ótima base de dados para resolução de problemas, mas quando a resposta não está entre os 20 primeiros tópicos, a paciência começa a ir pelo ralo, principalmente quando clicamos em um link quebrado...

De qualquer forma, problemas existem e precisam ser resolvidos de alguma forma. Nessa oportunidade, não vamos apresentar uma simples relação de defeitos e (possíveis) soluções, mas sim como trabalhar "em cima deles" com o famoso e também temido Debug.

Ajuda inútil

Infelizmente vários desenvolvedores de software têm o mau hábito de oferecer ajuda inútil. Embora ofereça várias informações importantes e vitais para o trabalho de desenvolvimento, manutenção e outros, a MS também oferece uma boa quantidade de informações que beiram o inútil, como essa do link http://support.microsoft.com/default.aspx?scid=kb;[LN];888664. Sem falar de outras bem óbvias, como é o caso dessas duas sobre interface USB http://support.microsoft.com/default.aspx?scid=kb;[LN];835967 e http://support.microsoft.com/default.aspx?scid=kb;[LN];816843.



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.

Debug

Os profissionais da época do MS-DOS seguramente se lembram do utilitário Debug. De pouca utilidade para alguns, mas para muitos uma importante ferramenta de trabalho, não apenas para identificar problemas, mas também para a execução dos mais diversos testes, processos de manutenção (como um ClearCMOS via linha de comando quando a senha do BIOS é perdida) e também para a confecção de utilitários, como por exemplo o reboot.com, muito utilizado nos arquivos de lote (extensão bat). Pois bem, essa versão do Debug existe até hoje e está presente até no Windows XP, oferecendo as mesmas funcionalidades.

Com o advento do Windows, novas tecnologias surgiram e também novas operações precisavam ser "debugadas". O Debug tradicional já não conseguiria atendê-las, eis que surge então o Windows Debugging Tools (WDT).

A bem da verdade, o WDT, cujo principal executável é o WinDBG.EXE, faz parte do kit de desenvolvimento de drivers do Windows e, conseqüentemente, está disponível para todos os seus sistemas operacionais, exceto naqueles onde o suporte já foi suspenso, como é o caso do Windows 98. O kit do Windows Me ainda está disponível, porém o suporte já foi interrompido também.

O WDT está disponível para sistemas de 32 e 64 bits. No nosso caso utilizamos sobre um Windows XP Professional de 32 bits, cuja versão pode ser usada em todos os sistemas baseados no núcleo do Windows NT. A versão de 64 bits só deve ser utilizada se o "objeto" a ser "debugado" também se valer das instruções de 64 bits.

Para oferecer boa precisão no diagnóstico, o WDT depende de uma base de dados chamada de símbolos, mais precisamente de arquivos de símbolos (*symbol files*). De um modo bem sucinto, eles não são nada mais do que arquivos no formato de banco de dados do Access, que contém as informações sobre cada componente presente no Windows. Dessa forma, temos um relatório completo sobre praticamente qualquer falha.

Mas e se o componente não faz parte do Windows, e sim de um driver de dispositivo ou componente de software? O ideal seria ter os arquivos símbolos de todos os dispositivos, mas os fabricantes não os disponibilizam ao grande público. Porém, isso não significa que não seja possível realizar o diagnóstico e eliminar o problema. Significa apenas que não teremos muitas informações sobre o componente problemático, mas de qualquer forma ele será identificado.

Símbolos

Como já dissemos, os símbolos oferecem ao WinDBG as informações necessárias para a realização do processo de debug. Essas informações consistem de variáveis locais, funções, nomes de arquivo e outras estruturas típicas de linguagens de programação, disponibilizadas de modo online e offline e podendo ser públicas ou privadas.

Os pacotes de símbolos online são públicos e estão armazenados em um servidor web da Microsoft, em um endereço não navegável via browser. Ele contém apenas um resumo de informações. Já o Offline é completo, sendo classificado em *build* e *checked*.

Segundo informações contidas no site da MS, geralmente a *build* é suficiente para o debug em qualquer instalação do Windows. Já a *checked*, apenas quando o processo for realizado em alguma versão especial do Windows, que necessite de informação extra.

A criação dos arquivos de símbolos não é uma exclusividade da MS, eles são criados sempre que um programa é compilado a partir de um compilador da MS, como o Visual C++. Conforme o caso, então, como por exemplo o de uma empresa que desenvolve o seu próprio sistema de gestão, é muito importante que esse arquivo seja disponibilizado para o debug.

Durante nossos testes achamos o método offline mais eficiente, pois além de oferecer informações completas e um processamento muito mais rápido, no método online o diagnóstico estaria comprometido se o problema tivesse sua origem exatamente nas interfaces de comunicação (rede e modem), ou então diante de alguma outra falha com a conexão Internet.

O único senão de utilizar o pacote de símbolos offline é o espaço ocupado em disco, de aproximadamente 800MB. Os pacotes para download tem de 20MB a 250MB, conforme o sistema operacional e o service pack instalado. Os *Rollup updates* também são listados, há pacotes de símbolos apropriados a eles. A versão do WDT para sistemas de 32 bits pode ser baixada em www.microsoft.com/whdc/devtools/debugging/installx86.mspx, ou no link direto http://msdl.microsoft.com/download/symbols/debuggers/dbg_x86_6.7.05.1.exe. Já o pacote de símbolos pode ser encontrado em www.microsoft.com/whdc/DevTools/Debugging/symbolpkg.mspx (baixamos a versão *retail*). A instalação de ambos ocorre nos mesmos moldes de qualquer outro software, sendo simples e rápida.

Algumas considerações

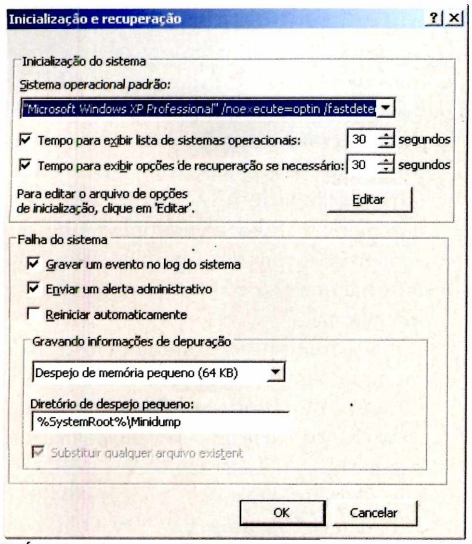
A lei de Murphy sempre age nas horas mais impróprias. Como testar o WDT se o Windows teima em se comportar direito? Por sorte, há vários procedimentos para forçar uma ocorrência da BSOD, e no arquivo de ajuda do WDT são demonstrados dois modos. Ambos bem simples. Antes que alguém se inspire no Cebim, o WinDBG informa que essa BSOD é completamente intencional.

A primeira é executada pelo teclado mesmo e a outra pelo prompt de comando do WinDBG. Para usar o primeiro método, abra o Regedit (Iniciar -> Executar -> regedit) e acesse HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\i8042prt\Parameters. Crie uma chave DWORD com o nome CrashOnCtrlScroll, coloque o valor 1 e reinicie o computador. Para executar, pressione Ctrl+Scroll Lock+Scroll Lock e teremos uma BSOD quase que instataneamente (algumas vezes é necessário repetir a sequência de pressionamento). A segunda é mais fácil, basta executar o WinDBG em *Kernel-mode debugging* e digitar .crash no prompt de comando do WinDBG para ter a BSOD. Se não executar, digite g e pronto, BSOD na hora.

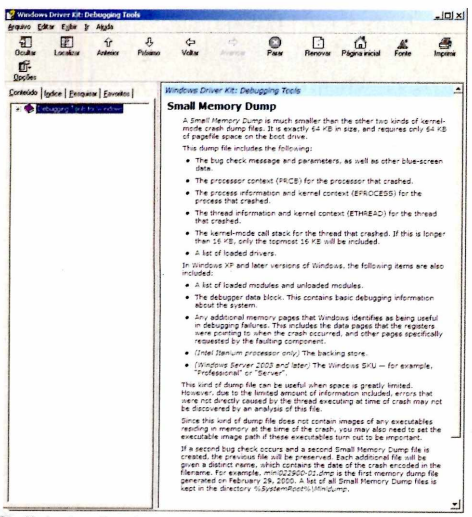
Na prática, esses dois meios são apenas para fins de teste ou mesmo monitoração do comportamento de algum componente do sistema através do WinDBG. Na realidade, é muito difícil encontrar uma computador com Windows que não tenha sofrido pelo menos uma BSOD e, consequentemente, criado um arquivo de *dump* (despejo) de memória.

Esse arquivo de *dump*, como o nome sugere, é onde são armazenadas as informações presentes na memória durante a ocorrência de uma BSOD. Sem dúvida, vários profissionais e usuários avançados já viram as configurações acerca dele nas propriedades do sistema > guia Avançado > botão Inicialização e Recuperação (figura 1), e com certeza já se perguntaram "como é que isso é utilizado?" É com esse *dump* que vamos realizar o Debug do sistema de um modo preciso e, conforme a disponibilidade de recursos, eliminar de vez o problema, poupando bastante tempo de uma possível saída do tipo formata e reinstala tudo.

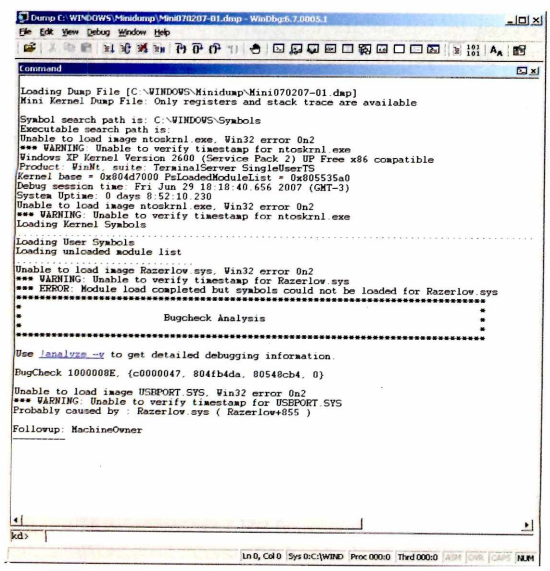
São três tipos de arquivo de *dump*: pequeno, kernel e completo. O *dump* pequeno oferece as informações necessárias para um procedimento de manutenção do sistema (figura 2). Ele contém todas as informações exibidas na tela azul, permitindo-nos ver através do WinDBG a informação que antes



F1. É nesta tela que configuramos o dump de memória do Windows.



F2. Help detalhando conteúdo do arquivo de dump pequeno: tamanho do arquivo nunca será maior que 64KB, sendo armazenado por padrão na pasta C:\Windows\Minidump.



era impossível de ser compreendida de "bate e pronto".

Já o *dump* de kernel grava toda informação utilizada pelo kernel do Windows e ignora o restante. O arquivo é denominado memory.dmp e fica armazenado na raiz do disco onde o Windows está instalado. Seu tamanho será de aproximadamente 1/3 do total de memória RAM instalada no sistema. Por último, o *dump* completo armazena toda a informação presente na memória RAM, resultando em um arquivo de mesmo tamanho da RAM instalada.

Segundo a documentação do WDT, a melhor opção é o *dump* de Kernel, pois contém todas as informações referentes ao hardware e demais componentes vitais do sistema. Na prática, a opção padrão do sistema, o *dump* pequeno, já é suficiente em boa parte das vezes.

Um *dump* pequeno pode não ser suficiente em casos como o de uma BSOD causada por um trojan ou spyware instalado no sistema. Nesse caso devemos tentar iniciar o sistema, mudar essa configuração e esperar pela BSOD, já que o modo de *crash* manual não será útil ao diagnóstico. Há também a opção de criar um arquivo de *dump* pequeno a partir do arquivo de *dump* do kernel ou do completo.

Uma utilidade mais prática para o *dump* completo é para identificar algum componente do sistema "faminto" por memória. Alguns usuários podem até comentar que através do Gerenciador de Tarefas é possível fazer a identificação. Isso não deixa de ser verdade, porém nem todos os componentes carregados são exibidos por ele. Há softwares de terceiros que podem fazer isso, mas dependendo do caso, pode não ser possível executar a instalação, pelos mais diversos motivos. O *dump* completo também pode ser interessante para analisar o comportamento errático de um driver.

Em tempo: o arquivo de *dump* não é criado apenas quando ocorre uma BSOD, seja "natural" ou forçada, mas também manualmente pelo WinDBG. Para o nosso propósito aqui, no entanto, que é o de manutenção do sistema, serão válidos apenas os criados a partir da ocorrência de uma BSOD.

Usando o WinDBG

A interface do WinDBG é bem simples, o que é natural para uma ferramenta dessa natureza. Quanto menos recursos consumir, melhor para o processo de debug. Antes de começar o processo de debug, é preciso se familiarizar com alguns recursos do WinDBG.

Para o nosso objetivo, vamos usar apenas uma fração do poder oferecido pelo WinDBG, essencialmente o arquivo de *dump*, o de símbolos e o *Workspace*. O arquivo de *dump* dispensa maiores comentários; em relação aos símbolos, temos de informar a sua localização; já o *Workspace* nada mais é do que o conjunto de configurações acerca do processo de debug. Por exemplo, para fins de organização, um desenvolvedor pode deixar os arquivos de símbolos separados por pastas, colocando um sistema de depuração visando o usuário local, e um outro visando o uso em rede.

Primeiro, vamos configurar o local do arquivo de símbolos. Acesse File > Symbol File Path. A janela aberta para a configuração do caminho é um tanto estranha, sugere que um caminho deva ser selecionado através dos botões, porém a caixa de texto ao lado é editável e não apenas para visualização, assim podemos entrar diretamente com o caminho. Para quem ainda está familiarizado com a operação do MS-DOS, o método de definição do caminho do arquivo de símbolos é o mesmo do velho comando Path, com direito até a ponto e vírgula. Na área de texto, digite o caminho correto, o padrão é c:\windows\symbols.

Caso opte por utilizar o servidor da MS, o caminho deve apontar um local para cache dos arquivos de símbolos e o endereço do servidor, como segue: srv**DownstreamStore*** **http://msdl.microsoft.com/download/symbols**. Troque *DownstreamStore* pela pasta local que servirá de cache, por exemplo **c:\symbolcache**. Não é recomendado usar os dois conjuntos de símbolos e alocá-los na mesma pasta. Procure sempre usar pastas diferentes.

Agora vamos ao *Workscape*. Se tivermos a sorte de eliminar o problema de primeira, será um desperdício de tempo salvar o *Workspace*, mas do contrário, vai ser uma mão na roda. O *Workspace* salva toda a configuração acerca da seção de debug, desde os caminhos dos arquivos de símbolos às configurações de visualização, dentre outras. Por ser possível manter vários *Workspaces*, estão disponíveis várias funções de gerenciamento (criar, deletar, salvar para arquivo, etc).

Finalmente chegamos ao ponto principal, o arquivo de *dump*. Basta ir em Open Crash Dump e selecionar o arquivo de *dump* a ser analisado. Lembre-se que os caminhos possíveis, considerando o padrão, são c:\ e c:\windows\minidump. Ao abrir o arquivo, o processo de depuração do WinDBG começa automaticamente (figura 3).

Analisando o resultado

A análise feita pelo WinDBG costuma ser bem rápida quando utilizamos o pacote de símbolos offline. Ao selecionar o arquivo, será aberta uma janela denominada Command, que é dividida em duas partes: uma área de visualização e uma outra para entrada de comandos, na base. No momento, vamos nos ater apenas à área de visualização, pois nela está o log do WinDBG sobre o arquivo de *dump*.

Por usarmos um arquivo de *dump* pequeno, o cabeçalho do arquivo nesse primeiro momento é maior que a informação acerca do problema. O cabeçalho da figura 3 contém diversas informações:

- Arquivo de dump analisado "Loading Dump File..."
- Tipo de arquivo de *dump* "Mini Kernel..."
- Caminho dos arquivos de símbolos "Symbol search path.."
- Caminho do executável "Executable search path..."
- Versão do Kernel do Windows, Service Pack e o SKU
- Base do kernel "Kernel base.."
- Tempo da seção de debug "Debug session time"
- Tempo de atividade do sistema até a ocorrência da falha "System uptime"

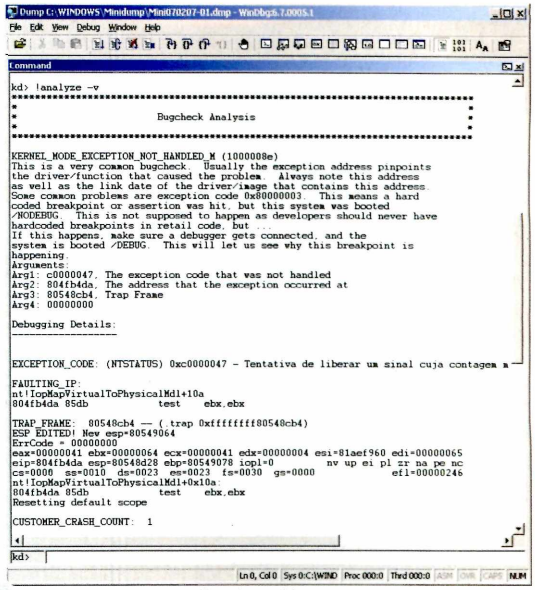
Após relatar tudo isso, os símbolos são carregados e, dependendo do caso, finalmente começamos a ter alguma noção do causador do problema. É indicado um erro de impossibildade de carregar o símbolo referente a um driver, e o nome do driver é informado. No nosso caso foi um problema com um arquivo dos drivers do mouse Razer Pro Solutions, o Razerlow.sys. Na seqüência, começa a derradeira análise do erro.

Screensaver BSOD

A MS oferece um screensaver baseado no Bsod (www.microsoft.com/technet/sysinternals/Miscellaneous/BlueScreen.mspx) que é muito, mas muito convincente.

Como não há um símbolo disponível para esse driver, outros erros são relatados, no caso é sobre o driver USBPORT.SYS. O Windows tem esse driver nativamente, mas possivelmente na instalação do driver o original foi substituído por uma versão mais recente que não "bate" com o símbolo disponível. Por isso é muito importante usar o pacote de símbolos apropriados ao sistema operacional.

Novamente é feita uma referência ao arquivo Razerlow.sys, já que segundo as informações disponíveis no relatório, foi por causa dele que não foi possível realizar o *Timestamp* (data e hora de compilação do módulo) do USBPORT.SYS, possivelmente por causa da substituição na instalação do mouse.



F4. Informações para análise do problema.

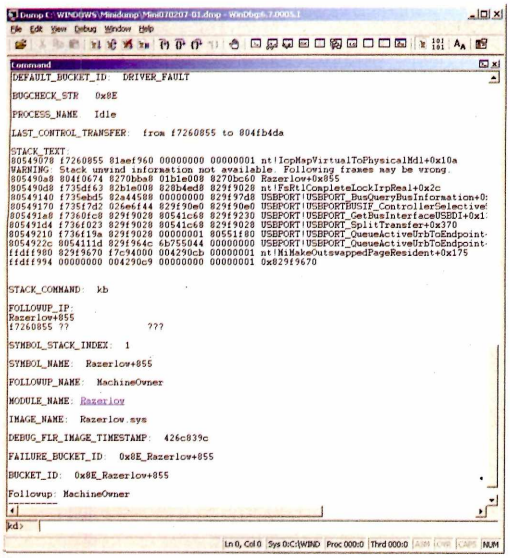
Nesse momento podemos pular algumas etapas e partir para a substituição dos drivers do mouse e também verificar os referentes à interface USB. Com um pouco de sorte, o problema será sanado. Mas para ter certeza que o problema é do driver, é mais prudente continuar a análise do debug.

Note que há um link, o "!analyse -v". Podemos digitar o comando no prompt do WinDBG ou simplesmente clicar nele. O !analyse é apenas um dos vários comandos oferecidos pelo WinDBG, e também é um dos mais utilizados para identificar os problemas. Depois de executar o comando, teremos um bom relatório, bem completo. Esse relatório é de suma importância, pois com ele teremos informação suficiente para concluir quem é o culpado do problema e quem é a vítima.

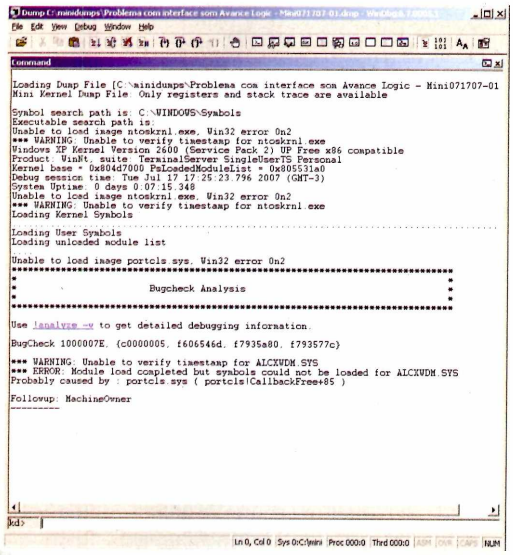
O !analyse também oferecerá um cabeçalho, só que bem mais curto, informando o erro, no caso o KERNEL_MODE_EXCEPTION_NOT_HANDLED_M (1000008e), e logo a seguir uma breve explicação sobre a característica do erro, se é um problema comum ou não, e quais são as condições típicas para a sua ocorrência. Logo após são apresentados os detalhes do problema.

Os detalhes são apresentados em tópicos, com nome e a respectiva explicação (figura 4). Conforme o caso e as características do problema, cada detalhe terá mais ou menos importância. São eles:

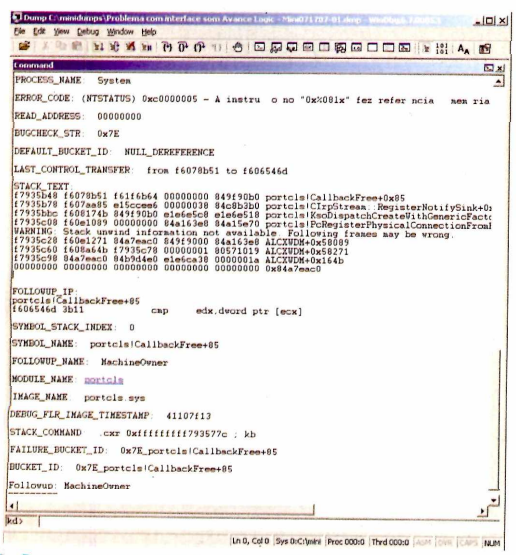
- EXCEPTION_CODE: indica o código de erro. No caso é um erro NTSTATUS 0xc0000047 – Tentativa de liberar um sinal cuja contagem máxima teria sido ultrapassada.
- FAULTING_IP e TRAP_FRAME: ambos informam sobre endereços de memória.
- CUSTOMER_CRASH_COUNT: contagem de falhas.
- DEFAULT_BUCKET_ID: indica o tipo de erro, no caso indica uma falha de driver (DRIVER_FAULT).
- BUGCHECK_STR: informa o código de erro indicada por DEFAULT_BUCKET_ID.
- PROCESS_NAME: informa o nome do processo onde ocorreu a falha. No caso foi *idle*, ou seja, o sistema não estava executando qualquer programa, a falha simplesmente ocorreu. Quando a falha ocorre por causa de um programa, o nome de seu executável é exibido.
- LAST_CONTROL_TRANSFER: exibe os últimos endereços de chamada do controle de transferência, no caso, uma chamada do endereço f704a855 para 804fb4da.
- STACK_TEXT: exibe uma lista de chamadas relevantes que culminaram na falha. São exibidos endereços e os arquivos ou módulos que foram utilizados.
- STACK_COMMAND: exibe o meio utilizado para obter as informações disponibilizadas em STACK_TEXT.
- FOLLOWUP_IP: indica a instrução possivelmente responsável pela falha, no caso o Razerlow+855.
- SYMBOL_NAME: co-relacionado a FOLLOWUP_IP, informa o nome



F5. Responsável pelo travamento: Mouse da ProSolutions.



F6. Problema com interface de áudio.



F7. Desta vez o culpado foi o próprio Windows.

do arquivo de símbolo necessário (pois nem sempre ele pode estar disponível).

- FOLLOWUP_NAME: co-relacionado a FOLLOWUP_IP, indica o que solicitou as informações.
- MODULE_NAME: co-relacionado a FOLLOWUP_IP, exibe o nome do módulo problemático.
- IMAGE_NAME: co-relacionado a FOLLOWUP_IP, mostra o nome do arquivo do módulo.
- DEBUG_FLR_IMAGE_TIMESTAMP: co-relacionado a FOLLOWUP_IP, mostra o endereço onde a falha ocorreu.
- FAILURE_BUCKET_ID: basicamente exibe as informações disponíveis em BUGCHECK_STR e SYMBOL_NAME.
- BUCKET_ID: demonstra a mesma informação de FAILURE_BUCKET_id.
- Followup: geralmente o mesmo que FOLLOWUP_NAME.

Identificando a origem do problema

Cientes do significado de cada informação, agora chegamos ao ponto principal, achar os culpados pelo erro. Para a maioria dos casos, os tópicos mais relevantes para localizar a origem do problema são:

- EXCEPTION_CODE: exibe o código da falha, dando uma idéia do que enfrentaremos, se vamos ter quer mexer apenas no software (atualizando programas, drivers ou qualquer outro componente dessa natureza), no hardware, ou em ambos.
- DEFAULT_BUCKET_ID: exibirá a natureza da falha, se a origem é no hardware, software, aplicativo, etc, apontando-nos o caminho que deve ser seguido.
- BUGCHECK_STR: informa o código de erro que usaremos para procurar no arquivo de ajuda do WinDBG. Ao contrário de outros arquivos de ajuda do Windows, ele oferece informações úteis que poderão ajudar na resolução do problema.
- MODULE_NAME: mostrará o nome do módulo onde a falha ocorreu, que pode nos indicar o objetivo a ser atingindo.
- IMAGE_NAME: será mostrado o nome do arquivo que tem o módulo problemático, indicando o que deve ser procurado (figura 5).

Dentre desse contexto, se a informação oferecida é muito genérica, note que a informação contida em DEFAULT_BUCKET_ID é um link. Em alguns casos, ele nos dará informações mais completas como o nome do fabricante do módulo e outras que podem auxiliar na resolução do problema.

No caso apresentado, com base nas informações de EXCEPTION_CODE podemos ver que foi um problema no comportamento de um componente ligado mais a software, e DEFAULT_BUCKET_ID confirma que o problema é um driver. MODULE_NAME nos indica claramente (pelo menos nesse caso) que o driver que apresentou a falha era o do mouse utilizado no sistema, e IMAGE_NAME nos mostra qual é o arquivo.

Concluímos que o driver do mouse apresentou um comportamento problemático, que pode ser originado do driver em si ou da porta USB. Assim removemos o driver problemático do mouse e atualizamos para uma versão mais nova, ou se a mais nova é a utilizada, optamos por uma anterior. Continuando na análise, atualizamos os drivers do chipset da placa-mãe ou mesmo verificamos se há alguma versão mais nova do módulo que se vitimou do problema, no caso o USBPORT.SYS, no site da MS.

Um outro caso

Agora vamos apresentar um problema com a interface de som (figura 6). Com base nos tópicos mais relevantes, o debug indicou um componente do Windows como o culpado. Nesse debug, observamos que ocorreu o mesmo que com o driver do mouse: a indicação de um arquivo do Windows e um arquivo de drivers de terceiros, mas em posições opostas. Ou seja, o arquivo do driver de som foi a vítima do erro e o componente do Windows foi o culpado (figura 7).

Assim, quando um arquivo é indicado, não significa que ele está com algum problema em si, ou seja, que é o vilão da história. Na verdade, ele pode ser

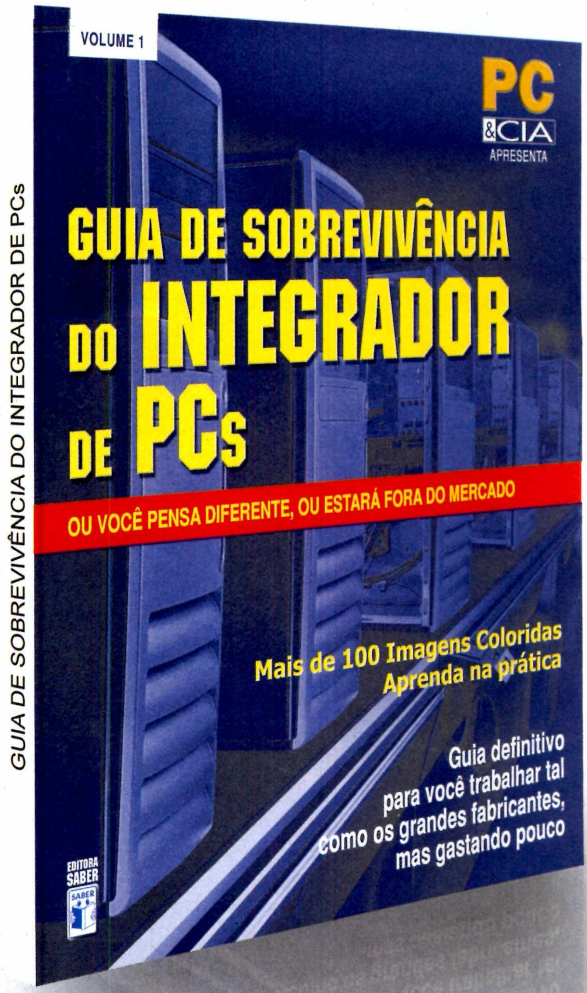
apenas a vítima. Para esse caso, tivemos que nos atentar a outros pontos. Observe que na figura 6 há um aviso de cuidado (*Warning*) no cabeçalho inicial, indicando não ter sido possível carregar os símbolos do arquivo ALCXWDM.SYS, que faz parte do driver da interface de som Advance Logic. Além disso, havia uma outra menção no tópico STACK_FAULT, sobre a sua presença na memória durante o erro. Embora o caminho tenha sido ligeiramente diferente, a solução foi a mesma: atualizar o driver.

Conclusão

Para muitos profissionais, a solução mais simples é reinstalar tudo, não apenas pela questão da aparente facilidade dessa técnica, mas pelo simples fato de não dispor de tempo hábil para efetuar uma pesquisa mais apurada acerca do problema. Um dos problemas disso é que nunca é somado algo à experiência e, conseqüentemente, se o problema ocorrer de novo, ele ficará de mãos atadas e mais uma vez terá de apelar para a reinstalação. Na verdade, não há técnica alguma nisso, o profissional passa a ser visto como um simples trocador de peças, ou reinstalador de sistema.

O emprego do WDT é extremamente dinâmico, podemos definir previamente diversas variáveis de ambiente, bem como salvar arquivos de *dump* de outros sistemas e abrir em um outro computador saudável. Dentre outros recursos, um que é muito interessante é o debug remoto. Nesse caso, ainda haverá esperança de resolução mesmo quando você se deparar com um problema cuja configuração do *dump* esteja para arquivo pequeno, esse não ofereça informações suficientes e não seja possível acessar o sistema para mudar. Além disso, saiba que também é possível criar seu próprio servidor de símbolos de modo a praticamente automatizar a resolução de problemas. Basta conectar a máquina do cliente a esse servidor para ter o diagnóstico do sistema em alguns minutos. Mas isso é assunto para uma próxima matéria. Ademais, agora quando você se deparar com uma tela azul durante a execução de um jogo, por exemplo, ao invés de procurar ajuda pelo código de erro e ficar batendo a cabeça na Internet, já sabe que há um caminho menos tortuoso para identificar a origem do problema. **PC**

Trabalhe como os grandes, mas gastando pouco!



Aprenda sobre:
- Construção de um laboratório técnico
- Mitos e verdades sobre o aterramento elétrico, como fazer e medir corretamente
- Equipamentos ideais para proteção elétrica
- Montagem passo a passo de uma bancada de baixo custo protegida contra ESD
- PCs confiáveis, o que você precisa saber para ter uma montagem à prova de falhas
- Execução de testes de estresse e burn-in
- Restauração automatizada do sistema: entregue mais valor para seus clientes
- Medição de temperatura
- Check-List para montagem e testes de micro

Veja mais detalhes em
www.editorasaber.com.br/livros

Pack de Ferramentas Windows

Apesar dos sistemas Windows serem fornecidos com um conjunto razoável de ferramentas que auxiliam o profissional de suporte a Redes e sistemas Microsoft, o dia-a-dia pode se tornar mais tranqüilo com as soluções que apresentaremos nesta matéria. Confira!



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

Para realizar uma administração avançada de um ambiente operacional de servidores e estações de trabalho, o profissional responsável deve possuir várias ferramentas de suporte. Considerando um ambiente baseado em tecnologia Microsoft, o sistema operacional possui diversas ferramentas nativas para a administração. No entanto, a fim de executar um trabalho mais abrangente, ter um maior controle sobre o ambiente e ir mais a fundo principalmente com relação ao aspecto de segurança, será necessário montar um pack de ferramentas adicional que o auxilie não apenas na resolução de problema e monitoração, mas também na documentação do ambiente através de logs e relatórios.

Algumas das melhores ferramentas do mercado estiveram disponíveis por muito tempo – e gratuitamente – num site denominado Sysinternals. Utilitários como o pacote PsTools tornaram-se bem populares, e ferramentas como o Process Explorer e NTFSDOS passaram a fazer parte do cotidiano dos profissionais de suporte.

Em julho de 2006, a Microsoft adquiriu uma empresa denominada Winternals e com isso, Russinovich e Cogswell, os programadores responsáveis pelo desenvolvimento e manutenção das ferramentas, passaram a ser funcionários da empresa. As ferramentas continuaram a ser gratuitas e existe a expectativa de que muitas delas passem a vir nativamente no sistema operacional.

Atualmente as ferramentas do Sysinternals também são compatíveis com o Windows Vista e podem ser baixadas do site oficial **www.microsoft.com/technet/sysinternals/default.mspx**. Recomendamos o acesso freqüente ao site, pois as ferramentas sofrem atualizações e melhorias constantes.

Gerenciamento de Arquivos e Discos

Nesta categoria destinada à monitoração e visualização da utilização de arquivos e discos, a primeira ferramenta que destacamos é a **AccessEnum**. Através dela, podemos fazer varreduras em um diretório ou chave do registro e listar as permissões atualmente configuradas. É uma boa opção para documentar as permissões de um servidor (figura 1).

A segunda opção é o **PsTools**, que consiste em um pacote de ferramentas para administração remota de servidores. É possível executar processos, exibir arquivos, listar informações sobre o sistema, mudar senhas de usuários e reiniciar um servidor, por exemplo.

Administração da Rede

O primeiro utilitário desta categoria é um editor avançado do Active Directory (AD). Conhecido como **Active Directory Explorer**, ele permite a navegação no banco de dados do AD, visualizando atributos e propriedades de objetos (figura 3).

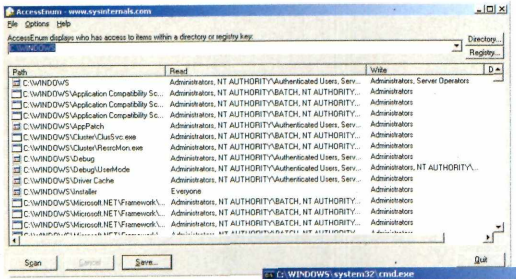
Na seqüência vem o **ADRestore**, uma ferramenta muito útil, porque é capaz de restaurar objetos deletados do AD (figura 4).

Por último, o **TCPView** é capaz de nos exibir a lista dos processos em execução, as portas TCP e UDP atualmente em uso por cada processo, o estado da conexão e outras informações úteis durante uma resolução de problemas na rede (figura 5).

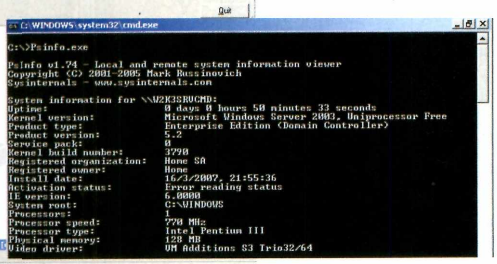
Segurança

Utilitários que auxiliam na monitoração e configuração de parâmetros de segurança. A primeira ferramenta destacada é a **LogonSessions**, capaz de exibir todas as sessões de logon ativas no servidor (figura 6).

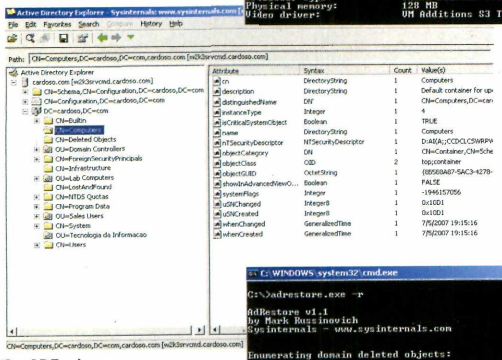
Já o **ShareEnum** faz uma varredura na rede, identificando todos os compartilhamentos existentes e as permissões de usuários atribuídas (figura 7).



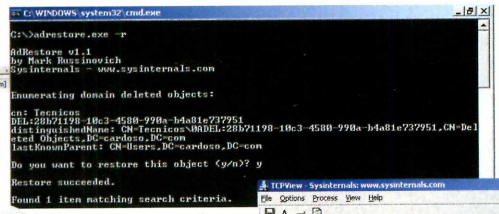
F1. AccessEnum varrendo diretório C:\Windows.



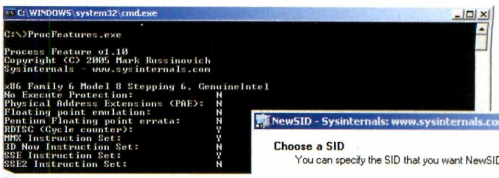
F2. Informações do servidor coletadas pelo Psinfo.



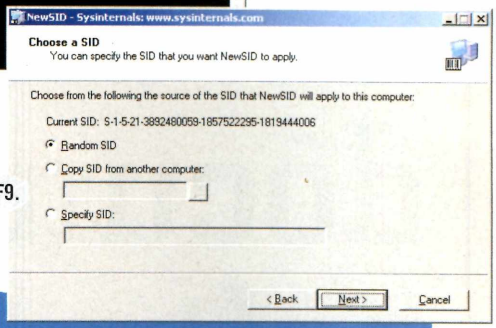
F3. ADExplorer: acesso direto à base de dados do AD.



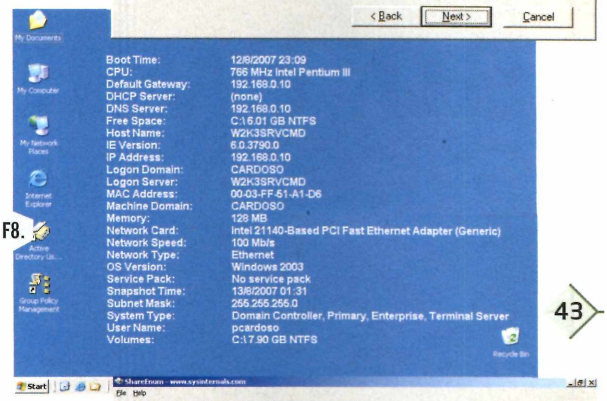
F4. ADRestore restaurando o grupo de usuários "Técnicos" que havia sido deletado do AD.



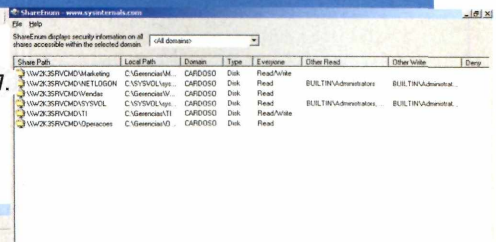
F10. Informações detalhadas sobre o processador com o ProcFeatures.



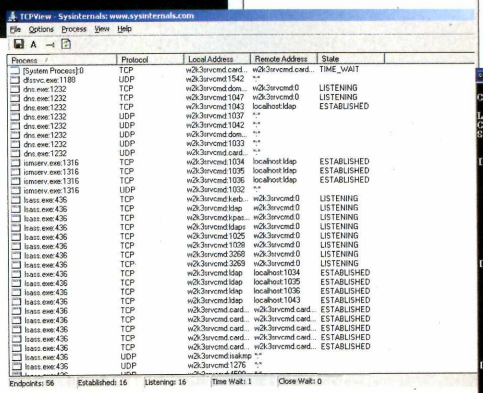
F9. NewSID: utilize quando for fazer clonagem de discos.



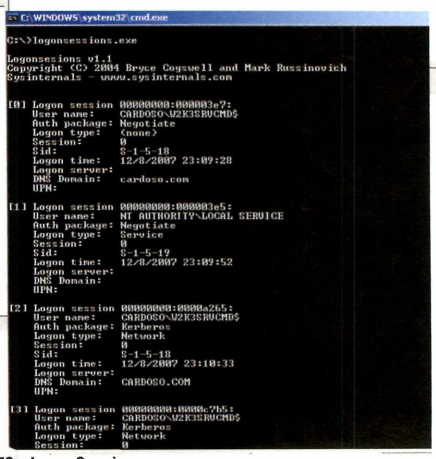
F8. Nome do computador, IP, domínio e Service pack estão entre as informações exibidas.



F7. ShareEnum exibe informações sobre os compartilhamentos de rede.



F5. TCPView listando conexões TCP e UDP abertas na máquina.



F6. LogonSessions lista as sessões de logon ativas.

Sistema

Ferramentas e utilitários para monitoração dos recursos do sistema. O **BgInfo**, por exemplo, exibe na área de trabalho um mini-inventário com informações da máquina (figura 8). Para que as informações sejam exibidas após cada boot, você deve colocar o arquivo executável do Bginfo na pasta Inicializar do perfil do usuário.

Enquanto isso, o **NewSID** é um utilitário desenvolvido para modificar o Identificador de Segurança (SID) da máquina. Durante uma clonagem de discos, por exemplo, é necessário gerar novos SID's para as máquinas de modo a evitar conflitos (figura 9).

Nossa última ferramenta é a **ProcFeatures**, a qual é capaz de exibir informações detalhadas a respeito do processador da máquina, verificando por exemplo se o mesmo possui suporte às instruções especiais multimídia SSE, à proteção contra execução de códigos em áreas reservadas a dados na RAM (No Execute Protection), entre outros (figura 10).

Conclusão

O profissional não deve se contentar apenas com as ferramentas e utilitários fornecidos pelo sistema operacional. Deve procurar por outras soluções que lhe permita realizar uma administração mais avançada e profissional.

Neste aspecto, as solúções da Sysinternals são indispensáveis a todo administrador, analista de redes e mesmo a usuários em geral que querem ter uma idéia exata do funcionamento de seus sistemas.

Quer aprender na prática a utilizar várias outras ferramentas não abordadas aqui para combater os malwares da Internet, por exemplo? Então acesse o nosso site **www.revistapcecia.com.br/artigos.asp** e confira na íntegra uma matéria publicada na PC&CIA 65. E como última dica fica o fórum oficial da Sysinternals (**http://forum.sysinternals.com**) para interagir com outros usuários. **PC**

Gerenciamento de documentos com software livre

Parte I

Jansen Carlo Sena

Em discos rígidos locais ou em máquinas da rede, em caixas postais de email, gavetas removíveis ou até mesmo em *pen drives*, o que não faltam atualmente são opções para armazenarmos nossos arquivos. Mas como encontrar a informação que você precisa na hora da emergência? Ela está em qual versão "daquele" arquivo? E como evitar acessos indevidos? Conheça aqui uma solução eficiente e gratuita, baseada em software livre, para organizar o que pode se transformar num verdadeiro caos e literalmente, dentre outros aspectos, até parar uma empresa.

Não são poucos os ambientes corporativos que possuem computadores para auxiliar nas suas tarefas diárias. O que parecia uma realidade distante há alguns anos, hoje é fato consumado. Computadores com capacidade de processamento e armazenamento cada vez maiores estão presentes mesmo em corporações de pequeno, médio e grande porte. Conectados em rede e muitas vezes com acesso à Internet, os computadores são itens presentes nas mesas de trabalho de muitas organizações ao redor do mundo.

A praticidade de armazenar e gerenciar informações no meio digital em substituição aos espaçosos formulários, relatórios e demais documentos impressos em papéis, associada ao custo cada vez menor do hardware, tanto dos computadores em si quanto de outros equipamentos periféricos como os utilizados para criar redes de computadores, são razões mais do que concretas para ajudar a justificar a presença dos equipamentos de informática nos ambientes corporativos. Embora existam diversos outros fatores e pontos de discussões envolvendo essa realidade, o fato é que muitas organizações simplesmente não funcionam ou pelo menos tem parte significativa dos seus negócios inoperante caso o seu ambiente computacional não esteja funcionando adequadamente.

Essa dependência dos recursos computacionais acaba depositando sobre essas tecnologias o bem mais precioso que muitas organizações possuem: as informações geradas e manipuladas no dia-a-dia de trabalho. Armazenadas em discos rígidos locais, nas caixas postais de email dos usuários, nos famosos *drives* de rede e até em *pen drives* e outros meios ainda menos adequados para armazenamento de arquivos de trabalho, com o passar do tempo as informações corporativas tendem a ficar ainda mais distribuídas, sem qualquer organização e muitas vezes difíceis de recuperar, uma vez que é prática comum deixar na "lembrança" do usuário a localização exata de certos dados. Nesse cenário, não é difícil ver um determinado colaborador dispender uma grande fatia de seu tempo para procurar determinados dados que seu chefe solicitou com a máxima urgência para alguma reunião importante da empresa.

Some-se a isso o fato de muitos documentos possuírem várias versões diferentes distribuídas, muitas vezes em pastas separadas com nomes que não obedecem a nenhum tipo de padrão ou controle mais apurado de versão, o que ajuda a aumentar ainda mais a confusão dos documentos corporativos eletrônicos. Uma verdadeira bagunça em forma de bytes! Por exemplo, como saber qual dos arquivos abaixo é o mais recente, contendo todas as revisões feitas para o fechamento de um contrato:

- `Contrato_Tux.odt`
- `Contrato_VersaoFinal.odt`
- `Contrato_VersaoFinal_Diretoria-20070817.odt`
- `Contrato_Tux_Jose.odt`
- `Contrato_Tux_impressao.odt`

Para resolver essa situação é preciso, por vezes, abrir todos os documentos e analisar o conteúdo de cada um deles. O problema pode ser pior ainda quando se precisa procurar por documentos que contenham determinadas palavras-chave em seus conteúdos.

Por fim, existe ainda um outro grave problema: controle de acesso! Em muitas corporações existem documentos cujo acesso deve ser controlado e não pode estar disponível para todos modificarem ou mesmo acessarem o conteúdo. Por exemplo, não é interessante que um arquivo de planilha eletrônica contendo os salários de todos os funcionários da empresa caia nas mãos de todos.

Tudo isso é comum na sua empresa? Caso sirva de consolo, isso é bastante comum em pequenas, médias e grandes organizações. Entretanto, saber que existem ambientes semelhantes não resolve o problema. Diante disso, é que vêm surgindo as soluções de DMS. Curioso? Então é hora de discutir um pouco mais sobre DMS... Vamos lá?

O que é um DMS?

DMS é uma sigla para *Document Management System* (Sistema de Gerenciamento de Documentos, em português) que descreve todo tipo de software cujo objetivo seja, como o próprio nome em inglês sugere, prover mecanismos para auxiliar no gerenciamento de documentos, incluindo recursos comuns tais como versionamento, controle de acesso, indexação de dados, dentre outros.

O interesse de muitas corporações em soluções de DMS vem crescendo à medida em que desperta-se para a necessidade de tornar mais ágil, organizado e seguro o acesso aos documentos corporativos. Esse pode ser um fator importante para a melhoria de processos internos que dependem das informações armazenadas em meios eletrônicos.

Diante disso, muitas alternativas de DMS vêm surgindo e evoluindo nos últimos tempos, e sendo implantadas em ambientes corporativos. Parte considerável dessas soluções são proprietárias e, dentre essas, as que possuem uma riqueza maior de recursos exigem o pagamento de onerosas licenças de uso que nem sempre cabem no orçamento de um mundo corporativo onde exige-se alta produtividade e baixo custo.

A boa notícia fica por conta do fato de que as soluções de DMS em software livre encontram-se prontas para atender as necessidades de instituições que desejam organizar seu "conhecimento digital" com segurança, robustez e facilidade sem, entretanto, precisar dispender investimentos financeiros para a aquisição de licenças de uso. De tabela, utilizar soluções de DMS baseadas em software livre ainda coloca à disposição a possibilidade de desenvolver novas funcionalidades, corrigir problemas e adaptar o software às necessidades mais específicas de cada corporação.

Um pouco sobre o OWL

O OWL é um DMS baseado em plataforma Web registrado sob a licença de software livre GNU GPL. O aplicativo permite que, uma vez realizado o *upload* de um documento, várias ações possam ser executadas para sua manutenção no servidor, tais como: políticas de controle de acesso para cada grupo ou usuário do sistema, encaminhamento de um documento por email diretamente pelo OWL, monitoração de mudanças em arquivos e/ou pastas, controle do histórico de versões anteriores de um determinado documento, dentre outros.

Em especial, um recurso interessante que existe no OWL é o fato dele indexar o conteúdo de arquivos com formato PDF, ODT, ODS, ODP, TXT, DOC, XLS e outros formatos comuns. Isso significa dizer que no momento das buscas por arquivos, você pode escolher a opção de considerar o que está inserido dentro dos arquivos e não somente em seu nome e demais dados "externos". Em outras palavras, uma busca por "PCCIA", por exemplo, retornará também, caso a opção de busca no conteúdo de arquivos esteja selecionada, arquivos que contenham internamente essa palavra! Essa funcionalidade é muito interessante quando não se tem noção do nome do arquivo e sim alguma idéia do que se pode ter em seu conteúdo. Imagine o quanto não pode ser interessante obter como resultado alguns documentos que você sequer lembrava, mas que podiam ter as palavras que você usou em sua pesquisa!

Sob o ponto de vista de sua estrutura de armazenamento, o OWL mantém no banco de dados os metadados dos arquivos gerenciados por ele, tais como permissões de acesso, por exemplo. Os arquivos propriamente ditos podem ser armazenados no sistema de arquivos do servidor ou no banco de dados junto com os metadados. Essa decisão pode ser tomada nas configurações do OWL.

Preparando o seu sistema para instalar o OWL

O OWL é um software do tipo LAMP. Esse conceito vem, cada vez mais, sendo utilizado para agrupar aplicativos que utilizam tecnologias livres, como Linux, Apache, MySQL e PHP/Python/Perl. Essa combinação mostrou-se bastante poderosa, ágil e de baixo custo por ser composta por soluções livres. Diante disso, antes de partir para os procedimentos de instalação e configuração do OWL, é necessário instalar em seu sistema GNU/Linux o servidor Web Apache, o servidor de banco de dados MySQL e seus componentes comuns, a linguagem PHP e seu módulo para acesso a bancos de dados MySQL.

Os exemplos apresentados estão tomando como base um servidor com Ubuntu Server 7.04 (*Feisty Fawn*) instalado utilizando o kernel padrão dessa versão, o 2.6.20-15. Entretanto, caso você esteja utilizando outra versão do Ubuntu, ou ainda o Debian GNU/Linux e outras distribuições baseadas nele, não devem existir diferenças significativas para o processo de instalação do OWL. Se sua distribuição possui um mecanismo de gerenciamento de pacotes diferente do APT-GET, presente nas distribuições mencionadas anteriormente, consulte a documentação para obter mais informações a respeito dos procedimentos para a instalação dos softwares utilizados pela arquitetura LAMP, necessária para a instalação do OWL.

Para instalar toda a estrutura LAMP a partir de um sistema Ubuntu Server 7.04, basta executar, a partir de um terminal de comandos com privilégios de super-usuário, o comando apresentado na figura 1. O tempo para instalação dos pacotes dependerá da velocidade de sua conexão à Internet. Entretanto, vale ressaltar que o Ubuntu Server já contém no seu CD de instalação todos os softwares mencionados para a configuração de uma arquitetura LAMP.

Portanto, caso o sistema de gerenciamento de pacotes esteja configurado para utilizar o CD de instalação como fonte de obtenção de pacotes, ao invés de acessar a Internet, você será convidado a somente inserir o seu CD de instalação. Por fim, se você tiver disponibilidade de instalar o

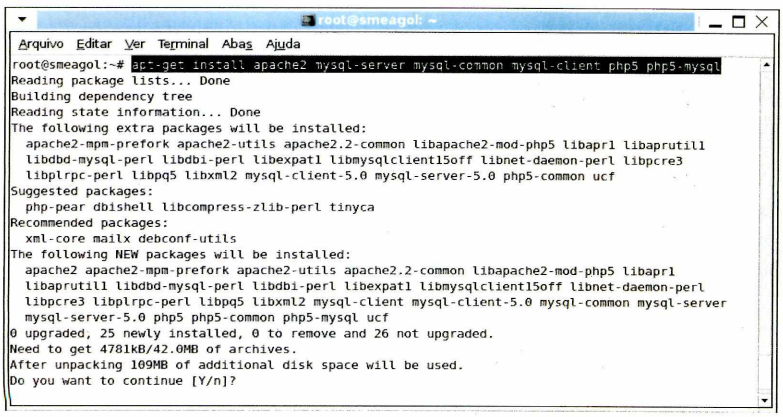
ambiente servidor desde o seu início, no final do processo de instalação o Ubuntu Server apresenta a opção para já deixar instalado no sistema os pacotes para a arquitetura LAMP. Fica a seu critério qual solução utilizar!

Obtendo o OWL

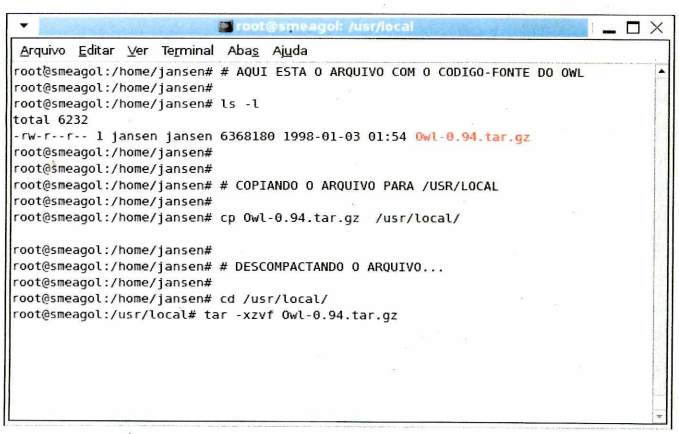
O OWL já possui versões "empacotadas" para muitas distribuições GNU/Linux, inclusive para o Ubuntu. Entretanto, nessa oportunidade será utilizado o aplicativo partindo do código original, uma vez que essa alternativa provê uma garantia maior de se utilizar versões mais recentes do software.

Para obter o código-fonte do OWL, basta acessar a sessão de downloads de sua página no SourceForge, no seguinte endereço: **http://sourceforge.net/project/showfiles.php?group_id=9444**. Você precisará baixar o arquivo indicado na opção "OWL". No momento da escrita desse artigo, a versão mais recente correspondia ao arquivo `Owl-0.94.tar.gz`. Opcionalmente, deixe o pacote que contém suporte para outras línguas além da original do software que é em inglês, na opção "OWL Language Packs". Infelizmente, ainda não existe versão para português. Entretanto, por se tratar de um aplicativo livre, é possível implementar o suporte ao português sem precisar esperar pelo time oficial de desenvolvimento do software. Na sessão de download existe ainda a opção para fazer o download da documentação do OWL, a qual pode lhe ser útil num futuro muito próximo.

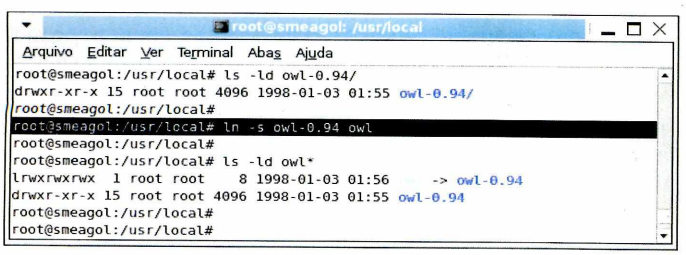
Uma vez obtido o arquivo `Owl-0.94.tar.gz`, copie-o para o diretório `/usr/local` e descompacte-o. Após descompactar (figura 2), um diretório chamado `owl-0.94` será criado em `/usr/local`. Para tornar sua instalação um pouco mais organizada, de forma que não fique tão explícita a versão do OWL que está sendo utilizada, crie um *link* simbólico chamado "`owl`" apontando para "`own-0.94`", de acordo com o exibido na figura 3.



F1. Instalação da estrutura LAMP.



F2. Descompactação do OWL.



F3. Criação do link simbólico.

Configurando o banco de dados

O banco de dados é uma parte fundamental para o funcionamento do OWL. Portanto, é importante dedicar especial atenção aos seus procedimentos de configuração. Uma vez que todas as informações mais importantes do OWL, incluindo as políticas de controle de acesso aos arquivos e pastas do DMS, ficam armazenadas no banco de dados, torna-se crucial adotar algumas medidas básicas de segurança durante o seu processo de configuração. Que tal começar pela senha do administrador do banco de dados?

Por padrão, após a instalação do MySQL, o usuário `root`, administrador do banco de dados, é criado com uma senha nula. Isso significa que qualquer usuário do seu sistema pode entrar no banco de dados e usufruir dos poderes do super-usuário sem sequer ter a necessidade de informar qualquer senha. Para verificar se essa é a situação do seu sistema de banco de dados recém-instalado, basta digitar, a partir de um terminal, o seguinte comando:

```
# mysql -u root -p
```

No momento em que for solicitada a senha, simplesmente pressione *Enter*. Caso o *prompt* do MySQL seja exibido, de acordo com o mostrado na figura 4, bingo! Seu sistema está com a senha vazia para o super-usuário.

Inserir uma senha para o `root` é simples e rápido. Basta executar o seguinte comando:

```
mysqladmin -u root password jethrotull
```

Nesse caso, a senha do `root` passou a ser "`jethrotull`". Lembre-se de que esse procedimento não irá funcionar caso o usuário `root` de seu banco de dados já tenha uma senha não nula.

Outra alternativa para alterar a senha do super-usuário consiste em entrar no *prompt* do MySQL e alterar diretamente na tabela do banco que armazena os seus usuários e os respectivos privilégios. Isso pode ser feito por meio dos comandos apresentados na figura 5.

O próximo passo consiste na criação do banco de dados que será utilizado pelo OWL. Para tal, efetue o *login* como super-usuário, já utilizando a nova senha que você acabou de inserir, e, em seguida, execute o comando:

```
create database nome_do_banco
```

A figura 6 apresenta um exemplo para a criação do banco de dados chamado `owl` que será utilizado nos próximos passos. Para verificar se a nova base de dados foi criada corretamente, utilize no *prompt* do MySQL o comando "`show databases`" e confira se o novo banco aparece listado, conforme apresentado na figura 7.

Uma vez que o banco de dados esteja criado, é necessário criar as tabelas que serão utilizadas para armazenar as informações do OWL. Isso pode ser feito utilizando-se um *script SQL*, incluso no próprio pacote do software descompactado anteriormente.

```
$ cd /usr/local/owl/DOCS/sql
$ mysql -p owl -u root < mysql-tables.sql
```

Após digitar a senha, solicitada durante a execução do comando `mysql` anterior, o *script* será carregado e as tabelas serão criadas. Para conferir se as tabelas foram importadas corretamente, acesse o *prompt* do MySQL, configure a utilização do banco "`owl`" por meio do comando "`use owl`" e, em seguida, execute o comando "`show tables`". O resultado deve listar as tabelas criadas pelo *script* SQL executado anteriormente (figura 8).

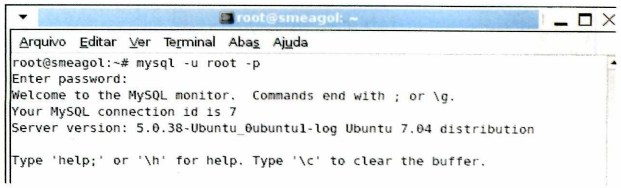
Para manipular seus dados no MySQL, a configuração do OWL exige a utilização de um usuário válido no banco de dados que tenha permissões sobre as tabelas da base `owl` criada recentemente. Nada lhe impede de utilizar a conta do super-usuário para esse propósito, a não ser pelo fato de ser uma medida inadequada do ponto de vista de segurança. Isso porque de uma forma ou de outra será necessário expor a senha desse usuário em algum arquivo de configuração. Além disso, o usuário `root` no MySQL tem plenos poderes sobre todas as bases de dados e o OWL só precisa de acesso à sua própria base. Diante disso, caso seja utilizado o acesso de `root` na configuração do OWL, lembre-se de que uma vez comprometida sua senha, o atacante terá acesso completo a todas as outras bases de dados do seu servidor MySQL.

Para criar um usuário, efetue o *login* no servidor MySQL usando a conta do super-usuário e no *prompt* de comandos, execute a seguinte sentença:

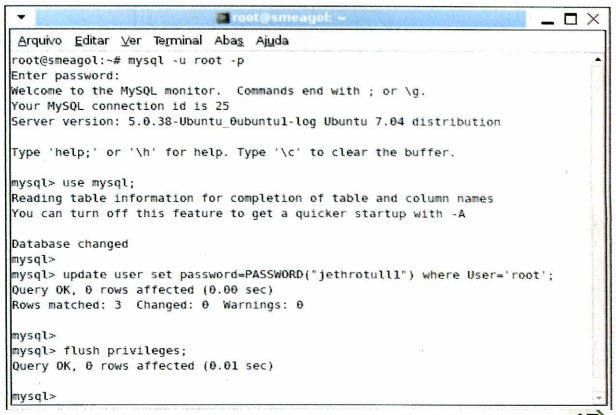
```
GRANT ALL PRIVILEGES ON owl.* TO owluser@localhost IDENTIFIED BY 'aqualung' ;
```

O comando anterior irá criar um novo usuário para o MySQL, chamado `owluser`, o qual terá permissões de acessar o MySQL a partir da mesma máquina onde o banco está instalado ("`localhost`"). Esse usuário terá permissão ("`GRANT`") de executar todas as tarefas ("`ALL PRIVILEGES`") sobre as tabelas do banco de dados `owl` ("`owl.*`"). A figura 9 mostra a confirmação de que o usuário foi, de fato, criado. A senha desse usuário será "`aqualung`". Criado o usuário `owluser`, as configurações do OWL não precisarão fazer qualquer referência à conta do `root` de seu servidor MySQL.

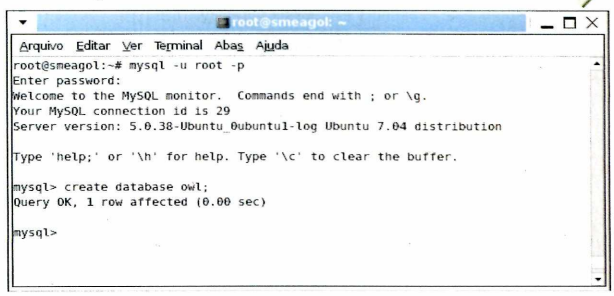
Caso o OWL não estivesse sendo instalado na mesma máquina do servidor de banco de dados, a conta do usuário deveria ter acesso a partir do computador onde o software estava sendo instalado. Nesse caso, no momento da criação do usuário, o *alias* `localhost`, que designa sempre a própria máquina, deveria ser substituído pelo nome da máquina onde o OWL estaria sendo instalado.



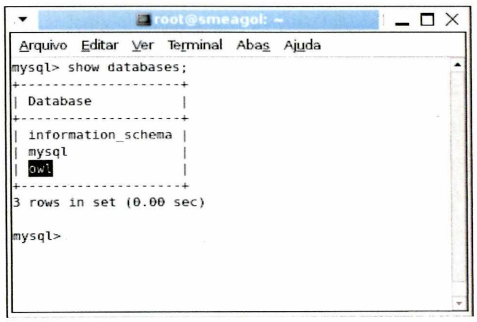
F4. Acesso ao prompt do MySQL.



F5. Alteração da senha do usuário root.



F6. Criação do banco "owl".



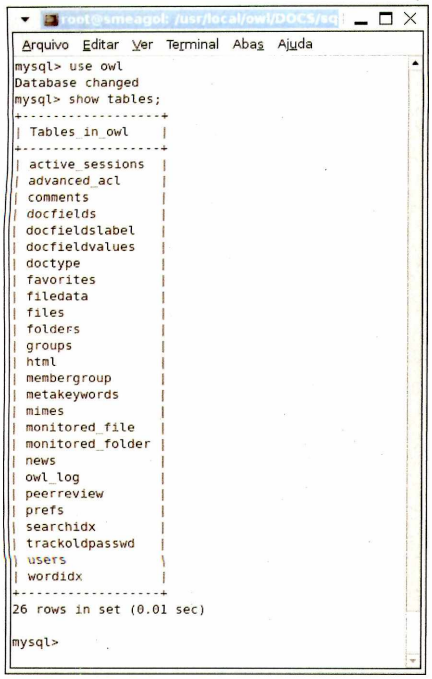
F7. Consulta aos bancos criados.

Instalando e configurando o OWL

O primeiro passo da configuração do OWL consiste em disponibilizar o diretório que contém os seus arquivos no seu servidor Web. No caso do Ubuntu, os diretórios considerados pelo Apache, por *default*, ficam localizados no diretório `/var/www`. Diante disso, esse procedimento resume-se em criar nesse diretório um *link* simbólico para o diretório onde se encontra, de fato, o OWL, que no caso do exemplo apresentado é `/usr/local/owl` (figura 10).

A parte mais significativa da configuração inicial do OWL, entretanto, resume-se, basicamente, na edição do arquivo `owl.php`, localizado no diretório `/usr/local/owl/config`. Preparado? Então vamos lá!

O primeiro parâmetro a ser configurado em `owl.php` é o `$default->owl_root_url`, localizado logo no início do arquivo. Ele deve refletir a pasta do servidor Web onde está o OWL. Lembra do *link* simbólico criado há pouco no diretório `/var/www`? Ele será visto pelo servidor Web exatamente como o diretório onde estão os arquivos do OWL.



F8. Consulta às tabelas existentes no banco "owl".

Portanto, é o nome desse diretório que deve estar como valor do parâmetro mencionado, de acordo como mostrado a seguir:

```
$default->owl_root_url  = "/owl";
```

Existem duas opções do OWL para armazenar os arquivos que serão submetidos pelos usuários ao servidor: utilizar o próprio sistema de arquivos ou o banco de dados. Quem determina qual será o tipo de repositório utilizado pelo OWL é o parâmetro `$default->owl_use_fs`. Como o próprio nome indica, caso o valor seja "`true`" (verdadeiro), os arquivos serão armazenados no sistema de arquivos (do inglês *File System*, daí a sigla "`fs`" no nome do parâmetro). Nesse momento, será utilizado o valor *default*, que indica o uso do sistema de arquivos, conforme apresentado abaixo:

```
$default->owl_use_fs = true;
```

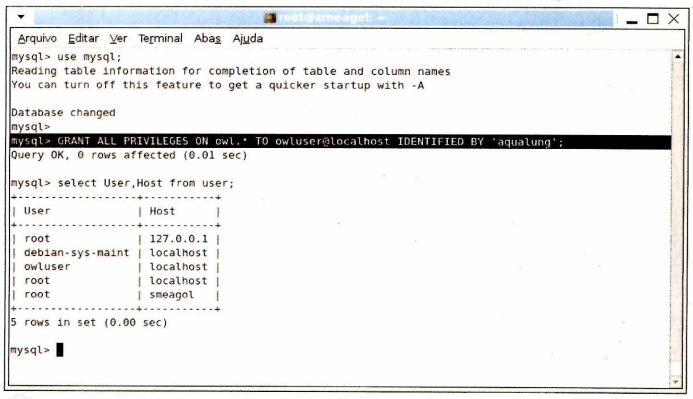
Uma vez confirmado o armazenamento em sistema de arquivos, é necessário alterar o dono da pasta onde o OWL irá guardar seus arquivos para o usuário do servidor Web, que no caso de distribuições como o Ubuntu e o Debian, trata-se do `www-data`. Essa tarefa pode ser feita por meio da utilização do comando `chown` na pasta `/usr/local/owl/Documents`, local *default* para armazenamento de arquivos do OWL. A figura 11 apresenta o estado original do diretório, a execução da mudança para o usuário `www-data` e, por fim, o estado final após a mudança de propriedade da pasta. Caso esse passo não seja feito, qualquer tentativa de submeter um arquivo ou criar uma pasta no OWL retornará uma mensagem de erro de permissão.

Em sua configuração, é possível indicar o nome de cada tabela criada na base de dados para armazenar os dados do OWL. Entretanto, por ter sido utilizado o *script* SQL padrão para criação do banco, não será necessário alterar qualquer parâmetro nesse sentido.

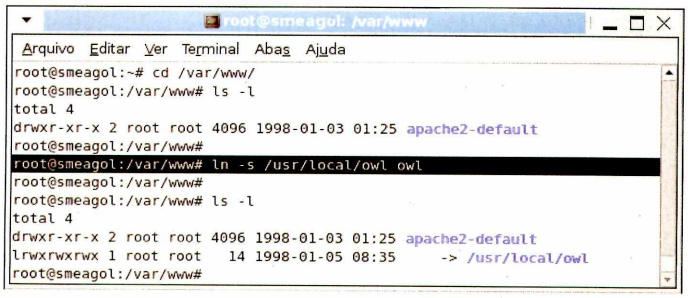
O próximo passo consiste na configuração do acesso ao banco de dados por parte do OWL. Essas configurações encontram-se na seção denominada "`Database info`" do arquivo `owl.php`, cujos parâmetros originais devem estar parecidos com aqueles mostrados no Quadro 1.

São quatro os parâmetros básicos a serem configurados. Os dois primeiros, `$default->owl_db_user[0]` e `$default->owl_db_pass[0]`, armazenam o usuário e a senha, respectivamente, para acessar o banco criado para o OWL no MySQL. Na seção "*Configurando o banco de dados*" foi criado um usuário chamado "`owluser`" com senha "`aqualung`". São esses, então, os valores a serem associados aos parâmetros em questão.

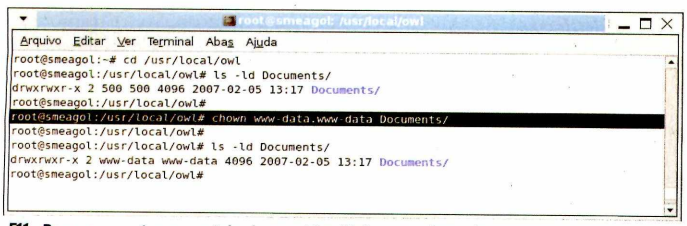
O próximo parâmetro deve indicar o nome ou endereço IP do computador onde está instalado o banco de dados. Como na estrutura utilizada no decorrer do texto a



F9. Criação do usuário "owluser".



F10. Criação do link simbólico e consulta para confirmar sua existência.



F11. Passos para ter o usuário do servidor Web como dono do repositório usado pelo OWL.

```
//**************************************
// Database info BEGIN
//**************************************

$default->owl_default_db = 0;

// First Database Information

$default->owl_db_id[0] = "0";
$default->owl_db_user[0] = "root";
$default->owl_db_pass[0] = "";
$default->owl_db_host[0] = "localhost";
$default->owl_db_name[0] = "owl090";
$default->owl_db_display_name[0] = "Intranet";
$default->owl_db_ldapserver[0] = "your.ldap.server.address";
$default->owl_db_ldapdomain[0] = "";
//$default->owl_db_FileDir[0] =  "/var/www/html/owl-0.90";
$default->owl_db_FileDir[0] =  $default->owl_fs_root;
$default->peer_auto_publish[0] = "false";
```

Q1. Parâmetros originais de configuração do banco de dados no arquivo owl.php.

aplicação OWL e o banco de dados encontram-se na mesma máquina, basta utilizar o nome especial "`localhost`" que, conforme já foi dito, sempre indica o nome de uma máquina localmente.

Por fim, o nome do banco de dados criado para o OWL deve ser associado ao parâmetro `$default->owl_db_name`. O banco criado para essa finalidade foi "`owl`", certo?

Os parâmetros que referem-se ao LDAP, `$default->owl_db_ldapserver` e `$default->owl_db_ldapdomain`, podem ser comentados, inserindo "`//`" no início da linha, uma vez que um banco de dados está sendo utilizado para armazenar as contas dos usuários do OWL e a configuração com LDAP não será abordada nessa oportunidade.

Com essas modificações, os parâmetros de configuração do banco de dados deverão estar conforme o Quadro 2.

A configuração básica do OWL encerra-se por aqui... Ansioso por ver os resultados? Então, siga em frente!

Testando sua instalação

O teste mais simples consiste em acessar o OWL para verificar se a página de *login* é corretamente apresentada. Supondo que a instalação foi feita em um computador cujo endereço IP é 192.168.1.100, basta digitar a seguinte URL na barra de endereços de seu *browser* preferido:

http://192.168.1.100/owl

Caso tudo ocorra bem, você verá a página inicial do OWL como apresentado na figura 12.

Se algo não ocorreu como esperado, o primeiro item a ser verificado é se o servidor Web está funcionando no computador em que você instalou o OWL. Uma das maneiras de verificar é por meio do comando "`ps -ef | grep apache`". Caso o retorno seja semelhante ao apresentado na figura 13, o servidor está em execução e esse pode ser o momento de você verificar todos os passos anteriores para certificar-se de que não ficou faltando algo.

Se, por outro lado, o retorno for parecido com o da figura 14, você precisa iniciar o servidor Web por meio do seguinte comando:

```
/etc/init.d/apache2 start
```

Esse *script* pode ter nomes diferentes em outras distribuições que não sejam o Ubuntu ou o Debian GNU/Linux.

Utilizando o OWL

O seu primeiro acesso ao OWL pode ser feito por meio da conta do adminstrador cujo *login* e senha são "`admin`". Se tudo ocorrer bem, o painel de administração será mostrado (figura 15).

Para testar as funcionalidades do OWL, é interessante criar, de imediato, um grupo e uma conta de usuário convencional, selecionando a opção "*New Group*" e "*New User*", respectivamente, mostradas logo na tela inicial após o *login* como usuário "`admin`". O formulário para criação do grupo (figura 16) e da conta (figura 17) é simples e intuitivo.

Uma providência interessante a ser tomada imediatamente (caso sua instalação vá ser utilizada por outros usuários) é trocar a senha do usuário "`admin`". Isso

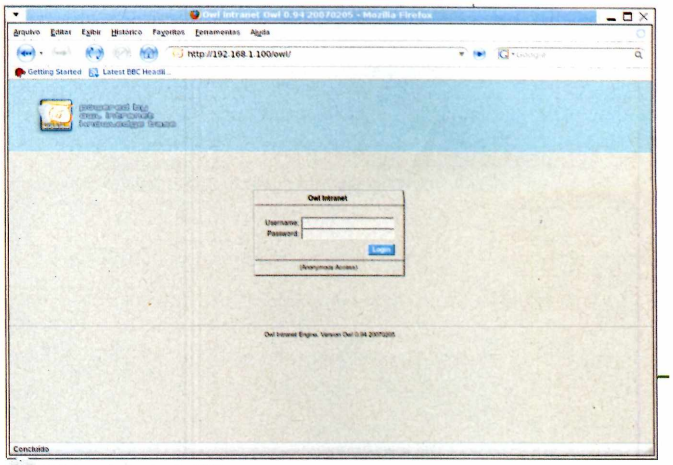
```
//**************************************
// Database info BEGIN
//**************************************

$default->owl_default_db = 0;

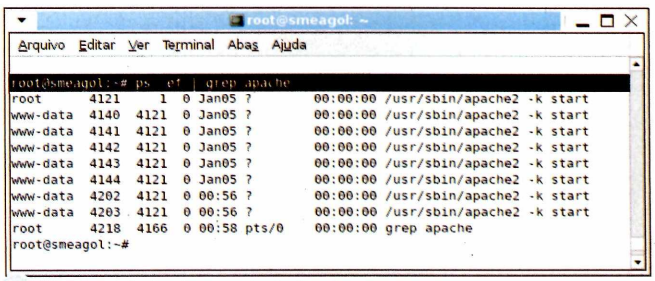
// First Database Information

$default->owl_db_id[0] = "0";
$default->owl_db_user[0] = "owluser";
$default->owl_db_pass[0] = "aqualung";
$default->owl_db_host[0] = "localhost";
$default->owl_db_name[0] = "owl";
$default->owl_db_display_name[0] = "Intranet";
//$default->owl_db_ldapserver[0] = "your.ldap.server.address";
//$default->owl_db_ldapdomain[0] = "";
//$default->owl_db_FileDir[0] = "/var/www/html/owl-0.90";
$default->owl_db_FileDir[0] = $default->owl_fs_root;
$default->peer_auto_publish[0] = "false";
```

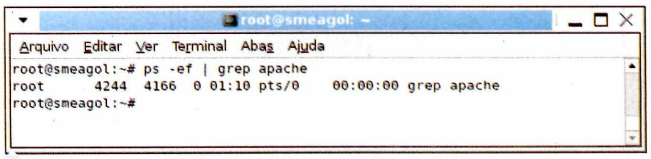
Q2. Parâmetros de configuração do banco de dados no arquivo owl.php.



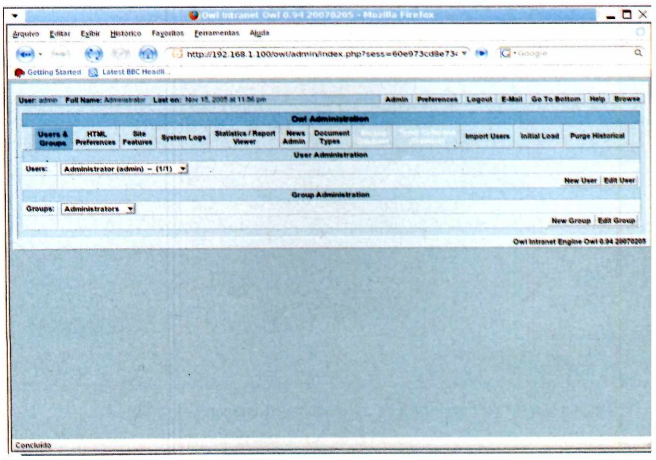
F12. Página de login do OWL.



F13. Checagem do funcionamento do Apache.



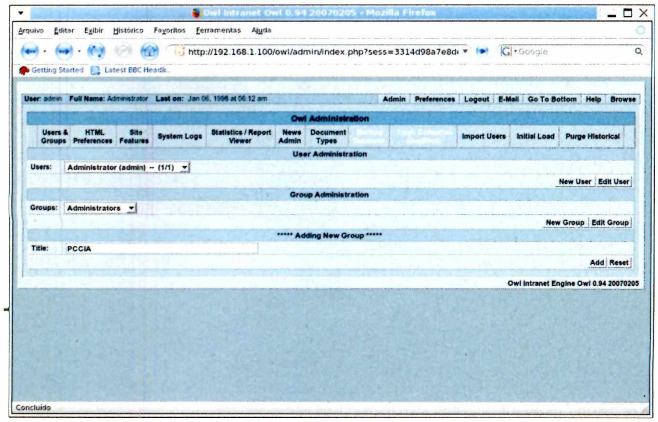
F14. Apache não está funcionando.



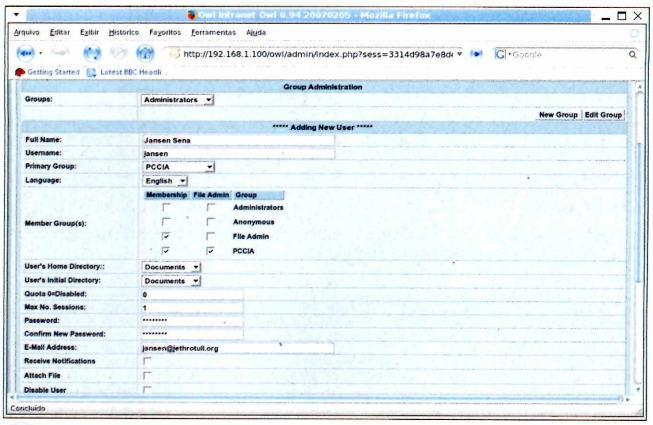
F15. Painel de admnistração do OWL.

pode ser feito selecionando a opção "*Preferences*" que fica na barra superior do OWL. No formulário que será mostrado, basta digitar a senha antiga e repetir duas vezes a nova senha.

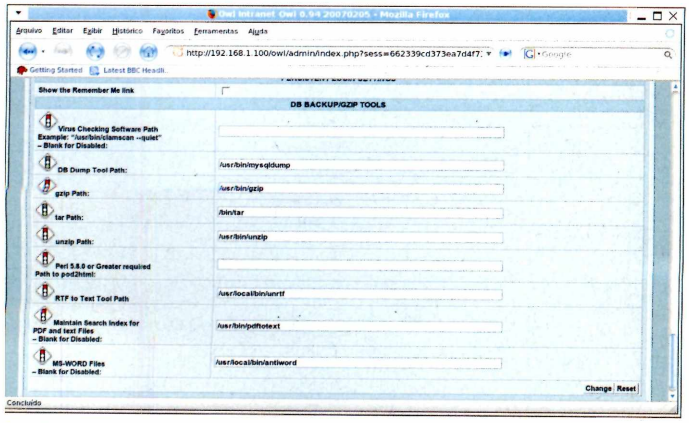
Para poder indexar o conteúdo de documentos e executar outras tarefas, o OWL utiliza alguns utilitários externos como o `antiword`, o `unrtf` e o `gzip`. Entretanto, é preciso inicialmente saber se esses utilitários encontram-se instalados em seu sistema e se o caminho para acessá-los está correto na configuração do OWL. Isso pode ser verificado na seção "*DB Backup/GZIP Tools*" da opção "*Sites Features*", na barra superior apresentada quando a opção "*Admin*" é selecionada. O pequeno semáforo vermelho indica que não foi possível encontrar o aplicativo. Ao contrário, o sinal verde significa que o utilitário está instalado e seu caminho está correto na configuração do OWL (figura 18).



F16. Formulário para criação do grupo.



F17. Formulário para criação do usuário.



F18. Estado inicial do caminho dos aplicativos utilizados pelo OWL.

Note que na situação atual o utilitário `gzip` aparece com problemas. Entretanto, esse utilitário já é instalado, por padrão, na grande maioria das distribuições, incluindo o Ubuntu e o Debian GNU/Linux. Diante disso, a execução do comando "`whereis`" no servidor pode revelar uma verdade: que o `gzip` já se encontra instalado (como apresentado na figura 19). O OWL não está enxergando, porque o caminho para acessá-lo está errado.

A configuração do OWL mostra "`/usr/bin/gzip`", enquanto o comando `whereis` relevou que o caminho correto é simplesmente "`/bin/gzip`". Se esse for o seu caso, corrija essa informação rapidamente no OWL.

Os outros aplicativos, no ambiente utilizado como exemplo desse texto, não estavam de fato instalados. Para resolver esse problema, basta utilizar o sistema `apt-get` para obter e instalar os pacotes:

```
# apt-get install
zip unzip antiword
unrtf xpdf-utils
```

Confira o caminho dos utilitários e atualize a configuração do OWL. Em seguida, clique em "*Change*" e após a página ser recarregada, vá até a seção "*DB Backup/GZIP Tools*" e confira se o estado da configuração dos aplicativos indica um sinal positivo (figura 20).

Manipulando documentos no OWL

Agora é o momento de conferir o que o OWL pode fazer pelo gerenciamento de seus documentos! Efetue o *logout* com a conta do `admin` e autentique-se no OWL usando a conta do usuário criado anteriormente. Feito isso, crie uma pasta clicando na opção "Add Folder" e insira os dados da nova pasta a ser criada, conforme apresentado na figura 21.

Após adicionar algumas pastas para organizar seus documentos eletrônicos, o OWL começa a apresentar uma estrutura capaz de dar ordem à bagunça de documentos espalhados nos HD's e drives de rede de sua empresa! Veja a figura 22.

Para submeter um arquivo clique na opção "*Add Document*". No formulário que será aberto, selecione o arquivo a ser encaminhado ao OWL e preencha os outros campos. Dê atenção especial ao campo "*Keywords*". Ele deve conter palavras-chave a respeito do conteúdo do arquivo. Isso pode facilitar em muito a busca posterior por informações (figura 23).

Um dos recursos mais importantes do OWL é o seu processo de busca. Para buscar alguma informação basta preencher os termos da pesquisa no campo "*Search*" e pressionar o botão correspondente. Caso você deseje que a pesquisa busque pelas informações dentro do conteúdo dos arquivos, antes de clicar em "*Search*" selecione a opção "*Search Within*". A busca apresentada na figura 24 tem como resultado os arquivos apresentados na figura 25.

Observe que as estrelas ao lado esquerdo dos arquivos retornados na pesquisa representa uma espécie de *ranking* indicando quais dos arquivos têm mais popularidade diante da busca realizada.

Outras operações como renomear, copiar e mover arquivos; monitorar um determinado arquivo; encaminhar um arquivo diretamente por email; adicionar um comentário; manipular as permissões de um arquivo, entre outras, podem ser acessadas simplesmente encostando-se o mouse sobre o nome do arquivo na coluna "*File*".

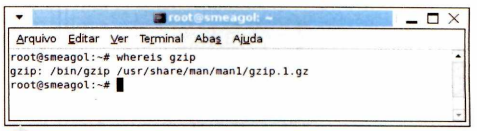
Conclusão

Muitas empresas costumam armazenar grande parte de suas informações em seus ambientes computacionais. Entretanto, com o passar do tempo, a quantidade de informações armazenadas em uma estrutura

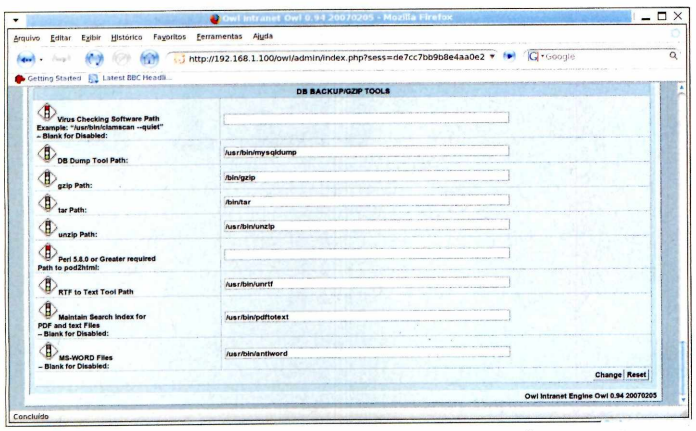
não organizada e sem recursos adequados pode complicar a busca de informações e o seu gerenciamento. Nesse contexto, um DMS pode ajudar, em muito, a estruturar os documentos eletrônicos, tornando mais fácil, ágil e seguro o acesso às informações corporativas. De fato, um sistema DMS pode até mesmo ser adequado para armazenar informações pessoais, uma vez que, da mesma maneira que o mundo corporativo, atualmente muitas informações pessoais são armazenadas em computadores domésticos.

Mesmo diante das soluções proprietárias que exigem altos investimentos quanto ao pagamento de suas licenças de uso, soluções em software livre possuem maturidade suficiente para atender demandas de muitos ambientes corporativos de pequeno, médio e grande porte. O OWL está entre essas soluções.

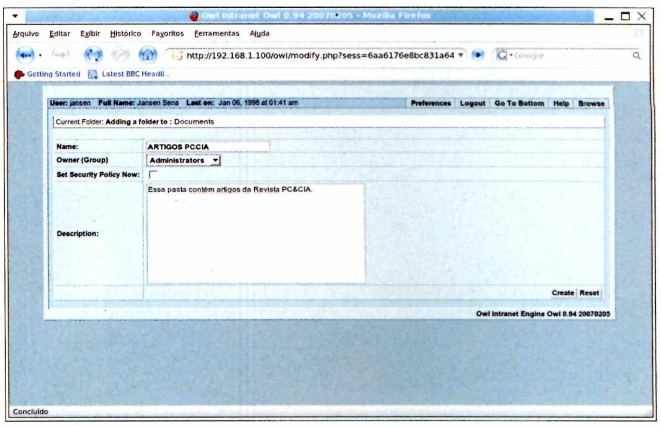
Agora, resta-lhe explorar mais os recursos do OWL e aguardar o que vem por aí no próximo mês! **PC**



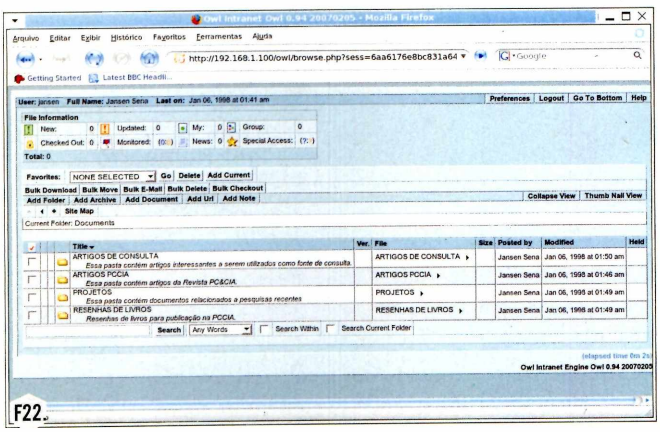
F19. Checando instalação do gzip.



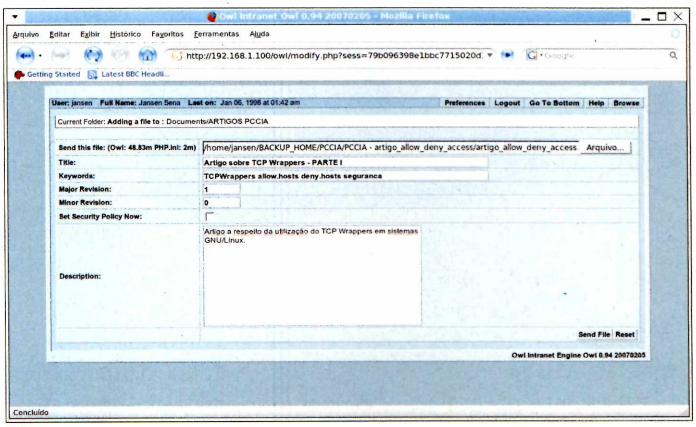
F20. Resultado dos ajustes feitos para resolver as situações pendentes quanto aos utilitários externos utilizados pelo OWL.



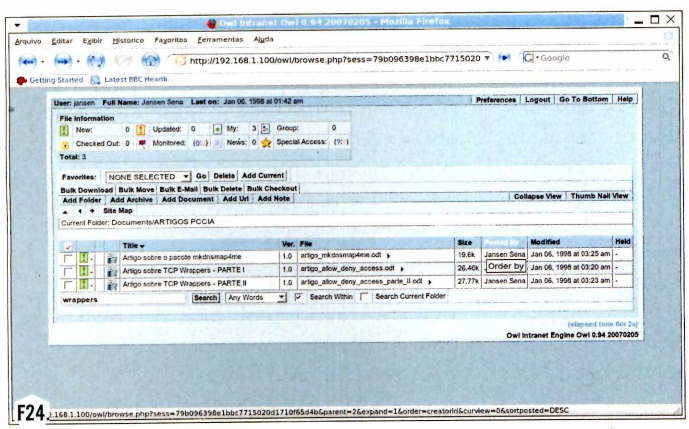
F21. Criação da pasta.



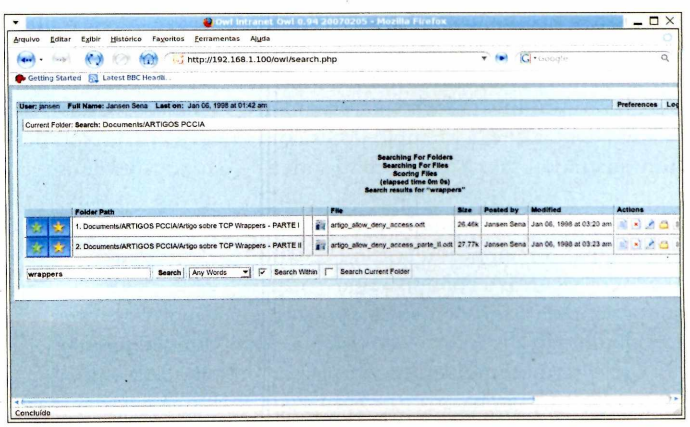
F22. Exemplo de um conjunto de pastas criadas no OWL.



F23. Exemplo de submissão de arquivo ao OWL. Após terminar, clique em "Send File" e pronto!



F24. Critério para busca é a palavra "wrappers".



F25. Resultados da busca: agora fica fácil localizar arquivos.



Certificação Microsoft MCTS

PARTE 3

Nesta terceira matéria da série preparatória para o exame 70-620, começaremos a falar dos recursos de segurança disponíveis no Vista, tais como o User Account Control (UAC) e o Windows Defender. Ambos são assuntos bastante abordados no exame.

Igor Humberto e
Paulo Sant'anna

Cenário atual

Nos sistemas operacionais baseados na plataforma NT, é preciso ter uma conta de usuário para trabalhar. As contas são organizadas em grupos e estes possuem níveis de acesso pré-configurados no sistema operacional. É através deles que determinamos os níveis de acesso desejados a cada usuário. No grupo Administradores, por exemplo, *estão as contas* que, a exemplo do usuário Administrador, têm acesso a praticamente qualquer item do sistema (existe ainda a conta que representa o próprio sistema operacional, a qual possui acesso irrestrito a *todos os recursos*). Por outro lado, contas que participam do grupo Usuários possuem acesso limitado aos recursos do sistema.

Uma prática comum que acaba se transformando em um problema é o fato da maioria dos usuários (doméstico ou corporativo) utilizar o sistema com uma conta que possui privilégios administrativos. Isso porque o nível de exposição do sistema aumenta absurdamente. Contas com privilégio administrativo só devem ser usadas, como o próprio nome sugere, para executar tarefas administrativas, tais como instalação de programas, configurar recursos no sistema, compartilhar recursos (pastas e/ou impressoras) etc. Para acessar a Internet, ler e-mails, utilizar os seus aplicativos de escritório, jogar, entre outras tarefas cotidianas, não é necessário possuir privilégios elevados.

A grande desculpa para isso é a comodidade. Para que iniciar como usuário comum e depois ter de fazer um logoff e um novo logon como administrador para executar algumas tarefas, se já posso iniciar como administrador? É o que normalmente pensam os usuários, porém muitos possuem um conhecimento limitado dos recursos do Windows e, mesmo quando os conhecem, não são criativos para usá-los de forma adequada. Faz muito tempo, por exemplo, que o sistema possui o recurso **Executar como** (ferramenta de linha de comando RUNAS), o qual permite ao usuário executar determinadas tarefas usando outras credenciais. Através dele podemos trabalhar o tempo todo usando uma conta com privilégios limitados e, apenas quando necessário, lançar mão do **Executar como** para executar uma determinada tarefa usando as credenciais de uma conta com privilégios administrativos.

Na prática o **Executar como** ainda é pouco utilizado. Um dos problemas de trabalhar como Administrador do sistema é que se uma aplicação hostil for carregada, ela será executada com o mesmo nível de privilégio da conta logada, isto é, a de Administrador.

E agora, como impedir o administrador de fazer alguma coisa no sistema? É possível escrever no registro do sistema, na pasta Windows, criar outras contas, instalar outros aplicativos etc. Isso é um prato cheio para um usuário mal intencionado.

Configurando o User Account Control (UAC)

Trata-se de um dos mais importantes recursos incluídos no Windows Vista para minimizar sua dependência em relação ao usuário, no que diz respeito à proteção. A idéia por detrás do UAC é bastante simples: permitir aos usuários trabalharem sempre com o nível de privilégio de um usuário comum (limitado), mesmo que o logon seja feito a partir de uma conta com privilégios administrativos.

O primeiro passo para isso foi repensar os níveis de privilégios conferidos pelo sistema. Algumas tarefas que antes exigiam privilégios administrativos para serem executadas, agora não exigem mais (tabela 1). A configuração de uma conexão Wireless e o ajuste do fuso horário são alguns exemplos.

Além disso, sob o entendimento de que nem sempre é seguro dar mais privilégios para o usuário comum, foram criados serviços adicionais que permitem a execução segura de algumas tarefas. O Active X Installer, por exemplo, permite que um administrador pré-aprove sites que possuam controles Active X confiáveis. O Desfragmentador de discos, por sua vez, pode ser executado como um processo agendado e, assim, permitir a otimização do disco.

E no caso das aplicações que ainda exigirem um login a partir de uma conta com privilégios administrativos para serem executadas (em teoria, apenas as anteriores ao Windows Vista trabalham dessa forma), o UAC usa um sistema que "engana" a aplicação. O objetivo é fazer com que ela "imagine" que o usuário atende ao requisito de privilégio exigido.

Por último, considerando situações como configuração de sistema e instalação de programas, por exemplo, as quais exigem o nível de privilégio mais elevado para serem executadas, o UAC possui um **Executar como** reformulado que pode ser utilizado com muito mais facilidade. Quando o sistema percebe a necessidade de elevação de privilégios, uma verificação determina se a conta do usuário logado pertence ao grupo Administradores. Uma vez satisfeita esta condição, uma caixa será exibida perguntando se o usuário deseja continuar (figura 1).

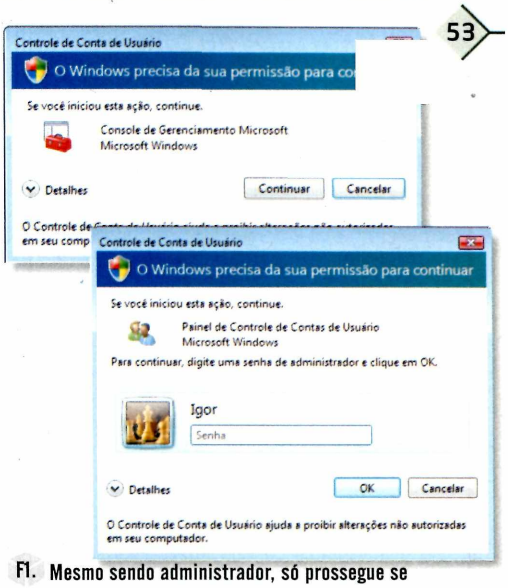
Privilégio	Função
Visualizar a hora do sistema e o calendário	Pode-se abrir a hora e o calendário, mas não é possí... fazer alterações em função, por exemplo, do registro de informações no log de segurança (auditoria)
Alterar a zona do fuso horário	É possível alterar a zona do fuso horário, por exemplo, quando o usuário estiver viajando
Instalar WEP para permitir conexões wireless criptografadas	Permite que usuários se conectem a redes WiFi usando criptografia de dados
Alterar configurações de vídeo	Usuários podem alterar as configurações de vídeo, de acordo com as suas necessidades
Alterar configurações de gerenciamento de energia	Permite aos usuários alterarem esquemas de energia para, por exemplo, maximizar a autonomia da bateria do notebook
Instalar fontes	Auto-explicativo
Adicionar impressoras ou outros dispositivos que possuam drivers instalados no sistema, ou que tenham sido fornecidos por um Administrador	Usuários podem instalar dispositivos pré-aprovados que usem a tecnologia Plug and Play
Criar e configurar conexões VPN	Usuários agora podem criar conexões seguras criptografadas com os seus locais de trabalho
Fazer o download e instalar atualizações críticas usando um instalador compatível com o UAC	Usuários de notebooks, por exemplo, podem manter os seus equipamentos atualizados mesmo se estiverem muito tempo desconectados dos seus respectivos ambientes corporativos

T1. Novos privilégios incluídos no Vista.

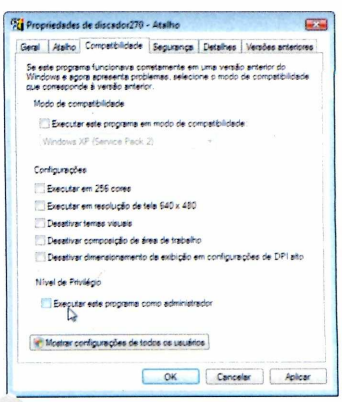
Nesse ponto, você talvez esteja se perguntando: não seria suficiente colocar a conta de um usuário como membro do grupo Usuários avançados? No Windows Vista o referido grupo ainda existe apenas por uma questão de compatibilidade com sistemas antigos. Para a maioria das tarefas que exigiam privilégios oferecidos para usuários membros dos grupos Usuários avançados ou Administradores, a conta do usuário padrão já será suficiente.

Aplicações legadas x UAC

As aplicações desenvolvidas para trabalharem no Windows Vista foram desenhadas com o UAC em mente. Isso significa que se elas precisarem de uma elevação de privilégios, isso será solicitado ao UAC. Já no caso de uma aplicação legada, que seja incapaz de conviver amistosamente com o UAC, é necessário realizar alguns ajustes. Lembra de quando precisávamos configurar os atalhos de algumas aplicações no Windows XP para tentar garantir a compatibilidade com aplicativos que tivessem sido originalmente desenhados para trabalharem em versões anteriores, tais como o Windows 98? Isso era feito através da guia Compatibilidade, disponível quando abríamos as propriedades de algum atalho de aplicativo. No Windows Vista essa guia ainda existe (figura 2), porém, uma opção especial, denominada Executar esse programa como administrador, informa ao UAC que essa aplicação necessitará de elevação de privilégios para funcionar a contento.



F1. Mesmo sendo administrador, só prossegue se ele confirmar intenção; abaixo, caixa exibida para usuário comum e solicitação por senha de administrador.



F2. Opções para a configuração de aplicações legadas no Windows Vista.

Diretiva	Configuração de segurança
Alternar para a Área de trabalho segura ao pedir elevação	Ativado (Default)/Desativado
Comportamento do prompt de elevação de administradores no Modo de Aprovação de Administrador	Pedir Consentimento (Default)/ Elevar sem aviso/Pedir credenciais
Comportamento do prompt de elevação de usuários padrão	Pedir credenciais (Default)/ Negar automaticamente solicitações de elevação
Detectar instalações de aplicativos e aviso de elevação	Ativado (Default)/Desativado
Elevar somente executáveis assinados e validados	Ativado/Desativado (Default)
Eleve apenas aplicativos UIAccess que estejam instalados em locais seguros	Ativado (Default)/Desativado
Executar todos os administradores no Modo de Aprovação de Administrador	Ativado (Default)/Desativado
Modo de Aprovação de Administrador para a conta de Administrador Interno	Ativado/Desativado (Default)
Virtualizar falhas de gravação de arquivos e Registros para locais para usuários	Ativado (Default)/Desativado

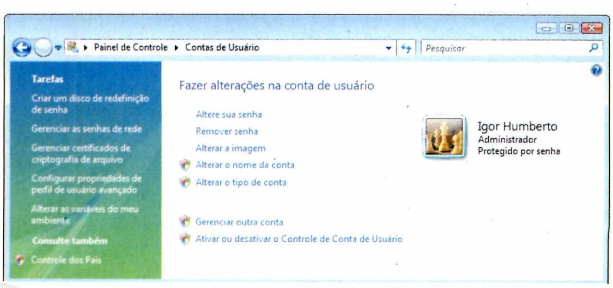
T2. Ao abrir cada diretiva, você verá uma guia Explicar dentro da caixa de configuração, a qual, como o nome sugere, fornece mais informações.

Configuração do UAC

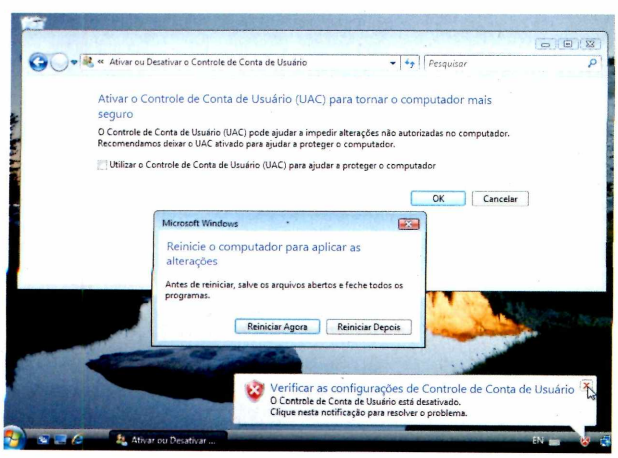
É possível configurar o UAC a partir das diretivas ou via painel de controle.

Configuração por diretiva

O Windows Vista vem acompanhado de uma série de novas diretivas que visam a proporcionar um maior controle do sistema operacional para o administrador. Ao abrir o console de Diretivas de Segurança Locais (SECPOL.MSC), você encontrará algumas diretivas que tratam especificamente do UAC. Para encontrá-las, navegue até Configurações de segurança/Diretivas locais/Opções de segurança. Agora, basta localizar a categoria Controle de contas de usuário. Na tabela 2 você verá quais diretivas estão disponíveis e como é possível configurá-las.



F3. Controle de contas vem ativado por padrão.



F4. Central de segurança do Vista irá alertá-lo sobre a configuração que potencialmente expõe o sistema a riscos.

Configuração através do Painel de controle

Outra forma de alterar o comportamento do sistema diante do UAC é usando o Painel de controle. Após abri-lo, abra o aplicativo Contas de usuário. As opções de configuração são basicamente as mesmas presentes no Windows XP, porém, agora você encontrará também uma opção chamada Ativar ou desativar o Controle de contas de usuário (figura 3).

Se você desmarcar a opção, o Windows reagirá apresentando uma nova tela e solicitando a reinicialização para efetivar a configuração (figura 4).

Para maiores informações sobre o UAC, consulte PC&CIA 69 ou o blog do Fernando Cima, em **http://blogs.technet.com/fcima/archive/2007/02/22/uac-e-fronteiras-de-seguranca.aspx**.

Configurando o Windows Defender

Atualmente a Internet faz parte do nosso cotidiano, a navegação cresce a cada dia, assim como os riscos e a possibilidade de ter algum software malicioso e indesejável instalado na máquina. Além de um bom antivírus, é mais do que recomendável utilizar um software anti-spyware para detectar e demover essas ameaças. No ano passado, a Microsoft lançou o Windows Defender, uma ferramenta simples e inicialmente disponível para o Windows XP, via download do site da empresa. Agora o Defender ganhou uma nova versão e já vem como ferramenta nativa no Windows Vista, dispensando a validação realizada pelo Windows Genuine Advantage (WGA), tal como ocorre com o XP.

O Windows Defender é uma ferramenta pró-ativa que pode funcionar de forma programada ou pontual para fazer varreduras em busca de spywares e malwares no sistema (figura 5).

São utilizados agentes de segurança para monitorar ações e áreas normalmente exploradas por softwares spyware, a exemplo de: downloads realizados a partir do Internet Explorer; configurações do sistema e do Internet Explorer; serviços e drivers do Windows; softwares inicializados com o Windows e execução de aplicações. Se alguma atividade realizada por um spyware for identificada, ela será paralisada e um aviso será exibido. A tabela 3 lista as três opções de varredura do Windows Defender.

As informações a respeito dos spywares e suas características ficam armazenadas na base de dados do Windows Defender. Para manter o sistema seguro e confiável, a atualização dessa base de dados deve ser feita freqüentemente, via site Windows Update. Vale citar que não é necessário reinstalar o Defender para fazer a sua atualização. Não faz muito sentido ter o Defender instalado com a base de dados antiga, já que a cada dia temos novas ameaças e vulnerabilidades exploradas (tabela 4).

Em linhas gerais, temos que ter atenção e sempre verificar as identificações realizadas pelo Windows Defender, pois algum software pode ser classificado de forma errada. Cabe ao administrador verificar isso e liberar a utilização do mesmo.

Utilização via Linha de Comando

Podemos gerenciar o Windows Defender via Linha de Comando através do utilitário MpCmdRun.exe, encontrado em C:\Arquivos de programas\Windows Defender caso a instalação padrão tenha sido feita. É uma boa opção para utilização em scripts e automatizações de tarefas. Sintaxe:

```
mpcmdrun.exe [-opções]
```

Opções do comando:

- RemoveDefinitions [-All]: Retorna as definições da base de dados do Windows Defender ao seu estado original;
- RestoreDefaults: Retorna as configurações do Windows Defender no Registro ao seu estado original;
- SignatureUpdate: Verifica se existem novas definições (atualizações) para a base de dados do Defender;
- Scan [-TipodeScan]: Executa o scan, sendo 0 para o scan padrão, 1 para Quick scan e 2 para Full scan;
- GetSWE: Exporta informações sobre os softwares instalados no computador para um arquivo;
- GetFiles: Coleta todos os logs gerados pelo Defender e os armazena em um arquivo compactado;
- Trace [-Grouping] [-Level]: Permite especificar quais componentes e tipos de eventos serão verificados.

Exemplo de utilização do comando:

```
mpcmdrun.exe -scan -2
```

para executar o scan completo (Full Scan) no sistema.

Ferramentas disponíveis

Para visualizar as configurações e ferramentas que o Windows Defender oferece, na barra superior da interface clique em Tools para exibir a tela demonstrada na figura 6.

Em Settings, temos:

- Options: Definição do modo de execução do Defender, tais como horário de scan, arquivos que não devem ser verificados, entre outras coisas. Procure realizar uma varredura completa diariamente para verificar se a máquina está realmente segura;
- Microsoft Spynet: Possibilita a participação em uma comunidade online, onde podemos ver como os outros participantes respondem aos alertas do Windows Defender. O objetivo é facilitar a tomada de decisão de cada usuário. Quando o usuário participa, o Defender envia algumas informações automaticamente à Microsoft. A adesão não é obrigatória.

Em Tools, temos:

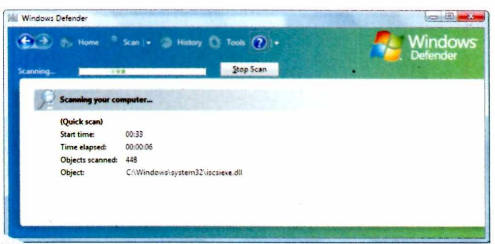
- Quarentined Items: Remoção ou restauração de software identificado pelo Defender como uma possível ameaça. Vale citar que quando o software está na quarentena, na verdade ele se encontra inoperante, aguardando que alguma ação seja tomada;
- Software Explorer: Verifica e monitora todos os softwares em execução no computador. Aqui podemos especificar quais programas poderão ser inicializados junto com o Windows (figura 7).
- Allowed Items: Os programas adicionados a esta lista não serão sequer considerados durante a varredura do Defender e, portanto, terão seu funcionamento liberado.
- Windows Defender Website: Faz a chamada para o site do Windows Defender, onde podemos encontrar maiores informações online e novidades.

Tipo de Scan	Descrição
Quick Scan	É a opção mais simples. Realiza a verificação nas áreas do disco rígido onde a presença de spywares é mais comum
Full Scan	Opção completa. Faz a verificação em todas as áreas do sistema e, como tal, demora mais
Custom Scan	Opção personalizada. Podemos especificar as áreas que serão verificadas pelo Defender

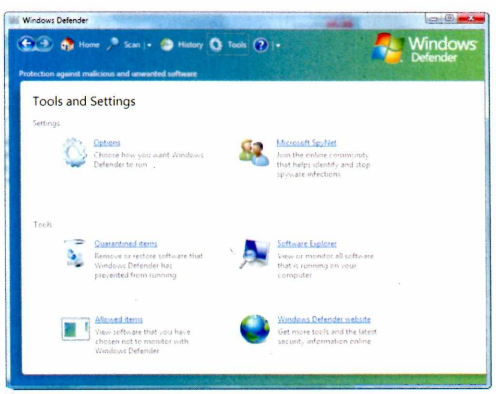
T3. Opção de atuação do Defender.

Opção	Descrição
Ignore	Não é tomada qualquer ação e no próximo scan o software será detectado novamente
Quarantine	O software é colocado em uma área de quarentena, sendo possível a realização de um teste antes da sua remoção do sistema
Remove	O software é removido do sistema
Always Allow	Não é tomada qualquer ação e o programa é adicionado à lista de Itens autorizados (Allowed), não sofrendo verificações nos próximos scans

T4. Qual ação devemos tomar na presença de malwares? Essa é a lista de opções disponíveis para o Defender.



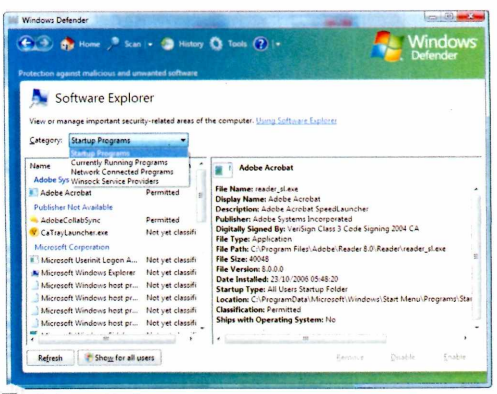
F5. Windows Defender realizando varredura.



F6. Interface principal para configuração do Defender.

Conclusão

Conhecer os recursos de segurança disponíveis no Windows Vista é essencial não apenas para ter sucesso no exame 70-620, mas também para o dia-a-dia do profissional que trabalha com tecnologia e sistemas Microsoft. Abordamos inicialmente o User Account Control e o Windows Defender. Na próxima matéria continuaremos no assunto, abordando mais recursos e ferramentas de segurança. **PC**



F7. Software Explorer.

Servidor de Terminais com segurança



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.

Seja para acessar remotamente um servidor, ou preparar um ambiente que envie sessões de terminais aos usuários para reduzir custos com licenças e manutenção, confira nesta matéria um guia para implementar a solução com segurança, usando a plataforma Microsoft.

Em uma rede de computadores, nem sempre o administrador consegue estar presente no ambiente em que os servidores estão instalados. Quando algum problema acontece é necessário fazer com que outra pessoa, podendo ser um administrador que o auxilie na tarefa de administração ou até mesmo um estagiário, trabalhe como se fosse os seus olhos e suas mãos.

Já deve ser possível imaginar os problemas que podem acontecer se isso for feito, não é? A questão então passa a ser: como ter um ambiente seguro para o administrador acessar os servidores remotamente?

Outro cenário interessante para essa matéria é o do parque que demanda uma versão mais atualizada de um determinado software, mas o hardware das máquinas não atende aos requisitos mínimos para instalação. Já pensou no custo de ter de fazer um upgrade completo das máquinas!? É por isso que os **Servidores de Terminais** estão em "alta" no momento. Seja utilizando as máquinas modestas atuais, ou trocando-as pelos Thin Clients, o fato é que os programas podem ser processados com conforto no servidor, e este envia apenas as janelas com os resultados aos usuários.

Aliás, num cenário ideal, a experiência é tão boa que o usuário sequer sabe que seu trabalho é realizado à distância e enviado através da rede.

Terminal Services

Para atender a estas duas necessidades, a plataforma Windows Server oferece um recurso já bastante conhecido, denominado **Serviços de Terminal (TS – Terminal Services)**. Através dessa tecnologia, o administrador poderia usar qualquer forma de acesso à Internet para abrir uma sessão de terminal no servidor.

No segundo cenário descrito acima, as estações clientes só precisariam executar algum cliente dos serviços de terminais (**Conexão da Área de Trabalho Remota**, no mundo Microsoft, ou o **RDESKTOP** do mundo Linux, por exemplo) para também abrir uma sessão de terminal no servidor. Mesmo a mais antiga estação poderia executar com conforto aqueles programas que, de outra maneira, demandariam um upgrade completo no hardware. Além disso, é possível ter um maior controle do que o usuário pode ou não executar.

No Windows 2000 Server, o TS deveria ser instalado separadamente como um componente do Windows. Durante a instalação, o administrador era apresentado a dois modos de operação: **Administração remota**, o equivalente ao que hoje conhecemos no Windows Server 2003 como **Área de trabalho remota**, ou **Servidor de aplicativos**, que seria conhecido hoje como modo **Terminal Services**.

A partir do Windows Server 2003, o TS já vem instalado por padrão no modo **Área de trabalho remota**, o qual não exige licenciamento especial e fica desativado por padrão. Para iniciar o uso, basta ativá-lo através das **Propriedades do sistema**, na guia **Remoto**. A opção é a **Permitir que usuários se conectem remotamente a este computador**, não sendo necessário marcar a opção que ativa o recurso de **Assistência remota**. Para trabalhar no modo **Terminal services**, o administrador do Windows Server 2003 precisa selecioná-lo através do **Adicionar/Remover componentes do Windows**. Esse modo exige licenciamento especial após um período de 120 dias.

No futuro Windows Server 2008, apesar do TS continuar essencialmente o mesmo, ele virá com diversos novos recursos. São tantos que isso renderá uma matéria exclusiva posteriormente.

Independendo do modo de operação escolhido, a comunicação com o servidor de TS é feita através do protocolo **RDP – Remote Display Protocol** (Protocolo de Exibição Remota), o qual escuta na porta **TCP 3389** (essa é a porta padrão, mas é possível alterá-la via registro). Durante a comunicação, apenas as atualizações de tela são transmitidas e, conseqüentemente, o tráfego na rede é reduzido. Além disso, o RDP oferece um nível de criptografia que visa a evitar que os dados, caso interceptados, sejam interpretados por um usuário mal-intencionado.

Criptografia de dados

Antes da chegada do Service Pack 1 do Windows Server 2003, se o administrador abrisse as propriedades do protocolo RDP, existente dentro de **Conexões** no console **Configurações dos Serviços de terminal** (por padrão, esse console pode ser encontrado dentro de **Ferramentas administrativas**), logo na guia **Geral** seria possível definir o nível de criptografia usado pelo mesmo (tabela 1).

Quem é o servidor?

Tudo o que foi dito até aqui serve para proteger de alguma forma a comunicação com o servidor de terminais, mas não garante a identidade do mesmo. Num ataque do tipo **Man in the middle**, tal como o ARP Poison (http://en.wikipedia.org/wiki/ARP_spoofing), por exemplo, seria possível enganar um usuário, levando-o a acessar um servidor falso. Para solucionar este problema, a partir do SP1 a Microsoft incluiu no Server 2003 o suporte a conexões com o servidor de terminais baseadas no protocolo **Transport Layer Security 1.0 (TLS 1.0)**. Com o TLS é possível ter a criptografia dos dados e simultaneamente garantir a identidade do servidor.

O que é o protocolo TLS?

O TLS é um padrão de protocolo que permite garantir comunicações seguras na Internet ou Intranet. Através dele, tanto os clientes quanto o servidor podem ser autenticar mutuamente.

Para quem nunca ouviu falar, o TLS seria uma versão melhorada de outro protocolo de segurança bastante conhecido, chamado **Secure Socket Layer (SSL)**. Podemos dizer que a principal diferença entre o protocolo TLS e o SSL é que o primeiro trabalha com o que chamamos de **HMAC (Hash for Message Authentication Code)**, enquanto o SSL, agora na **versão 3.0**, trabalha apenas com o MAC (**Message Authentication Code**). Para obter mais informações sobre o TLS/SSL, consulte o link **http://go.microsoft.com/fwlink/?LinkID=19646**, ou a RFC 2246 (**http://go.microsoft.com/fwlink/?LinkID=40979**).

Para atender ao propósito de autenticação, é usado um certificado emitido por uma **autoridade de certificação** (CA). Imagine-se apresentando a sua carteira de habilitação como um documento de identificação nos Estados Unidos. As autoridades de lá não iriam aceitar tal documento, uma vez que o Detran não é reconhecido como uma fonte confiável para elas.

Nesse caso, o passaporte seria o documento a ser usado, uma vez que as autoridades norte-americanas reconhecem a Polícia Federal como uma autoridade confiável para a emissão de tal documento. Da mesma forma funcionam os certificados digitais. Para confiar em um certificado apresentado por alguém, você precisa primeiramente confiar na autoridade de certificação que o emitiu.

Essa **Autoridade de certificação** pode ser de terceiros ou então aquela que é oferecida quando instalamos o **Serviço de certificados** que acompanha o próprio sistema operacional. A única questão é que você deve fazer com que as partes envolvidas (servidor e cliente, por exemplo) confiem na mesma autoridade de certificação para que os certificados emitidos por ela sejam aceitos.

Possuindo uma CA confiável no seu ambiente, basta fazer com que o seu servidor de terminais solicite um certificado com a finalidade de autenticar um servidor. Como o cliente só confiará em certificados emitidos por uma autoridade confiável, não teria como colocar uma CA falsa para emitir um certificado para um servidor de TS também falso a fim de tentar enganar o cliente, porque o mesmo simplesmente não confiaria no certificado apresentado para identificar o servidor.

Configurando o cenário para os testes

Em nosso ambiente de testes, iremos configurar um domínio chamado teste.local, no qual teremos dois servidores com o Windows Server 2003 SP2 (sem o R2), além de uma estação com o Windows XP Professional SP2, que será chamada de XP1. Um dos servidores, que chamaremos de **DC2003.teste.local**, exercerá as funções de **Controlador de domínio, Servidor DNS, Servidor web (IIS 6.0)** e **Autoridade de certificação** (que deverá ser configurada como uma **Autoridade de certificação raiz corporativa**, uma vez que será a nossa primeira CA) para o domínio **Teste.local**. O segundo servidor, que chamaremos de **2003srv.teste.local**, estará com o **Serviço de terminais** instalado.

Depois que o DC2003 estiver preparado, ou seja, com as suas devidas funções de servidor instaladas e configuradas, já poderemos iniciar a preparação do servidor 2003srv. Como estamos trabalhando num ambiente de domínio, não precisaremos nos preocupar com a questão da confiança

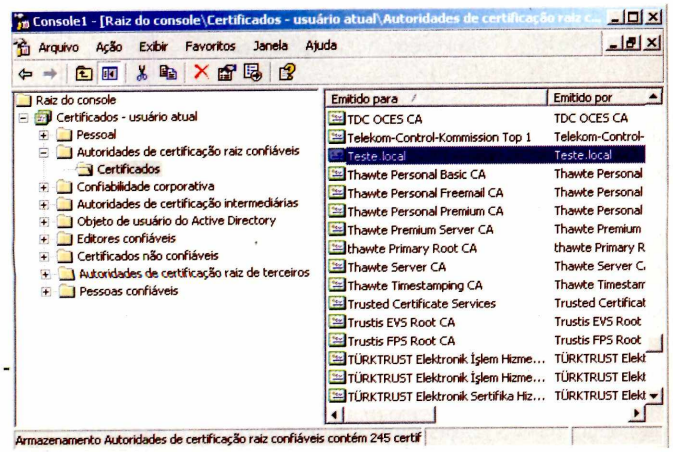
Nível de Criptografia	Descrição
Alto	Todos os dados enviados entre o cliente e o servidor são criptografados com uma chave de 128 bits. Para usar este nível de criptografia, o cliente da área de trabalho remota precisa ter a versão 5.2 ou superior (já está disponível a versão 6.0). Se não houver suporte, o cliente não se conecta.
Compátivel com o cliente	Este nível criptografa os dados usando a chave *máxima* suportada pelo cliente. Esta opção é a ideal quando o servidor de terminal se encontra em um ambiente misto e/ou com clientes antigos.
Baixo	Neste nível, é usada uma criptografia de 56 bits apenas sobre o tráfego direcionado do cliente ao servidor. No sentido contrário, as informações vão "abertas".
Compatível com FIPS (Federal Information Processing Standard)	Este nível encripta e decripta os dados enviados do servidor para o cliente, e vice-versa. São usados algoritmos de encriptação FIPS que trabalham com os módulos de criptografia Microsoft. No link http://go.microsoft.com/fwlink?/LinkID=36329 você encontra mais informações sobre o padrão FIPS.

T1 Configurações de criptografia disponível em versões do Server 2003 anteriores ao SP1.

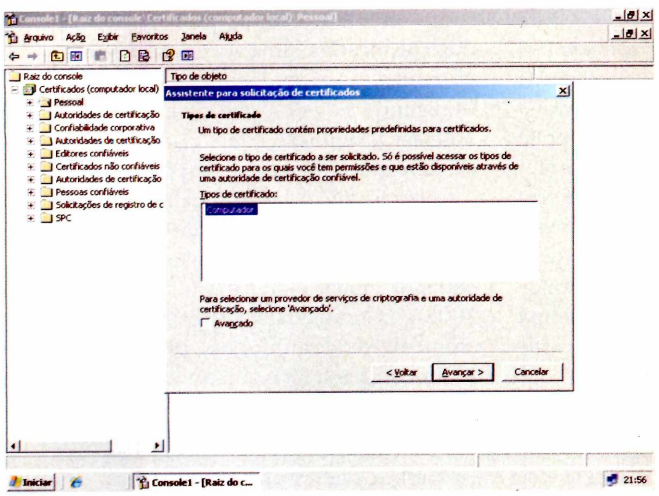
na **CA** instalada, uma vez que o certificado da mesma é distribuído automaticamente por diretiva a todas as máquinas do mesmo domínio. Sendo assim, no **2003srv**, ao abrir o **MMC** com o **Snap-in de certificados de usuário** e expandir **Autoridades de certificação raiz confiáveis\Certificados**, é possível encontrar o certificado da **CA Teste.local** (figura 1). Isso indica que essa CA é confiável nesse sistema. Dessa forma, agora nós precisaremos solicitar um certificado à **CA** do domínio, cuja finalidade seja a de autenticar um servidor, ou seja, garantir sua identidade.

A solicitação do certificado para o servidor pode ser feita de duas formas:

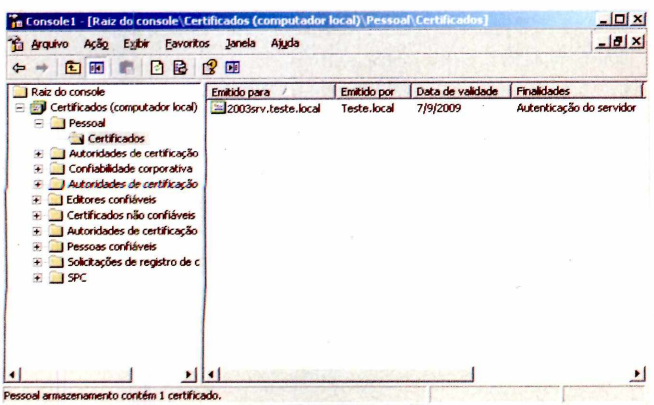
- Através do console de certificados (**MMC\Snap-in de certificados de usuário**);
- Através da **página da web do serviço de certificados**, a qual será preparada automaticamente uma vez que o **IIS** já está instalado no **DC2003**. Essa página poderá ser acessada através do link **HTTP://dc2003.teste.local/certsrv**.



F1. CA´s confiáveis distribuídas por padrão no domínio.



F2. Seleção do tipo de certificado.



F3. Certificado emitido para nosso servidor de terminais.

Vale ressaltar que, independendo do método escolhido, será necessário usar credenciais administrativas para realizar essa tarefa. No caso do **MMC**, você deve estar logado com a conta do administrador do domínio, por exemplo. No caso da solicitação via web, quando solicitado, a conta do administrador do domínio deverá ser fornecida.

Obtendo o certificado para autenticar o servidor

A solicitação via **MMC** é a mais simples. Basta abrir o **MMC**, adicionar o **Snap-in de certificados de usuário**, clicar com o botão direito na pasta **Pessoal**, selecionar **Todas as tarefas\Solicitar novo certificado**. O Assistente para solicitação será exibido, siga as instruções do mesmo. Numa das etapas do processo de solicitação, você verá que o certificado de **Computador** será oferecido como uma das opções disponíveis para a sua condição (figura 2).

Como o certificado de computador possui a finalidade de autenticar um servidor, ele atende ao nosso caso. Ao terminar o processo, o console deve estar parecido com o exibido na figura 3.

Apesar de mais simples, nem sempre a solicitação pode ser feita via **MMC**. Sendo assim, você pode usar o site citado anteriormente para realizar essa tarefa. Ao abrir o link mencionado, clique em **Solicitar um certificado**. Uma nova página será aberta. Clique no link **Solicitação avançada de certificado**. Na nova página, selecione **Servidor da web** na lista de **modelos de certificados**. Não existe uma opção chamada **computador** tal como acontece quando fazemos a solicitação via **MMC**, mas isso não atrapalha, visto que certificados desse tipo (**Servidor da web**) também possuem a finalidade de autenticar um *servidor*.

Ao selecionar o referido modelo de certificado, você verá que a página mudará de aparência. Um formulário será exibido e neste você deverá preencher da seguinte forma: no campo **Nome** da área **Informações de identificação para modelo off-line,** preencha com o **nome do servidor de TS**. Pode ser o FQDN (domínio completo), nome NetBIOS ou IP.

O sistema não irá verificar se você está digitando o nome certo (mas o certificado só funcionará adequadamente se o nome no certificado emitido corresponder ao nome correto do sistema). Portanto, o nome digitado nesse campo deve ser o nome que será usado no cliente da área de trabalho remota. Por exemplo, se a solicitação do certificado foi feita a partir do nome FQDN do servidor, e o usuário tentar usar o nome NetBIOS do servidor de TS ao abrir a Conexão da área de trabalho remota, o sistema apresentará uma mensagem de erro.

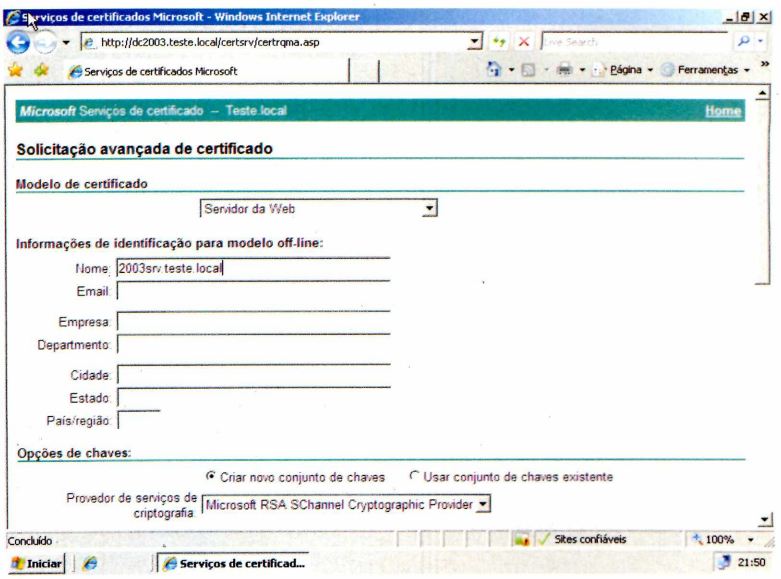
Depois de preencher o nome, na área **Opções de chaves**, certifique-se de que as seguintes opções estejam marcadas:

- **Criar novo conjunto de chaves;**
- Campo **Provedor de Serviços de Criptografia (CSP)**, selecione **Microsoft RSA SChannel Cryptographic Provider**. Este **CSP** oferecerá chaves que trabalham com os protocolos **SSL2, PCT1, SSL3 e TLS1**;
- Em **Uso de chave**, a opção **Exchange** deve estar marcada. Essa opção garante que a chave privada pode ser usada para habilitar a troca de informações;
- Marque a opção **Armazenar certificado no armazenamento de certificados do computador local**. Se essa opção não estiver marcada, o certificado não será atribuído ao computador e, sendo assim,

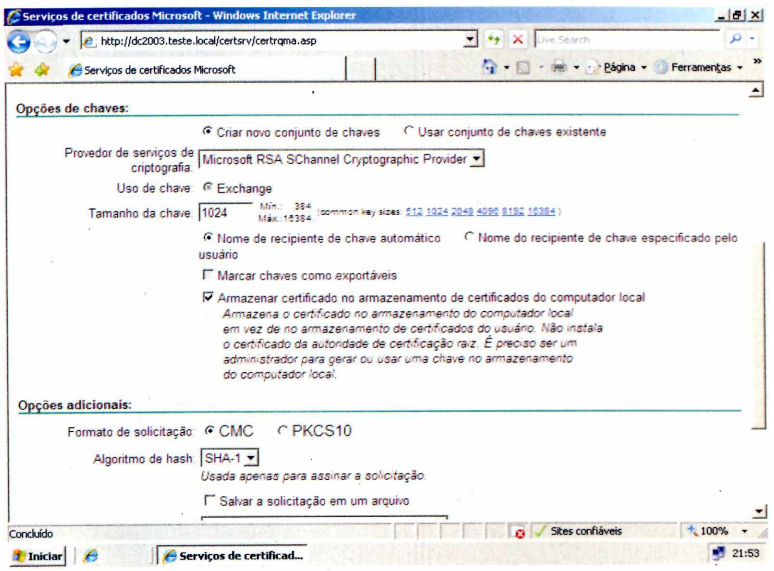
não poderá ser usado para a autenticação com o protocolo TLS;
- Os outros campos podem ficar com as opções padrão.

Agora é só clicar no botão **Enviar**, no final do formulário de solicitação. Siga as instruções que serão exibidas e, quando possível, instale o certificado. Nas figuras 4 e 5 você vê como deve ficar o formulário de solicitação.

Vale ressaltar que dentro do domínio a **CA corporativa**, quando configurada com as opções padrão (o nosso caso), emitirá os certificados automaticamente, mas isso pode ser alterado para acontecer manualmente. Isso aumentará a segurança, uma vez que associa a emissão dos certificados à autorização de uma pessoa, no caso, um administrador.



F4. Formulário para configuração do certificado.



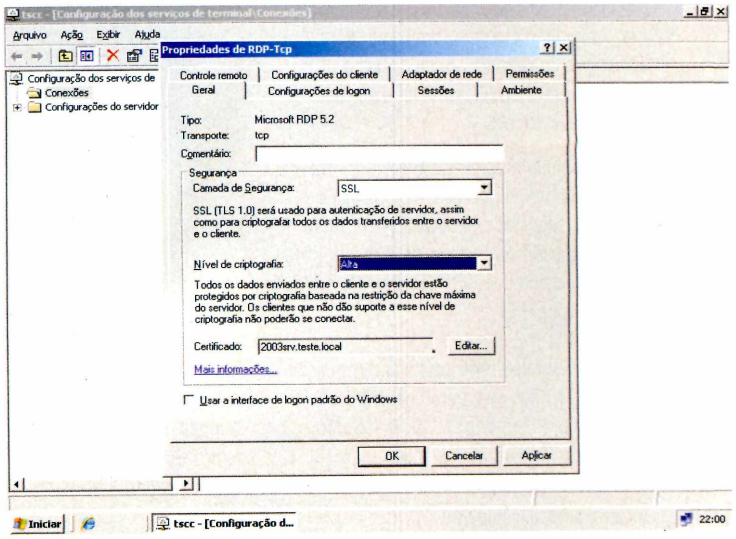
F5. Formulário para configuração do certificado.

Configurando o RDP

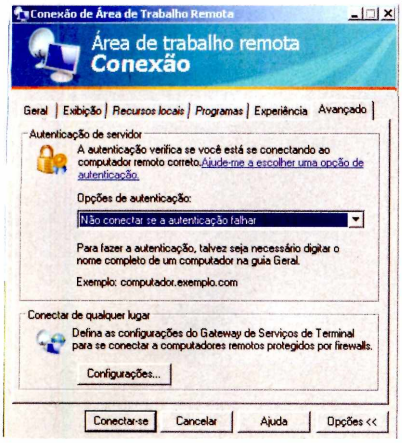
Agora que o servidor já possui um certificado e pode ser usado para garantir sua identidade o nosso próximo passo é configurar o protocolo **RDP** para usar este certificado. Para isso, abra **Configurações dos Serviços de terminal** no menu **Ferramentas administrativas**. No painel da esquerda do console que será aberto, clique na pasta **Conexões**. Na parte direita do console, clique com o botão direito do mouse no protocolo **RDP** e, então, selecione **Propriedades**. A caixa de **Propriedades do protocolo RDP** será aberta direto na guia **Geral**, conforme a figura 6.

No campo **Camada de segurança**, é possível escolher uma dentre três opções, que são: **Camada de segurança RDP, Negociar e SSL** (tabela 2).

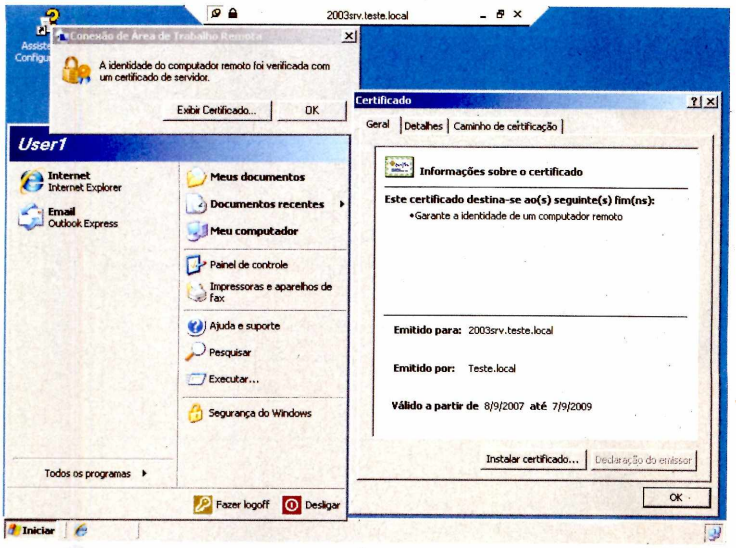
Para o nosso exemplo, iremos selecionar a opção **SSL**. Vale lembrar que, caso um certificado com o propósito de autenticar o servidor não tenha sido selecionado no campo **Certificado**, existente nesta caixa, a opção **SSL** não estará disponível. Apenas as opções para **RDP** e Negociar estarão habilitadas. Sendo assim, clique no botão **Editar** do campo **Certificado** e uma caixa será aberta. Se você fez corretamente a solicitação do certificado, o mesmo será apresentado. Selecione-o e depois clique em **OK**. Assim, a opção **SSL** ficará disponível e será possível fazer a autenticação do servidor. Além disso, toda a comunicação entre o servidor e o cliente (e vice-versa) será criptografada. Feito isso, a configuração do servidor está pronta. Agora só falta configurar o cliente.



F6. Propriedades do RDP.



F7. Em nosso exemplo, escolheremos a configuração mais segura, Não se conectar se a autenticação falhar.



F8. Consultando informações da sessão.

Configuração do cliente

Agora, a nossa tarefa de configuração será na estação XP1. A configuração será feita mais precisamente no cliente de **Conexão da Área de trabalho remota (MSTSC.EXE)**. Abra-o e clique no botão **Opções** e vá até a guia **Avançado**. No campo **Opções de autenticação** desta, você encontrará as seguintes opções (vale ressaltar que as opções citadas a seguir só estarão disponíveis com a versão 6 do cliente, a qual pode ser obtida, até mesmo, via Windows Update):

- **Sempre se conectar, mesmo se a autenticação falhar** (padrão): Essa é a configuração menos segura, entretanto é aquela que poderá ser usada caso o servidor de terminais esteja executando uma versão do Windows Server 2003 anterior à SP1, pois, nesse caso, esses sistemas não sabem se identificar. Dessa forma, ao escolher essa opção, a conexão será estabelecida sem que mensagens de erro sejam exibidas ao cliente;
- **Avisar se a autenticação falhar**: Essa configuração é considerada segura. Se o cliente não conseguir identificar o servidor, ou o nome do mesmo não corresponder ao nome digitado no campo **Computador** da guia **Geral**, um aviso será exibido ao usuário e este poderá escolher se deseja, ou não, estabelecer a conexão;
- **Não conectar se a autenticação falhar**: Essa é a configuração mais segura. Se o cliente não conseguir identificar o servidor, não será possível estabelecer a conexão (figura 7).

Feito isso, na guia **Geral**, digite o nome do servidor de **TS** (tem que ser o nome usado para fazer a solicitação do certificado) ao qual você deseja se conectar e clique no botão Conectar-se. Se tudo foi feito da forma certa, será exibida uma caixa solicitando as credenciais que serão usadas para o logon no servidor de terminais. Após digitar essas informações, basta clicar em **OK** e aguardar o processo de logon. Com a sessão iniciada, você perceberá que na parte superior da tela, mais precisamente naquela barra horizontal amarela, existe, ao lado do ícone de fixação da tela, um ícone de um pequeno cadeado. Ao clicar nele, você verá informações sobre o processo de identificação do servidor (se foi possível determinar a sua identidade, por exemplo) e poderá exibir o seu respectivo certificado (figura 8).

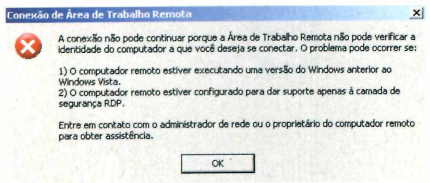
Problemas de conexão

Dentre os problemas que normalmente ocorrem ao se tentar estabelecer uma conexão com o seu servidor de TS, destacamos dois basicamente:

	Camada de Segurança	Encriptação	Níveis	
	Compatível com o cliente	Baixa – RC4 com 56 bits	Alto – RC4 com 128 bits	Compatível com FIP
RDP	Válido. Todavia, o TLS não será usado para a autenticação do servidor. A encriptação RDP será usada, mas limitada ao nível mais alto suportado pelo cliente.	Válido	Válido	Válido
Negociar	Válido. A camada máxima de segurança e o nível máximo de encriptação serão usados. Se o TLS for suportado para autenticação do servidor, o mesmo será usado ao invés do RDP, e será usado o nível de encriptação Alto ou compatível com FIPS.	Válido	Válido	Válido
SSL (TLS 1.0)	Válido. O TLS é necessário para a autenticação do servidor. O nível de encriptação Alto ou compatível com FIPS é usado. Se o TLS não for suportado, a conexão irá falhar.	Não é válido, assim como a opção Compatível com o Cliente. Somente o nível Alto ou Compatível com FIPS é usado, de acordo com a compatibilidade do cliente.	Válido	Válido

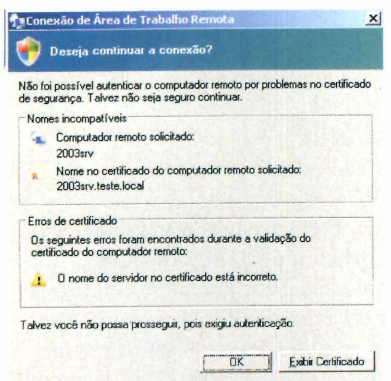
T2. Opções disponíveis para segurança do RDP.

• **Servidor não está configurado de forma adequada:** Nessa situação, suponha que nas propriedades do protocolo RDP não foi configurada a utilização do certificado para garantir a identidade do servidor e que, no cliente, foi configurado que a conexão só poderia ser estabelecida caso o servidor pudesse se identificar. Nesse caso, você verá uma mensagem como a exibida na figura 9. A próxima opção é a razão da nossa falha na conexão. Mas isso também poderia acontecer se não existisse suporte do cliente.



F9. Mensagem de erro durante tentativa de conexão.

• **O nome usado para estabelecer a conexão não corresponde ao nome apresentado no certificado:** Nesse caso, podemos reparar que o nome usado na solicitação de conexão foi o nome NetBIOS do sistema. O problema todo foi exatamente esse, ou seja, porque o certificado usa o nome FQDN do servidor (figura 10).

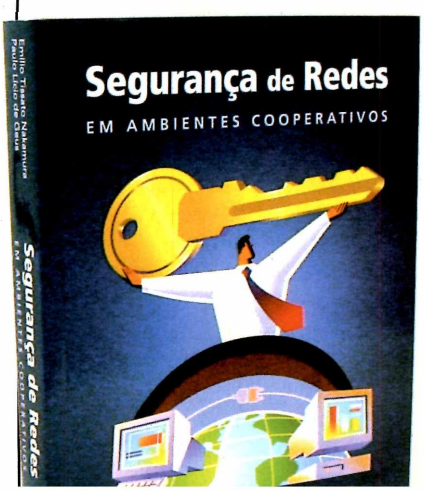


F10. Erro gerado quando nomes não batem.

Conclusão

Agora você já conhece mais uma solução para seu ambiente de Servidor de Terminais, desta vez com enfoque na segurança. Através do uso dos certificados digitais (para muitos considerados complexos, mas de uso simples), suas estações clientes poderão pegar uma sessão de terminal em um servidor Microsoft a partir de virtualmente qualquer local e com segurança. **PC**

Não é novidade que o domínio da língua inglesa é uma característica importante para os profissionais que desejem ingressar nos rumos da computação. Por se tratar de uma área muito dinâmica, que exige uma atualização permanente e capacidade para acompanhar a velocidade com que as evoluções da área ocorrem, não é aceitável aguardar a tradução de livros e artigos para nossa língua-pátria, sob pena de colocar-se sempre aquém das expectativas quanto à dinamicidade requerida aos profissionais dessa área.
Há algum tempo não muito remoto, basear-se somente em livros em português significava tornar-se refém de traduções pouco cuidadosas de material técnico especializado em computação, o que certamente comprometia o ensino e a aprendizagem de quem utilizava esse tipo de referência. Esse cenário parece estar mudando nos últimos tempos.
Apesar de não anular a necessidade de lidar bem com o inglês, ter bons livros na nossa língua pode colaborar em muito para a capacitação de profissionais, principalmente se esses livros são escritos nativamente na língua portuguesa, evitando o processo de tradução, onde raras são as vezes onde não se tem a compreensão comprometida em virtude de erros. Some-se a isso o fato de que bons livros produzidos por autores brasileiros significa ratificar a excelência em áreas antes pouco reconhecidas no Brasil. Esse certamente é o caso do livro **"Segurança de Redes em Ambientes Cooperativos"** (ISBN 978-85-7522-136-5), dos autores *Emílio Nakamura* e *Paulo Lício de Geus*, lançado neste ano pela Editora Novatec.
A área de segurança de redes vem ganhando cada vez mais importância à medida em que o sucesso do negócio de muitas corporações é diretamente proporcional à integridade, disponibilidade e o sigilo das informações presentes em seus ambientes de rede.



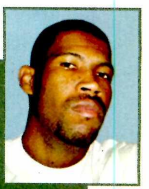
Embora essa seja uma demanda de mercado, o fato é que são poucos os profissionais que possuem capacitação suficiente para planejar, implementar e administrar soluções de segurança com qualidade. O livro de Emílio e Paulo Lício traz um panorama conciso a respeito de conceitos, técnicas e tecnologias envolvendo a área de segurança de redes.
A primeira parte do livro dedica-se a discutir conceitos básicos, a importância do uso das redes de computadores nos ambientes corporativos, a classificação dos tipos de atacantes e seus objetivos, a definição dos ambientes cooperativos e uma interessante discussão a respeito da necessidade de se entender a segurança de redes como parte estratégica e fundamental do negócio de muitas organizações.
Ainda na primeira parte são discutidas técnicas de ataques que se valem da arquitetura TCP/IP e, por fim, um capítulo para discutir os riscos envolvidos com o uso das cada vez mais populares e práticas redes sem fio. A segunda parte do livro dedica-se à discussão em torno de recursos de segurança tais como *firewalls* e seus principais componentes, tais como filtros, *proxies*, *bastion hosts*, DMZ, NAT, dentre outros. São discutidos ainda sistemas de detecção/prevenção de intrusos, criptografia, certificação digital, infra-estrutura de chave pública, VPNs e controle de acesso. A terceira e última parte do livro dedica-se a apresentar os modelos de redes dos ambientes cooperativos. Utilizando uma abordagem que apresenta desde os cenários mais simples até estruturas mais complexas, os autores discutem as vantagens e desvantagens de cada alternativa, buscando utilizar nas topologias parte dos conceitos e técnicas apresentadas nas partes anteriores.
O livro não trata de ferramentas específicas de segurança, muito menos de suas opções de configuração, mas de conceitos e técnicas que podem ser utilizadas com as mais diversas alternativas de software e hardware presentes no mercado. Talvez seja essa uma das grandes diferenças entre os bons e os maus profissionais de segurança. Os bons sabem da necessidade de entender conceitos e modelos para depois aplicá-los por meio do uso de ferramentas.
Enfim, a despeito desse que vos escreve ter sido um dos revisores do livro e, portanto, não estar acima de qualquer suspeita, tenha certeza de que **"Segurança de Redes em Ambientes Cooperativos"** deve ter lugar garantido na prateleira daqueles que querem levar a sério a área de segurança da informação.

resenha por: *Jansen Carlo Sena*

Edição: 1ª
Páginas : 488
Preço: R$ 81,00
Onde encontrar: **www.sabermarketing.com.br**

Servidor de backup para redes Linux e Windows

Aprenda a implementar uma estratégia de backup incremental baseada em servidor Linux, sem sobrecarregar sua rede e eliminando a necessidade de se investir em softwares especializados ou em drives de fita.



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

Um sistema de backup confiável é sem dúvida um dos primeiros serviços a serem idealizados quando implantamos uma nova estrutura de serviços de rede. É indispensável que o administrador possua mecanismos que possibilitem a recuperação de arquivos perdidos em decorrência de algum acidente operacional ou falha de hardware. Imagine o que ocorreria se todos os arquivos (planilhas, programas, relatórios, etc) presentes em seu servidor de arquivos fossem perdidos e não houvesse cópias de segurança a que recorrer.

Existem diversas estratégias de backup, nas quais são levados em consideração fatores como o volume de dados a ser armazenado, o tipo de hardware disponível para o armazenamento, o custo das mídias (Fita DAT, CD, CDRW, etc), como essas mídias serão gerenciadas, o tempo que o backup deve ser mantido, as peças de software envolvidas, entre outros. Um fator que a cada dia se torna mais evidente e relevante é a redução do custo dos HDs e dos *storages*, tornando muitas vezes possível a manutenção de backups em máquinas remotas, com boa capacidade de disco.

A estratégia que abordaremos aqui é especialmente interessante para redes que podem contar com um servidor de backup e armazenamento em HD, mas nada impede que seja adaptada para que backups antigos sejam transferidos para outras mídias como Fitas e CD. Esta estratégia foi idealizada para utilizar um excelente software Unix/Linux com licença GPL, que também conta com versões para Windows, chamado rsync. Através dele é possível sincronizar diretórios entre máquinas remotas, com a vantagem de que só o que foi alterado é copiado através da rede. O rsync já foi abordado pela revista PC&Cia e nessa edição faremos uma atualização do cenário com a introdução de uma nova ferramenta para Windows.

Cenário

Vamos implantar uma estratégia de backup incremental para dois pequenos servidores Web, um baseado em Linux/Apache e outro baseado em Windows/IIS. O objetivo desse backup é armazenar o estado dos sites em cada um dos dias da semana, de forma que, se necessário, possamos recuperar os arquivos tal qual estavam em qualquer um dos dias cobertos.

Nosso cenário será composto por três máquinas: um servidor Web Linux utilizando a distribuição Debian na versão Etch, um servidor Web Windows utilizando Windows 2000, e nosso servidor de backup em HD baseado em Linux e instalado com a distribuição Ubuntu, embora esse último possa utilizar qualquer sistema Unix sem que seja necessária qualquer alteração nas configurações apresentadas a seguir (figura 1).

Rsync no Linux

Todas as máquinas envolvidas na estratégia devem ter o rsync instalado, a diferença entre o servidor de backup e as máquinas que terão os dados resguardados estará na configuração utilizada.

Primeiramente vamos instalar o programa em nosso servidor Web Linux, para isso acesse a máquina utilizando o usuário root e então execute o comando apt-get install rsync (figura 2). Uma vez concluída a instalação, o rsync pode ser utilizado como um comando de sincronização de diretórios locais, ou seja, um tipo de "copy" aprimorado como veremos na seção seguinte. Mas o mais interessante é o fato dele ser capaz de fazer essa sincronização a partir de diretórios remotos, configurados em servidores rsync.

Utilização básica

Começaremos com a mais simples das funcionalidades. Vamos supor que você queira sincronizar dois diretórios em sua máquina local (/etc e /backup). Para isso execute rsync -a -v /etc/ /backup/ (figura 3). A opção -a indica *archive*, isto é, o rsync fará cópia recursiva por todos os subdiretórios e preservará permissões, links e tempos de acesso (MAC times) dos arquivos; já a opção -v indica modo *verbose*, para que o rsync informe todas as suas ações. É possível também utilizar a opção --delete, que indica que todo arquivo que for excluído no diretório de origem, será também excluído no diretório destino.

A maioria de nós está acostumada a lidar com comandos que não levam em consideração a inclusão ou não das barras no final dos nomes dos diretórios, como é o caso do cp. Suponha dois diretórios chamados a e b respectivamente, a execução de cp a b produz o mesmo resultado da execução de cp a/ b/. Entretanto, este não é o caso do rsync, pelo menos no que se refere ao argumento de origem. Vamos supor que no interior do diretório a exista um arquivo chamado carta.txt, quando executamos rsync -a a b o resultado é b/a/carta.txt, e quando executamos rsync -a a/ b, o resultado é b/carta.txt. A presença ou ausência da barra no diretório de destino é indiferente.

Como forma de transporte de arquivos entre máquinas remotas, o rsync pode utilizar sistemas de shell remoto como é o caso do rsh e do ssh, além da sua forma nativa de transporte que abordaremos mais adiante. Não há grande vantagem em se utilizar o rsh como modo de transporte, contudo com a utilização do ssh poderemos contar com toda a criptografia inerente a este sistema de shell, o que permitiria a transferência de informações de forma segura, através de uma rede pública e insegura como a Internet. Um exemplo deste tipo de utilização seria o comando: rsync -z -v -a -e ssh /home/ flavio@172.16.205.1:/opt/backup. No qual a opção -z solicita que os dados sejam compactados durante a transferência. A opção -e ssh indica que o ssh será utilizado para o transporte de informações, /home/ é o diretório de origem local, flavio será o usuário a ser autenticado via ssh na máquina 172.16.205.1 e /opt/backup será o diretório destino remoto a ser sincronizado (figura 4).

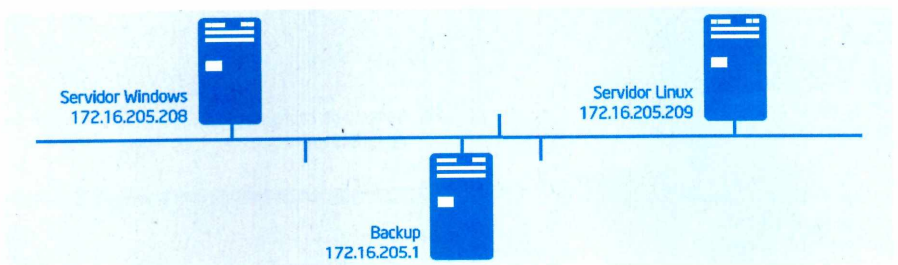
Servidor Rsync

Até agora nossa utilização do rsync foi apenas da porção cliente do programa. Entretanto, ele pode ser utilizado como servidor, executado na forma de *daemon* (em *background*), aceitando conexões remotas e servindo a seus clientes com informações como listagem de arquivos remotos, autenticação de usuários, logs com informações sobre as transferências que realiza, entre outras funcionalidades. Quando a transferência de dados é efetuada via servidor rsync, o método de transporte utilizado é uma conexão TCP comum na porta 873, sem nenhum tipo de criptografia portanto. O servidor rsync é útil na medida em que reduz o tráfego na rede e otimiza a busca por novas versões de arquivos.

Um dos arquivos de configuração que teremos que alterar para colocar o *daemon* em funcionamento é o /etc/rsyncd.conf, nele indicaremos quais diretórios estarão disponíveis para sincronização naquele servidor e em quais condições essa sincronização poderá ser feita. No caso do Debian esse arquivo sequer existe, sendo assim, utilize um editor de arquivos para criá-lo e no caso de nosso cenário o deixaremos conforme apresentado na figura 5.

O arquivo de configuração está organizado em opções globais e opções específicas para cada módulo. Para cada diretório a ser sincronizado, é necessário criar um módulo.

A seguir apresentamos passo-a-passo o que representa cada linha do arquivo de configuração, lembrando que o caractere # indica comentários e tudo que está à frente dele é ignorado pelo rsync.



F1. Cenário para a realização dos testes.

```
flavio@hercules: ~
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
debian:~# apt-get install rsync
Lendo lista de pacotes... Pronto
Construindo árvore de dependências... Pronto
Os NOVOS pacotes a seguir serão instalados:
  rsync
0 pacotes atualizados, 1 pacotes novos instalados, 0 a serem removidos e 15 não atualizados.
É preciso fazer o download de 261kB de arquivos.
Depois de desempacotar, 451kB adicionais de espaço em disco serão usados.
Obtendo:1 http://security.debian.org etch/updates/main rsync 2.6.9-2etch1 [261kB]
Baixados 261kB em 17s (15,3kB/s)
Selecionando pacote previamente não selecionado rsync.
(Lendo banco de dados ... 21471 arquivos e diretórios atualmente instalados.)
Descompactando rsync (de .../rsync_2.6.9-2etch1_i386.deb) ...
Instalando rsync (2.6.9-2etch1) ...
debian:~#
```

F2. Instalação do rsync.

```
flavio@hercules: ~
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
debian:/# rsync -a -v /etc/ /backup/
building file list ... done
./
Muttrc
Net
adduser.conf
adjtime
aliases
analog.cfg
at.deny
bash.bashrc
bash_completion
complete.tcsh
crontab
csh.cshrc
csh.login
csh.logout
debconf.conf
debian_version
deluser.conf
```

F3. Fazendo sincronismo dos arquivos.

```
flavio@hercules: ~
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
debian:/# rsync -z -v -a -e ssh /home/ flavio@172.16.205.1:/opt/backup
The authenticity of host '172.16.205.1 (172.16.205.1)' can't be established.
RSA key fingerprint is 75:c8:d8:7a:5c:55:ec:7c:d1:29:b9:df:88:11:ad:13.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.205.1' (RSA) to the list of known hosts.
flavio@172.16.205.1's password:
building file list ... done
./
flavio/
flavio/.bash_logout
flavio/.bash_profile
flavio/.bashrc
lost+found/

sent 1807 bytes  received 104 bytes  81.32 bytes/sec
total size is 2861  speedup is 1.50
debian:/#
```

F4. Sincronismo entre máquinas remotas.

```
flavio@hercules: ~
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
# Opções Globais
max connections=1
lock file=/var/run/rsyncd.lock
log file=/var/log/rsyncd

# Configurações de Módulos
[PCCIA]
comment=Backup do site de producao PHP...
hosts allow=172.16.205.1
path=/var/www
list=true
read only=true
uid=0
gid=0
~
~
~
~
~
"/etc/rsyncd.conf" 14L, 250C                                  1,1
```

F5. Arquivo /etc/rsyncd.conf no servidor de backup.

Configurações Globais

1. max connections=1 → indica que o servidor atenderá apenas uma conexão por vez;
2. lock file=/var/run/rsyncd.lock → determina o nome do arquivo de *lock*, utilizado para evitar que mais de um *daemon* rsync execute ao mesmo tempo;
3. log file=/var/log/rsyncd → indica o arquivo onde o *daemon* armazenará seus logs;

Configurações de Módulos

1. [PCCIA] → cria um módulo chamado PCCIA;
2. comment=Backup do site de producao PHP... → comentário que será exibido durante consultas ao servidor;
3. path=/var/www → determina o diretório a ser acessado pelo módulo PCCIA, ele também é utilizado pelo servidor para a execução do comando chroot, que altera o local da raiz do sistema durante a transferência por questão de segurança. Mais informações podem ser obtidas via man chroot. Em nosso caso, o diretório utilizado é o /var/www, pois esse é a raiz de nosso servidor Web;
4. read only=true → indica que os clientes não terão permissão de escrita no diretório;
5. list=true → permite a listagem deste módulo;
6. hosts allow=172.16.205.1 → indica que apenas o nosso servidor de backup, cujo endereço IP é 172.16.205.1, poderá receber dados desse módulo;
7. uid=0 e gid=0 → determinam que as leituras serão feitas com privilégios administrativos. O *daemon* rsync é executado com permissões de root, entretanto, quando ele está atendendo uma requisição remota, as leituras são efetuadas com o usuário *nobody* e, dessa forma, podem haver problemas de acesso aos arquivos que se deseja copiar. O ideal é que você crie uma configuração de grupo que lhe permita utilizar um usuário comum para as transferências e não o usuário root. Uma possibilidade para o nosso cenário seria o usuário www-data (uid=33 e gid=33), que é utilizado pelo Apache no Debian.

Uma vez efetuada a configuração do arquivo rsyncd.conf, precisamos agora habilitar a execução do *daemon* durante a inicialização da máquina. Essa configuração é feita através da edição do arquivo /etc/default/rsync, no qual devemos localizar a opção RSYNC_ENABLE e alterar o seu valor para true (figura 6). Feito isso, basta então efetuar a inicialização do serviço através do comando /etc/init.d/rsync start (figura 7).

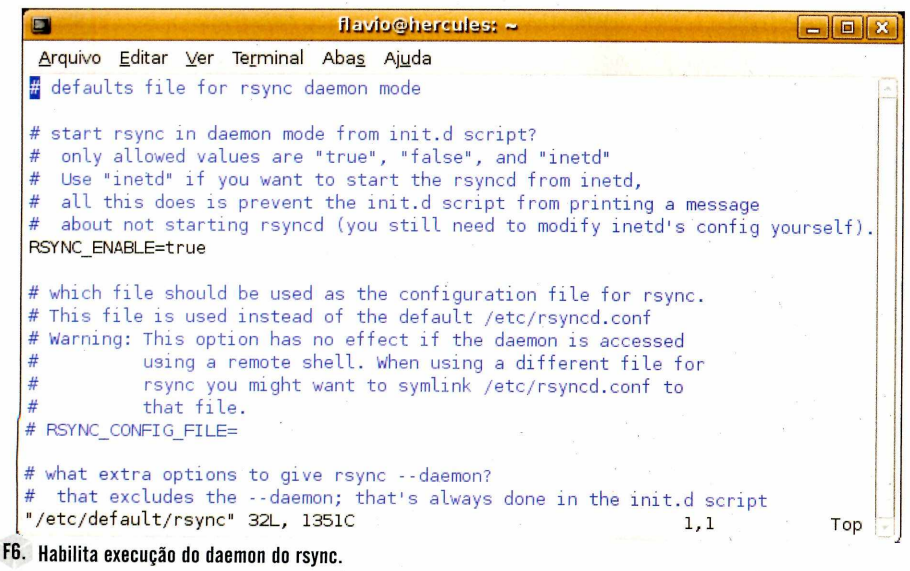
Para testar sua configuração, a partir de seu servidor de backup (no caso de nosso cenário é a máquina 172.16.205.1) execute o comando rsync -v 172.16.205.129:: e, se tudo correr bem, você deverá observar o resultado demonstrado na figura 8.

Rsync no Windows

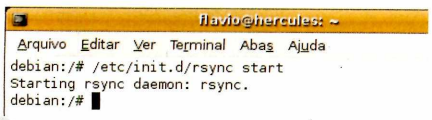
Apesar do Rsync ter sido desenvolvido inicialmente para os sistemas Unix, atualmente existem diversas versões para Windows, graças ao fato de se tratar de um software livre. Uma das versões ou portes (como costumamos chamar versões de software que migram de sistema operacional) mais interessantes é o DeltaCopy (**www.aboutmyip.com/AboutMyXApp/DeltaCopy.jsp**), que traz interfaces de configuração bem intuitivas em seu pacote de instalação, tanto para o servidor quanto para o cliente.

Para seguirmos com a configuração de nosso cenário, basta fazer o download da ferramenta (**www.aboutmyip.com/files/DeltaCopy.zip**), seguida da descompactação e execução do programa de instalação em nosso servidor Web Windows. Note que todas essas tarefas devem ser realizadas utilizando um usuário com privilégios administrativos.

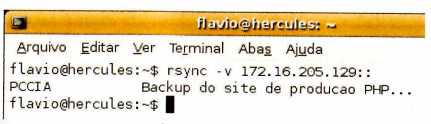
Ao final da instalação, abra o console de configuração do servidor rsync em Iniciar→Programas→DeltaCopy→DeltaCopy Server (figura 9) e então crie um novo módulo para o diretório raiz do servidor Web, assim como foi feito para o servidor Linux.



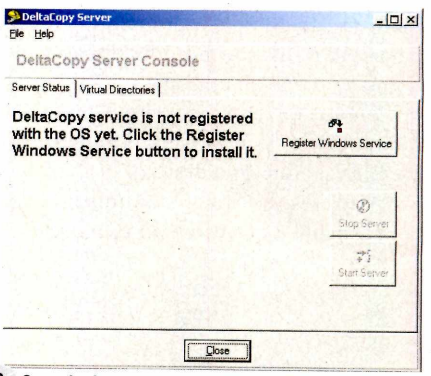
F6. Habilita execução do daemon do rsync.



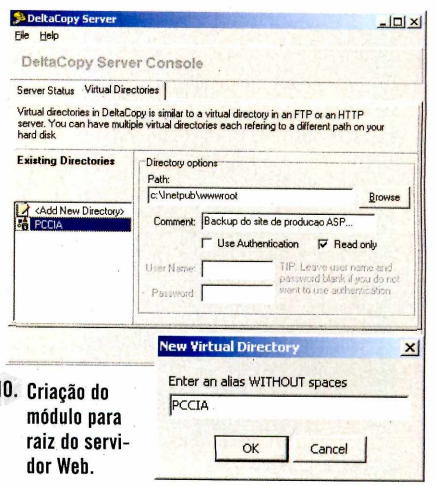
F7. Inicialização do rsync.



F8. Realização do backup: é fácil e prático sincronizar os arquivos.



F9. Console de configuração do DeltaCopy.

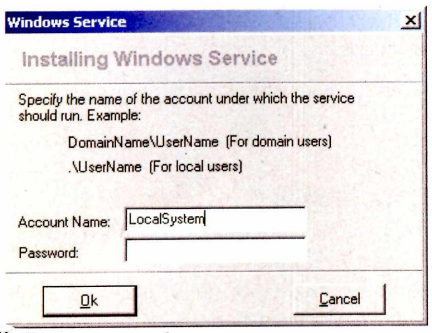


F10. Criação do módulo para raiz do servidor Web.

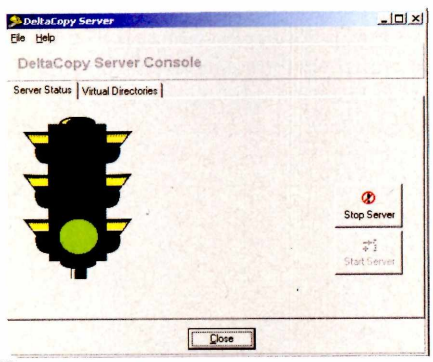
Para isso selecione a aba "Virtual Directories", dê um duplo clique em "Add New Directory", insira o nome do módulo (figura 10) e configure o diretório a ser sincronizado, o que em nosso caso é o C:\Inetpub\wwwroot, raiz de nosso servidor Web. O DeltaCopy traz um módulo chamado Backup configurado por default, para removê-lo basta clicar com o botão direito sobre o nome do módulo e selecionar a opção "Delete Directory".

Uma vez configurado o módulo, precisamos agora registrar o serviço Rsync e iniciá-lo em seguida. Selecione a aba "Server Status" da figura 9 e pressione o botão "Register Windows Service". Feito isso, o DeltaCopy irá solicitar o usuário a ser utilizado pelo serviço (figura 11). Preencha o campo "Account Name" com o usuário LocalSystem, deixe o campo "Password" em branco, pressione o botão "OK", pressione o botão "Start Sever", em seguida o botão "Close" (figura 12) e nosso servidor estará pronto e configurado para receber requisições.

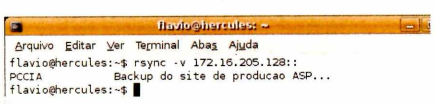
Para testar a configuração, execute o mesmo teste feito para o servidor Linux a partir do servidor de backup (figura 13). Em nosso caso, basta executar o comando rsync -v 172.16.205.128::.



F11. Usuário para serviço rsync



F12. Rsync no Windows pronto para receber solicitações.



F13. Backup manual do servidor Windows.

Um pouco de teoria: Hard Links

Fazendo uma analogia com o Windows, um link seria algo parecido com um atalho, utilizado para facilitar o acesso a arquivos e programas. Nos sistemas Unix existem basicamente dois tipos de link, um chamado de link simbólico e outro chamado de *hard link*, sendo que o link simbólico é aquele produzido pela execução do comando ln -s. Quando criamos um link simbólico temos praticamente um novo arquivo, exceto pelo fato de que na parte de dados existe um ponteiro para o arquivo de origem. Sendo assim, entradas são criadas no diretório ao qual o link pertence e um *inode* (estrutura comum a todos os arquivos Unix que endereça os blocos de dados no disco) é reservado para ele.

No *inode* de um arquivo são armazenados seus tempos de acesso, as suas permissões, ponteiros para os blocos de dados no disco e número de links que o arquivo possui. Note que este número de links não se refere aos links simbólicos, pois estes possuem *inodes* independentes. O número de links armazenado no *inode* de cada arquivo se refere aos *hard links*.

Quando criamos um *hard link*, criamos apenas uma nova entrada no diretório para um arquivo já existente. Sendo assim, o *inode* referenciado continua sendo o do arquivo de origem, que, por sua vez, tem seu número de links incrementado de uma unidade. Vamos a um exemplo: crie um *hard link* chamado teste.lnk para o arquivo /etc/rsyncd.conf em seu diretório /tmp com o seguinte comando ln /etc/rsyncd.conf /tmp/teste.lnk (figura 14).

Em seguida execute o comando ls -i sobre o *hard link* e sobre o arquivo /etc/rsyncd.conf (figura 14), lembrando que a opção -i do comando ls determina que ele exiba o número do *inode* do arquivo exibido. Note que obtivemos o mesmo número para os dois arquivos, indicando que na verdade trata-se do mesmo conjunto de dados em disco referenciado por dois nomes diferentes. Vale ressaltar que esse tipo de link só pode ser criado entre dois arquivos de uma mesma partição de disco.

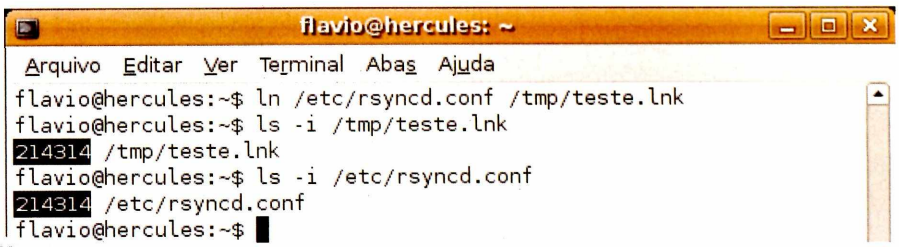
Agora você pode ficar realmente confuso: Quando eu removo o arquivo de origem, o *hard link* fica quebrado, tal como ocorre com o link simbólico? A resposta é não.

Na verdade, quando executamos rm sobre um arquivo, na verdade não estamos removendo seus dados e sim decrementando o número de links armazenados em seu *inode*. Caso esse número de links chegue a zero, mesmo assim os dados não são apagados imediatamente, nesta situação o *inode* é inserido em uma lista de *inodes* livres para reutilização posterior e só quando os seus blocos de dados são sobrescritos é que seus dados são finalmente apagados. O mais importante é que um *hard link* não se quebra, os dados do arquivo não são duplicados quando se cria um link deste tipo e conseqüentemente não há consumo de espaço em disco.

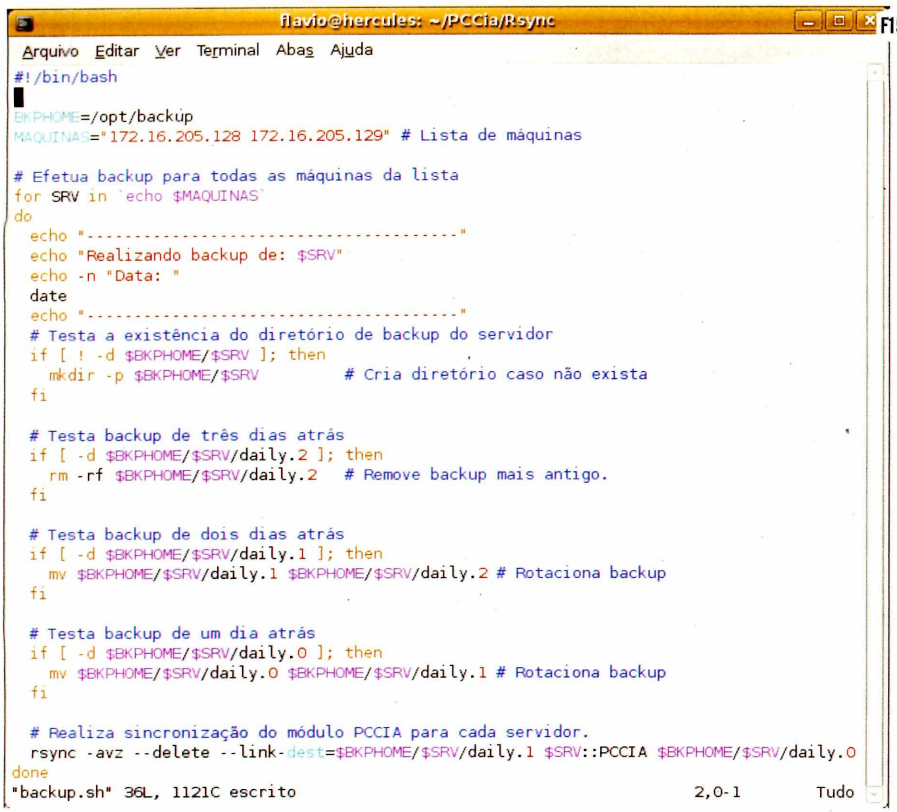
Backup Incremental

Uma estratégia de backup incremental comum é aquela em que há a criação de uma cópia inicial contendo todos os arquivos a serem protegidos e, nas cópias posteriores, são copiados apenas aqueles arquivos que foram alterados em relação às cópias anteriores, até que uma nova cópia completa seja efetuada. Um exemplo seria a realização de uma cópia completa na segunda-feira, o que chamamos de "full backup", e nos outros dias da semana são armazenadas novas cópias apenas dos arquivos que foram alterados ou criados, até que na próxima segunda-feira uma nova cópia completa seja feita. A estratégia que utilizamos é basicamente uma estratégia incremental, salvo algumas diferenças que ressaltaremos a seguir.

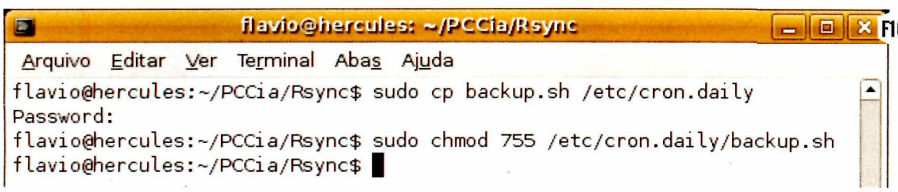
Em nosso servidor de backup será necessário criar um *script* shell para fazer a rotação das cópias, ou seja, este *script* será responsável pela gerência das versões do backup e pela exclusão das cópias mais antigas. Uma rotina simples para a rotação de backup é exibida na figura 15. Esta rotina armazena backup de arquivos copiados a partir dos endereços IP presentes na lista "MAQUINAS", por no máximo três dias. Para ampliá-lo para uma semana é muito simples, basta acrescentar os diretórios daily.3, daily.4 e assim por diante.



F14. Criação de um hard link.



F15. Script para gerenciar backups feitos de várias máquinas (download em nosso site www.revistapcecia.com.br).



F16. Comandos para automatizar a execução dos backups.

Gostaria de chamar a atenção para a última linha do *script*, onde há a execução do comando rsync. Note que ele foi invocado com uma opção (--link-dest=) ainda não mencionada até o momento. A opção --link-dest é extremante útil para a estratégia de backup que estamos apresentando aqui. Através desta nova opção temos a impressão que o diretório recém-criado (daily.0) possui todos os dados de sua versão remota original, quando na verdade ele possui *hard links* para os arquivos que não foram alterados e que foram originalmente copiados em backups anteriores. Quanto aos arquivos novos e também modificados, estes são realmente copiados novamente.

A impressão que temos é que em todos os dias da semana são realizados *full backups*, contudo, quando analisamos o consumo de disco, verificamos que esta estratégia está consumindo bem menos disco do que aparenta, graças ao mecanismo dos *hard links*.

Utilizando o Cron

Para automatizar a execução da rotina em nosso servidor de backup, iremos utilizar o Cron, que é o *daemon* padrão para agendamento de tarefas em todos os sistemas Unix. Para isso, basta copiar o arquivo que contém a rotina para o diretório /etc/cron.daily e fornecer permissões para sua execução, através do comando sudo chmod 755 /etc/cron.daily/<nome-do-arquivo> (figura 16).

Note na figura 16 a utilização do programa sudo para a obtenção de privilégios administrativos temporários, prática empregada maciçamente no Ubuntu e que não é necessária caso você já esteja utilizando o usuário root.

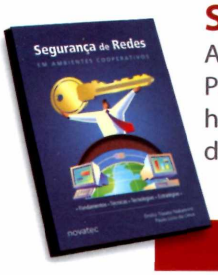
Agendando o arquivo desta forma, a rotina de backup será executada com as configurações *default* do pacote cron que acompanha o Ubuntu, ou seja, todos os dias às 6:25 h. Mais informações sobre o cron podem ser obtidas com os comandos man cron e man crontab.

Conclusões

O rsync é um programa muito simples e versátil. A possibilidade de utilizá-lo tanto no Linux quanto no Windows permite a uniformização da política de backup, o que por sua vez reduz os custos de manutenção do sistema. Além disso, a redução dos preços dos *storages* torna viável e muito interessante a estratégia de backup em HD até para corporações de médio porte. Até a próxima! **PC**

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.

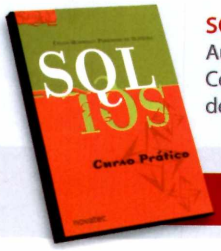
R$ 81,00

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



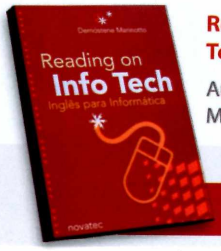
Java Guia do Programador
Autor: Peter Jandl Junior

R$ 119,00



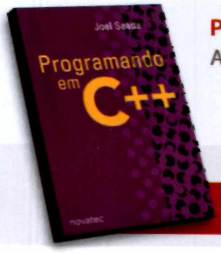
UML - Uma Abordagem Prática
Autor: Gilleanes T. A. Guedes

R$ 69,00



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

R$ 39,00



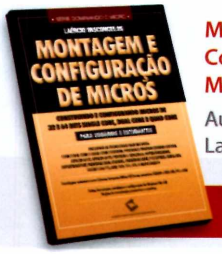
Programando em C++
Autor: Joel Saade

R$ 79,00



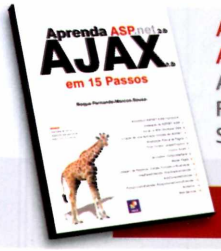
Manutenção de micros na prática
Autor: Laércio Vasconcelos

R$ 99,00



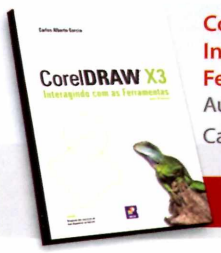
Montagem e Configuração de Micros
Autor:
Laércio Vasconcelos

R$ 39,00



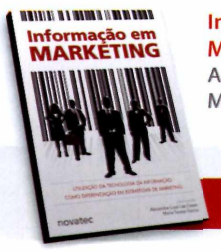
Aprenda ASP.NET AJAX em 15 Passos
Autor: Roque Fernando Marcos Sousa

R$ 53,10



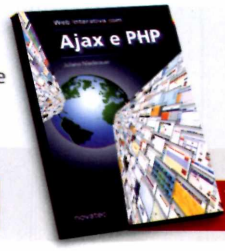
CorelDRAW X3 - Interagindo com as Ferramentas
Autor:
Carlos Alberto Garcia

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.

MSI
MICRO-STAR INTERNATIONAL
innovation with style

Dual Core Cell

Tenha o melhor desempenho - Sempre!

Inovador, Dinâmico, Exclusivo

945GCM5-F



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

K9N6SGM-V



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

Marching to Future Technology

www.msicomputer.com.br