



Edição 03 :: Ano I



**Monitoramento:
Internet e e-mails**

Entre a ficção e a realidade,
até onde podemos ir?

**Qualidade de Serviço e
Controle de Banda**

Conceitos e aplicações
com MasterShaper

A REVOLUÇÃO DO IPv6

CONHEÇA AS MELHORIAS E OS NOVOS RECURSOS

Instalação de Clientes via Push
Produtividade na instalação e
atualização de software

Implementando uma VPN
Como construir um ambiente para
comunicação seguro na Internet

Especial

Gerência de Redes de Computadores
Práticas e desafios de um gerente de redes de computadores

Gerenciando Ambientes Complexos
Utilizando a família de produtos MS
System Center

Os atuais riscos da Engenharia Social
Prepare sua equipe para lidar com a
Engenharia Social

Seu conhecimento vale muito na DevMedia

Publique artigos e vídeos gratuitamente no site e participe do programa **PayContent**.

Sua participação pode ser premiada: quanto mais você postar, mais chances de ganhar.



Para saber mais acesse:
www.devmedia.com.br/paycontent



Sumário

Olá, eu sou o **DevMan**! Desta página em diante, eu estarei lhe ajudando a compreender com ainda mais facilidade o conteúdo desta edição. Será um prazer contar com sua companhia! Confira abaixo o que teremos nesta revista:



Web

06 – Monitoramento: Internet e e-mails

Entre a ficção e a realidade, até onde podemos ir?

[Roberto Henrique]

Infra

10 – Gerência de Redes de Computadores

Práticas e desafios de um gerente de redes de computadores

[Érika Priscila Santana Santos]

Infra, Segurança

14 – IPv6: Nova alvorada para o protocolo Internet

Conheça as características, novos recursos e melhorias do IPv6

[André Koide da Silva]

Infra

24 – Instalação de Clientes via Push

Produtividade na instalação e atualização de software cliente

[Raphael Perez]

Infra

35 – Gerenciando Ambientes Complexos

Utilizando a família de produtos Microsoft System Center

[Marcelo Sincic]

Infra

40 – Qualidade de Serviço e Controle de Banda

Conceitos e aplicações com MasterShaper

[Edelberto Franco Silva e Eduardo Pagani Julio]

Segurança

51 – Os atuais riscos da Engenharia Social

Como preparar sua equipe para lidar com a engenharia social

[Yuri Diogenes]

Infra, Segurança

56 – Implementando uma VPN

Como construir um ambiente para comunicação seguro na Internet

[Mário de Mello Bittencourt Neto]

[Infra] Artigo que apresenta tecnologias relacionadas a questões de Infraestrutura.

[Segurança] Artigo dentro do contexto de Segurança: redes, servidores, sistemas operacionais, infraestrutura em geral.

[Web] Artigos sobre ou que envolvam tecnologias de infraestrutura para WEB.



Ano I • Edição 03 • 2011

Edição

Editor

Eduardo Spínola (eduspinola@gmail.com)

Produção

Jornalista Responsável Kaline Dolabella - JP24185

Atendimento ao leitor

A DevMedia possui uma Central de Atendimento on-line, onde você pode tirar suas dúvidas sobre serviços, enviar críticas e sugestões e falar com um de nossos atendentes. Através da nossa central também é possível alterar dados cadastrais, consultar o status de assinaturas e conferir a data de envio de suas revistas. Acesse www.devmedia.com.br/central, ou se preferir entre em contato conosco através do telefone 21 3382-5038.

Publicidade

publicidade@devmedia.com.br – 21 3382-5038

Anúncios – Anunciando nas publicações e nos sites do Grupo DevMedia, você divulga sua marca ou produto para mais de 100 mil desenvolvedores de todo o Brasil, em mais de 200 cidades. Solicite nossos Media Kits, com detalhes sobre preços e formatos de anúncios.

Fale com o Editor!

É muito importante para a equipe saber o que você está achando da revista: que tipo de artigo você gostaria de ler, que artigo você mais gostou e qual artigo você menos gostou. Fique a vontade para entrar em contato com os editores e dar a sua sugestão! Se você estiver interessado em publicar

um artigo na revista ou no site Easy Java Magazine, entre em contato com o editor, informando o título e mini-resumo do tema que você gostaria de publicar:

Eduardo Spínola - Editor da Revista
eduspinola@gmail.com

Editorial

A evolução das tecnologias nos proporciona acontecimentos impressionantes. A primeira versão do IP, por exemplo, foi um grande marco para as redes de computadores. Imagine como seria toda a estrutura que conhecemos e utilizamos hoje sem este protocolo? Agora, com o crescimento exponencial do número de dispositivos com acesso à rede, a necessidade de qualidade de serviço, maior segurança, entre tantos outros requisitos, mais uma grande revolução está sendo implementada. É sobre este tema que destacamos a matéria de capa da terceira edição da Infra Magazine, o protocolo IPv6.

IPv6: Nova alvorada para o protocolo Internet apresenta as principais características do protocolo IPv6, bem como os novos recursos e melhorias introduzidas em relação à versão anterior. Serão descritos os diferentes tipos de endereços especificados, suas representações, os mecanismos de autoconfiguração implementados, entre muitas outras características.

Monitoramento: Internet e e-mails aborda a temática segurança da informação sob a perspectiva do monitoramento de internet e e-mails. Para isso, serão discutidas dúvidas comumente encontradas nas organizações sobre a necessidade e legalidade em se adotar determinadas práticas de monitoramento.

A matéria **Gerência de Redes de Computadores** destaca uma breve visão sobre boas práticas e desafios de um gerente de redes de computadores em suas atividades diárias, envolvendo equipe, usuários, equipamentos, tipos de software que auxiliam o gerenciamento da rede, políticas de segurança e formas de detectar e resolver problemas nas redes de computadores.

O método push, se configurado de forma correta, é uma poderosa funcionalidade que facilita a vida do administrador SCCM na tarefa de instalação e atualização automática de clientes. Pensando nisso, **Instalação de Clientes via Push** descreve como é o processo de instalação de um software cliente utilizando este método. Aqui, veremos também como habilitar o método, configurar o cliente, fazer troubleshooting e muito mais.

Agora imagine gerenciar ambientes complexos, com dezenas de produtos diferentes, que vão desde o sistema operacional das estações, até gerenciadores de documentos e de impressão customizados, além de aplicações web. É neste cenário que está inserido o artigo **Gerenciando Ambientes Complexos**, utilizando a família de produtos Microsoft System Center.

Qualidade de Serviço e Controle de Banda retrata a utilização de controle de banda e qualidade de serviço a fim de racionalizar a utilização da banda disponível para o acesso à Internet pelos computadores em uma rede local. Serão expostos tanto os principais conceitos necessários ao entendimento deste tipo de solução quanto os mecanismos e técnicas existentes.

Os atuais riscos da Engenharia Social mostra o presente cenário da Internet e suas ameaças em uma visão onde as redes sociais são usadas para obter informações que podem traçar o perfil da vítima que será atacada. O artigo também foca nos cuidados necessários que devem ser tomados para evitar este tipo de situação.

Implementando uma VPN trata de como planejar e criar um espaço seguro de comunicação em um canal público de dados, a Internet. Este tema é importante principalmente em um ambiente no qual você esteja utilizando uma infraestrutura pública e deseja prover privacidade nas informações trafegadas quando se comunica com servidores corporativos de sua empresa.

Para finalizar esta edição, gostaria de convidá-los a acompanhar as notícias da Infra Magazine pelo Twitter (www.twitter.com/Infra_Magazine), e curtir a nossa página no Facebook (www.facebook.com/inframagazine).

Eduardo Oliveira Spínola
eduspinola@gmail.com
twitter.com/Java_Magazine



Dificuldades em encontrar conteúdo sobre .Net para iniciantes?

A DevMedia simplifica pra você!



Easy .Net Magazine:

A primeira revista digital feita especialmente para quem está dando os primeiros passos em .Net!

Você encontrará exemplos e modelos fáceis e práticos, noções introdutórias e conceitos básicos.

Conheça as vantagens:

- Vídeos e apresentações "embutidos" nas páginas;
- Ilustrações, diagramas e modelos apresentados em PowerPoint;
- Entrevistas em vídeo;
- Códigos-fonte que podem ser copiados com CTRL+C/CTRL+V.

A Easy.Net não é feita em PDF ou Flash!
Ela utiliza um aplicativo 100% online.



Acesse agora a edição Nº 1 totalmente grátis e comprove



www.devmedia.com.br/easynet

Easy.Net Magazine,
seu curso inicial de .Net!

Monitoramento: Internet e e-mails

Entre a ficção e a realidade, até onde podemos ir?

ROBERTO HENRIQUE

Estamos vivenciando atualmente a representação mais fiel do clássico romance 1984, do autor George Orwell, onde ele descrevia com uma riqueza de detalhes um mundo governado pelo Grande Irmão (Big Brother), que monitorava a tudo e a todos, como forma de preservar o sistema de governo totalitário. Pasmem, este livro foi lançado em 1948, no cenário pós 2ª Guerra Mundial e conseguiu como poucos ilustrar uma percepção de futuro até então encarada apenas como um cenário de ficção científica. É impressionante como o conceito de monitoramento ganhou espaço no nosso dia a dia, muitas vezes sem darmos conta da real dimensão que isso ocupa em nosso conceito de sociedade.

Em uma recente palestra que apresentamos na sede de nosso parceiro de soluções de segurança, BRconnection, abordamos o seguinte tema: Fraudes – Como Combater e Evitar Prejuízos. Entre as diversas questões levantadas e as soluções apresentadas, uma dúvida que se transformou em debate me chamou a atenção: O que realmente podemos monitorar nos computadores de nossas empresas para reduzir o risco de fraudes?

Pois bem, essa dúvida abre uma série de outras questões que se não forem elucidadas, podem trazer sérios problemas à empresa:

- Preciso ter a ciência dos funcionários, avisando formalmente que estão sendo monitorados?
- Eu posso monitorar webmail particular dos funcionários?
- Quais os problemas em deixar os funcionários acessarem a Internet e os e-mails na empresa livremente?
- Preciso controlar os horários de acessos dos usuários no trabalho?
- Preciso bloquear tudo então?

Como estamos diretamente envolvidos em atividades relacionadas à área de tecnologia e segurança da informação, muitas vezes passamos despercebidos por questões que em nosso meio já estão mais que claramente elucidadas e muito bem aplicadas em diversos clientes. Mas com a realização do evento, focado na participação de profissionais não ligados diretamente à área TI, obtivemos um retorno considerável de dúvidas dos participantes, que apontaram um dos principais fatores para falta de adoção de controles eficientes de segurança: a desinformação. Um dos significados da palavra desinformar é: “Informar mal ou de forma enganadora”. Para o nosso caso, vamos usar apenas o sentido de “Informar mal”.

Hoje praticamente toda empresa possui um firewall instalado, seja ele um produto de mercado ou simplesmente um servidor Linux configurado pelo responsável técnico da rede. Em ambos

Resumo DevMan

De que se trata o artigo:

Este artigo aborda a temática segurança da informação sob a perspectiva do monitoramento de internet e e-mails. Para isso, serão discutidas no artigo dúvidas comumente encontradas nas organizações sobre a necessidade e legalidade em se adotar determinadas práticas de monitoramento.

Em que situação o tema é útil:

As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques. Neste sentido, este artigo contribui para o entendimento da necessidade e legalidade do estabelecimento de políticas de segurança nas organizações.

Monitoramento: Internet e e-mails:

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

os casos encontramos muitos problemas, que vão desde parametrização de configurações até a gestão deste tipo de solução. Referente às configurações, há muito firewall por aí que está praticamente escancarado, tanto de fora para dentro como de dentro para fora. Isso acontece muitas vezes porque em determinadas situações críticas, medidas pontuais e emergenciais são tomadas com o objetivo de atender uma necessidade imediata. Como consequência desse tipo de intervenção, o técnico é “obrigado” a ignorar questões de segurança para resolver rapidamente a situação.

Em outros casos, a própria solução de firewall possui limitações ou características técnicas que impedem um controle mais prático, não garantindo uma proteção abrangente, deixando a empresa refém de uma tecnologia ineficiente. São nestes cenários que o conceito de desinformação ganha força em uma empresa.

O empresário, diretor ou gestor do negócio muitas vezes está exercendo sua atividade em uma zona de conforto, com plena convicção de que seu ambiente de rede está protegido, monitorado rigorosamente, pois como a empresa possui diversos sistemas de

segurança, como firewall para proteger a comunicação de dados, proxy para controlar a navegação na Internet, antispam para filtrar as mensagens do correio eletrônico e antivírus para impedir a infecção de sua rede, tudo está em seu devido lugar, em uma perfeita harmonia.

Puro engano! A tecnologia, por melhor que seja não garante a proteção efetiva do ambiente de rede. Se não houver uma política de acesso bem definida e divulgada de forma clara a todos os colaboradores da empresa, incluindo funcionários, fornecedores e terceiros, não haverá milagre tecnológico que impedirá os acessos indevidos utilizando os recursos da organização.

Para começarmos a nossa caminhada, vamos responder as questões apresentadas no início deste artigo:

1ª Pergunta: O que realmente podemos monitorar nos computadores de nossas empresas para reduzir o risco de fraudes?

Quando um funcionário ou terceiro utiliza algum recurso da empresa para a realização de suas atividades, ele deve ter no mínimo o discernimento para compreender que aquilo não lhe pertence. Mesmo quando o recurso utilizado é de propriedade do funcionário, como por exemplo, o notebook com o qual ele presta o seu serviço, isso não impede que a empresa possa monitorá-lo e auditá-lo conforme sua necessidade, desde que previamente acordado.

Um exemplo muito prático que uso para ilustrar este cenário é substituir o notebook ou o computador por um carro. Quando uma empresa disponibiliza o carro para o técnico de suporte realizar os seus atendimentos externos ele tem total ciência de que será monitorado ou auditado, para checar se a quilometragem está correta, se o veículo está sendo bem conservado ou ainda identificar possíveis registros de multas. Ninguém questiona este tipo de monitoramento, correto? E quando o veículo é de propriedade do funcionário, muda alguma coisa? A empresa vai reembolsá-lo pelo uso do seu veículo no trabalho, porém, ela precisa verificar se a sua quilometragem está de acordo com o deslocamento realizado até o cliente, a empresa precisa verificar se o funcionário está cuidando adequadamente da manutenção e conservação do veículo para evitar possíveis acidentes e também verificar se há registros de multas nos horários em que o veículo estava sendo utilizado para a prestação dos serviços. Alguém questiona este tipo de monitoramento, desde que devidamente acordado? Creio que não! E por que o funcionário acha que com um computador, seja da empresa ou de sua propriedade estaria isento deste tipo de avaliação?

Portanto, toda a informação acessada pelo funcionário utilizando recursos fornecidos pela empresa está passível de monitoramento, exceto ainda e-mails de contas pessoais, conforme veremos adiante.

2ª Pergunta: Preciso ter a ciência dos funcionários, avisando formalmente que estão sendo monitorados?

Sim. O Tribunal Superior do Trabalho e suas regionais estão alinhando suas percepções no entendimento de que a empresa

pode e deve monitorar os meios de comunicação eletrônicos utilizados pelos seus funcionários, com o objetivo de identificar mau uso dos recursos disponibilizados pela empresa. Em casos em que o funcionário cometa crimes como pedofilia, difamação ou discriminação de qualquer natureza utilizando estes recursos no seu ambiente de trabalho, é o IP da empresa que estará sendo exposto. Neste caso, se a empresa não identificar a autoria internamente, ela se torna corresponsável pelos atos de seu empregado.

SUA EMPRESA

Xxxx Xxxxxxxxxxxxxxxxxx, 00 de xxxx de 0000

Ao
Sr(a). Xxxxx Xxxxxxxxxxxxxxxxxx

Ref.: UTILIZAÇÃO DO USO DE INTERNET NA EMPRESA

Prezado Senhor(a),

Comunicamos à V.Sas. que nós nos utilizamos dos benefícios constantes do Livro I, da pessoa, Novo Código Civil Brasileiro – NCC, para monitorar a utilização do uso de nossa rede de dados interna e externa (Internet e Extranet), no que tange à utilização de e-mails, mensagens via MSN Messenger e tráfego na Web, com o intuito de preservar a imagem, nome e honra desta conceituada empresa.

Salientamos que, quaisquer infrações cometidas em virtude da utilização INDEVIDA e IMPRODUTIVA dos meios eletrônicos disponibilizados para uso EXCLUSIVO em benefício desta empresa, serão tratadas por meio judicial, utilizando-se das penalidades protegidas nas normas de tal Livro.

Estando as partes cientes, assinam o presente compromisso em duas vias de igual teor.

SUA EMPRESA

Sr(a). Xxxxx Xxxxxxxxxxxxxxxxxx

SUA EMPRESA 1

Figura 1. Modelo de carta, dando ciência ao usuário sobre o monitoramento

Quando falamos em deixar cientes os funcionários sobre o monitoramento de suas atividades, não significa apenas fazê-los assinarem um termo como o apresentado na Figura 1. Não que isso não seja importante, pelo contrário, é fundamental, porém mais do que o papel assinado, é importante que todos tenham compreensão exata dos motivos que levam a empresa a adotar tais medidas. Assim a empresa reduz o impacto da adoção destas regras e não gera ofensores ao negócio. Isso só é feito através de uma ampla campanha de treinamento e conscientização das Melhores Práticas de Segurança da Informação.

3ª Pergunta: Eu posso monitorar webmail particular dos funcionários?

Para evitar maiores transtornos, recomendo que não. Isso por que há uma grande discussão em volta da questão sobre invasão de privacidade, da empresa para com o funcionário, pois na interpretação de alguns juristas, mesmo que o funcionário esteja utilizando recursos da empresa no horário de trabalho, aquele conteúdo é estritamente pessoal. Por outro lado, é muito importante lembrar que qualquer atitude que infrinja a lei, realizada pelo funcionário utilizando sua conta de e-mail pessoal poderá envolver a empresa diretamente, justamente por esta fornecer os recursos para tal prática. Enquanto não for dada uma clara definição sobre o tema, é importante que cada empresa avalie criteriosamente se deve ou não bloquear este tipo de acesso, ainda mais nos tempos da geração Y assumindo cada vez mais postos no mercado de trabalho. Essa geração conectada nas mais diversas formas de redes sociais pode interferir negativamente no andamento do negócio, se as razões das restrições não forem bem divulgadas para toda a equipe.

4ª Pergunta: Quais os problemas em deixar os funcionários acessarem a Internet e os e-mails na empresa livremente?

As razões para adotar um sistema de controle e monitoramento de acesso à Internet e e-mails são as mais variadas, conforme apresentarei a seguir, porém se fosse resumir em uma única palavra o motivo para convencer o empresário da necessidade dessa gestão, eu diria exatamente está: PREJUÍZO!

- **Problemas jurídicos:** Conforme citado anteriormente, se na ocorrência de uma ação criminoso realizada através de recursos disponibilizados pela empresa o responsável não for identificado internamente, a empresa se torna corresponsável do crime, pois se entende que a empresa possui todas as condições técnicas para monitorar o uso dos seus recursos por parte de seus colaboradores.

- **Degradação do link:** Sem controle de acesso e monitoramento, os usuários têm caminho livre para trafegar o que quiser, quando quiser e como quiser. Já houve situação em que um cliente mantinha um servidor de e-mails com hardware defasado e mal parametrizado, sem limite de envio e recebimento de anexos. Isso permitiu por duas vezes que um fornecedor enviasse anexos acima dos 300MB, derrubando o serviço de e-mail local. Há outras situações em que a degradação do link se dá pela realização de downloads ou transmissões online de áudio e vídeo, além de jogos, normalmente em mais de uma estação na rede.

- **Vazamento de informações:** Cada vez mais nos deparamos com clientes que tiveram informações estratégicas ao seu negócio desviadas por funcionários internos e até terceiros com pleno acesso aos recursos da rede, com um único objetivo: o lucro fácil. Quando falamos em espionagem industrial não devemos mais achar que isso acontece somente dentro de grandes corporações que desenvolvem projetos ultrassecretos. Hoje a espionagem industrial está presente nos mais variados setores da economia, seja em órgãos públicos ou privados, pequenas ou grandes empresas, o que importa para estas pessoas é a possibilidade de ganho fácil.

Algumas empresas que buscam vantagens competitivas pagam altos preços pela obtenção de alguma informação que possa ser revertida em lucro, seja adquirindo o segredo de uma fórmula química, desenhos de projetos, informações críticas de clientes ou planos estratégicos do concorrente, tudo isso vale dinheiro, muito dinheiro. Muitas vezes este espião acaba sendo um funcionário interno, com acesso irrestrito ou mal gerenciado aos sistemas da empresa.

- **Perda de produtividade:** Pesquisas realizadas no Brasil por diferentes órgãos apontam que brasileiros perdem cerca de 6 horas semanais com acessos não relacionados com suas atividades na Internet durante o horário de trabalho. Fazendo uma conta simples, o usuário acaba trabalhando quatro dias por semana. Se uma empresa permite isso, sem um mínimo de controle, é mais vantajoso deixar o funcionário descansar em casa um dia por semana, pelo menos ainda economiza no transporte, alimentação e demais gastos. Ou então a empresa assume o risco de fornecer uma lan house remunerada para seus usuários.

5ª Pergunta: Preciso controlar os horários de acessos dos usuários no trabalho?

Esta questão deve ser avaliada internamente, de acordo com as necessidades do negócio e as regulamentações trabalhistas de cada setor. Já identificamos situações em clientes em que funcionários deixavam computadores ligados e conectados à Internet após o expediente para realizar downloads de filmes e jogos durante toda a noite e madrugada adentro. Outro caso interessante de um de nossos clientes é a de uma funcionária que agendava o envio de e-mails para um horário posterior ao seu batimento de ponto. Ela guardou cópias destes envios após o horário de expediente e exigiu o pagamento de horas extras no momento em que estava sendo desligada da empresa. Estas e outras situações são muito comuns e devem ser levadas em conta na hora de permitir ou não este tipo de acesso fora do horário.

6ª Pergunta: Preciso bloquear tudo então?

Claro que não. Cada empresa deve criar os seus perfis de acesso de acordo com a necessidade do negócio. Entre bloquear tudo e liberar tudo, podemos fazer qualquer coisa. O que deve ser levado em conta além dessa análise crítica dos privilégios de acesso de cada departamento da empresa é a capacidade técnica da ferramenta em permitir tais ajustes, de maneira que não engesse as atividades dos colaboradores e nem do departamento de TI.

Servidores de Internet e e-mails customizados pela equipe interna de TI ou apenas por um técnico com conhecimento em Linux normalmente tendem a ter limitações que acabam dificultando a gestão de acesso (ver **Figura 2**). Como em muitos casos o controle é feito na linha de comando, fica inviável bloquear sites por palavras ou URLs digitadas linha a linha, pois o conteúdo na Internet é muito dinâmico. Ou o servidor acaba bloqueando demais ou liberando o que não devia. Até o monitoramento fica comprometido, pois há certa limitação na geração de relatórios.

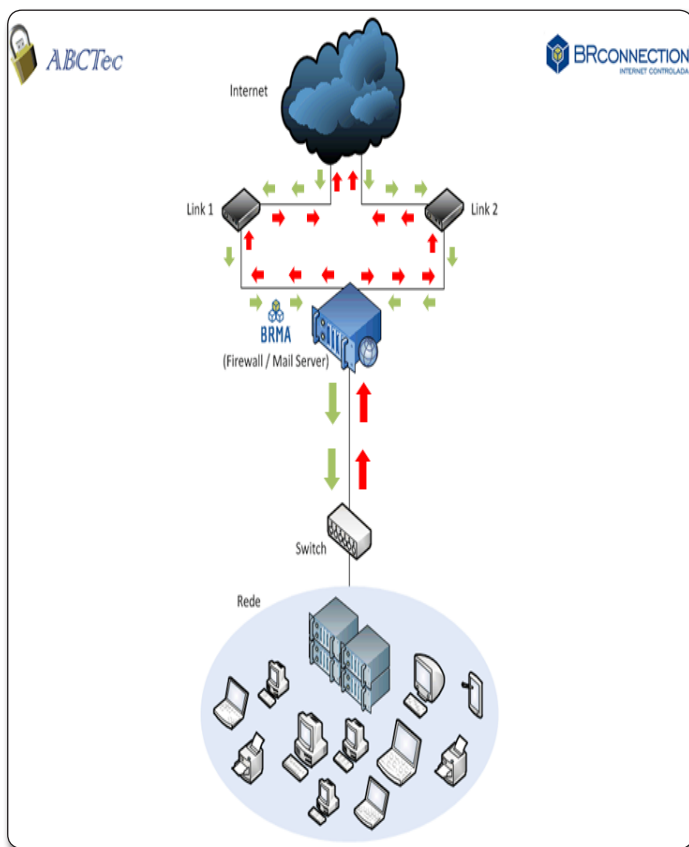


Figura 2. Exemplo de uma rede controlada por um servidor de Internet / e-mails

Possuir um sistema que permita gerenciar o bloqueio de sites por categorias é algo fundamental para garantir uma fácil administração, sem se preocupar em ficar digitando infinitas palavras ou URLs (ver Figura 3).



Figura 3. Tentativa de acesso bloqueado pelo servidor BRMA

Mas o mais difícil mesmo é a definição do que será ou não bloqueado e como serão divididos os níveis de privilégios de acesso. Este é o calcanhar de Aquiles de muitos departamentos de TI, porque diversos deles estão bem capacitados tecnicamente, mas

não possuem expertise em gestão. É comum notar que muitos departamentos de TI são mal vistos internamente pelos demais setores da empresa, pois quase sempre as decisões que deveriam ter o aval de todas as áreas são de certa forma impostas, muitas vezes por pressão da própria Direção.

Quando a definição do que pode ou não pode ser acessado na rede fica a cargo de um único departamento, é notório o conflito interno, pois o departamento de TI sempre tende a tomar decisões de acordo com sua percepção do negócio, sendo que o negócio é composto por um todo, com diferentes pontos de vista. Pior ainda é quando a percepção do negócio se quer parte da equipe de TI, mas de uma única pessoa, normalmente o administrador ou coordenador da área.

Para evitar a pessoalidade nas decisões importantes como a adoção de regras de monitoramento de acesso de uma empresa, devemos compartilhar as decisões com todas as áreas estratégicas da organização, dividindo assim a responsabilidade pelo cumprimento integral das diretrizes estabelecidas. Para direcionar estas medidas, utilizamos normas, leis e regulamentações amplamente difundidas no mercado como forma de validar a sua aplicação e facilitar sua aceitação. Alguns exemplos são:

- Norma ABNT NBR ISO/IEC 27002:2005;
- Regulamentação PCI DSS – Payment Card Industry Data Security Standard;
- Artigo 932, inciso III, do novo Código Civil - A responsabilidade civil do empregador perante o novo Código Civil;
- Lei 9.609 – Proteção de propriedade intelectual de programa de computador e Lei 9.610 – Direitos Autorais;
- HADOPI 2 – Projeto de lei da França contra pirataria virtual;
- Projeto de Lei Azeredo ou PL 84/99 – Lei sobre crimes de informática.

Conclusão

Estes itens citados acima são alguns exemplos que auxiliam na argumentação para adoção de tais controles. Há ainda outras regulamentações de setores específicos que podem auxiliar na elaboração das regras de acesso.

Por fim, é importante ter em mente que o segredo do sucesso deste tipo de serviço é o alinhamento de Tecnologias, Processos e Pessoas.



Roberto Henrique

roberto@abctec.com.br

Roberto Henrique é consultor da ABCtec, com 13 anos de experiência na área de TI (Suporte, Gestão, Consultoria), especializado em análise de vulnerabilidades e no tratamento de incidentes de segurança da informação. Formado em Análise e Desenvolvimento de Sistemas, possui as certificações Microsoft MCP/MCDST, F-Secure Certified Sales Professional - FCSP, D-Link DBC. Membro do Comitê Técnico ABNT/CB21:CE27 sobre Segurança da Informação e membro do Núcleo de TI do CIESP - São Bernardo do Campo.



Gerência de Redes

Práticas e desafios de um gerente de redes de computadores

ÉRIKA PRISCILA SANTANA SANTOS

A gerência de redes de computadores é fundamental para garantir a disponibilidade dos serviços, manter o funcionamento da infraestrutura de comunicação e acompanhar seu crescimento ao longo de toda sua existência.

No projeto de implantação existem muitos pontos a serem analisados e que são fundamentais ao bom desempenho da rede, destacando:

- Os serviços que estarão disponíveis, seus protocolos e as suas configurações;
- O valor das informações que tráfegarão nesse ambiente;
- A proporção dessa rede, necessidades e prioridades;
- A capacidade média de fluxo de dados para saber a capacidade mínima e desejável dos meios físicos e equipamentos que serão usados;
- Avaliar os custos versus os benefícios;
- Definir a topologia e mapeamento dos equipamentos da rede.

Os itens mencionados compõem uma série de informações necessárias ao planejamento de uma rede, e objetivam minimizar erros de projeto e retrabalho.

Quanto a ampliação de uma rede, há outros pontos que são interessantes de serem observados:

- Os serviços e configurações serão os mesmos?
- Os meios físicos e equipamentos existentes suportarão a demanda de fluxo de dados após a ampliação?
- Qual o horário em que essas modificações serão realizadas?
- Como será atualizado o mapeamento da infraestrutura?

Veja que, até o momento, os itens abordados fazem referência ao planejamento de implantação e/ou ampliação, mas ao decorrer do tempo é bastante comum que o ambiente sofra modificações. A exemplo, a contratação de funcionários que motivam a aquisição de computadores, ou a necessidade de se configurar rede sem fio em salas de reuniões para que coordenadores e gerentes se mantenham conectados nesse ambiente.

Os exemplos citados sobre as pequenas modificações são bastante comuns no cotidiano e estão associados a ampliação da rede, ou disponibilização de algum serviço adicional, que por sua simplicidade, são tratados sem a devida importância, culminando em complicações.

Como boa prática o ideal é que toda a documentação referente ao projeto, de implantação ou de ampliação, não seja apenas arquivado e esquecido, mas sim atualizado mesmo quando houver pequenas alterações, pois esse procedimento auxiliará bastante,

Resumo DevMan

De que se trata o artigo:

Uma breve visão sobre boas práticas e desafios de um gerente de redes de computadores em suas atividades diárias, envolvendo equipe, usuários, equipamentos, tipos de software que auxiliam o gerenciamento da rede, políticas de segurança e formas de detectar e resolver problemas nas redes de computadores.

Em que situação o tema é útil:

Indicado para estudantes, professores, profissionais da área de tecnologia da informação, e até mesmo empresários que desejam ampliar seus conhecimentos e que queiram obter mais informações a cerca de gerenciamento de redes de computadores e as principais funções atribuídas a esse cargo, bem como seus maiores desafios.

Gerência de Redes:

Entender as boas práticas e desafios inerentes ao gerenciamento de redes é fundamental para que esta se mantenha funcional e ofereça confiabilidade, interoperabilidade e segurança. Neste contexto, é apresentada uma breve visão sobre os pontos críticos e responsabilidades assumidas por um gerente de rede de computadores em suas atividades diárias.

tanto para um melhor entendimento da infraestrutura, quanto para a identificação de problemas, entre outras situações.

Conhecendo melhor a infraestrutura da rede

O profissional responsável pela gerência necessita inicialmente buscar as informações essenciais sobre o ambiente em questão. Tais informações podem ser obtidas por meio dos documentos de implantação do projeto da infraestrutura, ou por meio de softwares que façam o inventário da rede, caso as documentações estejam desatualizadas.

Existem vários tipos de softwares destinados à realização de inventário que podem auxiliar na ambientação do profissional e em demais atividades cotidianas. Estes softwares identificam dispositivos de rede e mostram suas configurações, sistema operacional, aplicações, memória, espaço em disco, endereço IP, entre outras.

Tendo conhecimento sobre todos os dispositivos conectados e suas configurações, o gerente terá subsídios para a tomada de decisões assertivas por dispor de informações precisas sobre sua rede, geradas a qualquer momento.

Tais softwares ajudam, entre outros pontos, nas seguintes tomadas de decisão:

- Aquisição de novos equipamentos – evitando que existam equipamentos obsoletos na rede;
- Análise da segurança – evitando que dispositivos acessem ou ofereçam serviços indesejados na rede, agindo como espião e colocando a perder todo o investimento feito na infraestrutura;
- Verificação de softwares – evitando a instalação sem autorização de diferentes aplicativos, o que está associado à segurança do ambiente da rede.

Contabilização da rede

Após o conhecimento da rede, se faz necessária sua contabilização, que corresponde ao entendimento das atividades realizadas pelos usuários e suas necessidades de acesso, ambas obtidas através de diálogos com os gestores de cada departamento. É importante ressaltar que as políticas de segurança da empresa devem ser consideradas/atualizadas para o contexto atual e, em casos extremos, novas políticas devem ser criadas.

Após conhecer o funcionamento e serviços disponíveis na rede, é fundamental a análise de seu desempenho, avaliando se existem pontos de falhas, saturação de banda, violação de regras de cabeamento, indisponibilidade de serviços, serviços intermitentes e tentativas de ataque. Tais informações são obtidas facilmente por meio de softwares de gerenciamento, que podem ser gratuitos ou não.

Políticas de segurança

Ao disponibilizar recursos de rede como: hardware, softwares, serviços de telefonia, impressão, entre outros, de certa forma, a empresa possibilita que seus funcionários os utilizem para benefício particular. Neste caso, cabe ao gerente visualizar a rede da mesma forma que seus usuários, a fim de perceber como estes recursos estão sendo mal utilizados.

O gerente precisa ficar atento a todos os recursos e planejar formas de controlá-los, de maneira que sua utilização ocorra dentro das necessidades das atividades relacionadas apenas ao trabalho.

É preciso entender que não é apenas o uso de ferramentas que irá garantir a segurança na rede e o controle dos recursos disponíveis para o usuário dentro da empresa, mas sim, o uso dessas ferramentas aliado à colaboração dos usuários. Tal nível de conscientização é alcançado apenas com o apoio de todos os envolvidos.

É importante que as políticas de segurança da empresa sejam de conhecimento de todos e, principalmente, que seus usuários compreendam sua necessidade e os benefícios que elas agregam ao seu trabalho.

É comum que as redes sejam atacadas por seus próprios usuários, que são motivados pelo descontentamento com sua função, salário, entre outras causas, o que reforça a necessidade de políticas de segurança e controle de acesso.

Redução de custos da área de TIC

A associação de contabilização e políticas de segurança reflète tanto no desempenho e segurança, quanto no custo da área de TIC.

Os usuários, quando conscientizados, tendem a consumir menos recursos e terem mais responsabilidade com os dados manipulados, possibilitando assim maior segurança para a rede, o que inclui minimizar a propagação de vírus e possíveis tentativas de ataque. Consequentemente, a rede possuirá um melhor desempenho, diminuindo problemas e falhas, resultando em menores custos de manutenção.

Há muitas empresas que já perceberam que o investimento realizado em TIC é convertido em benefícios para outros departamentos, sendo estes custos distribuídos para todos os setores da empresa. No entanto, essa prática ainda é pouco comum.

O desafio do gestor está na observação dos benefícios propiciados pelas novas tecnologias, contrapondo-se às possibilidades financeiras da empresa, até mesmo ao adquirir e implantar soluções que contribuam para a diminuição dos custos atuais.

Vale ressaltar a importância de reservar recursos para a capacitação da equipe de TIC, o que será revertido em melhor aproveitamento dos recursos disponíveis.

Arquitetura dos sistemas de gerenciamento

Os itens aqui abordados referem-se às funcionalidades de cada um dos elementos que merecem atenção do gestor da rede:

- Elementos gerenciados – corresponde a todos os computadores, servidores, comutadores, roteadores e impressoras;
- Estações de gerência – pode ser um ou mais computadores distribuídos geograficamente, conforme a proporção da rede, que analisam e fazem o monitoramento do tráfego, hosts e ativos de rede;
- Softwares de gerenciamento – são configurados nas estações de gerência e auxiliam justamente na obtenção das informações sobre o estado dos equipamentos e fluxo de dados;
- Protocolos de gerência – são usados pelos softwares para buscar as informações que serão apresentadas por eles.

Não basta implantar os softwares nas estações de gerência, é necessário acompanhar e interpretar as informações apresentadas por eles e agir quando for identificada alguma falha. Também é importante definir o padrão de consumo dos recursos da rede para que problemas possam ser identificados e alarmados em tempo hábil e assim evitar que seus serviços sejam prejudicados.

Atribuições de um gerente de TIC

As atribuições de um profissional de gerência de redes de computadores são muitas, tais como:

- Avaliar o desempenho da equipe de TIC;
- Dar suporte à equipe para a resolução de problemas;
- Gerenciar os custos;
- Controlar o acesso a rede e a seus recursos;
- Analisar relatórios de desempenho e contabilização da infraestrutura;
- Definir e avaliar políticas de segurança;
- Acompanhar procedimentos;
- Analisar os inventários da rede;
- Estar atento às tecnologias;
- Gerenciar backups, softwares e licenças.

Um outro ponto de atenção está na definição de problemas críticos, o que diz respeito à priorização de atendimento por criticidade, ou seja, se existe um problema do setor de vendas e um problema no setor de compras, é mais interessante resolver primeiro o de vendas.

Diante das várias atribuições apresentadas, é fácil compreender que trata-se de um cargo de grande responsabilidade e desafios, e que se torna cada vez mais essencial, uma vez que todos tendem a se manter conectados independentemente de onde estejam.

A seguir são listados os principais elementos que fazem a gerência de redes possuir um papel tão importante na área de TIC:

1. **Dependência tecnológica** – pode-se dizer que as empresas não funcionam mais sem as redes de computadores, e que falhas na rede podem comprometer a saúde financeira da mesma;
2. **Necessidade de identificar falhas e problemas da rede** – a identificação de falhas na rede deve ser de forma imediata, para que possa garantir a disponibilidade de serviços e recursos sem interferir no desempenho das atividades realizadas pelos usuários;
3. **Complexidade das redes** – quanto maior a empresa mais complexa é a administração de sua rede, demandando mais recursos para fazê-la;
4. **Diversidade das redes** – a diversidade de hardwares, sistemas operacionais, softwares, em geral desenvolvidos em linguagens de programação distintas, vários tipos de comunicação entre hosts e ativos de rede, aumentam sua complexidade;
5. **Qualidade de serviço** – é importante minimizar o retardo de transferência (retardo de acesso associado ao retardo de transmissão) e manter o desempenho da rede aceitável, para que venha a atender as necessidades do usuário;
6. **Planejamento ou reestruturação da rede** – montar a topologia da rede, definir os meios físicos e nós de comutação que serão utilizados, analisar os pré-requisitos da rede e exigências dos serviços que serão disponibilizados para manter os serviços sempre disponíveis.

Identificação de falhas e problemas

Dentre as atribuições relacionadas ao profissional da área de TIC, a identificação de falhas e problemas é uma das atividades mais importantes. A exemplo, quando um host perde sua conexão com a rede local ou com a internet, cujo motivo pode ter origem em vários fatores, desde os mais simples e comuns até os mais complexos e raros.

No momento da falha, porém, é possível que não se tenha ideia de quais procedimentos ou testes deveriam ser realizados para a detecção de sua causa.

Para tanto, é interessante seguir a Metodologia Geral de Detecção, Diagnóstico e Resolução de Problemas, porém, tal metodologia perde sua utilidade quando não se tem conhecimento sobre redes de computadores, arquitetura de redes e certa experiência com a rede que está sendo gerenciada.

Apesar disso, não há garantias de que o problema será solucionado ao adotar esta metodologia, pois ela faz apenas referência a boas práticas de resolução de problemas.

Para auxiliar a prática da metodologia, a **Tabela 1** mostra os principais problemas associados a cada camada do modelo OSI (Interconexão de Sistemas Abertos):

- Camada física – onde trabalham os adaptadores de rede, cabeamento, repetidores e hubs;
- Camada de enlace – que corresponde aos switches e bridges;
- Camada de rede – onde atuam os roteadores;
- Camada de aplicação – que representa os softwares.

Camada	Problemas relacionados
Física	Placa de rede defeituosa Tipo errado de cabo Cabo rompido ou danificado Interferência do cabo
Enlace	Interface desabilitada Validade do cache ARP inadequada
Rede	Máscara de rede incorreta DNS e DHCP mal configurados VLANs não configuradas Equipamento inserido em VLAN incorreta
Aplicação	Serviço de nomes desabilitado Filtro IP barrando tráfego DNS

Tabela 1. Principais problemas relacionados ao RM-OSI

A metodologia geral de Detecção, Diagnóstico e Resolução de Problemas defende o método de resolução de problemas com base na arquitetura de redes de computadores. Assim, a busca inicia pelos possíveis problemas relacionados à camada física (primeira camada) do RM-OSI.

O referido procedimento se deve à importância dos elementos relacionados à camada física e ao impacto que a rede sofre quando essa camada não está funcionando como deveria.

Segue-se de fato uma lógica bem definida, já que as demais camadas dependem da camada física para que possam permanecer funcionais e operantes.

Para identificar falhas na rede, a metodologia geral de DDRP segue um roteiro prático que é apresentado a seguir:

1. Detecção do problema – o problema é detectado pela abertura do chamado por parte do usuário, pela análise contínua da rede, pelos alertas gerados nas estações de gerência e/ou por decorrência de outros problemas, geralmente envolvendo perda de conexão ou lentidão;
2. Buscar informações – saber o que ocasionou o problema, se todos os usuários estão sofrendo do mesmo, se é intermitente, se afeta apenas os usuários pertencentes a uma VLAN ou departamento específico, se é um problema corriqueiro da rede, ou se gera alguma mensagem de erro;
3. Desenvolver hipóteses – significa criar uma lista de situações que podem gerar o problema com base em informações obtidas. Caso essas informações não sejam suficientes para criar uma lista de hipóteses, será necessário o levantamento das hipóteses genéricas, levando em consideração as possíveis modificações realizadas recentemente. Para facilitar a identificação do problema, ordene a lista de hipóteses com base na arquitetura de rede, iniciando da camada mais baixa (física), para a camada mais alta (aplicação) e posteriormente inicie a fase de testes das hipóteses;
4. Solucionar o problema – ao finalizar os testes das hipóteses, será

muito provável que se saiba o que está ocasionando o problema na rede, mas caso o problema não seja identificado, deve-se voltar à primeira fase e tentar obter mais informações. Tão logo o problema seja identificado, este deve ser resolvido. Muitas vezes é inevitável uma solução paliativa, que deve ser substituída pela solução definitiva o quanto antes. Nesta etapa não se deve esquecer de fazer os testes necessários para ter certeza de que a solução não é momentânea;

5. Documentar – deve-se documentar todo o esforço despendido para a resolução do problema, relatando desde hipóteses até os testes, mesmo que a solução do problema não tenha sido encontrada, identificando sua causa. Estas informações poderão ser utilizadas em procedimentos futuros. A documentação de todas as informações coletadas, hipóteses e solução encontrada para o problema, serão facilitadores para a resolução de futuras dificuldades para toda a equipe. Sabe-se que diante de um problema, dificilmente se terá tempo disponível para se limitar a essas especificações sugeridas pela metodologia geral de DDRP, porém, após documentar as primeiras informações, hipóteses e soluções adotadas, as demais documentações irão se basear nessa primeira e assim sucessivamente.

Uma boa prática é anotar palavras ou frases pequenas que retratam cada uma das fases da metodologia geral de DDRP, com o intuito de não atrasar o processo de resolução do problema, o que pode ser feito após a resolução de cada problema.

A metodologia apresentada não é obrigatória, entretanto muitas equipes a seguem, por vezes mesmo sem saber de sua existência, em razão de sua sequência lógica para a resolução de problemas.

Para otimização do tempo, pode-se aproveitar o momento da resolução de um problema para realizar a manutenção preventiva do equipamento em questão. Vale lembrar que esse procedimento deve ser agendado com os usuários que dependem do serviço, sendo muitas vezes realizado em um horário de pouca ou nenhuma utilização dos recursos que ficarão indisponíveis, para não interferir no desempenho das atividades dos usuários.

Principais desafios de um gerente de redes de computadores

Além dos elementos já abordados, existem pontos adicionais que estão ligados às pessoas que fazem uso da rede, quer sejam usuários quer sejam administradores, e como suas atitudes podem afetar direta e indiretamente o desempenho e manutenção da mesma.

A seguir são listados alguns dos vários desafios vivenciados pelos gestores de redes de computadores para que estes fatores tenham o menor impacto negativo possível:

- **Falta de conscientização dos usuários** – como visto anteriormente, as políticas de segurança e utilização da rede são fundamentais para conscientizar os usuários e iniciar o processo de mudança de visão de um usuário comum para a visão de um usuário consciente. Tais políticas podem ser apresentadas ao usuário no momento da contratação, solicitando sua assinatura de aceitação quanto às políticas

estabelecidas e as consequências de não segui-las. Se necessário, a equipe de TIC pode planejar palestras de conscientização. Sendo assim, uma vez que o usuário assine o termo de responsabilidade, poderá sofrer as consequências do seu descumprimento, acarretando desde uma advertência à demissão por justa causa. Entretanto, esse procedimento nem sempre é realizado, fazendo com que as políticas de segurança sejam apenas documentos informativos sem nenhum valor;

- **Falta de investimento** – acontece por falta de subsídios que justifiquem os prejuízos que acarretam. Deve-se registrar, assinar e arquivar documentos, e-mails enviados e suas respostas para que o gestor da rede possa se eximir de acusações de negligência quanto às necessidades de melhorias na rede que administra, bem como sanções administrativas da empresa;

- **Equipe desmotivada** – se apenas o gerente trabalhar em prol do bom funcionamento da rede, verá seus esforços caindo por terra. É importante que toda a equipe esteja motivada, capacitada e disposta ao trabalho, o que envolve outros fatores, como: reconhecimento da empresa, salário, possibilidade de crescimento, porte da empresa, atitudes profissionais, relacionamento com a equipe, entre outros. O gerente, enfim, precisa administrar fatores externos às suas atribuições, impedindo-os que interfiram negativamente nas atividades desempenhadas por todos, mantendo um ponto de equilíbrio.

Conclusão

Como visto, as responsabilidades de um gerente de redes de computadores não são poucas, mas os pontos observados neste artigo o auxiliarão em seus desafios.

Nesta área, é importante que o trabalho seja realizado de forma transparente e muito bem documentado, evitando problemas em atividades de manutenção/atualização futuras e também fornecendo subsídios à continuidade das atividades de gerência por parte de outros profissionais.



Érika Priscila Santana Santos

priscila.erika@gmail.com

Bacharel em Sistemas de Informação, experiência com suporte a help-desk, políticas de segurança, criação de procedimentos, documentação e controle de custos da área de TIC. Professora do curso Técnico em Redes de Computadores na ETEMERB.



Artigo “Gerência de Redes de Computadores – A Necessidade de Gerenciamento”

http://www.malima.com.br/article_read.asp?id=279

Artigo “Gestão de Redes de Computadores”

<http://www.juliobattisti.com.br/tutoriais/alexasantos/gestaoredescomputadores001.asp>

Artigo “Gerenciamento de Redes”

<http://www.gta.ufrj.br/~alexsz/ger/snmppcmip.html>



IPv6: Nova alvorada para o protocolo Internet

Conheça características, novos recursos e melhorias

ANDRÉ KOIDE DA SILVA

O IPv6 (Internet Protocol version 6) representa a nova geração do protocolo Internet. Impulsionado pelas constantes demandas das indústrias de comunicação de dados e tecnologia da informação, o IPv6 procura tratar algumas das lacunas de seu antecessor, o protocolo IPv4 (Internet Protocol version 4), entre elas: maior número de endereços lógicos, expansão da tabela de roteamento, melhor suporte à qualidade de serviço (QoS – Quality of Service), mais segurança e autoconfiguração.

Para a compreensão destas deficiências e das novas características incorporadas, é importante analisar historicamente a evolução do protocolo Internet e suas limitações de crescimento, bem como descrever seu funcionamento básico, detalhes do cabeçalho, representação e tipos de endereços. Este artigo detalhará também os mecanismos de autoconfiguração stateless e stateful (responsáveis pela alocação dinâmica de endereços aos dispositivos conectados à rede), as principais técnicas concebidas para a transição, a coexistência entre a nova versão do protocolo IP e a sua antecessora, os novos recursos de segurança e a mobilidade para os usuários.

Origem da Internet e do protocolo IPv4

As redes nasceram a partir da necessidade da troca de dados entre as pessoas e os computadores, possibilitando o acesso a documentos, imagens, planilhas, arquivos de áudio e vídeo, entre outros, armazenados fisicamente em locais diferentes daqueles onde as pessoas se encontravam. As redes de computadores também permitiram a integração entre os sistemas, pois as informações podiam ser facilmente localizadas, coletadas, armazenadas e processadas.

A Internet originou-se de um projeto patrocinado pelo governo estadunidense (EUA) no final dos anos 1960, época da Guerra Fria, por intermédio da Agência de Projetos de Pesquisa Avançada de Defesa (DARPA – Defense Advanced Research Projects Agency), que visava o estabelecimento da comunicação entre os computadores dos centros militares e os de pesquisa. Seu objetivo principal era formar uma rede robusta que pudesse, mesmo com a indisponibilidade de alguns de seus dispositivos (também chamados nós), manter operacional a troca de dados entre os componentes restantes.

Os primeiros nós desta rede, a qual recebeu o nome ARPANET, foram instalados em 1969 em SRI (Stanford Research Institute), UCLA (University of California at Los Angeles), UCSB (University

Resumo DevMan

De que se trata o artigo:

Neste artigo serão apresentadas as principais características do protocolo IPv6, bem como os novos recursos e melhorias introduzidas em relação à versão anterior. Serão descritos os diferentes tipos de endereços especificados, suas representações e os mecanismos de autoconfiguração implementados. Também será contextualizado um panorama atual da adoção do IPv6, além dos principais fatores que tornam morosa sua aceitação. Por fim, serão expostas as técnicas de transição, a coexistência entre a nova versão do protocolo e o seu antecessor, as ferramentas de segurança e os aspectos de mobilidade.

Para que serve:

A Internet continua a expandir-se vertiginosamente. O protocolo IPv4 se apresenta como grande limitador deste crescimento, pois não será possível alocar um endereço válido para todos os dispositivos que necessitam se conectar à rede. A única alternativa para evitar este colapso é a implantação maciça do protocolo IPv6. Desta forma, este artigo tem por objetivo descrever as principais características do novo protocolo, conscientizar os leitores sobre a importância do tema e fornecer a fundamentação teórica para o debate e o planejamento de sua adoção pelas organizações e usuários.

Em que situação o tema é útil:

Os pontos destacados neste artigo serão úteis para a compreensão do panorama atual da implementação do IPv6, bem como de suas principais diferenças quando comparado ao IPv4. Os conceitos expostos também permitirão a contenda e o aprofundamento técnico do tema pelos profissionais e usuários da área de infraestrutura de tecnologia da informação.

of California at Santa Barbara) e UTAH (University of Utah). A ARPANET cresceu rapidamente com a associação de organizações militares, acadêmicas e de pesquisas. O conjunto de protocolos TCP/IP (Transmission Control Protocol/Internet Protocol) foi consolidado em 1978 e, em 1983, passou a ser requerido para conexão à rede da DARPA, permitindo seu crescimento ordenado e resolvendo as restrições dos protocolos anteriores.

A especificação do IPv4 foi publicada em setembro de 1981 e sua popularização se deu quando passou a ser distribuído pelo Berkeley Software Distribution UNIX (BSD Unix), versão 4.2c, em 1983. O célere crescimento da Internet acentuou-se ainda mais com sua utilização comercial, a partir de 1993, com a criação do protocolo

HTTP (HyperText Transfer Protocol), que iniciou a era WWW (World Wide Web). O Hobbes' Internet Timeline, de Robert H. Zakon, apresentado na **Figura 1**, ilustra o crescimento do número de hosts (clientes e servidores) conectados à Internet desde dezembro/1969 até maio/2010.

O protocolo IPv4 mostrou-se fácil de ser implantado, interoperável e robusto, sendo ainda hoje extensivamente utilizado. Porém, com o crescimento dos dispositivos conectados à Internet, foi possível observar que o número de endereços IPv4 (aqueles que identificam unicamente cada cliente ou servidor ligado à rede) seria insuficiente, pois, como são formados por 32 bits (4 bytes), tornam possível somente um total de 232 endereços (pouco mais de 4 bilhões).

Os bytes do endereço IPv4, para facilitar sua representação, comumente são escritos na forma decimal (0 a 255) e separados por pontos, ao invés da notação binária, conforme ilustrado na **Figura 2**.

O conjunto total de endereços IPv4 (232 combinações) foi dividido em cinco diferentes faixas, para atender às necessidades das redes de computadores com diferentes tamanhos, conforme descrito na **Tabela 1**. Assim, um endereço de classe A, pode ser usado por organizações com grande número de hosts em sua rede, embora atenda somente 126 distintas; já os endereços de classe B podem ser empregados em até 16.384 redes, com até 65.534 hosts. A classe C satisfaz 2.097.152 empresas com poucos hosts (até 254) e por fim, as classes D e E foram reservadas para aplicações específicas, como transmissões multicast e pesquisas, respectivamente.

É preciso destacar ainda que algumas faixas de endereços foram reservadas, ou seja, não podem ser utilizadas para comunicação na Internet (**Tabela 2**). As faixas reservadas para uso interno nas organizações (redes privadas) são detalhadas na RFC 1918 – veja a **Nota DevMan 1**.

Com o passar do tempo, a criação das faixas de endereços IPv4 mostrou-se ineficiente: a classe A atendia a um número pequeno de redes e consumia 50% de todos os endereços disponíveis. Inicialmente, faixas desta classe foram atribuídas às

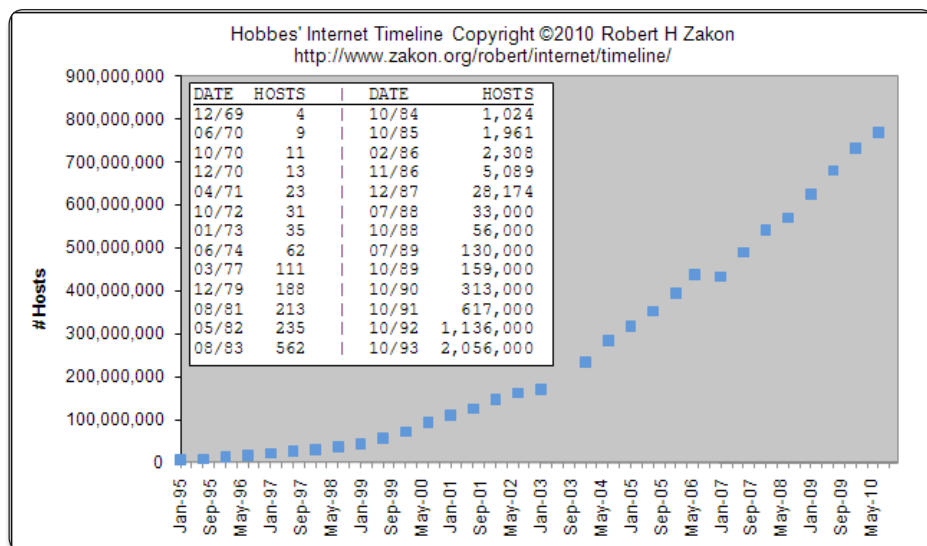


Figura 1. Número de hosts conectados à Internet desde dezembro/1969 até maio/2010

11001000.11001000.00000001.10010111 (notação binária)
200.200.1.151 (notação decimal)

Figura 2. Representação do endereço IPv4

Faixa	End. início	End. término	Redes	Hosts
Classe A	1.0.0.0	126.255.255.255	126	16.777.214
Classe B	128.0.0.0	191.255.255.255	16.384	65.534
Classe C	192.0.0.0	223.255.255.255	2.097.152	254
Classe D	224.0.0.0	239.255.255.255	Reservado para multicast	
Classe E	240.0.0.0	255.255.255.255	Uso experimental	

Tabela 1. Faixas de endereçamento IPv4

Faixa	End. início	End. término	Reserva
Classe A	0.0.0.0	0.255.255.255	Não utilizável (rede local)
Classe A	10.0.0.0	10.255.255.255	Uso em redes privadas
Classe A	127.0.0.0	127.255.255.255	Testes (loopback)
Classe B	172.16.0.0	172.31.255.255	Uso em redes privadas
Classe C	192.168.0.0	192.168.255.255	Uso em redes privadas

Tabela 2. Endereços IPv4 reservados

grandes empresas, como IBM, Xerox, HP, entre outras. Para redes com cerca de 5.000 hosts, era necessário utilizar faixas de classe B, desperdiçando mais de 60.000 endereços; já os 254 endereços possíveis na classe C não supriam a maior parte das redes das organizações.

Diante deste cenário, verificou-se a necessidade de soluções para o esgotamento do endereçamento IPv4. Porém, antes da resolução definitiva, algumas alternativas paliativas foram adotadas, a fim de se



Nota do DevMan 1

RFC – Request for Comments – é um conjunto de documentos de referência junto à comunidade da Internet que descreve, especifica, padroniza e debate a maioria das normas, padrões, tecnologias e protocolos ligados às redes.

racionalizar a forma como os endereços eram alocados e reduzir a demanda pelos mesmos. Estas opções serão relacionadas na próxima seção.

Alternativas para evitar o esgotamento do endereçamento IPv4

A seguir, estão descritas as principais alternativas adotadas para evitar o esgotamento dos endereços IPv4:

1. Endereçamento privado: conforme apresentado na seção anterior, existem três faixas de endereços privados (RFC 1918) que podem ser empregadas nas redes locais (**Nota DevMan 2**), evitando a atribuição de um endereço IPv4 público (também conhecido como endereço válido) para cada host;

2. NAT (Network Address Translation): deve ser utilizado conjuntamente com o endereçamento privado para possibilitar a conexão à Internet por meio de um número menor de endereços IPv4 válidos (no melhor caso, somente um único é necessário). Na rede local, cada host recebe um endereço privado utilizado nas comunicações internas. Quando um host necessita de acesso à Internet, este é traduzido em um endereço IPv4 público; vários hosts distintos podem utilizar o mesmo endereço. Tipicamente equipamentos como firewalls e roteadores são os responsáveis pela implementação desta funcionalidade. Assim, uma organização com 200 hosts pode atribuir endereços privados a cada um destes e utilizar um único endereço IPv4 válido para que todos acessem a Internet. O uso do NAT resulta em diversas limitações, pois altera o modelo fim-a-fim da Internet, não permitindo conexões diretas entre os hosts, dificultando o funcionamento de aplicações de voz, segurança, entre outras. Além disso, possui baixa escalabilidade, pois existe a restrição no número de conexões simultâneas;

3. CIDR (Classless Inter Domain Routing): eliminou as classes de endereços IPv4, permitindo a alocação de faixas com tamanho arbitrário, conforme a necessidade; deste modo, possibilitou o uso racional dos endereços disponíveis. Também viabilizou a agregação da informação nas tabelas de roteamento (veja a **Nota DevMan 3**), que cresciam exageradamente, contribuindo para suportar a expansão da Internet;

4. DHCP (Dynamic Host Configuration Protocol): protocolo que tornou possível a alocação dinâmica de endereços IPv4, por meio de sua reutilização, visto que os hosts não estão todo o tempo conectados à rede. Este recurso é particularmente útil para provedores de acesso à Internet, pois são alocados endereços IPv4 temporários a seus clientes vinculados.

Estas alternativas reduziram o consumo de endereços IPv4, enquanto era especificada sua nova versão. Todavia, como efeito colateral, também contribuíram para morosidade de sua adoção. A **Figura 3** apresenta um interessante gráfico do Núcleo de Informação e Coordenação do ponto BR (NIC.br) onde era esperado um crescimento acentuado na implantação do protocolo IPv6 concomitantemente à redução dos endereços IPv4 disponíveis. Porém, conforme observado na **Figura 4**, o ritmo de adoção do IPv6 ficou muito aquém da previsão inicial.

Além das alternativas desenvolvidas para adiar o esgotamento dos endereços IPv4, também contribuíram para a morosidade da adoção do IPv6: a necessidade de investimentos na infraestrutura (software e hardware) dos provedores de



Nota do DevMan 2

LAN: Redes locais ou LAN (Local Area Network) são interconexões de hosts localizados em uma mesma sala ou em um mesmo prédio.



Nota do DevMan 3

Tabela de Roteamento: Tabelas de roteamento são registros de endereços de destino e como chegar até eles.

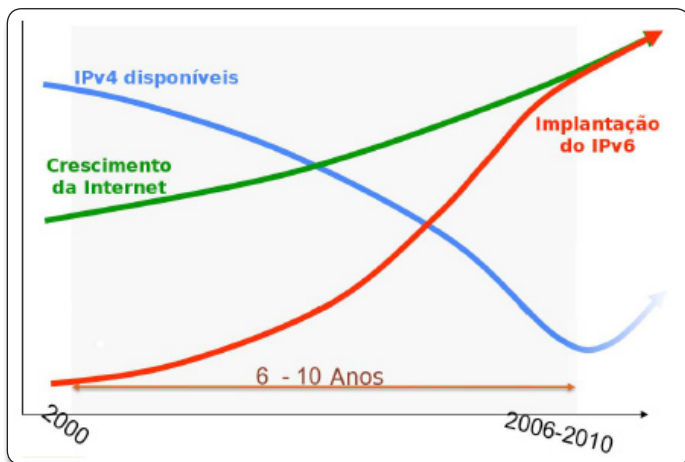


Figura 3. Expectativa inicial de implantação do IPv6

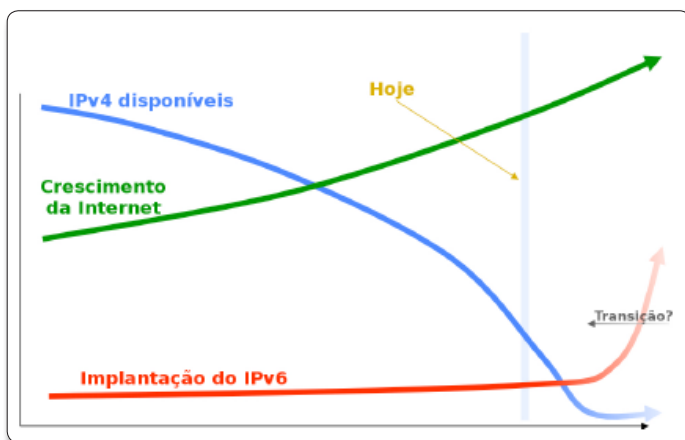


Figura 4. Situação atual da implantação do IPv6

acesso à Internet, as mudanças conceituais em sua operação que demandam treinamento e capacitação da equipe técnica, a dificuldade de implementação das estratégias de transição, entre outras.

Na próxima seção serão descritas as principais características técnicas do IPv6. Assim, será possível a compreensão do contexto envolvido e da situação atual da implantação deste protocolo.

IPv6: Características gerais

O protocolo IPv6, além de solucionar a questão da quantidade de endereços disponíveis, oferece novos serviços e benefícios. Segundo a RFC 2460, as principais mudanças em relação ao IPv4 são:

- **Simplificação do formato do cabeçalho:** diversos campos do cabeçalho IPv4 foram excluídos ou tornados opcionais, gerando um cabeçalho simplificado. Desta forma, foi reduzido o custo do processamento dos pacotes nos roteadores;
- **Capacidade para identificação do fluxo:** o remetente de um determinado fluxo pode solicitar seu tratamento especial, como qualidade de serviço diferenciada (QoS) ou transmissão em tempo real;
- **Suporte para campos opcionais e extensões:** os campos opcionais possuem menos restrições quanto ao seu tamanho e há maior flexibilidade para a introdução de novas extensões no futuro;
- **Capacidade de autenticação e privacidade:** foram especificadas extensões para a autenticação, integridade e confidencialidade dos dados;
- **Capacidade de endereçamento expandida:** cada endereço IPv6 utiliza 128 bits, ou seja, existem 2^{128} combinações distintas ($3,4028 \times 10^{38}$ ou 79 octilhões de vezes a quantidade disponível no IPv4). Para ilustrar a grandeza deste valor, supondo que a área do planeta Terra é $510.065.500 \times 10^{12} \text{ mm}^2$, teríamos $6,6713 \times 10^{17}$ endereços IPv6 por mm^2 . Porém, como existem faixas reservadas, ou seja, nem todos os endereços são possíveis, vamos supor que efetivamente sejam utilizados 64 bits dos 128 bits, ainda assim, existiriam mais de 36.000 endereços IPv6 por m^2 . Esta expansão da capacidade do endereçamento proporciona a identificação de mais hosts conectados à rede e simplifica a implementação de mecanismos de autoconfiguração, além de suportar níveis mais específicos de hierarquização dos endereços.

O cabeçalho do protocolo IPv6 tem tamanho determinado (40 bytes) e possui 8 campos obrigatórios, diferentemente do IPv4, cujo tamanho é variável (entre 20 e 60 bytes) e contém 12 campos fixos (pode conter também campos opcionais). A **Figura 5** ilustra estas diferenças, apresentando os campos que foram mantidos (cor laranja), os descartados (cor rosa), aqueles que sofreram alterações em seu nome e posicionamento (cor azul) e um novo campo adicionado (cor verde).

A lista a seguir descreve brevemente os campos do protocolo IPv6:

- **Version (versão) – 4 bits:** versão do protocolo Internet;
- **Traffic class (classe de tráfego) – 8 bits:** utilizado para permitir a diferenciação de tráfego (classes de tráfego) e os mecanismos de prioridade, para que os roteadores possam prover tratamento apropriado em cada caso;
- **Flow label (identificador de fluxo) – 20 bits:** possibilita que a origem atribua uma identificação (padronizada) a um fluxo, para que este receba tratamento especial por um roteador (qualidade de serviço – QoS, tráfego de tempo real, reserva de banda, entre outros);
- **Payload length (tamanho dos dados) – 16 bits:** tamanho (em bytes) dos dados enviados junto ao cabeçalho IPv6. É importante

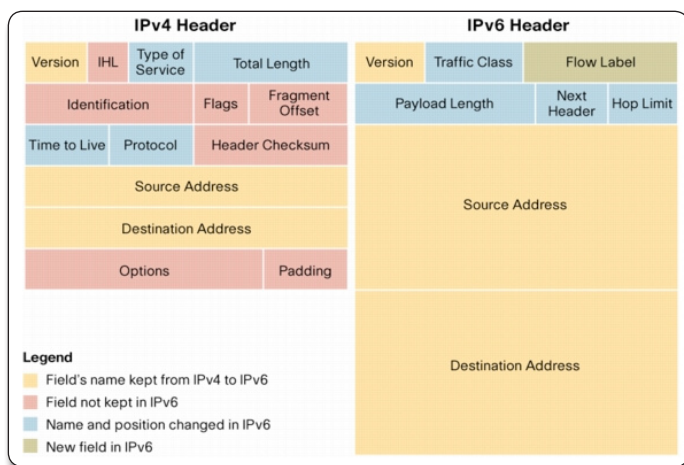


Figura 5. Comparação entre os cabeçalhos dos protocolos IPv4 e IPv6

notar que os cabeçalhos de extensão também são incluídos no cálculo do tamanho;

- **Next header (próximo cabeçalho) – 8 bits:** identifica o próximo cabeçalho que se segue ao do IPv6;
- **Hop limit (limite de encaminhamento) – 8 bits:** número máximo de roteadores que o pacote pode passar antes de ser descartado;
- **Source address (endereço de origem) – 128 bits:** endereço lógico do remetente do pacote;
- **Destination address (endereço de destino) – 128 bits:** endereço lógico do destinatário do pacote.

É interessante observar que, mesmo utilizando endereços com 128 bits (quatro vezes maior que os 32 bits do IPv4), o IPv6 tem o cabeçalho apenas duas vezes o tamanho mínimo de seu antecessor.

Em relação ao suporte para campos opcionais e extensões, este é tratado por meio do extension header (cabeçalho de extensão), que possui tamanho variável (necessariamente múltiplo de 64 bits). A **Figura 6** apresenta a estrutura de um pacote IPv6. Este pode ter um ou mais campos de extensão, desde que indicado no next header (**Figura 7**). Geralmente, somente o destinatário processará os extension headers, que devem ser analisados exatamente na ordem em que aparecem. A lista abaixo enumera todos os tipos que devem ser suportados por nós IPv6:

- **Hop-by-hop options (opções hop-a-hop):** informações gerais que devem ser processadas por todos os nós ao longo do caminho do pacote. Por exemplo, uma opção já especificada é o suporte aos pacotes maiores que 64kB, também conhecidos como jumbogramas;
- **Routing – type 2 (roteamento – tipo 2):** empregado para suporte a mobilidade em IPv6;
- **Fragment (fragmento):** utilizado quando o pacote a ser enviado é maior que o MTU (Maximum Transmission Unit), para gerenciar sua fragmentação;
- **Destination options (opções de destino):** também usado para suporte à mobilidade em IPv6;

- **Authentication (autenticação):** habilita a autenticação dos pacotes;
- **Encapsulating security payload (encapsulamento de segurança dos dados):** garante confidencialidade e integridade aos pacotes.

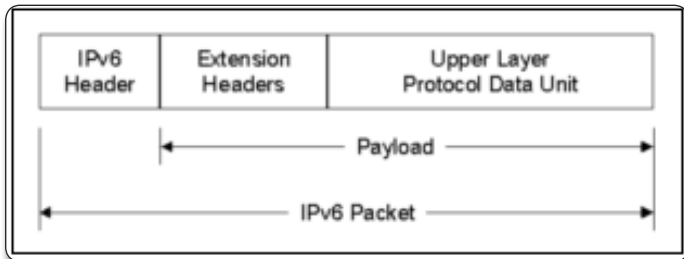


Figura 6. Estrutura de um pacote IPv6

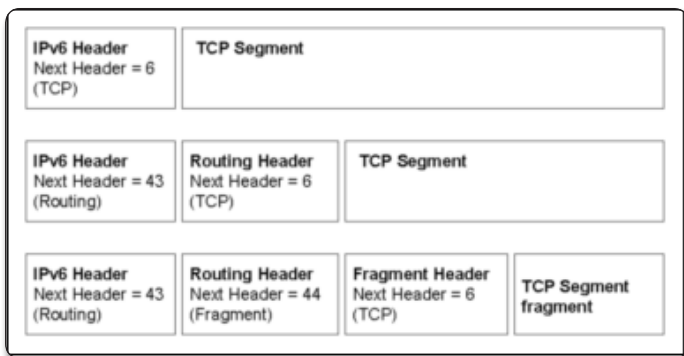


Figura 7. Exemplos de IPv6 extension headers

Para evitar que todos os nós tenham que percorrer a cadeia de cabeçalhos de extensão, estes devem respeitar uma determinada ordem. Ou seja, aqueles que são importantes para todos os nós envolvidos no roteamento devem ser colocados em primeiro lugar; já os cabeçalhos relevantes apenas para o destinatário final são posicionados ao final da cadeia. Desta maneira, a sequência recomendada é apresentada abaixo:

1. Hop-by-Hop options;
2. Routing – type 2;
3. Fragment;
4. Authentication;
5. Encapsulating Security Payload;
6. Destination Options.

O endereço de 128 bits do IPv6 é composto por oito conjuntos de números hexadecimais (16 bits cada) separados por dois pontos, conforme ilustrado na Figura 8.

2001:12A3:ABCD:CACA:98EF:CAFE:2001:108C

Figura 8. Exemplo de um endereço IPv6 (representação completa)

É importante notar algumas regras em sua representação:

- Podem ser utilizados caracteres maiúsculos ou minúsculos (Figura 9);

2001:A312:C1D1:CAFE:98CD:BEBE:2001:8ACF (maiúsculo)
2001:a312:c1d1:cafe:98cd:bebe:2001:8acf (minúsculo)

Figura 9. Representação do endereço IPv6 com caracteres maiúsculos e minúsculos

- Sequências contínuas de zeros podem ser representadas por “::” (sem aspas), uma única vez em cada endereço, para não gerar ambiguidade (Figura 10);

2001:0000:0000:0000:98CD:BEBE:0000:0000 (representação completa)
2001::98CD:BEBE:0000:0000 (representação abreviada - sequência inicial)
2001:0000:0000:0000:CAFE:98CD:BEBE:: (representação abreviada - sequência final)

Figura 10. Representação do endereço IPv6 com supressão de sequências contínuas de zeros (parte inicial e parte final)

- Os zeros à esquerda podem ser omitidos (Figura 11).

2001:0000:0000:0000:98CD:BEBE:0000:0000 (representação completa)
2001::98CD:BEBE:0:0 (representação abreviada - sequência inicial e omissão de zeros)
2001:0:0:0:98CD:BEBE:: (representação abreviada - omissão de zeros e sequência final)

Figura 11. Representação do endereço IPv6 com supressão de sequências contínuas de zeros (parte inicial e parte final) e omissão de zeros à esquerda

A representação de um prefixo IPv6 é similar à notação CIDR utilizada no IPv4, ou seja, endereço “IPv6/prefixo” (sem aspas), conforme apresentado na Figura 12. Note que um mesmo endereço pode ser representado de formas diferentes, seguindo as regras descritas anteriormente.

54DC:0:0:EF1:0:0:0:0/60
54DC::EF1:0:0:0:0:0/60
54DC:0:0:EF1::/60

Figura 12. Diferentes representações de um prefixo IPv6

Na arquitetura do protocolo IPv6 foram especificados somente três tipos de endereços, a saber:

- **Anycast:** endereço atribuído a mais de uma interface de rede, sendo que um pacote enviado a esse endereço será entregue à interface mais próxima, de acordo com os protocolos de roteamento;
- **Multicast:** também é um endereço alocado a mais de uma interface de rede, porém, os pacotes serão entregues a todas as interfaces associadas a este endereço;
- **Unicast:** endereço de uma única interface de rede. Um pacote enviado a esse endereço será entregue somente a esta interface.

O conceito do endereço de broadcast (pacotes enviados a todos os nós de um mesmo domínio) foi removido.

Os endereços unicast IPv6 são, ainda, decompostos em subtipos. Os mais relevantes são:

- **Global Unicast:** endereço que será globalmente utilizado na Internet, similar ao endereço público IPv4. Atualmente, a alocação de endereços é feita a partir da faixa 2000::/3, ou seja, dos endereços de 2000:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff (cerca de 13% do total de endereços);

- **Unspecified Address:** sinaliza a ausência de um endereço. É definido como 0:0:0:0:0:0:0:0 ou “::” (sem aspas). Usado como endereço de origem em estações que ainda não obtiveram um endereço IPv6 – aquelas que não foram inicializadas;
- **Loopback Address:** utilizado quando um nó envia um pacote para si mesmo (função semelhante em IPv4). Representado por 0:0:0:0:0:0:0:1 ou “::1” (sem aspas);
- **Unique-Local:** suporta apenas comunicações locais, com alta probabilidade de ser globalmente único. Sua função é similar aos endereços privados IPv4 (RFC 1918). Identificado pelo prefixo FC00::/7 seguido por 64 bits derivados a partir do endereço físico da interface (MAC Address), segundo o formato IEEE EUI-64 (veja a seguir);
- **Link-Local:** definido para uso interno apenas no enlace específico onde a interface está conectada para funções como autoconfiguração, descoberta de vizinho, entre outras. Utiliza o prefixo FE80::/64 e também deriva os demais 64 bits a partir do endereço físico da interface (MAC Address), segundo o formato IEEE EUI-64.

Para formar o endereço IEEE EUI-64, basta efetuar a operação complemento de 1 para o sétimo bit mais à esquerda (se for 0, trocá-lo por 1 e vice-versa) e inserir os caracteres hexadecimais FF-FE na parte central do endereço, como apresentado na **Figura 13**.

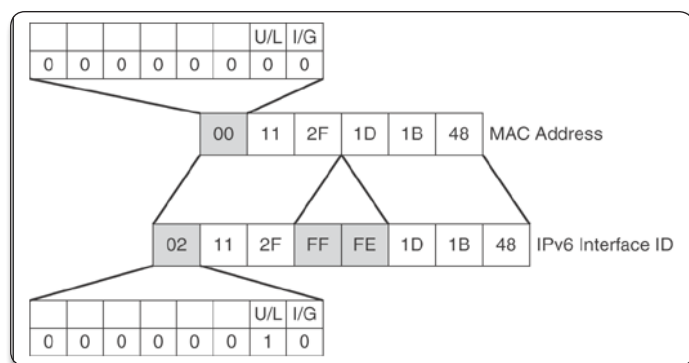


Figura 13. Formação do endereço EUI-64 a partir do MAC Address

Para finalizar, é importante observar que, a uma interface de rede, podem ser atribuídos múltiplos endereços, independentemente do seu tipo (anycast, multicast ou unicast) ou subtipo (unique-local, loopback, global, entre outros).

A próxima seção apresentará os mecanismos de autoconfiguração do IPv6, mostrando como um host obtém de forma automática um endereço unicast.

Auto-configuração do IPv6

O IPv6 oferece suporte à autoconfiguração, mecanismo que possibilita a alocação automática de endereços unicast aos nós IPv6. Basicamente esta atribuição dinâmica pode ser implementada por meio de duas abordagens:

- **Autoconfiguração stateless:** possibilita a configuração automática dos endereços IPv6 unicast sem a necessidade de servi-

dores DHCP. Para tanto, o host utiliza seu endereço link local (FE80::/64) para enviar uma mensagem multicast RS (Router Solicitation) para todos os roteadores do segmento – esta é parte do Neighbor Discovery Protocol (NDP). Desta maneira, é solicitado o prefixo IPv6 e o endereço a ser configurado como default gateway. O roteador responde às informações requisitadas em uma mensagem RA (Router Advertisement) – ver **Nota DevMan 4**. A seguir, o host combina o prefixo recebido com o endereço físico de sua interface (MAC Address), segundo o formato IEEE EUI-64. A **Figura 14** ilustra o processo de autoconfiguração stateless;

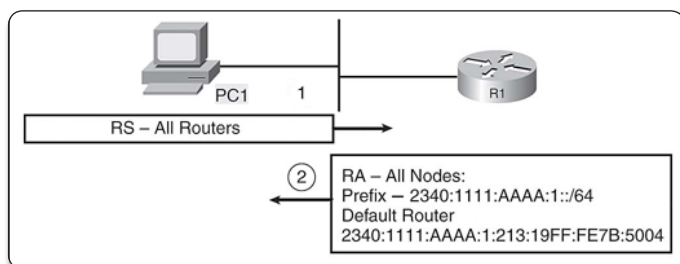


Figura 14. Mecanismo de auto-configuração stateless



Nota do DevMan 4

Router Solicitation e Router Advertisement: Router Solicitation, ou RS, é utilizada por hosts para solicitar aos roteadores o envio imediato de mensagens router advertisement.

Router Advertisement, ou RA, é enviada ciclicamente ou em resposta a uma RS. É utilizada pelos roteadores para anunciar sua presença no enlace; contém diversas informações referentes à configuração da rede.

- **Autoconfiguração stateful:** técnica opcional à stateless que utiliza o protocolo DHCPv6 para obtenção do endereço IPv6, default gateway, servidores DNS (Domain Name System), NTP (Network Time Protocol), entre outros parâmetros para configuração da interface de rede. Os hosts clientes utilizam seu endereço link local para enviar e receber as mensagens DHCPv6, por intermédio de mensagens multicast.

Por intermédio da autoconfiguração, os hosts IPv6 recebem seu endereço e podem iniciar a transmissão de dados nas redes. Mas, como ocorre a comunicação com hosts executando a versão anterior do protocolo Internet? Pensando nisso, a próxima seção apresentará as formas de transição e a coexistência entre o IPv4 e o IPv6.

Transição e a coexistência entre o IPv4 e IPv6

A implementação do protocolo IPv6 não implica na criação de uma nova Internet, paralela à atual, tampouco, será programado um dia para desativação completa do IPv4. Ambos os protocolos coexistirão nas redes por um período longo e imprevisível. Já existem diversos equipamentos de rede que suportam os pro-

toscolos IPv4 e IPv6. As versões mais recentes de vários sistemas operacionais também são compatíveis, como as distribuições Linux e Microsoft Windows.

Durante a criação do IPv6 foram idealizados diversos procedimentos de transição, organizados em três categorias principais:

- **Pilha dupla (Dual-stack):** neste mecanismo, os dispositivos suportam simultaneamente as duas pilhas de protocolos, permitindo que hosts IPv6 se comuniquem com hosts IPv4 e vice-versa (**Figura 15**). Esta técnica exige duas tabelas de roteamento com funções de administração e gerenciamento similares, sendo que os hosts também possuem dois endereços configurados em sua interface. É muito utilizada, pois, atualmente, grande parte dos hardwares e softwares de rede possuem suporte IPv4 e IPv6. Além disso, permite que a implantação deste último seja feita sem mudanças na arquitetura de redes atual;

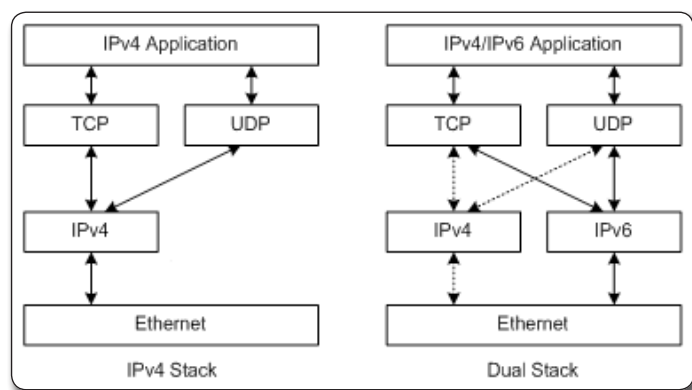


Figura 15. Comparação entre a pilha IPv4 e a pilha dupla IPv4/IPv6

- **Túneis (Encapsulation):** neste método, um pacote IPv6 é transmitido como parte dos dados de um pacote IPv4, criando um túnel entre os nós (**Figura 16**). No futuro, este túnel também suportará o inverso, ou seja, redes IPv4 conectadas por redes IPv6. É importante notar que, nos dois cenários, os nós nas extremidades do túnel devem ser compatíveis com ambos os protocolos.

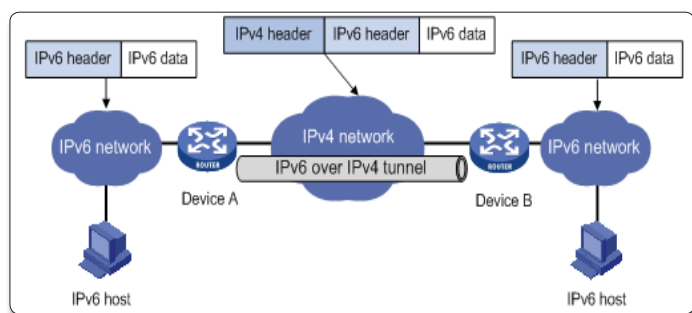


Figura 16. IPv6 sobre túnel IPv4

- **Traduções:** nesta técnica, um dispositivo com suporte aos protocolos IPv4 e IPv6 interage com os demais nós que desejam estabelecer a comunicação, traduzindo os pacotes IPv6 em IPv4 e vice-versa.

A coexistência entre as diferentes versões do IP aumenta ainda mais as preocupações com as questões relacionadas à segurança dos dados, pois, como diversos tipos de transações ocorrem por meio da infraestrutura suportada por estes protocolos, as informações podem ser capturadas e alteradas por usuários mal-intencionados. Assim, a próxima seção apresentará os principais aspectos de segurança em redes IPv6.

Segurança da informação em redes IPv6

Originalmente, o IPv4 visava o estabelecimento da comunicação entre os computadores dos centros militares e os de pesquisa, ou seja, as informações percorriam somente locais seguros e com acesso restrito. Posteriormente, seu uso comercial demandou um nível maior de segurança, que possibilitasse a identificação dos usuários e a privacidade dos dados transmitidos. Neste contexto, o IPSec (IP Security) foi criado para prover os seguintes serviços:

- **Autenticação:** para ratificar a identidade das partes envolvidas na troca de mensagens;
- **Integridade:** garantindo que os dados não fossem alterados durante sua passagem pelos diferentes dispositivos de rede;
- **Privacidade:** restringindo a compreensão da mensagem somente ao emissor e ao destinatário da comunicação por intermédio de técnicas de criptografia;
- **Não-repúdio:** para impedir que as partes envolvidas na comunicação negassem sua participação no evento.

O IPSec, suportado opcionalmente pelo IPv4, foi desenvolvido como parte integrante do IPv6, através dos cabeçalhos de extensão AH (Authentication Header) – usado para autenticar o emissor dos dados e assegurar a integridade dos mesmos – e ESP (Encapsulation Security Payload) – empregado para prover privacidade entre o originador e o receptor dos dados.

Entretanto, para que duas entidades possam se comunicar utilizando o IPSec, é necessário estabelecer uma associação de segurança (AS) para determinar os algoritmos a serem configurados, as chaves criptográficas, o tempo de expiração destas chaves, entre outras especificações. As associações de segurança podem ser estáticas ou dinâmicas: no primeiro caso, os parâmetros são configurados manualmente no emissor e no destinatário; já no segundo, são determinados automaticamente por protocolos como o IKE (Internet Key Exchange).

A seguir são ilustrados dois exemplos de ataques comumente observados em redes IPv4 e a maneira como são mitigados pelo IPv6/IPSec:

- **IP Spoofing:** técnica que consiste no envio de pacotes com o endereço de origem adulterado. Desta maneira, os pacotes de retorno nunca regressam para o falsificador. No IPv6, o cabeçalho de extensão AH obriga o usuário mal-intencionado a calcular um hash (**Nota DevMan 5**) semelhante àquele que seria gerado entre a entidade falsificada e a vítima; no entanto, para a obtenção deste, seria necessário conhecer os parâmetros da AS, incluindo as chaves criptográficas e os algoritmos. Assim, caso a vítima receba um pacote com o hash incorreto, esta deve descartá-lo;

• **Sniffing:** ataque em que os pacotes são capturados com o objetivo de verificar seu conteúdo, explorando aplicações que não utilizam nenhum tipo de criptografia no envio de seus dados, como FTP (transferência de arquivos), Telnet (acesso/login remoto), entre outras. Para evitar este tipo de ataque, pode-se lançar mão do cabeçalho de extensão ESP, para criptografar os dados e promover a privacidade entre as partes envolvidas na comunicação.



Nota do DevMan 5

Função Hash: Uma função hash é uma equação matemática que utiliza dados de entrada para criar um resumo da mensagem (message digest).

É importante destacar que, mesmo suportando nativamente o IPSec, seu uso não é obrigatório. No entanto, utilizar o IPv6 sem este recurso, torna-o vulnerável às mesmas fragilidades de seu antecessor.

Além do IPSec, outras ferramentas de segurança são adicionalmente implementadas pelo protocolo Internet versão 6, a saber:

- **Cryptographically Generated Address (CGA):** segundo a RFC 3972, este tem seus últimos 64 bits (identificação da interface do host) derivados a partir de uma função hash da chave pública do proprietário do endereço;
- **Estrutura dos endereços:** a própria estrutura de endereçamento do IPv6 pode impedir alguns tipos de ataque, pois sua varredura torna-se um procedimento complexo e demorado devido ao grande número de combinações possíveis; também contribuíram as diferentes formas de compor os últimos 64 bits, que dificultam a localização dos endereços efetivamente em uso na rede;
- **Extensões de privacidade:** são complementares ao mecanismo de autoconfiguração stateless e possibilitam a geração de endereços aleatórios e temporários, resultando na ineficiência do rastreamento de dispositivos advindos de redes com suporte a este recurso;
- **Secure Neighbor Discovery (SEND):** extensão de segurança do Neighbor Discovery Protocol (NDP) que impõe o estabelecimento de uma infraestrutura de chaves públicas na rede, com o objetivo de autenticar os dispositivos que possam se anunciar na rede.

A implementação nativa do IPSec, bem como das novas ferramentas de segurança apresentadas, são importantes avanços do IPv6. Comparado a sua versão anterior, este também permitiu diversas melhorias na mobilidade dos dispositivos conectados à Internet, conforme será exposto na próxima seção.

Mobilidade IPv6

A motivação para o desenvolvimento de mecanismos de mobilidade é uma consequência natural da integração de redes wireless (sem fio) à Internet. Até a introdução desta tecnologia, os usuários se limitavam a acessá-la por meio de locais pré-determinados, como por exemplo,

em suas residências ou nas empresas onde trabalhavam. As conexões wireless tornaram realidade o uso de laptops, tablets, celulares, entre outros dispositivos, como clientes de acesso à rede.

Desta maneira, foi desenvolvido o MIPv6 (Mobile Internet Protocol version 6), com o objetivo de suportar o deslocamento de um dispositivo móvel de uma rede para outra sem a necessidade da reconfiguração de seu endereço IPv6, tornando esta movimentação transparente às diferentes aplicações.

Para compreensão do MIPv6, é importante conhecer as seguintes terminologias (Figura 17):

- **Mobile Node (nó móvel) – MN:** dispositivo móvel que pode transitar entre diferentes redes sem perder suas conexões estabelecidas, continuando acessível através de seu endereço de origem;
- **Home Address (endereço de origem) – HoA:** endereço permanentemente alocado ao MN. É por meio deste que o nó móvel se conecta a rede de origem;
- **Home Network (rede de origem) – HN:** rede onde o nó móvel está conectado e que fornece seu endereço de origem;
- **Home Agent (agente de origem) – HA:** roteador localizado na rede de origem do nó móvel e que mantém a associação entre seu endereço de origem e o remoto;
- **Care of Address (endereço remoto) – CoA:** endereço associado ao nó móvel quando este se encontra em uma rede remota;
- **Foreign network (rede remota) – FN:** qualquer rede, diferente da HN, onde o nó móvel se encontra;
- **Correspondent node (nó correspondente) – CN:** nó (móvel ou estático) com o qual o nó móvel se comunica.

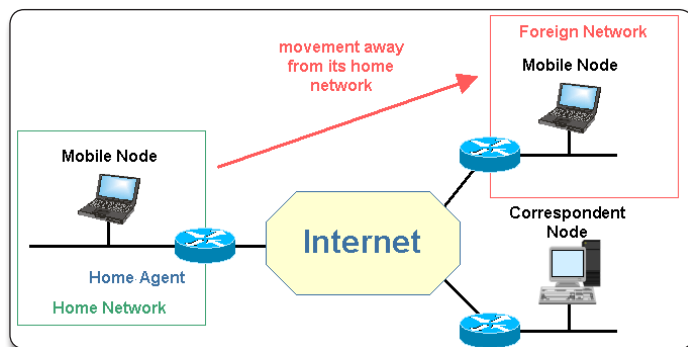


Figura 17. Principais componentes do MIPv6

Os passos a seguir descrevem o funcionamento básico das redes com suporte ao MIPv6:

1. A rede de origem (HN) aloca um endereço HoA para o nó móvel (MN), o qual não será alterado mesmo quando o MN se desloca para uma rede remota (FN);
2. Quando o MN se dirige a uma FN, este recebe um endereço CoA por intermédio de mecanismos de autoconfiguração (stateless ou stateful), constituído por um prefixo válido;
3. O nó móvel associa seu endereço de origem (HoA) ao remoto (CoA) e registra seu novo endereço no agente de origem (HA) enviando uma mensagem Binding Update. O HA confirma a recepção desta por meio da mensagem Binding Acknowledgement

(Figura 18). Note que este procedimento assegurará que os pacotes IPv6 destinados ao endereço de origem sejam recebidos pelo nó móvel na rede remota;

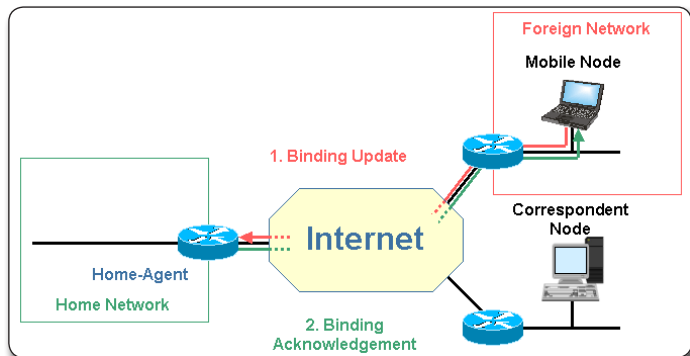


Figura 18. Registro do CoA no agente de origem

4. O agente de origem, ao receber pacotes IPv6 endereçados ao nó móvel, intercepta-os e os envia encapsulados para o endereço remoto através de um túnel. Este mecanismo é conhecido como triangulação (Figura 19);

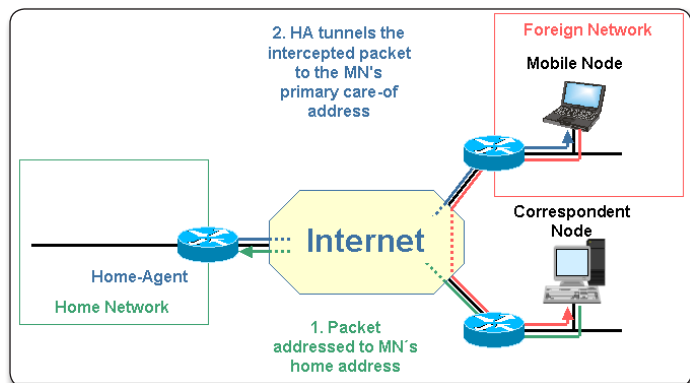


Figura 19. Triangulação da comunicação entre o MN e o CN

5. Para otimizar o fluxo de dados, é possível habilitar a comunicação direta entre o nó correspondente (CN) e o nó móvel (MN), ou seja, sem a necessidade de passar através da rede de origem e pelo agente de origem (Figura 20). As mensagens Binding Update, Binding Acknowledgement e Binding Refresh Request são usadas pelo CN para aprender dinamicamente o endereço remoto do nó móvel. É importante observar que neste caso, o CN também deverá suportar a mobilidade IPv6;

6. Quando o nó móvel retorna para sua rede, este envia a mensagem Binding Update para informar ao agente de origem que os pacotes não devem mais ser encaminhados ao seu endereço remoto.

A mobilidade utiliza o cabeçalho de extensão Mobility para suportar a troca de mensagens relacionadas ao estabelecimento e ao gerenciamento das associações de endereços. A lista abaixo descreve brevemente seus campos (Figura 21):

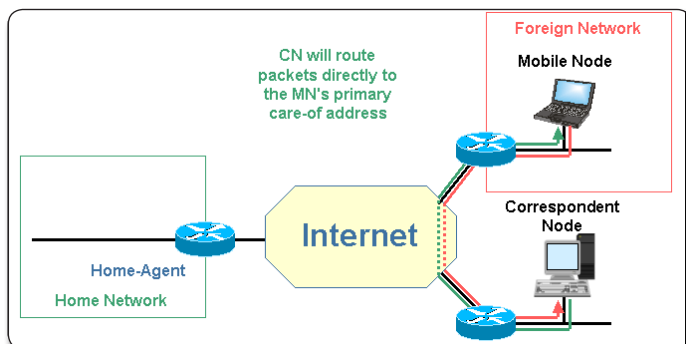


Figura 20. Comunicação otimizada entre o MN e o CN

Next Header	Length	MH Type	Reserved
Checksum		Message Data	

Figura 21. Campos do cabeçalho de extensão mobility

- **Next header (próximo cabeçalho):** indica o próximo cabeçalho – atualmente, apenas o valor 59 (em decimal) é implementado, sinalizando que não existe próximo cabeçalho, porém há a possibilidade de uma expansão futura;
- **Length (tamanho):** tamanho do cabeçalho de extensão Mobility, necessariamente múltiplo de 8 bytes;
- **MH Type (tipo do cabeçalho de mobilidade):** identifica o tipo da mensagem de mobilidade: Binding Refresh Request, Binding Update, entre outras;
- **Checksum (soma de verificação):** verifica a integridade dos dados;
- **Data (dados):** mensagem a ser enviada.

Conclusões

O protocolo IPv6, além de resolver a limitação imposta à expansão da Internet pelo seu antecessor, oferece novos serviços e melhorias, tais como: a simplificação do formato de seu cabeçalho, a identificação dos fluxos de dados, o suporte para campos opcionais e extensões, recursos para autenticação e privacidade, mecanismos de autoconfiguração, entre outros. O espaço total de endereços utilizando 128 bits (quatro vezes maior que os 32 bits da versão anterior) possibilita $3,4028 \times 10^{38}$ (340.282.366.920.938.463.463.374.607.431.768.211.456) combinações diferentes, número suficientemente grande para atender as demandas atuais e projetadas para o futuro.

Embora sua adoção fosse imprescindível, as alternativas criadas para adiar o esgotamento do IPv4 (endereços privados, NAT, CIDR e DHCP), necessárias para que houvesse tempo hábil para a especificação do novo protocolo, contribuíram para a morosidade de sua disponibilização pelas organizações e usuários. Também cooperaram para esta realidade, a facilidade de implementação, a interoperabilidade e a robustez da versão 4 do protocolo Internet.

Atualmente, algumas barreiras ainda dificultam a aceitação do IPv6, entre elas: a necessidade de investimentos na infraestrutura,

pois, muitas vezes, o hardware e o software legados não são compatíveis com a nova versão do protocolo; as mudanças conceituais em sua operação demandam treinamento e capacitação da equipe técnica; por fim, a definição da implantação das estratégias de transição requer um planejamento adequado ao particular cenário onde estão inseridas.

Estes fatores permitiram a sobrevivência do protocolo IPv4. Entretanto, não há mais como ignorar a situação atual, pois brevemente os provedores não terão endereços disponíveis para alocar aos seus usuários. Desta forma, a única alternativa para evitar um colapso nas comunicações e a retração no crescimento da Internet é a adoção maciça do protocolo IPv6.



André Koide da Silva

andre@aksilva.com

Mestre em Engenharia pela Escola Politécnica da Universidade de São Paulo, especialista em Redes de Computadores pela Universidade Estadual de Campinas e bacharel em Sistemas de Informação pela Universidade Presbiteriana Mackenzie. Atualmente

é especialista em redes de computadores pelo UOL Diveo, com ampla experiência em projetos e implementação de soluções Cisco Systems, Brocade Communications Systems e Juniper Networks. Atua também como professor na Faculdade Impacta Tecnologia. Trabalhou em empresas como Goldnet TI, EDS (Electronic Data Systems do Brasil) — atual HP Brasil (Hewlett-Packard), Alog Data Centers e Gennari & Peartree Projetos e Sistemas. Experiência de onze anos na área de redes de computadores e tecnologia da informação, além de cinco anos como docente do ensino superior nestas áreas. Certificado Cisco IP Communications Express Specialist, Cisco Certified Network Associate (CCNA), Extreme Network Associate (ENA), 3Com Certified Wireless Expert, Juniper Networks Certified Internet Specialist (JNCIS-M), Project Management Professional (PMP), Information Technology Infrastructure Library (ITILv3) e ISO/IEC 20000 - IT Service Management.



Hobbes' Internet Timeline 10.1 by Robert H. Zakon

<http://www.zakon.org/robert/internet/timeline>

IPv4 & IPv6 Services

http://www.h3c.com/portal/Products_Solutions/Technology/IPv4_IPv6_Services/

Mobile IPv6

<http://www.ibk.tuwien.ac.at/~ipv6/mipl.htm>

Apostila "Curso IPv6 básico" do NIC.br

<http://curso.ipv6.br>

Artigo "IPv4 e IPv6", escrito por George Marcel M. A. Smetana

<http://www.abusar.org.br/ftp/pitanga/Redes/ArtigoIP.pdf>

Artigo "Impactos da transição e utilização do IPv6 sobre a segurança de ambientes computacionais", escrito por Jansen C. Sena, Paulo Lício de Geus e Alessandro Augusto

http://bastion.las.ic.unicamp.br/paulo/papers/2002-WSeg-jansen.sena-Impactos_IPv6.pdf



DÊ UM SALTO EM CONHECIMENTO!



Acesse o maior portal para desenvolvedores da América Latina!

17
mil
posts

280
mil
cadastrados

5
milhões de
page-views
por mês

Instalação de Clientes via Push

Como habilitar o método Push, configurar o cliente e fazer troubleshooting

RAPHAEL PEREZ

O System Center Configuration Manager 2007 (antes conhecido como Microsoft System Management Server ou SMS e aqui chamado de SCCM) é uma solução completa de inventário, implementação e atualização de servidores, clientes e dispositivos – em ambientes físicos, virtuais, distribuídos e móveis. Ele tende a levar a TI a um patamar mais produtivo e efetivo, reduzindo tarefas manuais e habilitando o foco para projetos de maior valor, maximizando investimentos em hardware e softwares, além de aumentar a produtividade do usuário final com o software correto no momento correto.

Para isso, o SCCM trabalha com o conceito de cliente. Um cliente do SCCM é qualquer computador que o SCCM possa gerenciar. Pode ser um computador desktop ou laptop do usuário, uma Workstation, um dispositivo móvel ou um servidor, incluindo os servidores SCCM.

Nesse contexto, este artigo irá apresentar como é o processo de instalação de um software cliente via método push de forma que possamos gerenciar o computador onde será feita a instalação. Além disso, veremos também como habilitar o método, configurar o cliente, fazer troubleshooting e muito mais.

O método Push

Para que o SCCM possa gerenciar um cliente, um software deve ser instalado. Para instalar o software, podemos instalar:

- Via GPO (Group Policy objects);
- Manualmente;
- Via Windows Update utilizando o WSUS (Windows Server Update Services);
- Via Método Push.

A instalação via push é utilizada pelo SCCM para instalar o software cliente automaticamente quando um novo recurso for descoberto, isto é, adicionado ao banco de dados do SCCM. Diferente dos outros, esse é o único método em que o servidor SCCM inicia a instalação. Nas próximas seções veremos o processo, como fazer a configuração necessária, tanto do lado do servidor quanto do lado do cliente, de forma centralizada e, também, como resolver alguns dos problemas mais comuns.

Desmistificando

Existe uma certa confusão em relação ao funcionamento da instalação de clientes pelo método push. O ponto principal está em entender a diferença entre habilitar a instalação do método push ou utilizar o Wizard.

Resumo DevMan

De que se trata o artigo:

O artigo descreve como é o processo de instalação de um software cliente via método push. No artigo veremos também como habilitar o método, configurar o cliente, fazer troubleshooting e muito mais.

Em que situação o tema é útil:

O método push, se configurado de forma correta, é uma poderosa funcionalidade que facilita a vida do administrador SCCM na tarefa de instalação e atualização automática de clientes.

Instalação de Clientes via Push:

Push é o método de instalação de clientes mais conhecido e, portanto, utilizado com muita frequência. Saber como ele funciona e como resolver os problemas mais comuns de instalação de clientes é uma das tarefas do dia-a-dia de um administrador do SCCM.

Ao habilitar a opção do método push, o servidor SCCM tentará instalar o cliente para todos os computadores que ainda não possuem o cliente instalado e que pertencem ao site, isto é, o endereço IP do computador pertence aos cadastrados na boundary do SCCM. Já o Wizard é um processo “manual” onde o administrador do SCCM pode também escolher por instalar o cliente para computadores não pertencentes ao site.

Quando o processo de descobrir novos clientes ocorre, um arquivo com extensão DDR (*Discovery Data Record*) é criado para cada novo computador descoberto. Esse arquivo é sempre criado, independente das configurações do método push.

Em seguida, caso a instalação automática esteja selecionada, ou quando o Wizard de instalação for concluído, um arquivo com extensão CCR (*Client Configuration Request*) é gerado pelo servidor para cada computador.

Isso somente é verdade se: 1) os recursos identificados fazem parte da boundary do site e, 2) o recurso descoberto está em conformidade com os selecionados.

Após a criação do arquivo CCR, ele é processado pelo componente CCM (*Client Configuration Manager*) e a instalação começa. Caso a instalação do cliente falhe, novas tentativas ocorrerão uma vez por hora, durante 168 horas (1 semana) antes da desistência.

Habilitando a instalação via Push

Quando se instala um cliente usando o método push, o SCCM utiliza uma conta de usuário do windows ou a própria conta de

computador do SCCM caso uma conta de usuário não seja especificada. Esta informação também é válida quando a conta especificada não possui direitos administrativos no computador cliente.

Para configurar essa conta no SCCM, siga os passos:

1. Na console do SCCM expanda **Site Database, Site Management, <Código do Site>, Site Settings**, e então clique em **Client Installation Methods**;
2. Dê um duplo-clique em **Client Push Installation** para abrir a janela de propriedades. Nesta janela pode-se habilitar a instalação para todos os novos computadores descobertos (ver **Figura 1**);

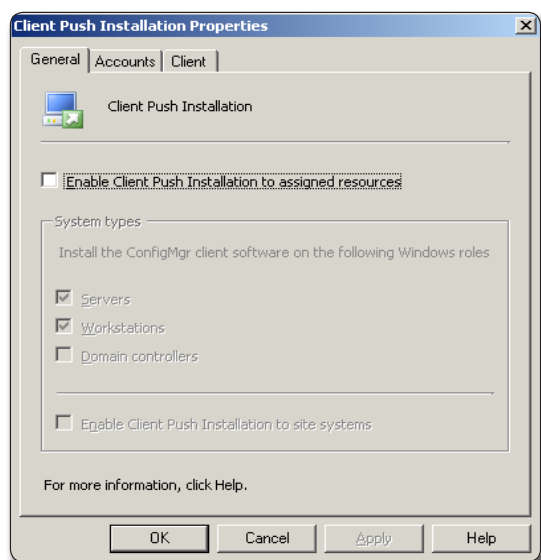


Figura 1. Client Push Installation Properties – Aba General

3. Selecione a aba **Accounts** e clique no botão **New** (Ícone amarelo que parece um sol);
4. Em **User name**, digite o nome de usuário que será utilizado para a instalação de clientes, em **Password** e **Confirm password**, digite o password e então clique **OK** (ver **Figura 2**).

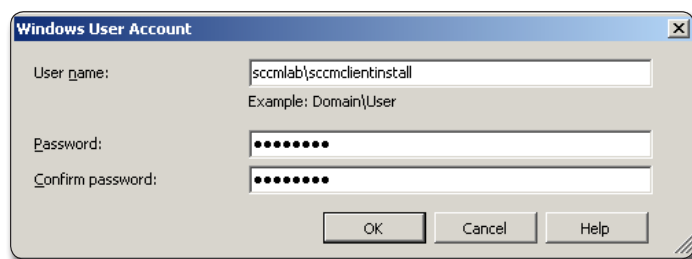


Figura 2. Windows User Account

5. Quando a janela de **Windows User Account** for fechada, verifique se o usuário digitado aparece na lista de usuários configurados para fazer a instalação via push;
6. Na aba **Client** e em **Installation properties** pode-se adicionar parâmetros à instalação. O parâmetro mais comum é a utilização do **FSP (Fallback Status Point)** (ver **Figura 3**);



Nota do DevMan

Boundary/Boundaries: O SCCM usa boundaries para determinar quando um cliente está dentro ou fora do site. Uma boundary pode ser definida através de sub-redes IP, ranges IP, prefixos IPv6 e sites do AD.



Nota do DevMan

FSP (Fallback Status Point): Quando utilizado o parâmetro FSP, mensagens de status dos clientes que não foram instalados corretamente, não puderam ser designadas a um site específico ou não puderam se comunicar de forma segura com o management point serão enviadas ao servidor SCCM.

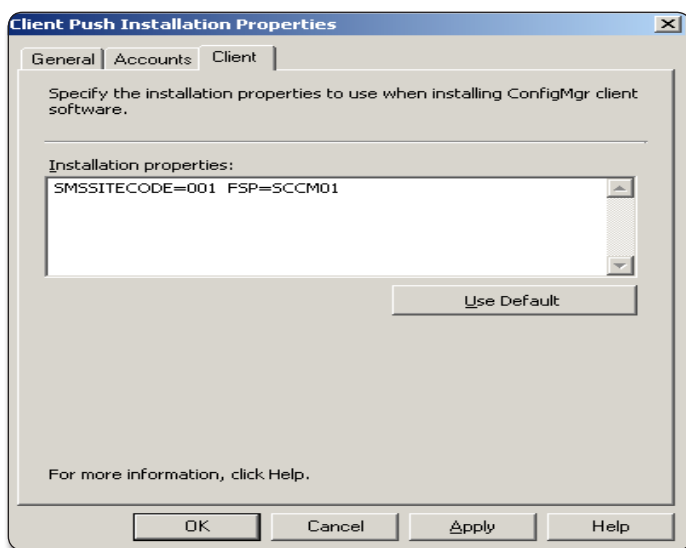


Figura 3. Client Push Installation Properties – Aba Client.

7. Clique **OK** duas vezes.

Agora que já habilitamos o método push, temos que configurar as opções de segurança para que a instalação seja feita com sucesso. Na próxima seção veremos como configurar essas informações via **GPO (Group Policy Object)**. A GPO é capaz de mudar configurações, restringir ações ou até mesmo distribuir aplicações em seu ambiente de rede. As vantagens são muitas, e podem ser aplicadas em sites, domínios e organizational units (OUs).

Configurando as opções de segurança via GPO

Quando ocorre a instalação via método push, alguns computadores podem não receber o software devido às configurações de segurança. Isso pode ser verificado no arquivo de log *ccm.log* onde pode-se encontrar as seguintes situações:

- O usuário que está sendo utilizado para instalar o cliente ou o servidor SCCM não pertence ao grupo de administradores locais da estação;

• A estação possui o firewall do Windows habilitado e sem as devidas configurações, isto é, permitindo o compartilhamento de arquivos e acesso remoto ao WMI (*Windows Management Instrumentation*).

Para corrigirmos os problemas acima citados, de forma centralizada, devemos:

- Configurar a conta usada para instalar o cliente como Administrador Local;
- Desabilitar ou criar exceções no firewall.



Nota do DevMan

GPO (Group Policy Object): GPO é um conjunto de configurações relacionadas à segurança e configurações de restrição para ambientes corporativos.

Configurando a conta usada para instalar o cliente como administrador local

A conta de usuário utilizada para instalar o cliente deve pertencer ao grupo Administradores Local da estação. Por padrão, o grupo “Domain Admins” e “Administrador” fazem parte desse grupo, porém, adicionar o usuário ao grupo “Domain Admins” não é uma prática de segurança recomendada, pois o usuário terá mais direitos do que necessita. Uma alternativa é adicionar o usuário manualmente ao grupo de administradores locais, estação por estação, algo trabalhoso quando muitas máquinas estão envolvidas. Nesse caso, podemos utilizar GPO para facilitar a tarefa.

Para configurar uma GPO, siga os passos:

1. Clique em **Start, Run** e digite **gpmc.msc** (ver Figura 4);
2. Na tela **Group Policy Management** expanda **Forest/Domains/SeuDomínio**. Clique com o botão direito do mouse em **Default Domain Policy** e escolha **Edit...** (ver Figura 5);
3. Feito isso, expanda **Computer Settings, Windows Settings, Security Settings** e clique em **Restricted Groups** (ver Figura 6);
4. Selecione **Restricted Groups** com o botão direito e clique em **Add Group** (ver Figura 7);
5. Em **Add Group** digite **Administrators**;
6. Em **Administrators Properties** clique em **Add**;
7. Em **Add Members** digite **Administrator** e clique **OK**. Repita o mesmo processo para **Domínio\Domain Admins** e para **Domínio\Usuário Push** (ver resultado na Figura 8);
8. Aguarde os clientes atualizarem as políticas ou atualize manualmente usando o comando **gpupdate /force** (ver Figura 9);
9. Para confirmar se os usuários foram adicionados à lista de Administradores locais, clique em **Start, Settings, Control Panel, Administrative Tools** e **Computer Management** (ver Figura 10);
10. Em **Computer Management**, expanda **Local Users and Group** e clique em **Groups**. Na lista de grupos, dê um duplo clique em **Administrators** para abrir suas propriedades (ver Figura 11).

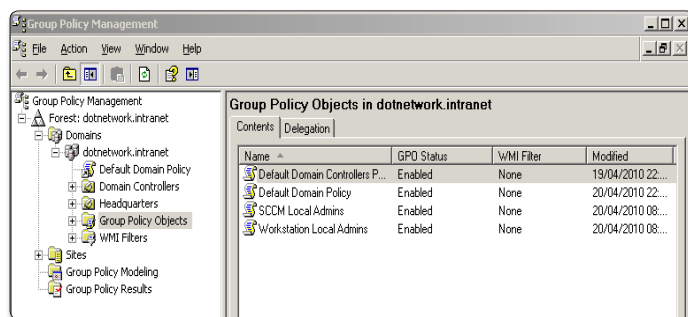


Figura 4. Group Policy Management

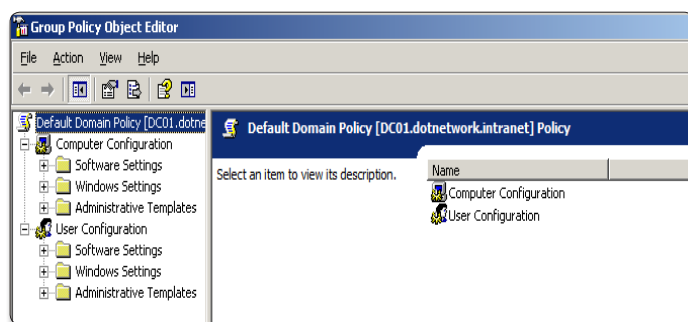


Figura 5. Group Policy Object Editor

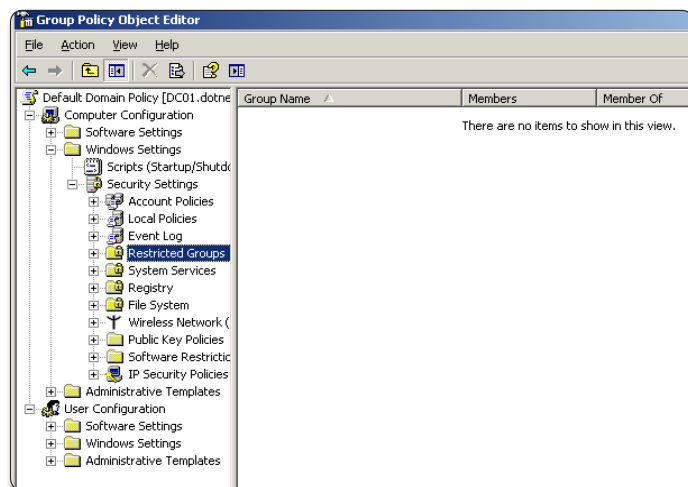


Figura 6. Group Policy Object Editor – Restricted Groups

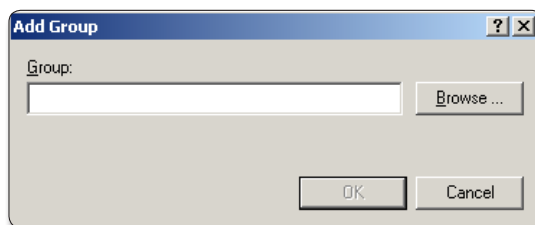


Figura 7. Add Group

Agora que já adicionamos o usuário que será responsável pela instalação do software cliente como administrador local das estações, é hora de configurarmos o firewall da estação, conforme veremos na próxima seção.

Configurando o firewall

Caso as políticas da empresa não permitam desabilitar o firewall, basta criarmos duas exceções, uma sendo **Compartilhamento de Arquivos e Impressoras** e a outra para o **acesso remoto ao WMI (Windows Management Instrumentation)**.

Estas tarefas são simples, porém trabalhosas quando muitas máquinas estão envolvidas. Nesse caso (mais uma vez) podemos utilizar uma **GPO** para facilitar a tarefa.

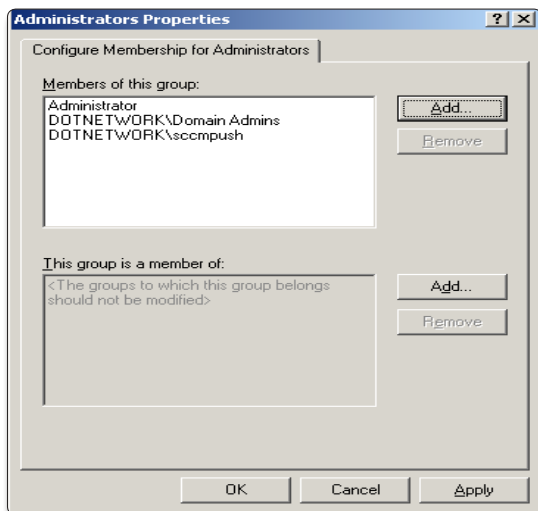


Figura 8. Janela Administrators Properties

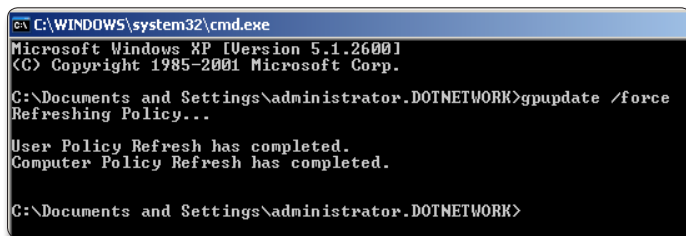


Figura 9. Utilizando o comando gpupdate

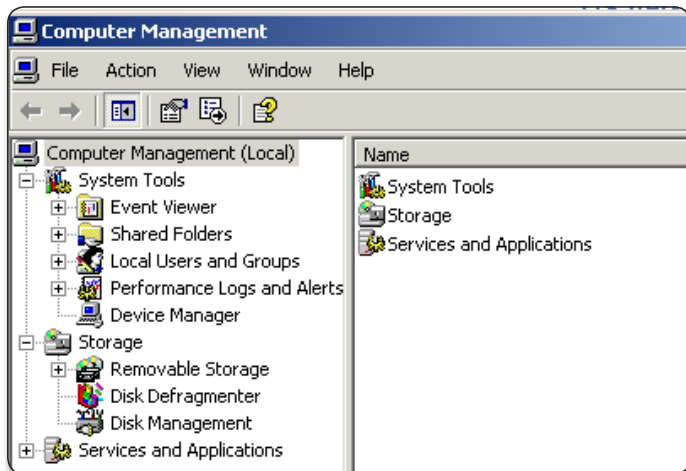


Figura 10. Computer Management

Para configurar esta **GPO**, siga os passos:

1. Clique em **Start, Run** e digite **gpmc.msc** (ver Figura 4);
2. Na tela **Group Policy Management** expanda **Forest/Domains/SeuDomínio**. Clique com o botão direito do mouse em **Default Domain Policy** e escolha **Edit...** (ver Figura 12); Expanda **Computer Settings, Administrative Templates, Network, Network Connections, Windows Firewall** e **Domain Profile** (ver Figura 13);

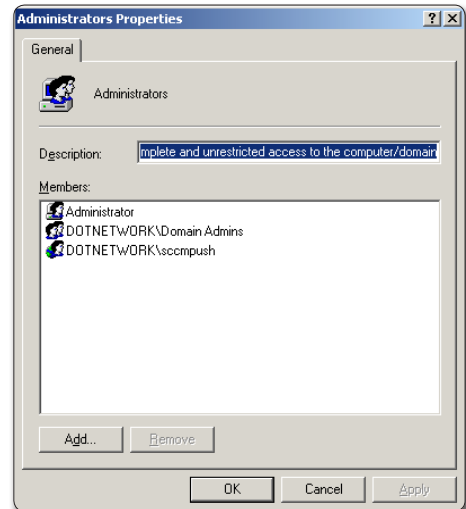


Figura 11. Administrators Properties.

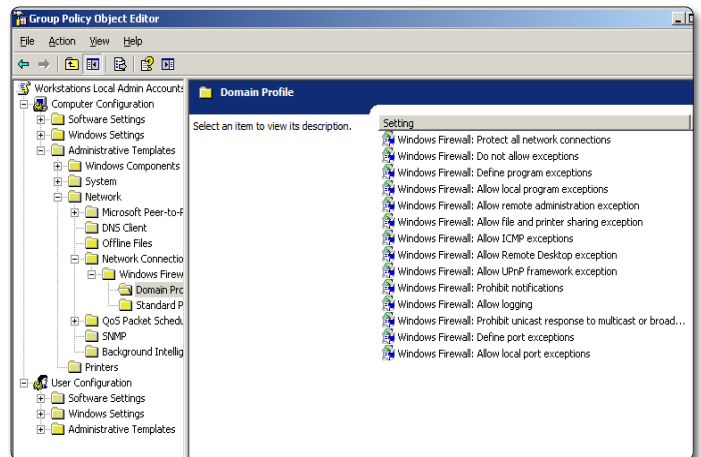


Figura 12. Group Policy Object Editor

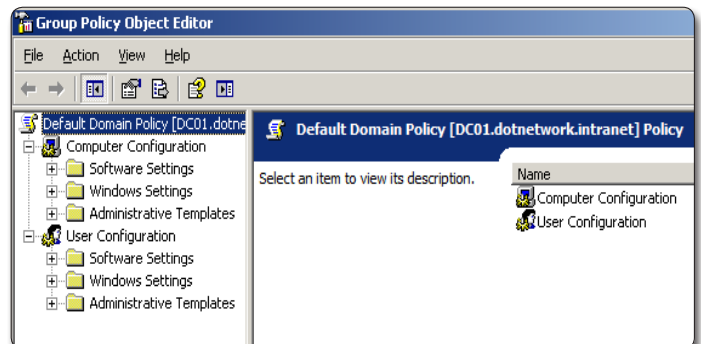


Figura 13. Group Policy Object Editor – Windows Firewall

3. Edite **Windows Firewall: Do not allow exceptions** e selecione **Disabled**. Isso faz com que exceções possam ser adicionadas ao firewall (ver **Figura 14**);
4. Edite **Windows Firewall: Allow remote administration exception**, selecione **Enabled** e em **Allow unsolicited incoming messages from** coloque o endereço IP do servidor SCCM e do Management Point. Isso faz com que apenas os servidores SCCM possam ter acesso ao WMI, mantendo assim um nível de segurança alto (ver **Figura 14**);
5. Edite **Windows Firewall: Allow file and printer sharing exceptions**, selecione **Enabled** e em **Allow unsolicited incoming messages from** coloque o endereço IP do servidor SCCM e do Management Point. Isso faz com que apenas os servidores SCCM possam ter acesso às pastas compartilhadas, mantendo assim um nível de segurança alto (ver **Figura 15**);
6. Aguarde os clientes atualizarem as políticas ou atualize manualmente usando o comando **gpupdate /force** (ver **Figura 16**);
7. Para confirmar se as regras do firewall foram habilitadas, clique em **Start, Settings, Control Panel** e em **Security Center** (ver **Figura 17**);
8. E depois clique em **Windows Firewall** e selecione a aba **Exceptions** (ver **Figura 18**).

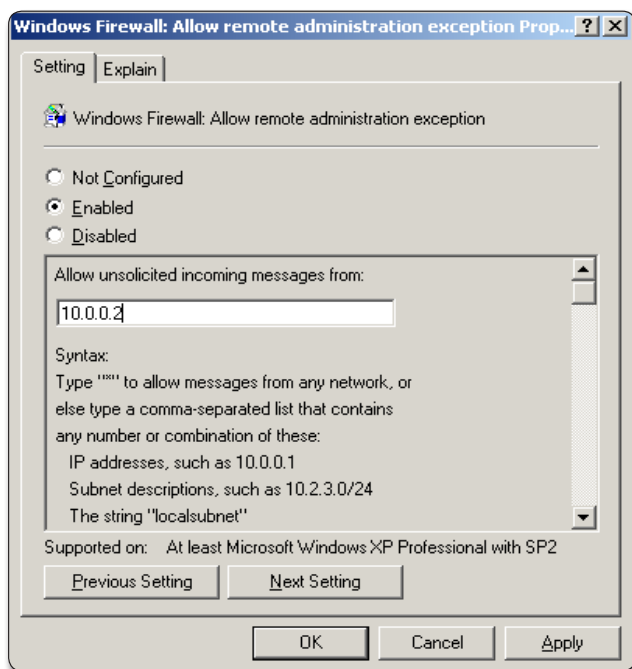


Figura 14. Windows Firewall: Remove Administration

Agora que já vimos como configurar as opções de segurança necessárias, devemos estar prontos para dar suporte quando algum cliente não for instalado.

Troubleshooting de instalação de clientes

Caso exista algum problema na instalação do cliente, as seguintes informações devem ser analisadas:

1. Verifique se o cliente está no mesmo **Site Boundary** definido para o site;
2. Verifique se o cliente está utilizando um servidor Wins nas propriedades de rede. Em caso de estar utilizando WINS para prover informações sobre o **Server Locator Point**:

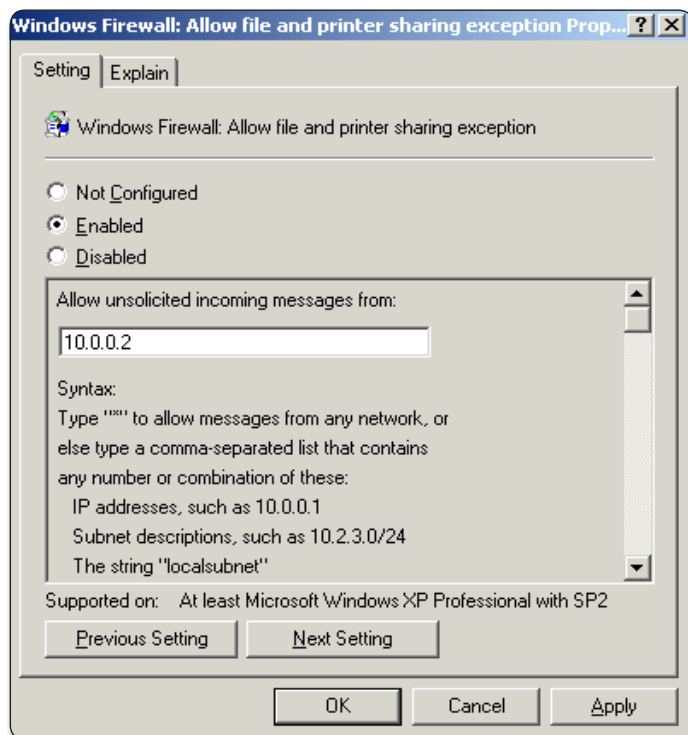


Figura 15. Windows Firewall: File and Printer

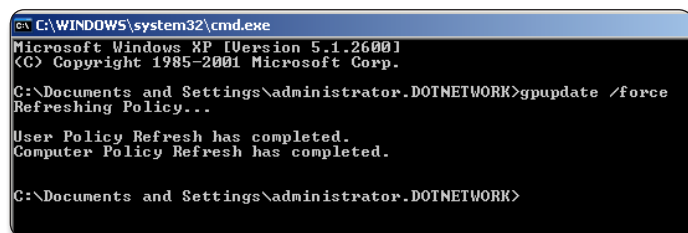


Figura 16. Utilizando o comando gpupdate



Figura 17. Windows Security Center

- a. Verifique se a conta utilizada pelo método push não está bloqueada no Active Directory Users and Computers.
 - b. Verifique se a resolução de nomes (Wins e DNS), tanto do servidor SCCM quanto do cliente, estão funcionando corretamente.
 3. Verifique se o cliente possui ao menos 5MB de espaço disponível;
 4. Verifique os logs criados em <DIRETÓRIO DE INSTALAÇÃO>\ccmsetup*.log;
 5. Expanda **Site Database**, **System Status**, **Site Status**, <Código do Site> e então clique em **Component Status**. Clique com o botão direito em **SMS_CLIENT_CONFIG_MANAGER**, selecione **Show Messages** e clique em **All** (ver Figura 19);
 6. Verifique a existência da **Message ID 3014**. Ela significa erro na instalação do cliente SCCM (ver Figura 20);
 7. Caso exista esse ID, as possíveis causas de erro são:
 - a. O computador não está acessível;
 - b. O computador está bloqueando a instalação do cliente SCCM.
- Desabilite o Firewall ou permita acesso do SCCM Server à porta local RPC TCP 135, ao Compartilhamento de Arquivos e WMI

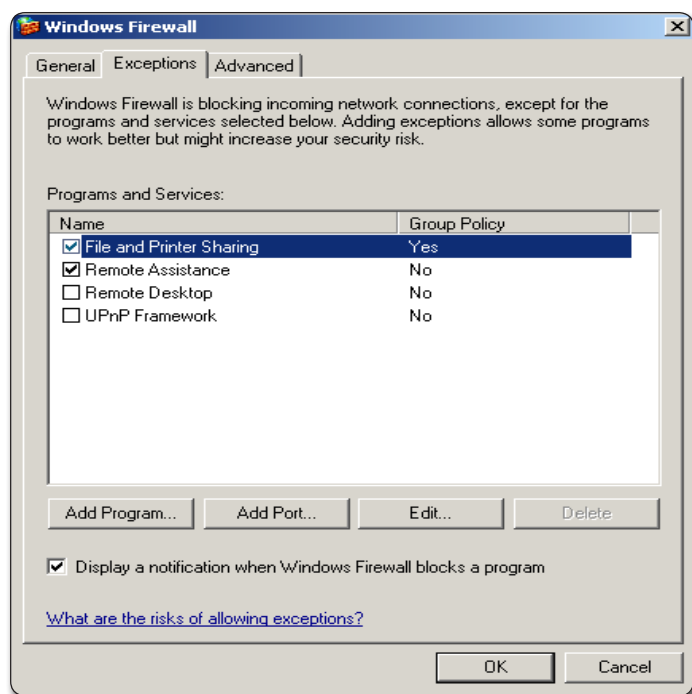


Figura 18. Windows Firewall

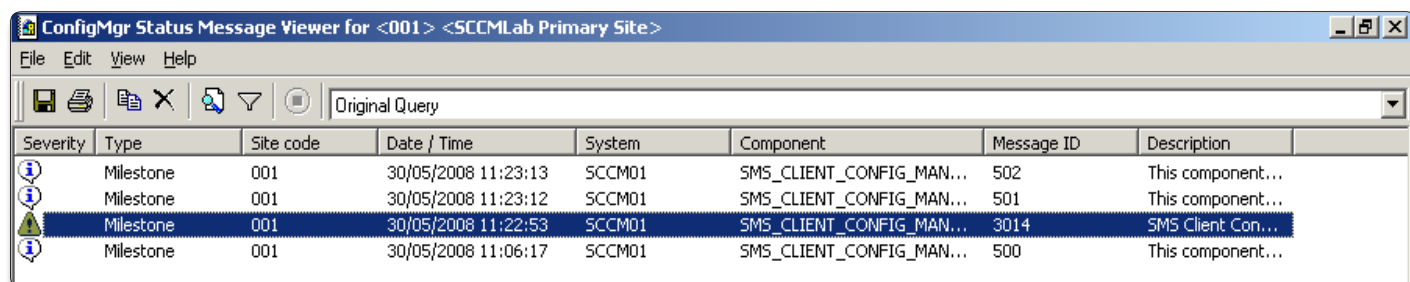


Figura 19. ConfigMgr Status Message

- Remoto (use o comando **netsh firewall set service remoteadmin enable** para habilitar o WMI Remoto ou uma GPO, conforme visto anteriormente);
- c. A conta de usuário que está sendo utilizada para instalar o cliente SCCM não está no grupo Local Administrators.
 8. Se utilizar um Windows 2000 com **BITS (Background Intelligent Transfer Service)** inferior ao 2.0, o processo irá instalar automaticamente a versão 2.0 e será necessário reiniciar o computador para finalizar a instalação;
 9. Verifique se a conta de máquina do computador em que está sendo instalado o cliente possui acesso de leitura à pasta \\NOME DO SERVIDOR\SMS-< CÓDIGO DO SITE >\Client. Caso não seja possível dar direitos de leitura a essa conta, instale o cliente manualmente /noservice ao final da linha de comando;
 10. Se for necessário, verifique mais informações no arquivo de log gerado em: <DIRETÓRIO DE INSTALAÇÃO DO SCCM>\Logs\ccm.log.

Quando ocorre algum problema com a instalação do cliente, o SCCM tenta instalá-lo novamente. Veremos os detalhes deste procedimento na próxima seção.



Nota do DevMan

BITS (Background Intelligent Transfer Service): Serviço do sistema operacional que facilita a transferência de arquivos entre computadores usando a largura de banda não utilizada.

CCRRetry

Quando a instalação do cliente iniciada pelo método push falha, o SCCM tenta novamente instalar o cliente, uma vez por hora, durante, no máximo, 168 horas. Depois disso, desiste. Cada vez que o SCCM tenta instalar o cliente e falha, o seguinte processo ocorre:

1. A linha **Stored request** "<Nome do computador>_<DOMINIO>", **machine name** "<Nome do computador>", in queue **"Retry"** será adicionada ao arquivo *ccm.log* (ver Figura 21);
2. Um arquivo <Nome do Computador>_<Nome do Dominio>.ccr será criado em <DIRETORIO DE INSTALACAO>\inboxes\ccrretry.box (ver Figura 22);
3. Ao abrirmos o arquivo no notepad, podemos ver qual a real causa do erro procurando por **Last Error Code** (ver Figura 23);

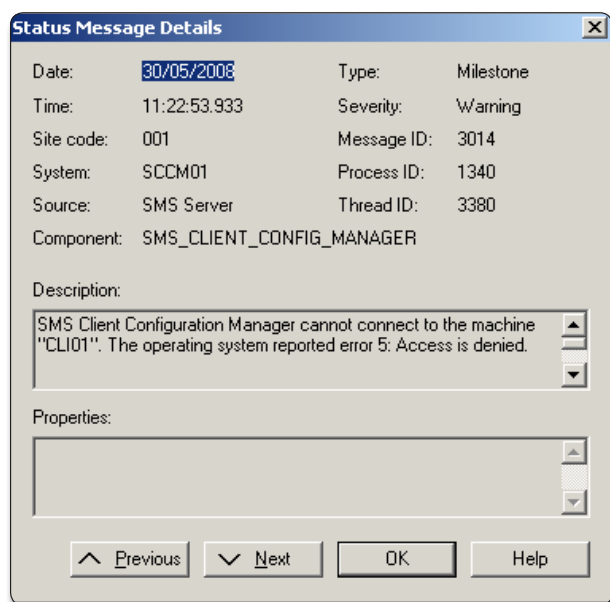


Figura 20. Message Details

4. Usando o comando **net helpmsg <Código do Erro>** no prompt de comando, podemos ver uma descrição do erro (ver Figura 24).

É interessante o processo de tentativa de instalação em caso de falha, mas como saber se o processo foi concluído com sucesso ou não e qual as possíveis causas de cada problema?

Exemplos de linha log e possíveis causas

Visualizar linhas de log nem sempre é uma tarefa fácil, ainda mais se não temos como compará-las com outras. Abaixo, apresentamos algumas das linhas de código que podem ser encontradas quando trabalhando com a instalação de clientes.

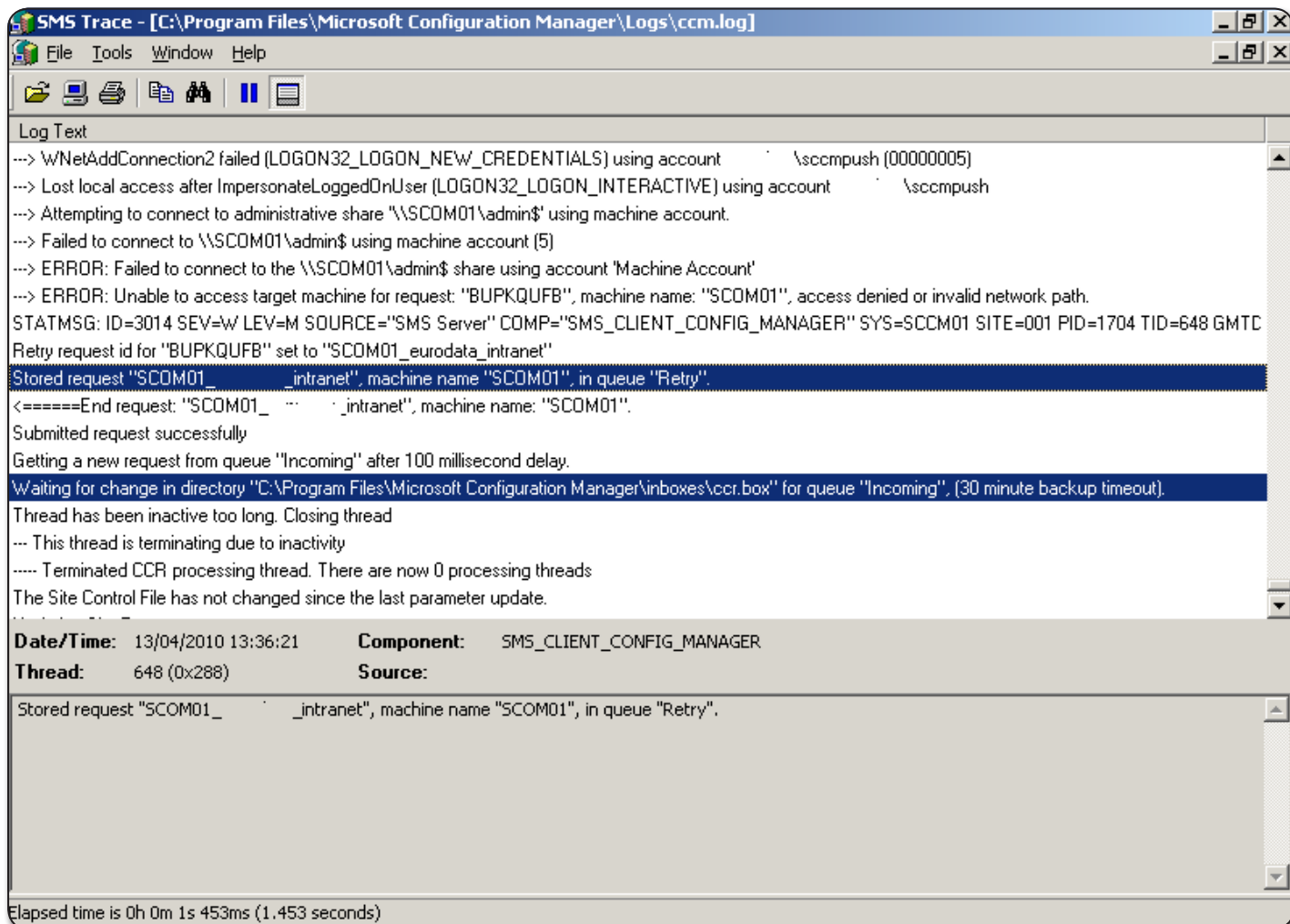


Figura 21. SMS Trace

No **exemplo 01**, o usuário utilizado pelo método push não é o administrador local da estação onde será instalado o cliente do SCCM, como podemos ver na linha 14 da **Listagem 1**.

Para remediar esta situação, basta adicionar o usuário ao grupo de administradores locais. Para mais informações, veja a seção “Configurando a conta usada para instalar o cliente como administrador local”.

No **exemplo 02**, o firewall do windows está habilitado mas sem nenhuma exceção, como podemos ver na linha 14 da **Listagem 2**.

Para remediar esta situação, basta configurar o firewall para aceitar conexões do tipo WMI Remoto e Compartilhamento de arquivos e impressoras oriundas do servidor SCCM e Management Point. Para mais informações, veja a seção “Configurando o firewall”.

No **exemplo 03**, o firewall do Windows está habilitado, mas apenas com o compartilhamento de arquivos e impressoras como exceções. Neste exemplo, o firewall está bloqueando acesso WMI remoto, como podemos ver na linha 15 da **Listagem 3**.

Para remediar esta situação, basta configurar o firewall para aceitar conexões do tipo WMI Remoto oriundas do servidor SCCM e Management Point. Para mais informações, veja a seção “Configurando o firewall”.

No **exemplo 04**, o usuário utilizado pelo método push é o administrador local da estação e o firewall do Windows está habilitado e configurado da forma correta, como podemos ver na linha 19 da **Listagem 4**.

Este é o caso onde tudo ocorre de forma correta, a única exceção que vemos no log acontece devido à tentativa de conexão ao WMI Remoto, com o erro sendo 0x8004100e (linha 13). Este é um erro normal, pois o SCCM tenta conectar a uma parte do WMI existente apenas quando um cliente do SCCM já está instalado. Por conta disso, não existe nada para se preocupar.

Por fim, no **exemplo 05**, o usuário utilizado pelo método push é o admi-

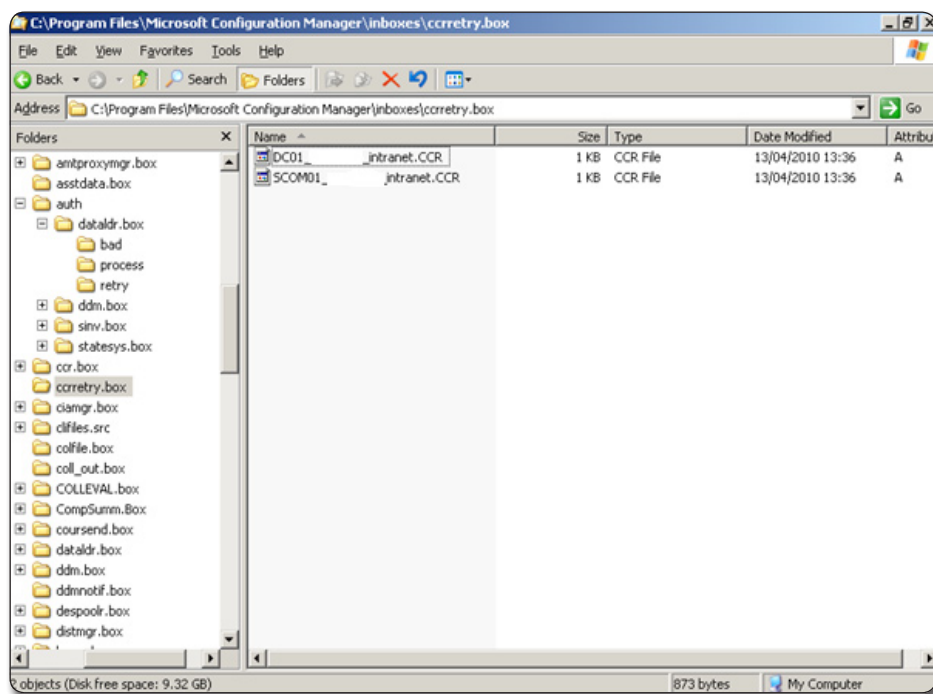


Figura 22. Windows Explorer

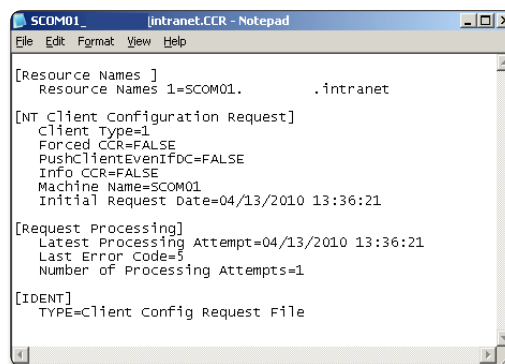


Figura 23. Exemplo de arquivo CCR

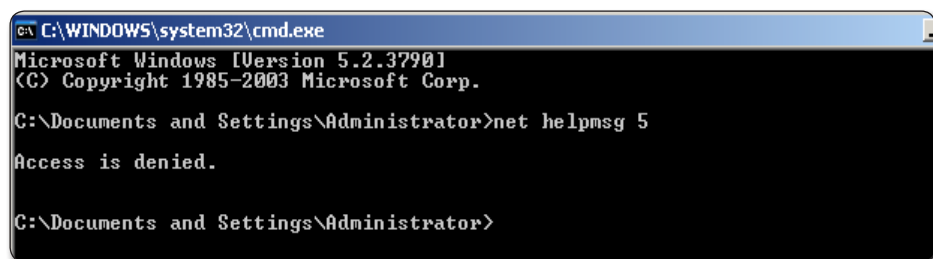


Figura 24. Net helpmsg

nistrador local da estação, o firewall do Windows está habilitado e configurado da forma correta e já existe um cliente do SCCM instalado, sendo necessária apenas a atualização para uma nova versão, como podemos ver na linha 12 da **Listagem 5**.

Conclusão

A utilização do método Push para instalação de clientes é a mais conhecida e utilizada pelos administradores do SCCM. Saber como funciona e como resolver problemas mais comuns é uma das tarefas diárias do administrador SCCM. Neste ar-

Listagem 1. Log do exemplo 01.

01. Received request: "LVGBTRAK" for machine name: "XP02" on queue: "Incoming".	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:40	2456 (0x0998)
02. Stored request "LVGBTRAK", machine name "XP02", in queue "Processing".	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:40	2456 (0x0998)
03. ----- Started a new CCR processing thread. Thread ID is 0x690. There are now 1 processing threads	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	2456 (0x0998)
04. Submitted request successfully	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	2456 (0x0998)
05. Getting a new request from queue "Incoming" after 100 millisecond delay.	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	2456 (0x0998)
06. Waiting for change in directory "C:\Program Files\Microsoft Configuration Manager\inboxes\ccr.box" for queue "Incoming", (30 minute backup timeout).	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	2456 (0x0998)
07. =====>Begin Processing request: "LVGBTRAK", machine name: "XP02"	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
08. --> Trying each entry in the SMS Client Remote Installation account list	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
09. --> Attempting to connect to administrative share "\\XP02.dotnetwork.intranet\admin\$" using account 'dotnetwork\scmcpush'	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
10. --> WNetAddConnection2 failed (LOGON32_LOGON_NEW_CREDENTIALS) using account dotnetwork\scmcpush (00000005)	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
11. --> Lost local access after ImpersonateLoggedOnUser (LOGON32_LOGON_INTERACTIVE) using account dotnetwork\scmcpush	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
12. --> Attempting to connect to administrative share "\\XP02.dotnetwork.intranet\admin\$" using machine account.	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
13. --> Failed to connect to \\XP02.dotnetwork.intranet\admin\$ using machine account (5)	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
14. --> ERROR: Failed to connect to the \\XP02.dotnetwork.intranet\admin\$ share using account 'Machine Account'	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
15. --> Trying each entry in the SMS Client Remote Installation account list	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
16. --> Attempting to connect to administrative share "\\XP02\admin\$" using account 'dotnetwork\scmcpush'	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
17. --> WNetAddConnection2 failed (LOGON32_LOGON_NEW_CREDENTIALS) using account dotnetwork\scmcpush (00000005)	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
18. --> Lost local access after ImpersonateLoggedOnUser (LOGON32_LOGON_INTERACTIVE) using account dotnetwork\scmcpush	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
19. --> Attempting to connect to administrative share "\\XP02\admin\$" using machine account.	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
20. --> Failed to connect to \\XP02\admin\$ using machine account (5)	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
21. --> ERROR: Failed to connect to the \\XP02\admin\$ share using account 'Machine Account'	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
22. --> ERROR: Unable to access target machine for request: "LVGBTRAK", machine name: "XP02", access denied or invalid network path.	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:42	1680 (0x0690)
23. STATMSG: ID=3014 SEV=W LEV=M SOURCE="SMS Server" COMP="SMS_CLIENT_CONFIG_MANAGER" SYS=SCCM01 SITE=001 PID=1948 TID=1680 GMTDATE=Thu Feb 04 16:08:42.997			
2010 ISTR0="XP02" ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:43	1680 (0x0690)
24. Retry request id for "LVGBTRAK" set to "XP02_dotnetwork_intranet"	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:43	1680 (0x0690)
25. Stored request "XP02_dotnetwork_intranet", machine name "XP02", in queue "Retry".	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:43	1680 (0x0690)
26. <=====End request: "XP02_dotnetwork_intranet", machine name: "XP02".	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:08:43	1680 (0x0690)

Listagem 2. Log do exemplo 02.

01. Received request: "HDMCICYP" for machine name: "XP02" on queue: "Incoming".	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:45:56	2692 (0x0A84)
02. Stored request "HDMCICYP", machine name "XP02", in queue "Processing".	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:45:56	2692 (0x0A84)
03. ----- Started a new CCR processing thread. Thread ID is 0xad. There are now 1 processing threads	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:45:58	2692 (0x0A84)
04. Submitted request successfully	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:45:58	2692 (0x0A84)
05. =====>Begin Processing request: "HDMCICYP", machine name: "XP02"	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:45:58	2780 (0x0ADC)
06. Getting a new request from queue "Incoming" after 100 millisecond delay.	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:45:58	2692 (0x0A84)
07. Waiting for change in directory "C:\Program Files\Microsoft Configuration Manager\inboxes\ccr.box" for queue "Incoming", (30 minute backup timeout).	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:45:58	2692 (0x0A84)
08. --> Trying each entry in the SMS Client Remote Installation account list	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:45:58	2780 (0x0ADC)
09. --> Attempting to connect to administrative share "\\XP02.dotnetwork.intranet\admin\$" using account 'dotnetwork\scmcpush'	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:45:58	2780 (0x0ADC)
10. --> WNetAddConnection2 failed (LOGON32_LOGON_NEW_CREDENTIALS) using account dotnetwork\scmcpush (000004b3)	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:28	2780 (0x0ADC)
11. --> WNetAddConnection2 failed (LOGON32_LOGON_INTERACTIVE) using account dotnetwork\scmcpush (000004b3)	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:29	2780 (0x0ADC)
12. --> Attempting to connect to administrative share "\\XP02.dotnetwork.intranet\admin\$" using machine account.	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:30	2780 (0x0ADC)
13. --> Failed to get token for current process (5)	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:30	2780 (0x0ADC)
14. --> ERROR: Failed to connect to the \\XP02.dotnetwork.intranet\admin\$ share using account 'Machine Account'	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:30	2780 (0x0ADC)
15. --> Trying each entry in the SMS Client Remote Installation account list	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:30	2780 (0x0ADC)
16. --> Attempting to connect to administrative share "\\XP02\admin\$" using account 'dotnetwork\scmcpush'	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:30	2780 (0x0ADC)
17. --> WNetAddConnection2 failed (LOGON32_LOGON_NEW_CREDENTIALS) using account dotnetwork\scmcpush (000004b3)	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:55	2780 (0x0ADC)
18. --> WNetAddConnection2 failed (LOGON32_LOGON_INTERACTIVE) using account dotnetwork\scmcpush (000004b3)	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:55	2780 (0x0ADC)
19. --> Attempting to connect to administrative share "\\XP02\admin\$" using machine account.	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:55	2780 (0x0ADC)
20. --> Failed to get token for current process (5)	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:55	2780 (0x0ADC)
21. --> ERROR: Failed to connect to the \\XP02\admin\$ share using account 'Machine Account'	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:55	2780 (0x0ADC)
22. --> ERROR: Unable to access target machine for request: "HDMCICYP", machine name: "XP02", access denied or invalid network path.	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:55	2780 (0x0ADC)
23. STATMSG: ID=3014 SEV=W LEV=M SOURCE="SMS Server" COMP="SMS_CLIENT_CONFIG_MANAGER" SYS=SCCM01 SITE=001 PID=1728 TID=2780 GMTDATE=Thu Apr 09 13:46:55.654 2009			
ISTR0="XP02" ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:55	2780 (0x0ADC)
24. Retry request id for "HDMCICYP" set to "XP02_dotnetwork_intranet"	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:55	2780 (0x0ADC)
25. Stored request "XP02_dotnetwork_intranet", machine name "XP02", in queue "Retry".	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:55	2780 (0x0ADC)
26. <=====End request: "XP02_dotnetwork_intranet", machine name: "XP02".	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:46:55	2780 (0x0ADC)
27. Thread has been inactive too long. Closing thread	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:56:55	2780 (0x0ADC)
28. -- This thread is terminating due to inactivity	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:56:55	2780 (0x0ADC)
29. ----- Terminated CCR processing thread. There are now 0 processing threads	SMS_CLIENT_CONFIG_MANAGER	09/04/2009 14:56:55	2780 (0x0ADC)

Listagem 3. Log do exemplo 03.

01. Waiting for change in directory "C:\Program Files\Microsoft Configuration Manager\inboxes\ccr.box" for queue "Incoming"; (30 minute backup timeout).	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:39:56	2696 (0x0A88)
02. Received request: "IYZNCMWI" for machine name: "XP02" on queue: "Incoming".	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:39:56	2696 (0x0A88)
03. Stored request "IYZNCMWI", machine name "XP02", in queue "Processing".	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:39:56	2696 (0x0A88)
04. ---- Started a new CCR processing thread. Thread ID is 0x47c. There are now 1 processing threads	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:39:58	2696 (0x0A88)
05. Submitted request successfully	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:39:58	2696 (0x0A88)
06. Getting a new request from queue "Incoming" after 100 millisecond delay.	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:39:58	2696 (0x0A88)
07. Waiting for change in directory "C:\Program Files\Microsoft Configuration Manager\inboxes\ccr.box" for queue "Incoming"; (30 minute backup timeout).	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:39:58	2696 (0x0A88)
08. =====>Begin Processing request: "IYZNCMWI", machine name: "XP02"	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:39:58	1148 (0x047C)
09. --> Trying each entry in the SMS Client Remote Installation account list	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:39:58	1148 (0x047C)
10. --> Attempting to connect to administrative share "\\XP02.dotnetwork.intranet\admin\$" using account 'dotnetwork\scmpush'	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:39:58	1148 (0x047C)
11. --> Connected to administrative share on machine XP02.dotnetwork.intranet using account 'dotnetwork\scmpush'	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:39:59	1148 (0x047C)
12. --> Attempting to make IPC connection to share <\\XP02.dotnetwork.intranet\IPC>	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:39:59	1148 (0x047C)
13. --> Searching for SMSClientInstall.* under "\\XP02.dotnetwork.intranet\admin\$\	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:39:59	1148 (0x047C)
14. CWmi:Connect(): ConnectServer(Namespace) failed. - 0x800706ba	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:40:00	1148 (0x047C)
15. --> Unable to connect to WMI on remote machine "XP02"; error = 0x800706ba.	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:40:00	1148 (0x047C)
16. --> Deleting SMS Client Install Lock File "\\XP02.dotnetwork.intranet\admin\$\SMSClientInstall.001"	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:40:00	1148 (0x047C)
17. Retry request id for "IYZNCMWI" set to "XP02_dotnetwork_intranet"	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:40:00	1148 (0x047C)
18. Stored request "XP02_dotnetwork_intranet", machine name "XP02", in queue "Retry".	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:40:00	1148 (0x047C)
19. <=====End request: "XP02_dotnetwork_intranet", machine name: "XP02".	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:40:00	1148 (0x047C)

Listagem 4. Log do exemplo 04.

01. Waiting for change in directory "C:\Program Files\Microsoft Configuration Manager\inboxes\ccr.box" for queue "Incoming"; (30 minute backup timeout).	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:43:59	2696 (0x0A88)
02. Received request: "WOREIUXI" for machine name: "XP02" on queue: "Incoming".	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:43:59	2696 (0x0A88)
03. Stored request "WOREIUXI", machine name "XP02", in queue "Processing".	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:43:59	2696 (0x0A88)
04. =====>Begin Processing request: "WOREIUXI", machine name: "XP02"	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:43:59	1148 (0x047C)
05. --> Trying the 'best-shot' account which worked for previous CCRs (index = 0x0)	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:43:59	1148 (0x047C)
06. --> Attempting to connect to administrative share "\\XP02.dotnetwork.intranet\admin\$" using account 'dotnetwork\scmpush'	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:43:59	1148 (0x047C)
07. --> The 'best-shot' account has now succeeded 1 times and failed 0 times.	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:43:59	1148 (0x047C)
08. --> Connected to administrative share on machine XP02.dotnetwork.intranet using account 'dotnetwork\scmpush'	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:43:59	1148 (0x047C)
09. --> Attempting to make IPC connection to share <\\XP02.dotnetwork.intranet\IPC>	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:43:59	1148 (0x047C)
10. --> Searching for SMSClientInstall.* under "\\XP02.dotnetwork.intranet\admin\$\	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:43:59	1148 (0x047C)
11. --> System OS version string "5.1.2600" converted to 5.10	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:43:59	1148 (0x047C)
12. --> Service Pack version from machine "XP02" is 2	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:43:59	1148 (0x047C)
13. CWmi:Connect(): ConnectServer(Namespace) failed. - 0x8004100e	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:00	1148 (0x047C)
14. --> Unable to connect to WMI (r) on remote machine "XP02"; error = 0x8004100e.	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:00	1148 (0x047C)
15. --> Creating \VerifyingCopying existence of destination directory \\XP02\admin\$\system32\ccmsetup.	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:00	1148 (0x047C)
16. --> Copying client files to \\XP02\admin\$\system32\ccmsetup.	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:00	1148 (0x047C)
17. --> Copying file "C:\Program Files\Microsoft Configuration Manager\bin\I386\MobileClient.tcf" to "\\XP02\admin\$\system32\ccmsetup\MobileClient.tcf"	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:00	1148 (0x047C)
18. --> Created service "ccmsetup" on machine "XP02".	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:00	1148 (0x047C)
19. Submitted request successfully	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:01	2696 (0x0A88)
20. Getting a new request from queue "Incoming" after 100 millisecond delay.	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:01	2696 (0x0A88)
21. Waiting for change in directory "C:\Program Files\Microsoft Configuration Manager\inboxes\ccr.box" for queue "Incoming"; (30 minute backup timeout).	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:01	2696 (0x0A88)
22. --> Started service "ccmsetup" on machine "XP02".	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:01	1148 (0x047C)
23. --> Deleting SMS Client Install Lock File "\\XP02.dotnetwork.intranet\admin\$\SMSClientInstall.001"	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:01	1148 (0x047C)
24. --> Completed request "WOREIUXI", machine name "XP02".	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:01	1148 (0x047C)
25. Deleted request "WOREIUXI", machine name "XP02"	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:01	1148 (0x047C)
26. <=====End request: "WOREIUXI", machine name: "XP02".	SMS_CLIENT_CONFIG_MANAGER	17/04/2009 14:44:01	1148 (0x047C)

Listagem 5. Log do exemplo 05.

01. Received request: "LPCTBIOM" for machine name: "XP02" on queue: "Incoming".	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:01	2456 (0x0998)
02. Stored request "LPCTBIOM", machine name "XP02", in queue "Processing".	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:01	2456 (0x0998)
03. =====>Begin Processing request: "LPCTBIOM", machine name: "XP02"	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:01	1680 (0x0690)
04. --> Trying the 'best-shot' account which worked for previous CCRs (index = 0x0)	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:01	1680 (0x0690)
05. --> Attempting to connect to administrative share "\\XP02.dotnetwork.intranet\admin\$" using account 'dotnetwork\scmpush'	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:01	1680 (0x0690)
06. --> The 'best-shot' account has now succeeded 1 times and failed 0 times.	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:02	1680 (0x0690)
07. --> Connected to administrative share on machine XP02.dotnetwork.intranet using account 'dotnetwork\scmpush'	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:02	1680 (0x0690)
08. --> Attempting to make IPC connection to share <\\XP02.dotnetwork.intranet\IPC>	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:02	1680 (0x0690)
09. --> Searching for SMSClientInstall.* under "\\XP02.dotnetwork.intranet\admin\$\	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:02	1680 (0x0690)
10. --> System OS version string "5.1.2600" converted to 5.10	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:02	1680 (0x0690)
11. --> Service Pack version from machine "XP02" is 2	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:02	1680 (0x0690)
12. --> Mobile client on the target machine has the same version, and 'forced' flag is turned on.	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:02	1680 (0x0690)
13. --> Creating \VerifyingCopying existence of destination directory \\XP02\admin\$\system32\ccmsetup.	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:02	1680 (0x0690)
14. --> Copying client files to \\XP02\admin\$\system32\ccmsetup.	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:02	1680 (0x0690)
15. --> Copying file "C:\Program Files\Microsoft Configuration Manager\bin\I386\MobileClient.tcf" to "\\XP02\admin\$\system32\ccmsetup\MobileClient.tcf"	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:02	1680 (0x0690)
16. --> Created service "ccmsetup" on machine "XP02".	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:03	1680 (0x0690)
17. --> Started service "ccmsetup" on machine "XP02".	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:03	1680 (0x0690)
18. --> Deleting SMS Client Install Lock File "\\XP02.dotnetwork.intranet\admin\$\SMSClientInstall.001"	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:03	1680 (0x0690)
19. --> Completed request "LPCTBIOM", machine name "XP02".	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:03	1680 (0x0690)
20. Deleted request "LPCTBIOM", machine name "XP02"	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:03	1680 (0x0690)
21. <=====End request: "LPCTBIOM", machine name: "XP02".	SMS_CLIENT_CONFIG_MANAGER	04/02/2010 16:19:03	1680 (0x0690)

neste artigo descrevemos o processo de instalação, como configurar tanto o servidor quanto os clientes e também como resolver alguns dos problemas mais comuns.

Como visto, utilizar o método Push não é muito complexo, mas requer determinados conhecimentos. Esperamos ter lhe ajudado a entendê-lo melhor e como utilizá-lo para facilitar a administração do SCCM.



Raphael Perez

dotraphael@gmail.com

Atua na área de TI desde 1994 e, desde 2000, com infraestrutura Microsoft. É graduado em Processamento de Dados e pós-graduado em Redes de Computadores e Telecomunicações, além de possuir as seguintes certificações: MCSA + Security, MCSE + Security, MCTS, MCITP, MCT e MVP. Atualmente trabalha como Consultor Técnico e está envolvido em Soluções de Segurança Microsoft e System Center Configuration Manager. Pode ser contactado através do web site www.dotnetwork.com.br ou blog.dotnetwork.com.br.



Configuração de Grupos restritos via GPO

[http://technet.microsoft.com/en-us/library/cc756802\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc756802(Ws.10).aspx)

Requisitos para Push de clientes

<http://technet.microsoft.com/en-us/library/bb632380.aspx>

Parâmetros que podem ser utilizados na instalação

<http://technet.microsoft.com/en-us/library/bb680980.aspx>

Portas utilizadas pelos clientes do SCCM

<http://technet.microsoft.com/en-us/library/bb694088.aspx>



FÓRUM DEV MEDIA

O lugar perfeito para você ficar por dentro de tudo o que acontece nas tecnologias do mercado atual



No novo Fórum da DevMedia você vai encontrar canais específicos de Delphi, ASP.NET, Java, Banco de Dados e Engenharia de Software; além de ter contato com profissionais qualificados da área para troca de informações, sugestões e muito mais.

ACESSE AGORA
www.devmedia.com.br/forum

Gerenciando Ambientes Complexos

Utilizando a família de produtos Microsoft System Center

MARCELO SINCIC

Gerenciar ambientes atualmente se tornou um desafio em razão da complexidade apresentada. Quando trabalhávamos no início da informática no Brasil, a linguagem de programação era Clipper, o sistema operacional era COM ou DOS e a plataforma de redes era Novell. Podíamos visitar dezenas de empresas que encontraríamos sempre os mesmos ambientes.

Hoje em dia, ao questionar ou visitar ambientes de clientes, frequentemente nos deparamos com os sistemas operacionais Windows e Linux, linguagens de programação como .NET, Java ou PHP, gerenciadores de banco de dados como SQL Server, Oracle, Firebird, dentre outros. Conhecer o ambiente do cliente, portanto, está mais difícil, não sendo à toa que levantamentos de ambiente para execução de projetos de reestrutura sejam tão comuns.

Agora imagine gerenciar estes ambientes, com dezenas de produtos diferentes, que vão desde o sistema operacional das estações até gerenciadores de documentos (GED) e de impressão customizados, além de aplicações web.

Somado a isto, ainda temos a necessidade e requisito de alta disponibilidade, não só do sistema operacional, mas de cada parte das aplicações e serviços individuais de rede.

Complexidade dos ambientes atuais

Quais seriam os problemas que a falta de ferramentas automatizadas para gerenciamento poderia trazer? Vejamos alguns deles e com certeza encontrará similaridades com situações já vivenciadas:

- Paradas de produção não planejadas: Ao não perceber erros e problemas quando estes começam a ocorrer, deixamos que o ambiente chegue ao estado crítico de parada do serviço;
- TI reativa e não proativa: Em ambientes não gerenciados os problemas são descobertos pelos usuários, quando não conseguem usar algum recurso, fazendo com que o seu sistema de alarme acabe sendo os usuários;
- Ambientes desorganizados e desconhecidos: A organização não sabe o que possui e muito menos quando algum dos componentes falha;
- A empresa não tem padrão para suporte: O mesmo problema é resolvido para diversos usuários, por vários técnicos e muitas vezes de formas diferentes e repetitivas;
- Procedimentos inadequados: Ao resolver um problema o técnico precisa procurar a solução individualmente e não registra em nenhum lugar;
- Dificuldades de comunicação com o usuário: Usuários não sabem a causa nem a sequência de um problema, apenas o sintoma.

Resumo DevMan

De que se trata o artigo:

Neste artigo veremos como gerenciar ambientes completos de TI com a família de produtos System Center da Microsoft

Em que situação o tema é útil:

Imagine gerenciar ambientes complexos, com dezenas de produtos diferentes, que vão desde o sistema operacional das estações, até gerenciadores de documentos (GED) e de impressão customizados, além de aplicações web. É neste cenário que está inserida a importância deste artigo.

Gerenciando Ambientes Complexos:

Este artigo demonstra algumas dificuldades que uma equipe de gerenciamento de TI enfrenta e como o uso de produtos da família System Center irá ajudar a controlar e gerenciar o ambiente completo e de forma unificada.

Sem sistema de gerenciamento é necessário “adivinhar” o que está acontecendo e depender do usuário para executar as correções;

- Muito tempo gasto com os mesmos problemas: Sem a base de conhecimento, um erro em cascata pode ser resolvido para diversos clientes ou equipamentos, na maioria das vezes atacando o sintoma e não a causa;
- Malefícios do parque desconhecido: Sem o parque inventariado, investimentos em hardware são para pessoas e não para aplicações, ou seja, “ganha” máquina nova quem grita mais alto e não quem tem necessidade de melhor equipamento;
- Licenciamento incorreto ou inexistente: Compra-se licença para 100 usuários quando apenas 60 realmente usam o software, mas o inverso também ocorre com frequência. Em outras situações, quem precisa de um software não tem a licença e esta pode estar instalada em outro equipamento para um usuário que não a utiliza;
- Investimentos mal direcionados: Gastos com licença e upgrades de hardware desnecessários, solução de pequenos problemas quando os maiores ficam em segundo plano e assim dificuldades conhecidas passam despercebidas;
- Problemas legais: Principalmente por causa do licenciamento incorreto e falta do inventário de software.

Além das citadas dificuldades gerenciais enfrentadas diariamente, temos problemas técnicos, em sua grande maioria, mais complexos, a exemplo:

- Gerenciar um parque de Virtual Machines;
- Gerenciar aplicações distribuídas em diversos computadores ou componentes;
- Distribuir softwares e atualizações de forma inteligente e sem sobrecarregar a rede;
- Atualizar o SO da máquina de forma “transparente” ao usuário;
- Controlar a frequência e efetividade na solução de chamados;
- Conhecer o parque de máquinas e direcionar ações a grupos específicos;
- Acompanhar o desempenho de servidores sem a necessidade de fazê-lo individualmente ou com leituras interpretativas manuais;
- Notificar os administradores de forma automática sobre problemas;
- Identificar ações preventivas ou mesmo proativas.

Para cada tipo de tarefa temos produtos que nos ajudam a gerenciar esta Babel que trabalhamos. Sendo assim, iremos focar os produtos da linha Microsoft System Center que permitem gerenciar, monitorar e controlar alterações em ambientes.

System Center Configuration Manager 2007 R3 (SCCM)

Conhecido anteriormente como SMS (System Management Server), é o produto mais antigo da família. Tem a finalidade de gerenciar um ambiente de infraestrutura da organização.

Originalmente, sua funcionalidade é inventariar software e hardware de toda a rede por meio do agente que é instalado no cliente. Porém, passou por uma evolução na questão dos inventários, em razão da funcionalidade *Asset Intelligence*, que compara os requisitos de um software no banco de dados de compatibilidade da Microsoft e indica, por exemplo, softwares que rodam em

uma estação e que não tem capacidade para tal. Também a esta funcionalidade podemos acrescentar a feature *Software Metering*, que permite o controle de licenças, por indicar quais softwares são utilizados realmente na empresa, reportando quantas vezes foi executado e aonde.

Outra funcionalidade importante do System Center Configuration Manager é a distribuição de software que, diferentemente do Active Directory, permite agendamento, distribuição por sistema operacional, data limite, instalação de batches ou execução de linhas de comando. A **Tabela 1** demonstra a diferença entre as funcionalidades do System Center Configuration Manager quando comparado ao Active Directory.

Recurso presente desde a versão SMS 1.0, o System Center Configuration Manager permite fazer acesso remoto à máquina do usuário. O acesso pode ser feito pelo Remote Desktop ou pela Assistência Remota do Windows.

A partir da versão do SMS 2.0, foi acrescentado um pacote chamado OSD (*Operating System Deployment*) que permite distribuir imagens de sistema operacional como se fosse um software. Porém, o System Center Configuration Manager tem a capacidade de copiar o perfil do usuário para o servidor, em seguida formatar a máquina do usuário e recolocar os dados do perfil. Em um modelo de atualização de sistemas operacionais esta funcionalidade é essencial para o sucesso de um projeto.

O System Center Configuration Manager permitirá que o administrador defina uma “Task Sequence” para a tarefa de distribuição de SO, indicando distintas ações que ocorreram antes ou após a instalação do novo SO. Assim teremos o ambiente totalmente funcional, diferente de apenas baixar a imagem, a exemplo de

	Active Directory	System Center Configuration Manager
Distribuição de pacotes	msi, zap, mst	Qualquer tipo de execução, desde bat, cmd, exe e com, até a simples cópia de um arquivo
Agendamento	Não possui agendamento de instalação, apenas validade	Permite agendar o início de uma distribuição, bem como a data de validade
Desinstalação	Ao deletar o pacote, desinstala dos clientes	Não possui, precisa ser criado um pacote com o comando de desinstalação
Distribuição geográfica	Baseado nos sites do AD, utilizando o Domain Controller mais próximo	Utiliza sites do AD ou ranges de IP para distribuição de pacote
Escalonar clientes	Pode ser por site, domínio ou OU	Utiliza as coleções e consultas ao banco de dados, podendo utilizar qualquer critério
Capacidades de hardware	É necessário criar queries WMI	Baseado em queries de banco de dados utilizando os inventários de software e hardware
Upgrade de versão	Automático quando definido que um pacote é a atualização de outro	Permite vincular um pacote a outro indicando a sequência
Sequenciamento de pacotes	Não possui, apenas upgrades	Permite indicar que um pacote depende de outro
Interação com usuário	Não permite	Vários níveis de interação
Grandes pacotes	Executa o msi diretamente da fonte	Realiza o download utilizando BITS e executa localmente ou diretamente da fonte
Distribuidores dedicados	Não permite	Permite escolher distribuidores para cada pacote
Execuções adicionais	Não permite	Cada pacote pode conter diversos programas e estes podem ser executados em sequência
Máquinas desligadas	Não instala	Permite utilizar pacotes WOL (Wake-up On Lan) que ligam a máquina no horário agendado

Tabela 1. Comparação entre distribuição de pacotes com o SCCM e com o AD (GPO)

updates, atualizações e outras ações que precisariam ocorrer após a instalação da imagem do novo SO.

A funcionalidade DCM (*Desired Configuration Management*) permite ao administrador criar perfis de hardware ou software para controlar o *compliance* dos agentes, indicando por meio de relatórios, aqueles que estão fora do padrão estabelecido. Por exemplo, podemos descobrir um agente que possui um determinado software CRM instalado na versão incorreta por criar uma regra DCM que valide a data do executável da aplicação.

Integrando o WSUS com o System Center Configuration Manager, ganhamos funcionalidades que agendam as atualizações e as organizam com relatórios completos de updates. Integrando com o SCUP, podemos utilizar o WSUS também para distribuir pacotes de atualização a outros produtos, incluindo atualizações de terceiros no catálogo. A **Tabela 2** faz

um comparativo do uso do WSUS integrado ao System Center Configuration Manager.

Por fim, outra funcionalidade acrescentada ao System Center Configuration Manager R3 é o gerenciamento de perfil de energia do Windows. Com este recurso podemos determinar de forma central os perfis de energia (**Figura 1**), que desligam o monitor e HD, colocam a máquina em hibernação ou modo de espera. Além disso, o System Center Configuration Manager R3 permite gerar relatórios (**Figura 2**) comparando o consumo das máquinas, com ou sem gerenciamento, além de indicar quais os drivers ou dispositivos consomem mais energia ou impedem o modo de espera.

System Center Operation Manager 2007 SP2 (SCOM)

Conhecido originalmente pelo nome de MOM (*Microsoft Operations Manager*), o produto de monitoração da Microsoft evoluiu muito nas últimas versões.

Seu funcionamento básico consiste em instalar um agente no servidor que monitora o Event Viewer do Windows (ou o SYSLOG no caso de Linux/Unix), logs de performance e outros contadores, permitindo detectar sintomas no sistema.

Cada aplicação ou serviço é monitorado por seguir regras estabelecidas em um conjunto chamado de Management Pack. Estes pacotes podem ser criados pela própria Microsoft ou parceiros. Os Management Packs criados pela Microsoft em geral são gratuitos e os de terceiros são pagos.

Atualmente encontramos mais de 800 Management Packs disponíveis no catálogo online da Microsoft (endereço disponível na seção **Links**), responsáveis pelo monitoramento de roteadores e até de mainframes e aplicações comerciais como SAP, dentre outros. Fabricantes de hardware, a exemplo da Dell, criaram Management Packs a fim de monitorar, por meio de SNMP: storages, servidores, switches e outros equipamentos.

Além disso, os Management Packs de terceiros, e alguns da Microsoft, contêm agentes que ampliam as funcionalidades de monitoração. Os Management Packs do Exchange 2007 e 2010, por exemplo, incluem um serviço que permite monitorar caixas de correios individuais e comportamentos que podem indicar problemas antes destes estarem registrados no Event Viewer.

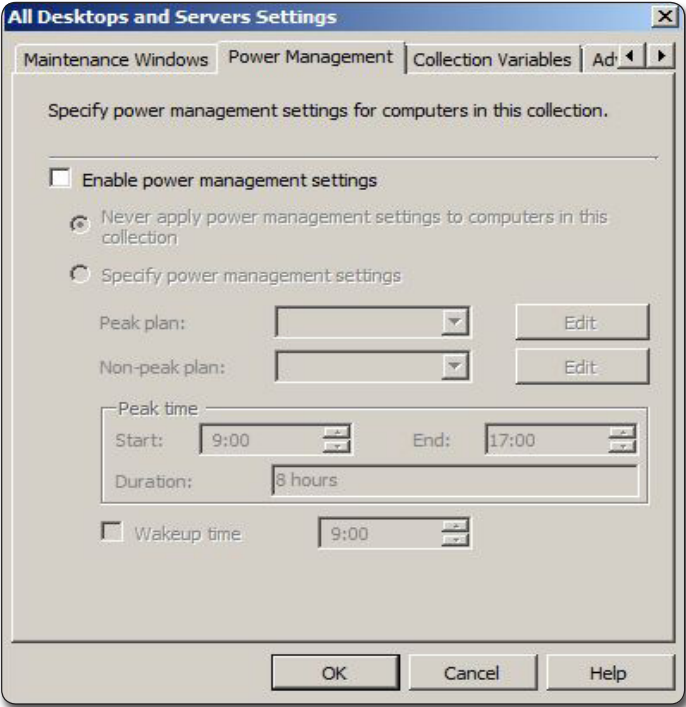


Figura 1. Configuração do modo de energia

	WSUS	System Center Configuration Manager integrado
Updates de SO	Disponível pelo catálogo da Microsoft	Disponível pelo catálogo, cliente de teste ou catálogo de terceiros
Updates de terceiros	Não permite	Permite por meio do SCUP baixar updates de hardware e software
Relatórios	Relatórios básicos	Relatórios avançados
Agendamento de updates	Não permite	Permite agendar os updates utilizando o modo de distribuição de pacotes
Infraestrutura geográfica	Não possui, apenas manualmente pelas GPOs	Utiliza a mesma estrutura da distribuição de pacotes, por site ou range de IP
Filtros de hardware ou software (requisitos)	Não possui, trabalha automaticamente	Permite utilizando as coleções e queries no banco de dados
Ligar máquinas	Não permite	Permite utilizar pacotes WOL (Wake-up On Lan) que ligam a máquina no horário agendado

Tabela 2. Comparativo do uso do WSUS com o SCCM.

Estas regras são simples ou elaboradas, podendo combinar regras de eventos individuais, conjuntas ou sequenciais. Tais regras também são baseadas em contadores de performance que, ao alcançarem determinado número por certo tempo, disparam alertas aos administradores (*Threshold*).

Uma regra de monitoração de eventos bem elaborada pode ser criada utilizando uma sequência na qual, após o evento 4000, esperamos por cinco minutos o evento 4001 a fim de saber se determinado serviço está instável. Igualmente interessante é a ausência de um certo evento, em um tempo específico, indicando a falta de um processo, como um backup que deveria ter ocorrido.

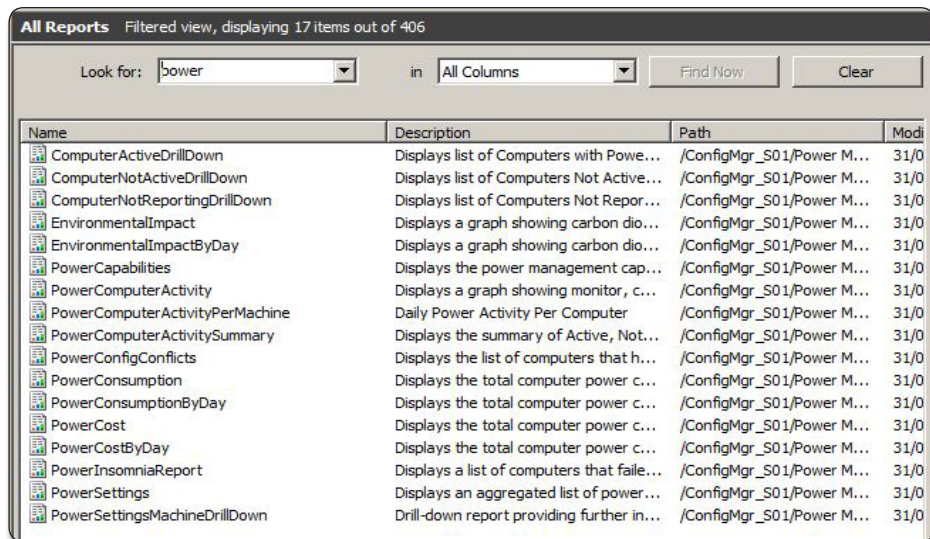
O System Center Operations Manager inclui disparadores para scripts, promovendo a vinculação de um alerta de evento ou performance a um script que pode reinicializar um serviço ou executar um comando, o estabilizando.

O gerenciamento do System Center Operations Manager, por sua vez, controla a abertura de alertas quando uma das situações indicadas acima ocorre, trabalhando com níveis customizados de serviço (SLA), incluindo o tempo máximo de solução. Com esta informação o System Center Operations Manager gera relatórios permitindo ao administrador acompanhar a efetividade da resolução de problemas.

Além disso, pode ser configurado para enviar e-mail, SMS ou executar um software com a finalidade de notificar o administrador e a equipe técnica quando certo tipo de alerta acontecer.

Assim, quando uma situação é resolvida, o responsável detalha o que foi realizado e, quando o mesmo alerta acontecer, automaticamente será enviado na notificação o histórico do mesmo com a descrição cadastrada no evento anterior, criando a base de conhecimento corporativa de sua equipe.

Um novo recurso do System Center Operations Manager na versão 2007 é o conceito de aplicações distribuídas, onde ele carrega uma série de componentes e nos permite criar diagramas que trabalham como uma unidade. Podemos usar,



Name	Description	Path	Modi
ComputerActiveDrillDown	Displays list of Computers with Powe...	/ConfigMgr_S01/Power M...	31/0
ComputerNotActiveDrillDown	Displays list of Computers Not Active...	/ConfigMgr_S01/Power M...	31/0
ComputerNotReportingDrillDown	Displays list of Computers Not Repor...	/ConfigMgr_S01/Power M...	31/0
EnvironmentalImpact	Displays a graph showing carbon dio...	/ConfigMgr_S01/Power M...	31/0
EnvironmentalImpactByDay	Displays a graph showing carbon dio...	/ConfigMgr_S01/Power M...	31/0
PowerCapabilities	Displays the power management cap...	/ConfigMgr_S01/Power M...	31/0
PowerComputerActivity	Displays a graph showing monitor, c...	/ConfigMgr_S01/Power M...	31/0
PowerComputerActivityPerMachine	Daily Power Activity Per Computer	/ConfigMgr_S01/Power M...	31/0
PowerComputerActivitySummary	Displays the summary of Active, Not...	/ConfigMgr_S01/Power M...	31/0
PowerConfigConflicts	Displays the list of computers that h...	/ConfigMgr_S01/Power M...	31/0
PowerConsumption	Displays the total computer power c...	/ConfigMgr_S01/Power M...	31/0
PowerConsumptionByDay	Displays the total computer power c...	/ConfigMgr_S01/Power M...	31/0
PowerCost	Displays the total computer power c...	/ConfigMgr_S01/Power M...	31/0
PowerCostByDay	Displays the total computer power c...	/ConfigMgr_S01/Power M...	31/0
PowerInsomniaReport	Displays a list of computers that faile...	/ConfigMgr_S01/Power M...	31/0
PowerSettings	Displays an aggregated list of power...	/ConfigMgr_S01/Power M...	31/0
PowerSettingsMachineDrillDown	Drill-down report providing further in...	/ConfigMgr_S01/Power M...	31/0

Figura 2. Relatórios de consumo de energia

portanto, um componente SQL Server e vincular ao banco de dados da aplicação. Em seguida, arrastamos o componente Web Server para indicar um site do IIS, que dá suporte a aplicações, e arrastar um componente Windows Service a fim de indicar que um determinado serviço do Windows precisa estar em execução para a aplicação funcionar. Em caso de parada ou queda de qualquer um dos três componentes (Banco de dados, site do IIS ou serviço do Windows), o System Center Operations Manager irá alertar os administradores indicando o nome da aplicação que se tornou indisponível, e não somente o componente, como ocorreria em um monitoramento individualizado.

Enfim, todas as funcionalidades do System Center Operations Manager podem ser consultadas pela sua interface Windows ou pela interface web.

System Center Data Protection Manager 2010 (DPM)

É um dos novos produtos da Microsoft na linha de gerenciamento de infraestrutura, estando em sua segunda versão. O SCDDPM permite realizar backups por meio de agentes para SharePoint, Windows, SQL Server, Exchange e Hyper-V. O Data Protection Manager não foi criado para fazer backup de qualquer sistema operacional, mas possui funcionalidades atraentes e específicas aos produtos da Microsoft.

O backup do Hyper-V é um dos mais interessantes, pois cria um snapshot das Virtual Machines, de forma rápida e efetiva, permitindo um restore veloz em caso de perda da mesma.

Todo o processo do Data Protection Manager se baseia no VSS (*Volume Shadow Service*), conhecido no Windows por *Shadow Copy*, que realiza operações em disco e em background com snapshots dos dados de forma rápida e confiável.

Seu funcionamento é similar ao de outros produtos de backup, criando grupos de proteção, que podem conter features de qualquer servidor. Assim, é possível criar grupos de sites do SharePoint, bancos de dados do SQL Server ou ainda, pastas de servidores de arquivos com maior ou menor importância e periodicidade.

Para cada grupo de proteção indicamos o tempo de retenção, a frequência do backup e o tipo de armazenamento em disco e/ou fita.

No quesito gerenciamento de fita (tape), o Data Protection Manager trabalha com “co-allocation”, permitindo que uma só fita contenha dados de mais de um grupo, além do tradicional, que é guardar vários conjuntos do mesmo backup.

Como é um produto integrado aos outros produtos da família Microsoft, permite uma granularização significativa na restauração, podendo escolher um único site, no caso do SharePoint, ou uma única caixa de correio no caso do Exchange.

System Center Virtual Machine Manager 2008 SP1 (Virtual Machine Manager)

Gerenciador para cluster ou implementações individuais de Hyper-V, este produto traz funcionalidades avançadas para gerenciar o ambiente de virtualização com recursos Microsoft. Por meio desta ferramenta podemos implementar *Live Migration* tanto de storages, como de Virtual Machines individuais.

Contudo, a funcionalidade mais importante do Virtual Machine Manager é a distribuição de carga quando o ambiente é de cluster. Isto porque, se um host possui alta carga e outro host está disponível, o Virtual Machine Manager irá mover, usando o *Live Migration*, algumas das Virtual Machines para o outro nó do cluster e deixar o ambiente, além de estável, mais performático.

Integrado ao System Center Operations Manager, o Virtual Machine Manager habilita um recurso chamado de “Pro Tips” que irá sugerir mudanças nas Virtual Machines, baseando-se nos contadores e Management Packs do Operations Manager, bem como irá utilizar estas métricas do Management Pack para fazer a distribuição das Virtual Machines de forma mais inteligente.

System Center Service Manager 2010 SP1 (SCSM)

Responsável por implementar a informatização de processos como ITIL, COBIT e diferentes padrões de gerenciamento de TI, é também produto recente da família System Center.

Diferentemente dos demais, não objetiva monitorar servidores e clientes, mas instrumentalizar a TI. O System Center Service Manager permite criar níveis de SLA, padrões de documentação, gerência de Mudanças (GMUD) e um portal.

O interessante deste produto é o fato dele integrar os dados do System Center Configuration Manager e, principalmente, do System Center Operations Manager gerando o *Configuration Management Database* (CMDB), com unificação do processo de resolução de problemas.

Com os três produtos integrados, conseguimos no System Center Service Manager criar os *workflows* (fluxos de trabalho) internos da equipe enviando alertas, gerando chamados e controlando a efetividade das soluções para cada alerta gerado.

Dessa forma, o administrador da equipe obterá relatórios completos com a produtividade dos membros individuais de sua equipe, bem como o gerenciamento de contratos de SLA ou mesmo atas de reuniões das GMUDs.

Conclusão

Atualmente, gerenciar um ambiente de TI é um grande desafio, mas com as ferramentas adequadas é perfeitamente possível minimizar retrabalhos, registrar soluções e criar um ambiente onde não seja mais o usuário o termômetro do ambiente, saindo de uma administração reativa para uma proativa.

Nas edições seguintes iniciaremos um estudo exemplificando cada um dos produtos citados neste artigo.



Marcelo Sincic

msincic@gmail.com

É consultor técnico do time de consultoria global da Dell Computadores, MVP Management Infrastructure, certificado Microsoft MCITP, MCTS, MCPD, MCSA, MCDBA, MCAD e MCT pela IBM como CLP Domino 6.5/7.0 e pela Sun como Java Trainer. É certificado em System Center OM/CM, Windows 7, Windows 2008, SQL Server 2008, SharePoint, Exchange, Forefront, ASP.NET 3.5 e Windows Mobile, recebendo o título Charter Member diversas vezes. Recebeu prêmio como um dos 5 melhores instrutores da América Latina. Trabalha com tecnologia desde 1988.



Microsoft TechCenter: Site oficial do System Center (inglês)

<http://www.microsoft.com/systemcenter/en/us/default.aspx>

PinPoint: Catálogo de Management Packs, DCMs e outros (inglês)

<http://systemcenter.pinpoint.microsoft.com/en-US>

Centro de Treinamento System Center Configuration Manager 2007 em português

<http://technet.microsoft.com/pt-br/hh264602>

Centro de Treinamento Nuvem Privada (Virtual Machine Manager) em português

<http://technet.microsoft.com/pt-br/gg578594>



Qualidade de Serviço e Controle de Banda

Conceitos e aplicações com MasterShaper

EDELBERTO FRANCO SILVA E EDUARDO PAGANI JULIO

Os recursos disponíveis à rede, como largura de banda, controle de acesso, priorização de tráfego, entre outros, devem ser observados atentamente pelo seu administrador com a finalidade de se obter a melhora no serviço prestado, aumentando assim a disponibilidade e confiabilidade para as aplicações que os usuários venham a utilizar neste ambiente.

É necessário entender que hoje o enlace de acesso à Internet se mostra como um dos pontos mais críticos dentro desse cenário. O compartilhamento do enlace por vários clientes simultâneos é comumente utilizado tanto nas pequenas quanto nas grandes empresas e ambientes operacionais. A motivação para tal compartilhamento vai desde a falta de endereços IPs (*Internet Protocol*) válidos disponíveis para todos os computadores (o que normalmente se “soluciona” com a utilização de NAT - *Network Address Translation*), passando pela utilização do modelo de *intranet*, bem como a diminuição dos gastos no aluguel de enlaces de acesso à Internet. O cuidado para a não escassez desse recurso deve ser um dos pontos priorizados, junto a outros, como a segurança, por exemplo. Algumas ferramentas, como *proxies* que realizam *cache* (armazenamento local) de conteúdo, programas de controle de banda e qualidade de serviço (*Quality of Service - QoS*), têm como um de seus objetivos auxiliar a otimização do desempenho, principalmente do acesso à Internet.

O controle de banda visa, sobretudo, a utilização da melhor forma possível dos recursos de rede no que diz respeito ao acesso por meio do enlace de rede. Basicamente emprega-se o controle de banda para garantir a certos serviços, ou clientes, velocidade de conexão. Já a qualidade de serviço visa priorizar aqueles serviços que apresentam maior necessidade de recursos, seja em relação à banda disponível ou atraso, por exemplo.

Este artigo apresenta os conceitos básicos de controle de banda e qualidade de serviço. Também apresenta os principais conceitos que envolvem essas técnicas a fim de auxiliar no ganho de desempenho da rede. Ao final, o leitor estará apto a instalar e configurar uma ferramenta que fornece recursos para a empregabilidade das técnicas relacionadas aos conceitos abordados. Essa ferramenta tem o nome de MasterShaper, é gratuita, de código-fonte aberto, e é totalmente configurável por meio de sua interface gráfica. A ferramenta em questão é executada sobre o Sistema Operacional Linux e seu guia disponível neste artigo descreve de forma genérica a sua instalação e configuração, o que facilita ao leitor instalá-la em qualquer distribuição Linux.

Resumo DevMan

De que se trata o artigo:

Este artigo aborda a utilização de controle de banda e qualidade de serviço a fim de racionalizar a utilização da banda disponível para o acesso à Internet pelos computadores em uma rede local. Serão expostos tanto os principais conceitos necessários ao entendimento deste tipo de solução quanto os mecanismos e técnicas existentes. Ao final, para firmar os conceitos expostos, um tutorial de instalação e configuração da ferramenta MasterShaper será apresentado.

Em que situação o tema é útil:

Muito utilizado em redes locais onde há várias máquinas acessando a Internet ao mesmo tempo, o controle de banda tem como intuito evitar que um usuário consuma toda a banda (ou grande parte dela) disponível para toda a rede. Uma utilização muito comum do controle de banda se dá em provedores de acesso à Internet, onde o cliente recebe a velocidade equivalente ao plano que pagou. A qualidade de serviço desperta maior interesse em empresas e ambientes corporativos, principalmente quando existe a intenção de melhorar os esforços quanto à garantia de um menor atraso às aplicações sensíveis, como são os casos de aplicações de vídeo-conferência e voz sobre IP.

Qualidade de Serviço e Controle de Banda:

Este artigo aborda a premissa de controle de banda com o intuito de preservar a qualidade dos serviços oferecidos sob uma rede baseada no melhor esforço, ou seja, uma rede onde não há garantias em relação ao atraso ou a entrega dos pacotes enviados. A intenção principal deste artigo é que se entendam os principais conceitos que envolvem uma melhor utilização dos recursos de banda disponível na rede e possa, ao final, empregar estes mecanismos em seu ambiente corporativo como auxílio ao ganho de desempenho da rede. Dessa forma, será conceituado este ambiente, assim como o que vem a ser controle de banda, e suas disciplinas mais utilizadas. Também será abordado o que vem a ser qualidade de serviço e o porquê de seu emprego. Neste artigo ainda serão apresentadas as ferramentas mais utilizadas, incluindo a ferramenta MasterShaper, para instalação em um servidor Linux.

Qualidade de Serviço

O princípio fundamental da qualidade de serviço pode ser descrito como a busca pelo respeito a uma faixa de requisitos da aplicação ou da rede, seja ela: a consideração de um atraso

mínimo para a entrega de um pacote, uma vazão (*throughput*) mínima ou uma perda mínima, por exemplo. O requisito de QoS mais comumente utilizado, e mais simples de ser administrado, diz respeito à vazão, ou velocidade do enlace dedicada a uma aplicação ou às aplicações de um computador da rede. Neste ponto, podemos citar o controle de banda, que será explicitado mais à frente neste artigo.

A qualidade de serviço pode ser observada de duas formas: do ponto de vista da aplicação ou da rede. Para uma aplicação, oferecer seus serviços com qualidade significa atender às expectativas do usuário em termos do tempo de resposta e da qualidade, muitas vezes subjetiva, do serviço que está sendo provido, ou seja, fidelidade adequada do som e/ou da imagem sem ruídos nem congelamentos, garantindo neste caso tanto a vazão quanto o atraso mínimo. Já a qualidade de serviço da rede depende das necessidades da aplicação, ou seja, do que ela requisita da rede a fim de que funcione bem e atenda, por sua vez, às necessidades do usuário que a utiliza. Esses requisitos são traduzidos em parâmetros que indicarão o desempenho da rede como, por exemplo, o atraso máximo sofrido pelo tráfego da aplicação entre o computador origem e destino.

Aplicações consideradas avançadas são mais exigentes que as aplicações convencionais. Pode-se considerar como aplicações avançadas: vídeo interativo, voz sobre IP (VoIP), telemedicina, entre outras. Aplicações de vídeo interativas requisitam da rede um limite máximo para o atraso fim a fim e uma baixa perda de pacotes, enquanto que as aplicações de vídeo não interativas toleram melhor uma pequena perda de pacotes e variação do atraso, comuns sobre o meio da Internet.

Outro exemplo de aplicações avançadas são aquelas que utilizam realidade virtual. Através delas os usuários podem interagir, colaborar, compartilhar um ambiente virtual como se estivessem num mesmo local, entre outras possibilidades. Uma aplicação deste tipo é a de torcida virtual, que consiste na transmissão de um vídeo de um jogo de futebol e permite que usuários participem remotamente da torcida, escolhendo um assento em um mapa de um estádio virtual. Para os usuários é dada a sensação de estarem juntos no estádio, participando da partida de futebol.

No modelo de serviço atual da Internet é empregado o melhor esforço (*Best Effort*), ou seja, não é prometido nada quanto à QoS que uma aplicação receberá. Será concedido à aplicação que utiliza seu meio o nível de desempenho (por exemplo, atraso fim-a-fim e perda de pacotes) que a rede estiver capacitada a dar naquele determinado momento. A Internet atual não diferencia o serviço de forma a dar um tratamento especial a algum tipo de aplicação sensível a atraso, por exemplo, como é o caso das aplicações avançadas já citadas anteriormente. O modelo de melhor esforço utiliza a política de enfileiramento dos pacotes FIFO (*First In First Out*), ou seja, o primeiro pacote a entrar é o primeiro pacote a sair, não priorizando àqueles mais sensíveis a este aguardo (atraso) em fila.

Mecanismos de Escalonamento e Regulação

A seguir serão detalhados mecanismos que tentam garantir tais necessidades em respeito à QoS, sendo abordados mecanismos de escalonamento de pacotes, assim como a aplicação da regulação da taxa de pacotes injetados na rede.

Mecanismos de Escalonamento

O modo como os pacotes são enfileirados nos *buffers* associados à saída de um enlace, comumente, roteadores, é chamado de disciplina de escalonamento do enlace e, dependendo da técnica utilizada, será possível auxiliar na garantia de QoS.

A Figura 1 ilustra o mecanismo básico utilizado conhecido como FIFO, e respeita a ordem de chegada dos pacotes não a alterando durante sua permanência no *buffer*. Neste caso, se o enlace estiver congestionado, os pacotes aguardarão até que o meio seja liberado para enviar os pacotes de sua fila. Como os pacotes podem ficar por tempos demasiadamente grandes em espera no *buffer*, e como estes não têm espaço infinito, haverá a necessidade de descarte de alguns pacotes conforme uma política adotada para isto, que pode ser, por exemplo, o pacote mais antigo no *buffer*.

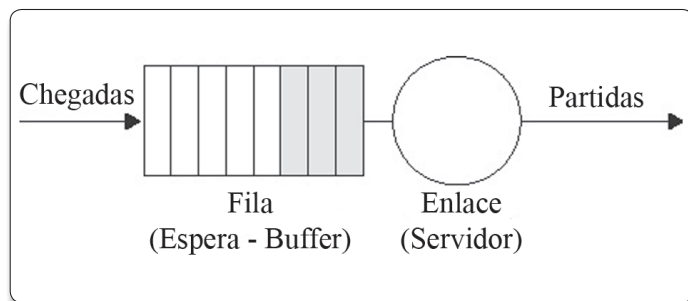


Figura 1. Enfileiramento FIFO, baseada em Kurose (2006)

Outro mecanismo classifica os pacotes por prioridade. É o chamado enfileiramento prioritário, e pode depender de uma marcação no cabeçalho do pacote (por exemplo, no campo *ToS – Type of Services* – do IPv4), do endereço IP de sua origem ou destino, ou do número da porta de origem ou destino, ou outro critério. Um grande problema desse modelo é a mudança, ou um computador intermediário que forja um cabeçalho com maior prioridade para ter sempre seus pacotes mais bem classificados durante o roteamento. Neste mecanismo é possível imaginar ilustrativamente como se houvessem duas filas em um roteador, conforme a Figura 2, sendo uma de maior e outra de menor prioridade.

Há ainda o mecanismo chamado por varredura cíclica, onde os pacotes são classificados como no mecanismo de enfileiramento prioritário, divididos em filas separadas conforme o número de classes. Porém, todas as classes devem ser atendidas da mesma forma. Sua essência se parece com o enfileiramento prioritário por ter várias filas, e não somente uma, como o FIFO. Como exemplo deste mecanismo, pode-se supor que hajam três classes (filas), e será enviado um pacote de cada fila a fim de não deixar o enlace ocioso e compartilhar de forma justa os recursos. Portanto, esse

mecanismo irá procurar um pacote de uma dada classe, mas caso não encontre nenhum à espera, verifica imediatamente a classe posterior, realizando a sequência de varredura cíclica.

Uma variação muito importante deste mecanismo é o WFQ (*Weighted Fair Queueing* – enfileiramento justo ponderado), onde além dos pacotes serem divididos em classes diferentes, essas classes têm pesos diferentes entre si e, com base em uma fórmula de ponderação, é possível estipular tempos de utilização do enlace diferentes para cada fila (classe). O WFQ é disponível em roteadores da empresa Cisco. Intranets que possuem roteadores com esse mecanismo de enfileiramento podem prover QoS ao fluxo interno concorrente da empresa.

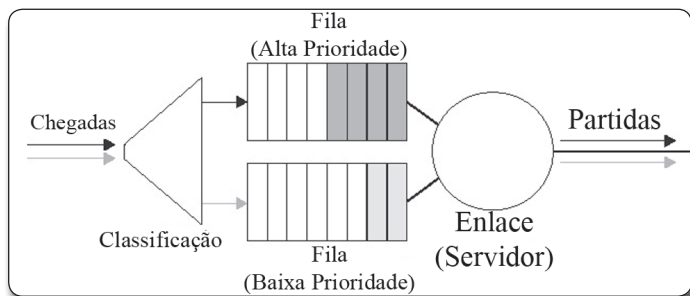


Figura 2. Enfileiramento Prioritário, baseada em Kurose (2006)

Após a introdução dos clássicos mecanismos de enfileiramento, serão abordadas arquiteturas específicas para o provimento de QoS. São elas o *Intserv* (arquitetura de serviços integrados) e o *Diffserv* (arquitetura de serviços diferenciados).

Intserv

A arquitetura de serviços integrados se baseia em duas características fundamentais: a reserva de recursos e o estabelecimento de chamadas. Para a reserva de recursos, um roteador tem que saber a quantidade de recursos, como *buffer* utilizado e largura de banda do enlace, e se estão alocados para as sessões existentes, onde esta reserva de recursos é sinalizada pelo RSVP (ver **Nota DevMan 1**). Já o estabelecimento de chamadas terá a participação de todos os roteadores no caminho da rede da origem ao destino. É quando os recursos serão reservados para esta conexão. Com base nos pedidos, cada roteador reserva recursos para aquela sessão de comunicação a ser iniciada com base nos recursos disponíveis, respeitando sempre a QoS das sessões em andamento e também daquele que realizou o pedido. Um roteador pode, portanto, aceitar ou negar esse pedido de reserva de recursos realizado pela fonte.

O Intserv, portanto, realiza uma reserva por fluxo e não é difícil imaginar que isso poderia gerar alguns problemas de escalabilidade, já que é necessário processamento dos roteadores que estão encaminhando o tráfego tanto no momento de reserva dos recursos quanto para manter o estado desse fluxo. Uma enorme sobrecarga extra é então inserida ao roteamento dos pacotes. Problemas como esse levaram ao desenvolvimento do Diffserv.



Nota do DevMan 1

RSVP (ReSeRVation Protocol – Protocolo de Reserva de Banda) é o protocolo de sinalização utilizado para avisar que uma aplicação necessitará de uma quantidade determinada de largura de banda reservada e espaço em buffer nos roteadores para sua garantia de QoS.

Diffserv

A ideia principal desta arquitetura é a diferenciação de serviço de forma escalável e flexível a fim de complementar o Intserv, uma vez que visa à manipulação de classes de tráfego de maneira diferente. O Diffserv não é um serviço específico para as classes e, ao invés disto, fornece componentes funcionais para a inclusão de novos serviços.

Dois conjuntos de elementos fundamentais são a base do Diffserv: a função da borda e a função central. Basicamente, o primeiro diz respeito à classificação e condicionamento dos pacotes e o segundo somente a seu envio. Ou seja, toda a complexidade fica na borda da rede, liberando o núcleo do processamento exaustivo, como o existente no Intserv.

Um ponto importante dessas duas arquiteturas é que foram propostas para sistemas fim-a-fim, ou seja, no caso da Internet, o domínio tem dimensões geográficas e econômicas que dificultam sua aplicação, uma vez que todos os ISPs (*Internet Service Provider* – Provedor de Acesso de Internet) devem estar acordados das configurações a serem utilizadas e as respeitarem.

Controle de Banda

A utilização de controle de banda visa, principalmente, o compartilhamento justo da banda que se tem disponível no ambiente operacional. Como forma de ilustração pode-se imaginar uma rede em que um único enlace de 2 Mbps fornece acesso a 10 computadores. Esse exemplo é facilmente visualizado em uma pequena empresa ou um laboratório de uma escola. Nesse tipo de ambiente, os usuários provavelmente estarão ligados ao mesmo tempo por este único enlace à Internet. Agora, também se pode imaginar como seria desagradável para o presidente desta empresa precisar realizar uma reunião por vídeo-conferência, porém outro funcionário está visualizando vídeos de entretenimento no YouTube e algum outro realizando o *download* de um arquivo de áudio, ocupando assim toda a banda disponível (ver **Nota DevMan 2**). Nesse ambiente, deve-se ser o mais justo possível, alocando de forma adequada uma largura de banda para cada cliente e priorizando àqueles que realmente necessitem mais dela.



Nota do DevMan 2

Determinação de valor fixo de banda a um IP: É possível, em várias ferramentas, determinar um valor fixo de banda a um IP, ou bloco de IPs, e permitir que, caso o link esteja ocioso, este IP, ou bloco de IPs, utilize um limiar que possa ser configurado como, por exemplo, o valor total do link para a Internet.

Técnicas de controle de banda fazem parte do esforço para a aplicação de *QoS* em um ambiente controlado. Outro exemplo onde o controle de banda se aplica comumente é em um ISP (*Internet Service Provider*) que fornecerá ao cliente não toda a banda disponível a ele, mas sim a banda contratada.

Disciplinas de Enfileiramento

As disciplinas de enfileiramento são responsáveis por como o tráfego será tratado. A partir dela é possível estabelecer diretrizes referentes à alocação de banda ou tratamento diferenciado para determinado tipo de pacote.

A ferramenta MasterShaper, abordada no final deste artigo, abrange as disciplinas HTB, HFSC e CBQ, descritas a seguir.

O HTB (*Hierarchical Token Bucket*) é baseado no conceito de balde de fichas (*Token Bucket* – ver Nota DevMan 3). É capaz de suportar uma configuração para alocação de banda mínima a uma classe de tráfego. Além disso, permite definir a largura de banda máxima que uma classe pode "pegar emprestado" de outras classes, caso esta largura de banda esteja ociosa. É possível definir o tamanho da rajada, ou seja, o tamanho máximo de pacotes enviados de uma só vez, assim como realizar a priorização das classes. Essa priorização servirá somente no momento em que a banda não utilizada estiver sendo distribuída. Dessa forma, prioridades mais altas ganham mais largura de banda.

Outra disciplina é a HFSC (*Hierarchical Fair Service Curve*), que é capaz de suportar um atraso máximo garantido de pacotes na rede. O atraso máximo garantido a que se refere essa disciplina é o tempo utilizado como limite máximo para envio de um pacote, onde serão priorizados aqueles pacotes cujo tempo seja menor, e consequentemente, necessitem de maior priorização no momento do encaminhamento. Isso é importante para aplicações em tempo real como Voz sobre IP (*VoIP*), onde os atrasos e o *jitter* (variação do atraso) têm um impacto negativo diretamente sobre a qualidade. Também com HFSC pode-se definir uma largura de banda mínima, alocada para cada uma das classes, e uma largura de banda máxima, que pode ser utilizada por esta classe.

Já a disciplina CBQ (*Class-Based Queueing*) é anterior ao HTB e apresenta menos opções que este último.

Alguns exemplos de ferramentas para manipulação de controle de banda são:

- *Traffic Shaper*: sistema para controle de banda em Linux, muito utilizada até meados do ano de 2000;
- CBQ: é possível criar classes para controle do tráfego tanto de *download* quanto de *upload*. Arquivos separados de configuração são criados para cada classe. Disponível para o sistema operacional Linux;
- HTB: permite que a banda ociosa seja utilizada por classes que necessitem em determinado momento. Uma mesma classe pode comportar vários clientes, diferentemente do CBQ. O HTB ainda apresenta uma interface mais clara que a utilizada pelo CBQ, se tornando em inúmeros casos seu sucessor. O *tc* é o comando referente à sua chamada no sistema operacional Linux;

- HTB-Tools: permite uma interface para configuração dos arquivos referentes ao HTB mais intuitiva que as linhas de comando padrão;

MasterShaper: este aplicativo será abordado neste artigo e foi considerado o mais simples para a utilização de controle de banda e *QoS* em um *gateway* empregando Linux. Suporta as três disciplinas de enfileiramento descritas: CBQ, HFSC e HTB.



Nota do DevMan 3

Token Bucket: tem como função a diminuição dos efeitos causados pelas rajadas. As rajadas representam o número máximo de pacotes enviados consecutivamente, em um período de tempo extremamente curto. A principal funcionalidade do Token Bucket é uniformizar a vazão e a latência (atraso do pacote). Uma rajada será encaminhada conforme um tamanho pré-determinado, conhecido como burst size. Uma quantidade de bps também é associada à técnica, determinando a quantidade de dados em média que podem ser enviados em uma determinada unidade de tempo. Ou seja, o intervalo de tempo referente ao tempo de duração da rajada.

MasterShaper

O MasterShaper é uma interface *web* para os serviços de controle e gerência de tráfego de rede para o sistema operacional Linux. Sua principal função é fornecer uma interface *web* de simples manipulação para os recursos de *QoS* disponíveis em Linux com *kernel* versões 2.4 e 2.6. Por meio de sua interface, é possível definir seus próprios conjuntos de regras para o tratamento dos fluxos da rede e também visualizar estatísticas sobre a largura de banda de forma gráfica.

A ferramenta MasterShaper realiza, portanto, *traffic shaping* em redes onde os recursos são conhecidos e é possível modelar seu tráfego, como é o caso de empresas, escolas e outros ambientes corporativos. Suas características visam àqueles administradores que não têm muita experiência com Linux, configuração e criação de *scripts* e outras ferramentas necessárias para fazer esse trabalho da forma convencional, ou seja, configurando vários arquivos texto. É possível utilizar o MasterShaper tanto em um computador configurado para trabalhar como um roteador como também sobre uma *bridge* transparente.

Requisitos para a instalação

Os requisitos para a instalação basicamente se fazem mais necessários à interface *web*, e são eles:

- Qualquer distribuição Linux, desde que rodando a versão 2.4 ou 2.6 do *kernel*;
- *iproute2*: contém o comando *tc*, necessário ao HTB;
- *web-Server* com suporte a PHP (Apache2, *mod_php4*, <http://httpd.apache.org/>);
- PHP4 (ou superior) com suporte a JPEG, LibGD e MySQL;
- Base de dados MySQL 4.1 ou superior;
- Módulos PHP DB & Net_IPv4;
- Perl com interface DBD (ou seja, DBI-MySQL);
- PHP Layers Menu (<http://phplayersmenu.sourceforge.net/>);
- JpGraph (<http://www.aditus.nu/jpgraph/>).

Para o guia de instalação do MasterShaper neste artigo, deve-se levar em consideração que o ambiente respeita a versão do *kernel* do Linux mencionada anteriormente. Não serão abordados neste artigo a instalação e configuração do servidor web Apache e do banco de dados MySQL, porém esses guias são facilmente encontrados na Internet.

Instalação e Configuração do MasterShaper

O primeiro passo que se deve realizar é a criação do diretório para manipulação da instalação. A **Listagem 1** mostra todos os passos para a realização da *download* e descompactação do arquivo referente ao MasterShaper.

Feito isso, deve-se copiar o conteúdo de *htdocs*, da pasta descompactada, para o seu diretório raiz *web*, que, por padrão, na maioria das distribuições Linux, é o */var/www/*, conforme a **Listagem 2**.

Listagem 1. Salvando e descompactando o MasterShaper.

```
mkdir /tmp/shaper
cd /tmp/shaper
wget http://www.mastershaper.org/files/mastershaper_0.44.tar.bz2
tar xvfz mastershaper_0.44.tar.bz2
```

Agora, cria-se um banco de dados para o MasterShaper. A **Listagem 3** mostra como este procedimento é executado. Este artigo não aborda a instalação do phpMyAdmin (<http://www.phpmyadmin.net/>), mas considera a instalação desta ferramenta para uma maior facilidade de administração dos bancos de dados MySQL.

Listagem 2. Copiando a pasta do MasterShaper para ser acessado via web.

```
mkdir /var/www/shaper
cp -r /tmp/shaper/htdocs/ /var/www/shaper/
```

O *JpGraph* é uma biblioteca em PHP consolidada para a geração dinâmica de gráficos. MasterShaper faz utilização desta biblioteca e então deve-se instalá-la. Sua instalação é simples e pode ser seguida conforme a versão do PHP que está sendo utilizada. Caso utilize o PHP4, deve-se seguir a **Listagem 4**, caso seja a utilizada a versão PHP5, a **Listagem 5**.

Como o MasterShaper procura a biblioteca *JpGraph* em uma pasta denominada *jpgraph* em seu próprio diretório corrente (*/var/www/shaper/*), é interessante criar um link simbólico com o comando *ln* ao invés de renomear a pasta (o que iria suprimir a versão do *JpGraph* que estamos utilizando).

Como próximo passo, deve-se instalar o *PHP Layers Menu*, responsável pela geração dinâmica em DHTML dos menus utilizados pelo MasterShaper. A **Listagem 6** mostra os passos necessários.

Da mesma forma que a biblioteca *JpGraph*, o MasterShaper procurará a pasta *phplayersmenu* em seu próprio diretório corrente (*/var/www/shaper/*), e é interessante criar um link simbólico com o comando *ln* ao invés de renomear a pasta (o que iria suprimir a versão do *PHP Layers Menu* que estamos utilizando).

Listagem 3. Criando o banco de dados do MasterShaper no MySQL.

```
create database db_shaper;
```

Listagem 4. Instalando o JpGraph para o PHP4.

```
Faça o download da versão 1.27.1 em
http://jpgraph.net/download/download.php?p=1.27.1
salve-o em /var/www/shaper/ e descompacte-o
cd /var/www/shaper/
tar xvfz jpgraph-1.27.1.tar.gz
ln -s /var/www/shaper/jpgraph-1.27.1 /var/www/shaper/jpgraph
```

Listagem 5. Instalando o JpGraph para o PHP5.

```
Faça o download da versão 3.0.7 em
http://jpgraph.net/download/download.php?p=1
salve-o em /var/www/shaper/ e descompacte-o
cd /var/www/shaper/
tar xvfz jpgraph-3.0.7.tar.gz
ln -s /var/www/shaper/jpgraph-1.27.1 /var/www/shaper/jpgraph
```

Listagem 6. Instalando o PHP Layers Menu.

```
Faça o download da última versão em http://phplayersmenu.sourceforge.net/ na
aba downloads
cd /var/www/shaper/
tar xvfz phplayersmenu-3.2.0-rc.tar.gz
ln -s /var/www/shaper/phplayersmenu-3.2.0-rc /var
/www/shaper/phplayersmenu
```

Se ainda não tiver o módulo *Net_Ipv4* do PHP-PEAR, um processo de instalação pode ser visto na **Listagem 7**. Este módulo é utilizado para validar endereços IPv4 e também para calcular informações como endereço de rede e endereço de *broadcast*.

Caso utilize uma instalação com suporte ao *apt-get*, por exemplo, Ubuntu ou Debian, pode-se realizar os procedimentos da **Listagem 8** como substituição às **Listagens 4, 5, 6 e 7**.

Listagem 7. Instalando o modulo Net_Ipv4 do Pear.

```
pear install DB_Net_Ipv4
```

Listagem 8. Instalando o iproute (tc), JpGraph, PHP-PEAR, sudo e PHP Layers Menu.

```
apt-get install iproute
apt-get install libphp-jpgraph
apt-get install php-pear
apt-get install sudo
apt-get install php-db
apt-get install php4-mysql
apt-get install libphp-phplayersmenu
pear install DB_Net_Ipv4
cd /var/www/shaper
ln -s /usr/share/php/libphp-phplayersmenu phplayersmenu
ln -s /usr/share/jpgraph jpgraph
```

A instalação padrão do MasterShaper utilizada neste guia não gera o arquivo onde as configurações realizadas utilizando a interface *web* deverão ser salvas, sendo assim, antes de iniciar as configurações por meio da interface *web* da ferramenta, torna-se necessário criar o arquivo que as armazenará. Para isso deve-se executar o comando da **Listagem 9**.

Após a realização de todos os passos iniciais de instalação do MasterShaper, será necessário acessar a interface *web* para finalizar a instalação. É possível acessá-la pelo endereço *http://localhost/shaper/*, ou trocando *localhost* pelo endereço IP da máquina onde o MasterShaper foi instalado. Feito isso, será exibida uma página conforme a **Figura 3**, cujos itens serão descritos logo a seguir.

O MasterShaper não possui suporte à língua portuguesa, portanto, todas as opções são apresentadas em inglês. A **Tabela 1** descreve cada uma das opções expostas pela **Figura 3**.



Nota do DevMan 4

IANA e seu papel: A Internet Assigned Numbers Authority (IANA) é o órgão responsável pela coordenação de alguns dos elementos-chave necessários para manter a Internet funcionando perfeitamente. Embora a Internet seja conhecida por ser uma rede mundial livre de coordenação central, há uma necessidade técnica para algumas peças-chave da Internet serem coordenadas, e esse papel de coordenação é realizado pela IANA. Por exemplo, os números de portas associados a serviços conhecidos e fornecidos na Internet.

Listagem 9. Criando o arquivo que armazenará a configuração.

```
touch /var/www/shaper/config.dat
```

O MasterShaper utiliza o comando *sudo* para a execução de comandos como o administrador do sistema. Neste caso, já foi configurado anteriormente, a partir da **Figura 3**, o caminho referente a esse comando, e agora será adicionado o usuário referente ao Apache (esse usuário pode ser encontrado no arquivo de configuração do Apache, normalmente localizado em seu sistema pelo nome de *httpd.conf*), para que possa executar os comandos configurados pela interface *web* como usuário administrador do sistema operacional

Linux (*root*). Normalmente esse usuário é o “*www-data*”, mas pode ser outro como “*apache*”, por exemplo. Para realização dos procedimentos descritos pela **Listagem 10** será preciso estar autenticado no sistema como *root*, ou outro usuário com o mesmo privilégio deste.

A partir deste momento tem-se todo o ambiente de configuração preparado para ser configurado e executado. Porém, se quiser visualizar as estatísticas, como a utilização de banda, é necessário realizar a tarefa da **Listagem 11**, que corresponde

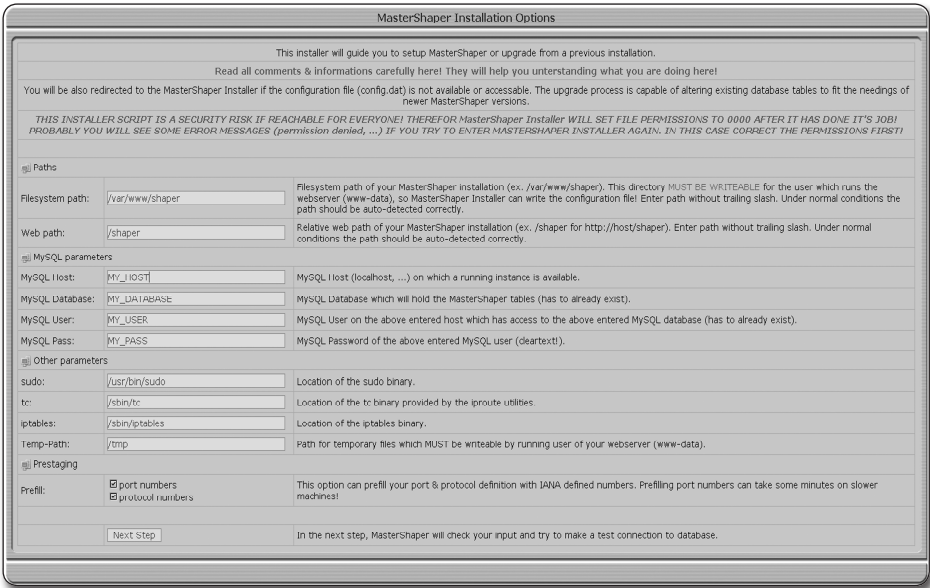


Figura 3. Tela de configuração inicial do MasterShaper

Opção	Valor	Justificativa
Filesystem path	/var/www/shaper	Caminho da pasta do MasterShaper no sistema.
Web path	/shaper	Caminho da pasta abaixo do diretório web do Apache. Em nosso caso, o diretório web é considerado /var/www.
MySQL host	localhost ou 127.0.0.1 (caso o servidor de banco de dados esteja no mesmo computador que o MasterShaper).	Endereço do servidor de banco de dados
MySQL Database	db_shaper	Nome da base de dados. A base criada na Listagem 3.
MySQL user	root	Usuário com poder de acesso à base db_shaper no banco de dados MySQL.
MySQL pass	sua senha	Senha correspondente ao usuário com acesso ao banco de dados.
sudo	/usr/bin/sudo	Caminho para o comando sudo, que permite a um usuário poderes administrativos (root).
tc	/sbin/tc	Caminho no sistema para o comando tc referente à ferramenta de traffic control
iptables	/sbin/iptables	O caminho no sistema para o comando iptables.
temp-path	/tmp	Caminho referente ao diretório de arquivos temporários do MasterShaper
Marca-se também “port numbers” e “protocol numbers” para que sejam utilizadas as associações de número de portas e nomes de protocolos padronizados pelo IANA – veja a Nota DevMan 4 . Por exemplo: a porta 21 é referente ao FTP (File Transfer Protocol).		

Tabela 1. Configuração inicial do MasterShaper

a um *script* em perl (*tc_collector.pl*) para a coleta de dados do *tc* e geração dos gráficos. Este *script* utiliza as informações armazenadas no *config.dat* (geradas após a configuração da **Figura 3**) para a coleta dessas estatísticas.

Listagem 10. Configurando o sudo para o usuário do Apache.

```
vim /etc/sudoers
adicione a linha ao final do arquivo
www-data ALL=NOPASSWD: /var/www/shaper/shaper_loader.sh
```

Listagem 11. Rodando o *tc_collector.pl*.

```
cd /var/www/shaper
./tc_collector.pl
```

Listagem 12. Rodando o *tc_collector.pl* como daemon em background.

```
cd /var/www/shaper
./tc_collector.pl -d
```

Caso se deseje que este *script* rode em *background*, ou seja, liberando o terminal, utiliza-se o mesmo comando, porém adicionando a flag “-d” ao final, como visto na **Listagem 12**.

Descrição dos principais termos utilizados pelo MasterShaper

A seguir são listadas as definições dos principais termos utilizados pelo MasterShaper. A intenção desta descrição é servir como um glossário dos termos e opções.

- **Bandwidth:** velocidade de seu link de conexão. Usa-se a representação do valor em kbits por segundo (kbps);
- **Protocols:** tipo de protocolo. Dividido em duas classes, tráfego IP (TCP e UDP) e tráfego *ICMP* (ping, por exemplo);
- **Ports:** portas da aplicação, associadas ao serviço e ao protocolo;
- **Targets:** endereço IP, que pode ser puro ou ainda o endereço da rede (por exemplo, 10.0.0.0/8) ou uma faixa de IPs (10.0.0.1-10.0.0.10);
- **Service Levels:** responsável por determinar um limite de banda a ser alocado para o serviço em questão. É possível utilizar as opções de enfileiramento HTB que permitem delegar valores diferentes para o tráfego de entrada e para o tráfego de saída, criando assim links assimétricos. Ou ainda, utilizar o HFSC, onde é possível configurar o máximo de atraso aceitável (maximum delay) dos pacotes da rede. Nessa opção serão criados os níveis, por exemplo: Diretoria com 1 Mbps, Administrativo com 500 kbps e demais com 500 kbps;
- **Filters:** filtros servem como padrões de tráfego e portanto serão comparados a um modelo de tráfego pré-definido. Por exemplo, “web-traffic” deve coincidir com HTTP & HTTPS, ou seja, utilizar as portas 80 ou 443 sob o protocolo TCP;
- **Chains:** é responsável pela atribuição do valor de largura de banda máxima disponível que será utilizada durante toda a configuração do sistema. Se tiver apenas uma *chain*, este valor normalmente é igual à sua velocidade de conexão. É importante citar que os valores serão sempre expressos em kbps, ou seja, 2048kbps equivale a 2 Mbps e 1024kbps a 1 Mbps. É possível definir *chains* para um IP ou um bloco de IPs, conforme foi configurado em *Targets*, dependendo do que ou quem se deseja limitar;

- **Pipes:** é neste ponto que é definido o controle de banda para cada tipo de serviço, o filtro por serviço. Cada pipe deverá estar associado a uma das Chains criadas anteriormente, o que consequentemente determinará a banda máxima a ser utilizada.

Configuração de um ambiente real

Após conhecer as opções mais importantes a serem notadas no MasterShaper, segue-se ao tutorial que, com poucas configurações, permitirá ter uma visão prática de como configurar a ferramenta a partir de um ambiente de exemplo.

Aqui serão considerados um roteador Linux com duas interfaces de rede, onde uma está conectada à Internet via WAN (*Wide Area Network*) e outra à rede interna LAN (*Local Area Network*), onde pacotes considerados pequenos e pacotes de acesso remoto para o SSH (*Secure Shell*) terão alta prioridade. O enlace de acesso à Internet, neste exemplo, é de 2048 kbps (2 Mbps). E a alocação de banda para o tráfego web, representado por HTTP e HTTPS, será de no máximo 1024 kbps (1 Mbps). Demais tráfegos usarão até, no máximo, 1536 kbps (1,5 Mbps) do enlace. A **Figura 4** mostra a topologia de rede para esse tutorial de forma simplificada.

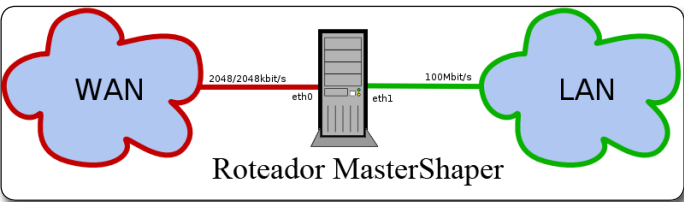


Figura 4. Topologia de rede para o tutorial

A tela ilustrativa da **Figura 5** mostra as opções referentes à configuração da rede, delegando os valores tanto referentes à largura de banda do enlace, quanto o controle do tráfego de entrada do enlace, como do tráfego de saída e a seleção da política de enfileiramento, no caso a HTB.

A configuração exposta pela **Figura 5** se encontra no menu *Options*, dentro de *Settings*. O ambiente de avaliação deverá apresentar os valores conforme a **Tabela 2**.

Opção	Valor	Descrição
Inbound Bandwidth	2048 kbit/s	Largura de banda do enlace de entrada
Outbound Bandwidth	2048 kbit/s	Largura de banda do enlace de saída
Incoming Interface	eth0	Interface de entrada do enlace
Outgoing Interface	eth1	Interface de saída do enlace
IMQ	no (não)	Se utilizará o dispositivo virtual de enfileiramento IMQ
Queueing discipline	HTB	Disciplina de enfileiramento de pacotes
Traffic filter	tc-filter	O tipo de filtro para execução das políticas de controle de banda
Mode	Router	Modo de operação, roteador ou bridge
Authentication	Yes	Autenticação ou não para acesso à administração do MasterShaper

Tabela 2. Configuração inicial da rede em MasterShaper

O próximo passo a ser realizado é a criação dos níveis de serviço, localizado no menu em *Service Levels*, dentro de *Settings*, como pode ser visto na **Figura 6**.

Os campos que a **Figura 6** dispõe devem ser configurados para cada um dos níveis de serviço escolhidos no início deste exemplo. As **Tabelas 3 a 7** apresentam cada um destes campos referentes ao primeiro exemplo de configuração.

Opção	Valor	Descrição
Name	"Mais Alta Prioridade"	Nome do Service Level
In-Bandwidth	32 kbit/s	Largura máxima desejada de banda de entrada
Out-Bandwidth	32 kbit/s	Largura máxima desejada de banda de saída
Priority	Highest (1)	Tipo de prioridade

Tabela 3. Configuração do Nível de Serviço de Mais Alta Prioridade no MasterShaper

Opção	Valor
Name	"Prioridade Alta"
In-Bandwidth	128 kbit/s
Out-Bandwidth	128 kbit/s
Priority	High (2)

Tabela 4. Configuração do Nível de Serviço de Prioridade Alta no MasterShaper

Opção	Valor
Name	"Tráfego Normal"
In-Bandwidth	128 kbit/s
In-Bandwidth Ceil	1024 kbit/s
Out-Bandwidth	128 kbit/s
Out-Bandwidth Ceil	1024 kbit/s
Priority	Normal (3)

Tabela 5. Configuração do Nível de Serviço para o Tráfego Normal no MasterShaper

Opção	Valor
Name	"Baixa Prioridade"
In-Bandwidth	128 kbit/s
In-Bandwidth Ceil	1536 kbit/s
Out-Bandwidth	128 kbit/s
Out-Bandwidth Ceil	1536 kbit/s
Priority	Low (4)

Tabela 6. Configuração do Nível de Serviço de Baixa Prioridade no MasterShaper

Opção	Valor
Name	"Velocidade da WAN"
In-Bandwidth	2048 kbit/s
Out-Bandwidth	2048 kbit/s
Priority	Ignore

Tabela 7. Configuração Referente à Velocidade da WAN

Agora pode-se criar os filtros referentes aos tipos de serviços/aplicações que serão tratados no exemplo, ou seja, o tráfego *web* e o tráfego de pequenos pacotes (ICMP) e de SSH. A **Figura 7** exibe a tela referente à configuração dos filtros, que pode ser acessada pelo menu *Filters*, dentro de *Manage*.

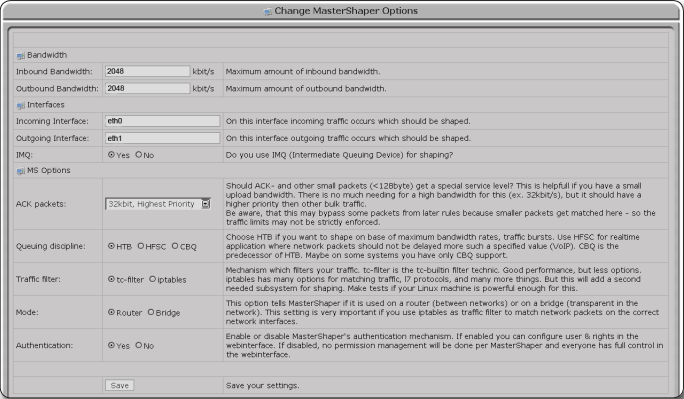


Figura 5. Configuração inicial da rede em MasterShaper

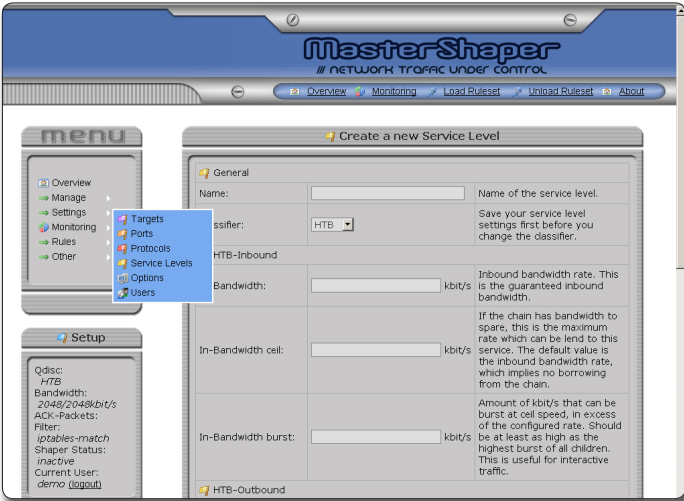


Figura 6. Configuração de Nível de Serviço no MasterShaper

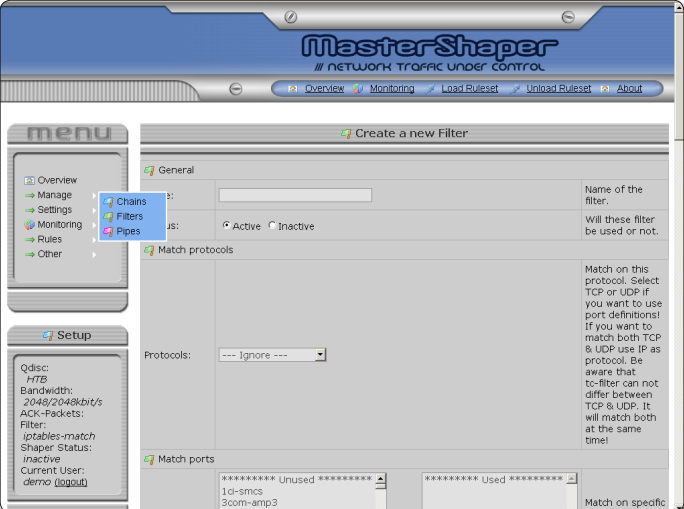


Figura 7. Configuração de Filtros no MasterShaper

As configurações referentes à **Figura 7** são descritas nas **Tabelas 8 a 10**, sendo que para a configuração do tráfego *web* são descritos cada um dos campos. Ainda são configurados os campos SSH, referente ao acesso remoto seguro e o ICMP, para o recebimento de respostas de retorno do protocolo da Internet, o IP.

Opção	Valor	Descrição
Name	"HTTP & HTTPS"	Nome do filtro
Protocols	TCP	Protocolo utilizado pela aplicação
Ports	Seleciona-se e clica-se para mover para a parte de used as opções http e https.	Portas que a aplicação a ser filtrada utiliza

Tabela 8. Configuração de Filtros no MasterShaper.

Opção	Valor
Name	"SSH"
Protocols	TCP
Ports	SSH

Tabela 9. Configuração do Filtro SSH no MasterShaper

Opção	Valor
Name	"ICMP"
Ports	ICMP

Tabela 10. Configuração do Filtro ICMP no MasterShaper

Após esses passos, pode-se retornar ao menu *Options*, dentro da opção *Settings*, já configurada logo no início, para selecionar a prioridade dos pequenos pacotes. No caso, seleciona-se a configuração de "Mais Alta Prioridade" para a opção "ACK Packets", cuja tela é a mesma da **Figura 5**. Pacotes de ACK, como sabemos, são pacotes de confirmação do recebimento de um pacote de dados para controle do remetente.

A **Figura 8** exibe a tela referente à criação de uma nova *chain*. Para configurá-la acesse o menu *Chain*, localizado dentro de *Manage*.

Para preenchimento dos campos expostos na **Figura 8**, utilize-se os valores apresentados na **Tabela 11**.

O próximo passo a ser executado se refere à criação das *Pipes*, ou seja, os serviços separados que serão analisados e tratados. Para tanto, deve-se acessar o menu *Pipes*, dentro de *Manage*. A **Figura 9** exibe a tela referente a esta opção.

Os campos das **Tabelas 12 a 14** se referem à configuração para cada uma das *pipes*, sendo exposta a descrição de cada campo para a primeira configuração referente ao *Ping*.

Pode-se agora seguir à configuração das *targets*, que se referem à configuração da rede. Para isso, deve-se acessar o menu *Targets*, em *Settings*. Será visualizada uma página conforme a **Figura 10**, e então deverá ser criada uma nova entrada com a configuração conforme a **Tabela 15**, respeitando seu IP da rede interna.

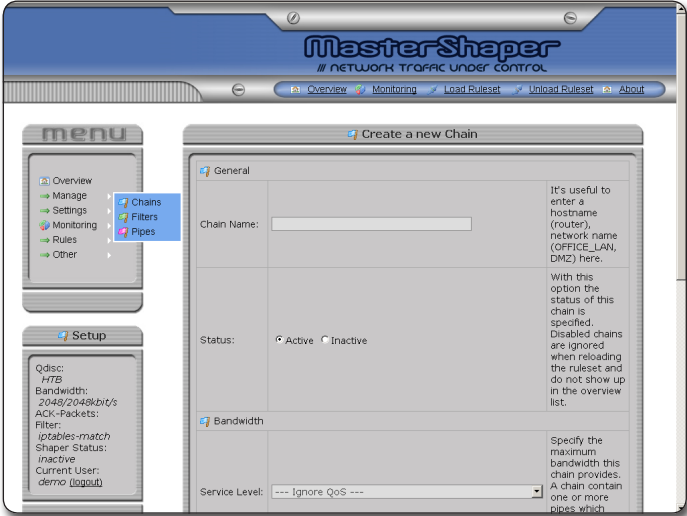


Figura 8. Configuração referente à velocidade da conexão à Internet

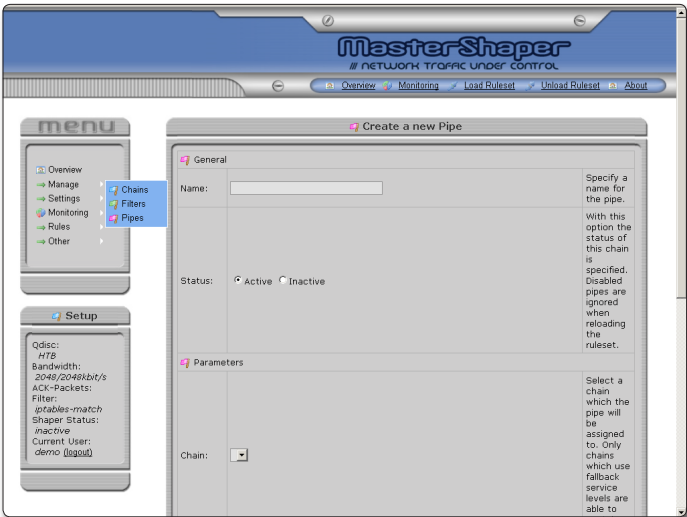


Figura 9. Configuração de Pipes, referente aos serviços no MasterShaper

Usualmente, em ambientes corporativos mais controlados, não se deseja restringir ou controlar o tráfego interno da rede, somente o tráfego que compreende a saída e entrada da Internet. Para isso, é possível configurá-lo de forma que seja totalmente liberado internamente. Para realizar tal configuração deve-se retornar ao menu já configurado *Chains*, em *Manage* (mesma tela da **Figura 8**), e adicionar a configuração da **Tabela 16**.

Uma observação que cabe a este ponto é a necessidade de se determinar a opção *overview*, no topo da interface *web* do MasterShaper, com a *Target* com valor LAN. Essa opção se encontra logo acima do valor *any <-> any* e serve para se ter uma visão geral de suas configurações.

Com todas as configurações realizadas, agora deve-se carregá-las pelo link chamado *load Ruleset*. Toda vez que houver uma modificação nas configurações do MasterShaper será necessário recarregar essa opção. Este link encontra-se no topo da interface *web*.

Opção	Valor	Descrição
Name	WAN	Nome da chain
Service Level	"Velocidade da WAN"	Associação do nível de serviço à chain
Fallback	"Baixa Prioridade"	Prioridade do retorno de mensagens de fallback (referentes a, por exemplo, mau funcionamento de um dispositivo)
Affecting	(Source) Any <-> Any (Destination)	Qual o sentido do fluxo que será afetado por esta regra

Tabela 11. Configuração referente à velocidade da conexão à Internet

Opção	Valor	Descrição
Name	Ping	Nome da pipe
Chain	WAN	Chain a ser utilizada
Direction	<->	Direção do tráfego a ser tratado
Filter	ICMP	Qual o filtro associado à pipe
Service Level	"Mais Alta Prioridade"	Nível do serviço a ser associado à pipe

Tabela 12. Configuração de Pipes, referente ao protocolo ICMP no MasterShaper

Opção	Valor
Name	Acesso Remoto
Chain	WAN
Direction	<->
Filter	SSH
Service Level	"Alta Prioridade"

Tabela 13. Configuração de Pipes, referente ao acesso via SSH no MasterShaper

Opção	Valor
Name	Tráfego Web
Chain	WAN
Direction	<->
Filter	HTTP & HTTPS
Service Level	"Tráfego Normal"

Tabela 14. Configuração de Pipes, referente ao acesso aos serviços de HTTP e HTTPS no MasterShaper

Opção	Valor	Descrição
Name	LAN	Nome da target
IP	192.168.0.24/24	Endereço IP ou bloco de IPs compreendido pela target

Tabela 15. Configuração referente ao bloco de IPs da rede interna

Opção	Valor
Name	LAN
Service Level	Ignore
Target	LAN <-> LAN

Tabela 16. Configuração referente à liberação de tráfego na rede interna

Observa-se do lado esquerdo de sua interface *web*, caso toda a configuração esteja correta e as regras tenham sido aplicadas com sucesso, a partir da tabela com título *Setup* (como mostra a

Figura 11), o valor *Active* em *Shaper Status*. Nessa mesma tabela é possível verificar de forma resumida suas configurações.

Para finalizar, é interessante observar no menu *Show*, em *Rules*, todas as configurações em modo texto que o MasterShaper gerou a partir de suas configurações.

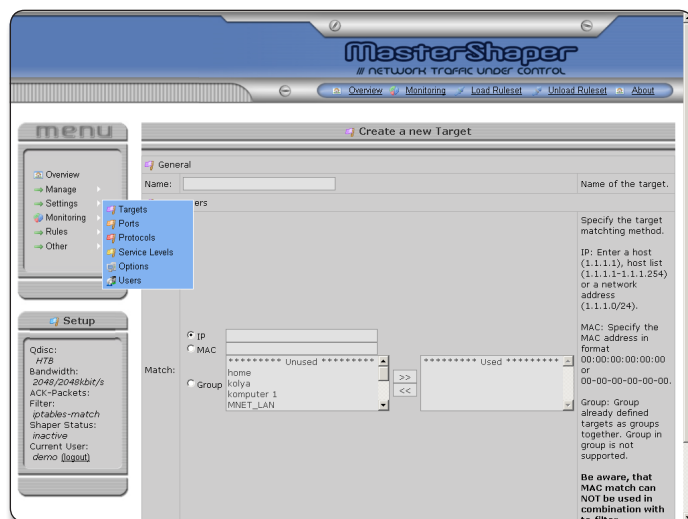


Figura 10. Configuração referente ao bloco de IPs da rede interna

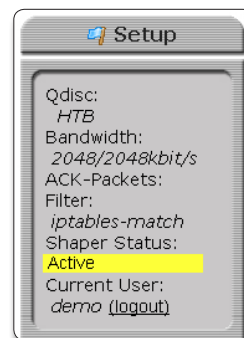


Figura 11. Resumo do status do MasterShaper

Conclusão

Foram apresentados neste artigo os principais conceitos de *QoS*, assim como uma ferramenta para implantação em um ambiente real, denominada MasterShaper. O MasterShaper é uma interface amigável ao administrador de rede para a configuração de recursos de controle de banda (*traffic shaping*) e *QoS* sem a necessidade de profundos conhecimentos das sintaxes de configuração dos módulos do *kernel* do Linux que realizam tais tarefas. Após a leitura deste artigo, acredita-se que vários conceitos básicos de *QoS* estão mais claros para o leitor e este pode pensar em como usufruir dessas técnicas para melhorar o desempenho de sua rede em um ambiente de trabalho compartilhado.

Com o MasterShaper é possível também realizar configurações que visam o compartilhamento de banda de forma mais justa, assim como a priorização de tráfegos mais importantes ao funcionamento do ambiente de rede por meio da utilização de *QoS*.

A exposição de um exemplo utilizando a ferramenta MasterShaper visou, além de ilustrar os conceitos apresentados pelo artigo, servir como uma referência durante a análise e implementação de qualidade de serviço e controle de banda em um ambiente corporativo. Por fim, se mostrou uma excelente ferramenta para o estudo da sintaxe dos módulos do *kernel* do Linux, uma vez que o código de *script* pode ser consultado pelo usuário após a conclusão da configuração.

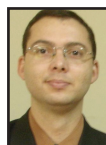
Pensar em *QoS* é pensar em compartilhar de forma justa e controlada a utilização dos recursos da conexão de sua rede.



Edielberto Franco Silva

esilva@ic.uff.br

Doutorando e Mestre em Computação pela Universidade Federal Fluminense. Tem como interesse as áreas de redes sem fio e segurança em redes. Atualmente desenvolve projetos relacionados à integração de serviços de autenticação para redes sem fio nas universidades federais brasileiras (Eduroam).



Eduardo Pagani Julio

epagani@gmail.com

Doutorando e Mestre em Computação pela Universidade Federal Fluminense. Atualmente é professor da Universidade Federal de Juiz de Fora em disciplinas ligadas à área de redes.



Endereço do MasterShaper

<http://www.mastershaper.org>

Rede Nacional de Pesquisa (RNP)

<http://www.rnp.br>

Site sobre CBQ

<http://www.icir.org/floyd/cbq.html>

Site sobre HTB

<http://luxik.cdi.cz/~devik/qos/htb/>

Site sobre HFSC

<http://www.cs.cmu.edu/~hzhzhang/HFSC/main.html>

Site sobre IANA

<http://www.iana.org/about/>



Os atuais riscos da Engenharia Social

YURI DIOGENES

Em tempos que a Internet tornou-se um fenômeno de uso em todo o mundo e no Brasil se proliferou pelas diversas classes sociais, a participação de pessoas de todas as idades em redes sociais é algo crescente. A exposição dos usuários à Internet saiu dos computadores e foi para os dispositivos móveis, fazendo com isso que o usuário sempre esteja conectado de alguma forma.

Ao passo que tal avanço traz uma série de benefícios, é fato também afirmar que uma série de novos riscos é introduzida por este cenário. Assim, a engenharia social, que durante muito tempo ganhou destaque pela persuasão através do contato físico, passa a ter um novo mecanismo de exploração. Neste contexto, este artigo mostra as principais áreas em que a engenharia social pode ser usada neste novo contexto da Internet e seus recursos sociais.

Entendendo o problema

A técnica de engenharia social vem sendo utilizada de forma criativa por uma diversa gama de hackers e organizações criminosas que procuram explorar o ponto mais fraco da cadeia de segurança: o ser humano. O foco da engenharia social é persuadir a vítima de forma a convencê-la a tomar uma determinada ação. Ao executar tal ação o usuário poderá estar expondo uma vulnerabilidade que mais tarde será explorada pelo criminoso que iniciou tal ataque.

A engenharia social não está diretamente relacionada ao uso de tecnologia para ser realizada com sucesso, na realidade o uso mais tradicional de engenharia social é basicamente a conversa. Um exemplo clássico disso é o simples fato de pegar o telefone e ligar para alguém dentro da empresa fingindo ser membro do departamento de TI e requisitando dados pessoais para fins de auditoria no ambiente.

Nos últimos anos a engenharia social vem ganhando novas formas de exploração e cada vez mais o nível de sofisticação dos ataques é aprimorado. Um caso recente (Abril de 2011) de engenharia social que ganhou manchetes foi o caso da RSA (divisão de segurança da EMC). Neste caso um funcionário da empresa recebeu um e-mail cujo assunto dizia “2011 Recruitment Plan” (Plano de Recrutamento 2011). Apesar de a tecnologia ter funcionado em prol do bem neste caso (pois o e-mail caiu direto na caixa de lixo eletrônico), o funcionário retirou o e-mail da caixa de lixo eletrônico e colocou de volta na caixa de entrada. Ele achou que o e-mail caiu nesta pasta por engano, devido ao fato do e-mail ter um teor tão original e parecer válido. Neste e-mail havia um arquivo do Excel anexado com um arquivo Adobe Flash embu-

Resumo DevMan

De que se trata o artigo:

O artigo mostra o cenário atual da Internet e suas ameaças em uma visão onde as redes sociais são usadas para obter informações que podem traçar o perfil da vítima que será atacada. O artigo também foca nos cuidados necessários que devem ser tomados para evitar este tipo de situação.

Em que situação o tema é útil:

O tema é útil para todos os usuários de Internet que utilizam redes sociais, para empresas que planejam implementar um treinamento básico de segurança para seus funcionários e para profissionais de TI que desejam entender como a engenharia social pode usar as redes sociais para obter informações de um usuário.

Os atuais riscos da Engenharia Social:

Este artigo mostra as principais áreas em que a engenharia social pode ser usada neste novo contexto da Internet e seus recursos sociais. O artigo expõe alguns cenários reais onde o uso da engenharia social foi capaz de burlar recursos tecnológicos de segurança e também mostra como as pessoas devem se preparar para lidar com situações semelhantes.

tido que explorava um “Zero Day” (CVE 20110609) – veja a **Nota DevMan 1**. Note que uma simples ação do usuário colocou toda a empresa em risco e trouxe uma série de efeitos negativos para a mesma.



Nota do DevMan 1

Zero Day: Um Zero Day é uma ameaça (threat) que tenta explorar uma vulnerabilidade que não é conhecida.

Este tipo de problema mostra a fragilidade dos usuários e prova que não adianta investir milhões em tecnologia se o corpo de funcionários da empresa não está adequadamente treinado do ponto de vista de conceitos básicos de segurança e como lidar com ameaças em potencial. Porém, é importante salientar que atualmente os usuários não estão apenas expostos a estes riscos vindos via e-mail, telefone ou até mesmo durante um bate papo informal no corredor da empresa, o risco ainda é maior quando usuários começam a usar redes sociais para compartilhar seus costumes.

Os Riscos das Redes Sociais

Não há como negar que as redes sociais vêm revolucionando as comunicações entre empresas e consumidores, mais ainda, está mudando a forma com que as pessoas interagem com os amigos e família de uma forma geral. Entretanto, assim como toda ferramenta que é criada para uma determinada finalidade, pode também se tornar uma arma contra o próprio usuário, caso não seja manuseada com responsabilidade. O que é possível notar é que as redes sociais estão cada vez mais sendo usadas para obtenção de informações de usuários para diversos fins, entre eles podemos citar comprometimento da privacidade, estabelecer perfil para fins maliciosos, obter informações de preferências (restaurante onde almoça, lugares que frequenta, etc.) e localização geográfica.

Existem diversos programas na Internet já disponíveis para facilmente criar um perfil do usuário baseado nas localidades de onde ele frequenta (devido a serviços de localização como o Foursquare), rotinas e hábitos mais comuns (informação que pode ser obtida através dos posts do Twitter) até mesmo, em alguns casos extremos, obtenção de informações pessoais (como data de nascimento e telefone), através de redes sociais como o Facebook. Um exemplo de uma ferramenta que pode ser usada para obter maiores informações de usuários do Twitter é o Cree.py (<http://ilektrojohn.github.com/creepify/>), apresentado na **Figura 1**.

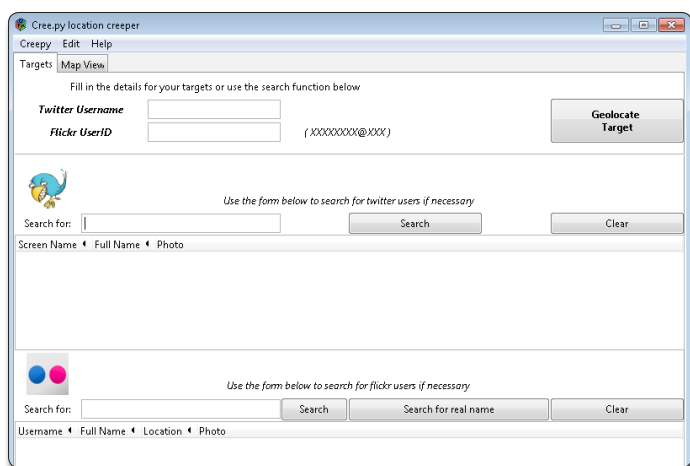


Figura 1. Interface do Cree.py

Com essa ferramenta você pode encontrar informações geográficas de onde está o usuário e os locais de onde ele efetuou o acesso (de onde ele “Tuitou”). Com isso é possível construir um mapa das localidades comumente frequentadas pelo usuário. Tendo posse destas informações, um criminoso terá uma área de atuação muito mais focada, pois ele conhecerá os passos da sua vítima e poderá planejar como e onde atacar.

Um número importante a ser citado vem do Relatório de Inteligência de Segurança da Microsoft (Volume 10). Nele é informado que o ataque do tipo “Phishing” (que é um ataque que utiliza o correio eletrônico para enviar uma mensagem falsa, porém com assunto e formato que parecem ser de uma origem confiável) usando redes sociais cresceu de 8.3% em Janeiro de 2010 para

84.5% em Dezembro de 2010. Em suma, isso demonstra que usuários ficam mais vulneráveis a ataques desta natureza vindo de origem que eles confiam, como o ciclo de amigos das redes sociais que eles frequentam. Muitos destes ataques visam à obtenção do nome do usuário e senha.

Uso da Engenharia Social em Ataques

Durante muito tempo o termo “Engenharia Social” foi sinônimo exclusivamente de ações envolvendo o ato de ludibriar pessoas através de conversas por telefone ou pessoalmente. Apesar destes vetores de ataque ainda serem usados na engenharia social, outras formas de explorar as fraquezas humanas vêm crescendo a cada dia. Trata-se dos ataques eletrônicos com uso de conceitos de engenharia social.

Conforme citado no início deste artigo, o envio de e-mail falso com teor verdadeiro para atizar a curiosidade do usuário e fazer com que o mesmo execute uma ação, que por sua vez pode ser um simples clique, é o um ataque crescente.

Os ataques do tipo Phishing, por exemplo, tentam usar da engenharia social para ludibriar o usuário afirmando que no seu último acesso à conta bancária foi detectado um vírus, sugerindo o download de uma solução para curar este vírus, conforme mostra a **Figura 2**.

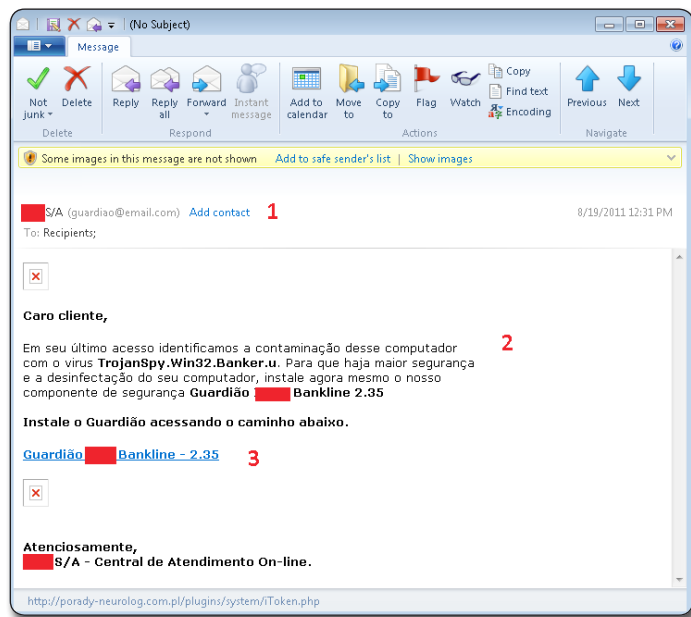


Figura 2. Um e-mail falso com a tentativa de ludibriar o usuário

No e-mail mostrado na **Figura 2** existem três áreas onde é possível identificar a farsa:

- O endereço de origem do e-mail geralmente vem de um domínio que não é o do banco em questão;
- O corpo do e-mail geralmente sugere algo que não está em acordo com as normas de segurança do banco que você frequenta;
- O link para download da solução sugerida redireciona para uma URL que não tem nada haver com o banco onde você tem conta (ver barra de status na parte inferior da tela).

Uma outra forma de usar engenharia social para propagar malware é através do ato de inserir o malware em um drive USB e entregar este USB para alguém. O usuário que recebe um drive USB geralmente insere no computador sem muitos cuidados, e se este computador estiver com o sistema operacional Windows e a característica de Autorun estiver habilitada, então uma janela automaticamente aparecerá para que o usuário abra o conteúdo do drive USB. Neste momento uma série de ações podem ser executadas em background para comprometer a máquina do usuário.

Este tipo de ataque (com uso do recurso de Autorun) é crescente no Brasil. De acordo com o Relatório de Inteligência de Segurança da Microsoft (Volume 10), a família de ameaça que predominou no Brasil em 2010 foi o Win32/Autorun, detendo 20.3% dos computadores afetados, conforme mostra a **Tabela 1**.

	Family	Percent of Computers Affected
1	Win32/Autorun	20.3%
2	Win32/Bancos	14.4%
3	Win32/Conficker	9.4%
4	HTML/FrameRef	8.5%
5	Win32/Banload	7.4%
6	Win32/Sality	7.0%
7	JS/Pornpop	6.7%
8	Dynamer	5.6%
9	Win32/Keygen	5.4%
10	Win32/Rimecud	4.9%

Tabela 1. Relatório de Famílias de Malwares que prevaleceram no Brasil em 2010

Isso mostra justamente que os usuários apenas seguem instruções que veem na tela, sem de fato atentar quanto aos riscos em potencial que tal ação pode ter. Muito disso dar-se devido à falta de informação e do conhecimento básico das premissas de segurança.

Preparando sua Empresa para lidar com estas Ameaças

Um funcionário de uma empresa hoje em dia está exposto a um mundo virtual que é imenso, e assim como em um mundo real, este mundo está cheio de riscos. Por este motivo, é importante conscientizar todos os funcionários acerca de tais riscos e como prevenir-se.

Estes riscos ficam ainda maiores quando se sabe que muitas vezes o funcionário utiliza seu computador pessoal para acessar dados da empresa. Isso pode expor a empresa a uma série de riscos caso o acesso remoto não seja feito de forma controlada. Em alguns cenários é possível destacar também o acesso feito através de computadores de terceiros. Como por exemplo, o colaborador que está em viagem, sem seu laptop, mas precisa enviar um e-mail para a empresa. Geralmente neste tipo de situação é comum que ele procure um computador no Hotel que está hospedado ou em uma Lan House nas proximidades onde se encontra. Os riscos de inserir suas credenciais neste computador são altos, pois não se sabe a procedência do mesmo. Muitas pessoas inclusive usam tais computadores para fazerem acesso às redes sociais e atualizar o status (informando onde está e o que está fazendo). Um típico

cenário de acesso remoto é mostrado na **Figura 3**. Neste cenário o usuário remoto está se conectando aos recursos da rede interna via VPN, que por sua vez é um método mais seguro.

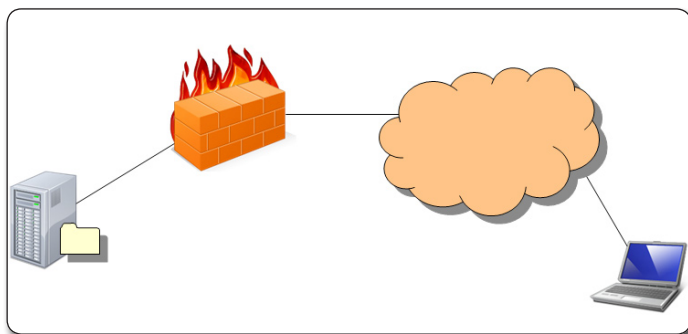


Figura 3. Típico cenário de acesso remoto através de VPN

Acima de tudo, é importante lembrar que mesmo que todos os controles de segurança e toda tecnologia cabível para tal ambiente estejam implementadas, no final é o usuário que tem o controle de tomar a decisão do que fazer. Lembre-se, muitas vezes basta um clique para comprometer todo o sistema.

É justamente por saber que o ser humano é o elo mais fraco da cadeia de segurança que o investimento em treinamento básico de segurança para todos é vital para as empresas hoje em dia. Portanto, todas as empresas hoje em dia precisam investir no chamado “Security Awareness Training” (Treinamento de Conhecimento de Segurança). Trata-se de um treinamento onde se traz ao conhecimento de todos os principais termos relacionados à segurança, incluindo:

- Definição de terminologias (malware, adware, etc.);
- Cuidados ao usar Redes Sociais;
- Conhecimento básico de Engenharia Social;
- Cuidados físicos no ambiente de trabalho;
- Cuidados com mídias removíveis;
- Uso dos recursos da empresa (laptops) durante viagens e acesso remoto.

É importante também salientar que tal treinamento precisa estar dentro do cronograma de treinamentos obrigatórios da empresa. Ou seja, o departamento de recursos humanos precisa exigir que tal treinamento seja feito e atualizado todo ano. Além disso, é importante que exista uma equipe de especialistas que atualize o treinamento todo ano, até mesmo porque novas tecnologias vão surgir e com isso também vão surgir novos riscos. O treinamento precisa cobrir assuntos da atualidade para que tenha de fato valor para o funcionário. Por sua vez, os funcionários precisam fazer o treinamento e assinar atestando que fizeram tal treinamento. A assinatura confirmando o treinamento é vital para que fique registrado que o funcionário fez o treinamento. Isso é importante para fins legais, ou seja, se um dia o funcionário infringir o código de conduta da empresa através da violação de algo que foi repassado no treinamento, ele não terá o argumento de dizer que não foi treinado naquele assunto.

No final deste artigo, na seção de **Links**, você encontrará um link para um artigo que pode ser usado como base para criação de um "Security Awareness Training".

E você, o que pode fazer?

Independente da empresa em que você trabalha ter ou não um programa de treinamento básico de segurança da informação, você deve proteger-se e ficar alerta quanto aos riscos expostos neste artigo. Segue abaixo as dez principais dicas para você se proteger de tais riscos:

- Assegure que as configurações de privacidade do seu perfil nas redes sociais que você utiliza estão configuradas de tal forma que informações pessoais não vazem para pessoas que você não confia;
- Se você usa serviços de localização (como o Foursquare), NUNCA faça o "check in" na sua residência ou em residências de parentes e amigos. Isso pode expor seu endereço ou os endereços de outros para todos na Internet;
- Se você usa serviços de localização para exercícios físicos (como o RunKeeper ou Endomondo), assegure que o mapa de onde você faz suas atividades físicas não é exposta para todos. Mantenha o mapa em sigilo apenas para as outras pessoas que fazem atividade física com você;
- Ao postar seu status em sites de relacionamento ou serviços como o Twitter, procure não revelar informações confidenciais, mesmo que esteja passando por um momento que precise desabafar. Muitas vezes os usuários ficam mais vulneráveis a continuar liberando mais e mais informações ao seu respeito em momentos como esse;
- Ao acessar sites de redes de relacionamento procure sempre usar a versão segura de acesso ao site com uso de HTTPS. Muitos sites já alternam automaticamente para HTTPS mesmo quando você não digita. Fique atento a isso e procure navegar sempre de forma segura. A não navegação de forma segura expõe sua navegação a um potencial ataque de captura de sessão (*session hijack*). Veja exemplo do firesheep nos **Links** ao final deste artigo;
- Evite usar computadores públicos, porém, se for usar, assegure que o computador tem um antivírus atualizado e que as informações do browser são apagadas após você finalizar a sessão;
- Ao usar redes wireless públicas, procure não entrar em sites que por ventura exponham dados sigilosos ao seu respeito. Procure apenas navegar em páginas que não comprometam sua privacidade enquanto conectado em locais públicos;
- Mantenha seu computador pessoal sempre atualizado do ponto de vista do sistema operacional e aplicações;
- Mantenha seu computador pessoal sempre com um antivírus atualizado e com uma solução de firewall pessoal habilitada;

- Nunca compartilhe suas credenciais (usuário e senha) de nenhum serviço online.

Conclusão

Neste artigo abordamos um pouco sobre os riscos envolvendo engenharia social nos dias de hoje e como as redes sociais podem ser utilizadas para obtenção de informação durante a preparação para um ataque. O artigo também mostrou outros vetores de exploração de engenharia social, como é o caso do uso de unidades removíveis (USB) e o crescente uso deste tipo de ataque no Brasil. Podemos concluir que a melhor forma de preparar-se para este novo mundo de ameaças online é nos munirmos de conhecimento acerca dos riscos e ensinar aos demais como lidar com tais situações. Sempre ensinando que o elo mais fraco da cadeia de segurança é o ser humano.



Yuri Diogenes

yuridiogenes@hotmail.com

Yuri Diogenes (CISSP, EC|CEH, E|CSA, CompTIA Security+, Network+, Microsoft MCITP, MCTS, MCSA/MCSE+Security, MCSE+Internet, MCSA/MCSE+Messaging, membro da ISSA North Texas e da American Society of Digital Forensics & eDiscovery) é autor de livros

na área de segurança da informação e ex membro do grupo de engenharia de suporte a produtos da linha Forefront TMG. Atualmente Yuri trabalha no grupo Windows IT PRO Security da Microsoft. Yuri também escreve no seu blog em inglês <http://blogs.technet.com/yuridiogenes> e em Português <http://yuridiogenes.wordpress.com>. Você também pode seguir o Yuri no Twitter (@yuridiogenes).



Caso de Brecha da RSA

<http://blogs.gartner.com/avivah-litan/2011/04/01/rsa-secrid-attack-details-unveiled-they-should-have-known-better>

Vulnerabilidade Explorada no ataque contra RSA

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0609>

Microsoft SIR (Security Intelligence Report)

http://www.microsoft.com/security/sir/threat/default.aspx?l=brazil_d

Informações sobre o Autorun

<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32/Autorun>

Security Awareness Training

<http://blogs.technet.com/b/yuridiogenes/archive/2011/07/06/security-awareness-training-why-is-this-so-important-nowadays.aspx>

Demonstração do uso do Firesheep para fazer Session Hijack

http://www.metacafe.com/watch/5472570/session_hijacking_with_firesheep/



RENOVE JÁ!

Sua assinatura pode estar acabando



Renovando a assinatura
de sua revista favorita
você ganha brindes
e descontos exclusivos.

Faça a renovação de sua assinatura agora mesmo.



www.devmedia.com.br/renovacao ou (21)3382-5038



Implementando uma VPN

MÁRIO DE MELLO BITTENCOURT NETO

O ambiente globalizado e competitivo no qual nos inserimos faz com que o trabalho remoto, quer seja a partir de casa, do aeroporto, no hotel ou em um Cliente seja uma realidade.

Nestas condições é cada vez mais comum que tenhamos que usar um canal de comunicação externo, e normalmente público, para acessar recursos sensíveis dentro de nossas redes corporativas.

Em função desse ambiente, este artigo apresentará alguns procedimentos necessários para se planejar e implementar uma solução open-source para a comunicação segura. Iremos criar um canal criptografado para a troca de informações entre um usuário externo e uma rede interna usando a Internet.

O cenário atual e o perigo envolvido

O trabalho em rede faz parte do nosso dia-a-dia já há algum tempo e o uso de sistemas cliente-servidor já é lugar comum dentro do ambiente corporativo. Este vem se intensificando nos últimos 15 anos com o advento e popularização da Internet comercial de alta velocidade.

Se somarmos a esse fato a globalização da economia, temos um contingente nunca antes visto trabalhando fora das redes corporativas. Hoje não é raro ver consultores trabalhando dos escritórios de seus clientes, desenvolvedores trabalhando de casa e designers interagindo remotamente a partir de hotspots em praças de alimentação de shoppings.

A ligação que une todos os profissionais acima é a Internet. Um meio de comunicação conhecido pela sua falta de segurança. É, entretanto, através dele que muitos de nós nos mantemos conectados com o mundo, quer seja para diversão ou trabalho.

A presença quase que universal do acesso faz com que muitas vezes não nos perguntemos como a segurança é tratada nesse meio. E na verdade a resposta seria em muitos casos que a segurança não é sequer um ponto relevante na construção e manutenção desse acesso.

Hoje em dia nenhum exemplo ilustra mais isso do que os pontos de acesso públicos utilizados em aeroportos e shopping centers. Estes pontos normalmente não utilizam nenhuma tecnologia para criptografar os dados e permitem, por exemplo, que qualquer membro da rede possa capturar todo o tráfego que por ela passa. Nessa situação, senhas, e-mails e quaisquer informações não protegidas pelo usuário podem ser acessados sem que o remetente ou destinatário saibam.

Ao considerarmos a gravidade dessa situação em nossas vidas pessoais é possível ver que o dano se estivermos trocando informações corporativas é ainda maior.

Resumo DevMan

De que se trata o artigo:

Este artigo trata de como planejar e criar um ambiente seguro de comunicação em um canal público de dados (Internet).

Para que serve:

Serve para garantir que os dados trafegados em um canal de dados públicos possam ser protegidos de acessos indevidos.

Em que situação o tema é útil::

Em um ambiente no qual você está utilizando uma infraestrutura pública, como a Internet, e deseja prover privacidade nas informações trafegadas quando se comunica com servidores corporativos de sua empresa.

Resta então nos perguntar o que pode ser feito para se mitigar o risco envolvido nessa comunicação.

Alternativas

Segurança na comunicação de redes é um assunto complexo e multi-disciplinar. Em nosso contexto avaliaremos que alternativas existem para tratar especificamente o trabalho remoto no qual um agente externo precisa acessar recursos da rede corporativa de uma empresa de forma segura.

Este problema não é novo e na verdade existia antes mesmo do advento da Internet comercial. As opções que existiam eram:

- Conexão discada;
- Conexão dedicada ponto-a-ponto.

Na conexão discada a empresa montava (ou contratava de operadoras de telefonia) uma estrutura de modems e linhas telefônicas similar à encontrada nas BBS (*Bulletin Board System*). O agente externo possuía um modem e discava para o número da empresa. Ao se conectar ele tinha acesso à rede da empresa.

Essa solução tinha algumas características limitantes, dentre elas a velocidade que era baixa e muito suscetível à qualidade das linhas telefônicas. A outra limitação era o custo que se tornava alto por conta da tarifação de consumo por minuto (ou pulso) e o fato de que se o agente estivesse em outro estado, ou país, o que se fazia era uma ligação interurbana ou internacional.

Na conexão dedicada ponto-a-ponto a empresa contratava um canal dedicado ponto-a-ponto entre seu endereço e o do agente externo. Eram colocados roteadores em ambos os lados e com isso a comunicação entre os computadores das redes ligadas podiam trocar informações.

Diferentemente da conexão discada, esta solução era conhecida por ter velocidades maiores e por ser dedicada tinha um custo normalmente fixo, independente do tempo ou dados trafegados.

Infelizmente ela compartilhava com a conexão discada uma característica negativa (custo elevado) e trazia uma desvantagem só sua: falta de mobilidade. Como a conexão era dedicada, ambos os pontos tinham que ser fixos, o que era perfeitamente aceitável para uma ligação entre matriz e filial, mas não realista para a força de trabalho móvel.

A verdadeira alternativa para o nosso ambiente veio com a adoção das características positivas de ambas as soluções com um novo ingrediente à época: a Internet.

A alternativa encontrada, batizada de VPN (*Virtual Private Network*) ou rede privativa virtual, consiste em se criar um canal que permita que as informações saiam de um ponto remoto e cheguem na rede corporativa como se estivessem em um canal ponto-a-ponto.

Como o canal é criado sobre a Internet e não sobre uma conexão ponto-a-ponto, ele é chamado de virtual por na prática usar o canal público para estabelecer esta comunicação, como demonstrado na **Figura 1**.

Veremos a seguir algumas tecnologias para estabelecimento de VPN antes de iniciarmos a configuração de nosso ambiente.

Tecnologias de VPN

Ao longo dos anos várias tecnologias foram apresentadas para tratar da criação de redes privativas virtuais. Dentre as existentes, destacamos três delas:

PPTP

A primeira das tecnologias que destacamos, PPTP (*Point-to-Point Tunneling Protocol*), foi criada por um consórcio de várias empresas, entre elas a Microsoft, Ascend (comprada pela Lucent) e 3Com. A sua especificação foi definida na RFC 2637 de 1999, e por ter a Microsoft como um participante do consórcio que criou o protocolo, este foi suportado pelos sistemas operacionais desta, o que ajudou a popularizar o acesso à criação de VPNs.

Entretanto, as escolhas técnicas adotadas para os métodos de autenticação e criptografia usados pelo protocolo foram

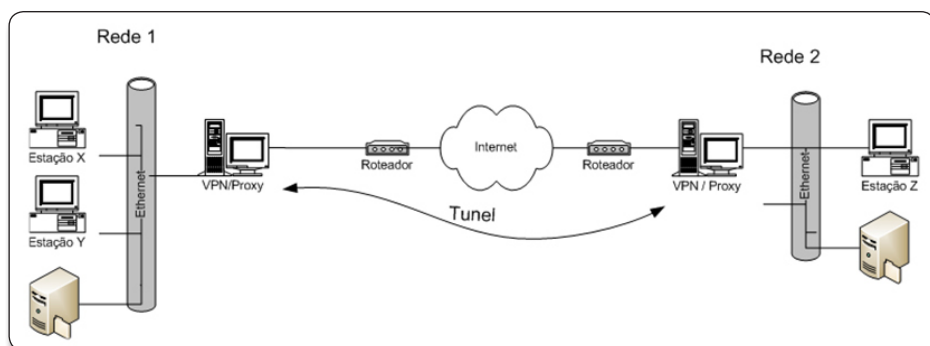


Figura 1. Uma VPN típica

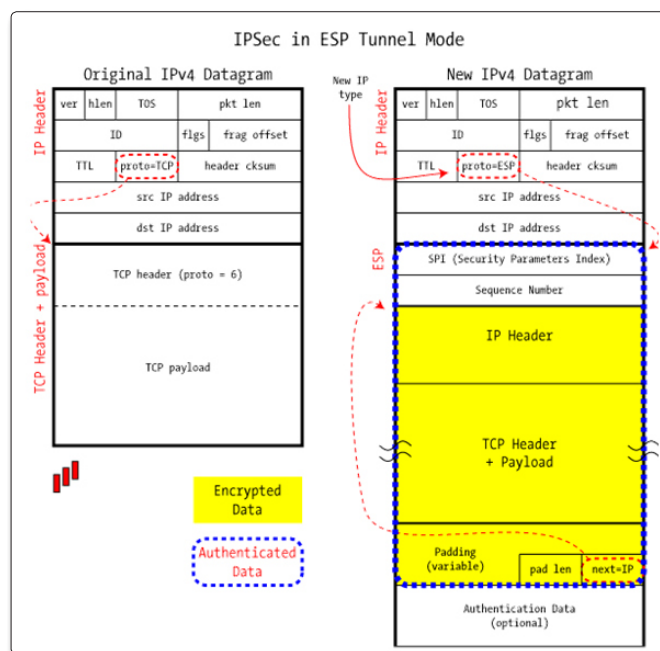


Figura 2. Encapsulamento do cabeçalho e dados originais dentro do túnel

amplamente criticados por suas vulnerabilidades intrínsecas.

Hoje, apesar de já existir suporte a esse protocolo em outras plataformas, tais como Cisco, Linux e Mac OS, o uso do PPTP tem se reduzido e não é recomendável frente às demais opções disponíveis.

IPSEC

A segunda opção, IPSEC (*IP Security*), consiste – na verdade – de se trazer uma funcionalidade existente na versão 6 do IP (*Internet Protocol*) e aplicá-la à versão 4, que é a atualmente em uso.

O IP na versão 4 não foi criado com a preocupação de segurança. Por esta razão, nas especificações deste não vemos questões como autenticação ou privacidade dos dados sendo trocados.

Quando da criação da nova versão, verificou-se que o ambiente na qual a nova

versão seria utilizada não seria possível abandonar essas premissas. Desta maneira incorporaram-se itens como criptografia diretamente no protocolo.

No entanto, com a demora na adoção do IPv6, decidiu-se que pelo menos as capacidades de segurança deste deveriam ser disponibilizadas para a versão atual, mesmo que sob a forma de uma funcionalidade opcional.

No caso do IPSEC, o processo de criação da VPN acontece na camada 2 do TCP/IP. Na **Figura 2** vemos um modo de trabalho do IPSEC no qual quando há a criação do túnel, o cabeçalho do pacote a ser transmitido é alterado de forma a esconder a real origem e destino do pacote antes de ser transmitido.

Todo o conteúdo original (destaque em amarelo) é criptografado de maneira a proteger a integridade deste enquanto ele trafega pelo canal público.

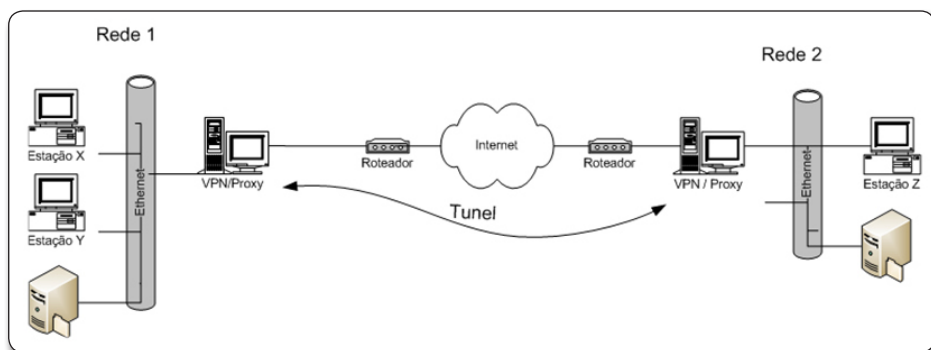


Figura 3. VPN rede a rede

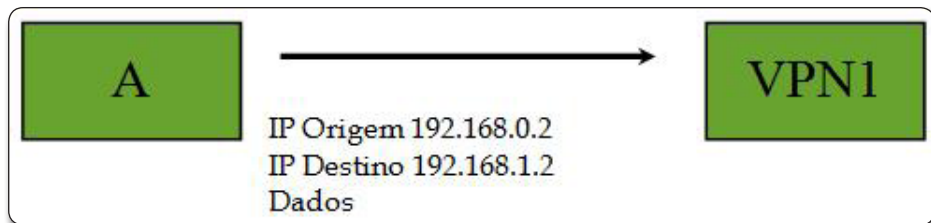


Figura 4. Tráfego original da estação e o gateway

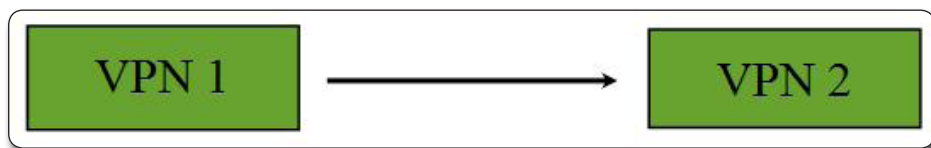


Figura 5. Transmissão entre os servidores de VPN

Do ponto de vista de segurança, o IPSEC apresenta uma solução muito mais segura e flexível do que o PPTP. Entretanto, a maneira como ele funciona, alterando-se o cabeçalho do IP, apresenta problemas com firewalls e sistemas que realizam o NAT (*Network Address Translation*) do endereço IP.

Estes sistemas, comuns em pontos de acesso como hotéis e hotspots, acabam por dificultar o uso do IPSEC no ambiente em geral.

OpenVPN

Nossa terceira opção, OpenVPN, é uma implementação da tecnologia chamada de SSL VPN. Essa tecnologia, conhecida também como user space VPN, utiliza um protocolo que atua na camada de aplicação chamado de SSL (*Secure Socket Layer*) e já conhecido por ser usado para prover a criptografia para acesso a sites.

Quando você acessa um site seguro (reconhecido pelo uso de https no endereço) a informação que sai de seu computador é

criptografada utilizando um par de certificados digitais e chaves de maneira a impedir que os dados transmitidos, mesmo que capturados, possam ser utilizados por outro ponto que não o destinatário.

O OpenVPN, assim como outras implementações do SSL VPN, usa a mesma tecnologia para criar um canal seguro entre o remetente e o destinatário. Por atuar na camada de aplicação, daí a denominação de user space VPN, o OpenVPN requer pouca modificação da estrutura de rede e trabalha bem com os firewalls e roteadores dos pontos de acesso existentes.

Outra característica interessante do OpenVPN é a interoperabilidade entre os sistemas operacionais. É possível ter um servidor Linux e acessá-lo a partir de uma máquina com Mac OS ou Windows sem problemas.

Cenário de uso

Neste artigo veremos dois cenários de uso para a VPN que são facilmente encontrados em nosso dia-a-dia.

Rede a rede

No cenário de rede a rede temos, como o próprio nome sugere, duas redes que serão interligadas pela VPN – conforme apresenta a **Figura 3**.

Nessa situação a VPN é estabelecida entre os dois servidores de ambos os lados. Os membros da rede local 1 desconhecem que exista a VPN e, sem alteração nenhuma em suas configurações, podem acessar as máquinas da rede 2.

Como funciona esse processo?

Suponha o ambiente abaixo:

- Rede 1: 192.162.0.0/24, servidor VPN com dois IPs, um da rede local (192.168.0.1) e outro da Internet (200.241.128.1);
- Rede 2: 192.162.1.0/24, servidor VPN com dois IPs, um da rede local (192.168.1.1) e outro da Internet (200.243.37.1).

Digamos que uma máquina (A) da rede 1, IP 192.168.0.2, deseja conversar com a máquina (B) da rede 2, de IP 192.168.1.2.

Deste modo, a máquina (A) irá enviar o pacote para seu gateway, 192.168.0.1. Ao receber este pacote o gateway identificará que o destino pertence à rede 2, conforme a **Figura 4**.

Ele irá então criar um novo pacote contendo como endereço de origem seu IP público, 200.241.128.1, e como endereço de destino o IP público do servidor de VPN da rede 2, 200.243.37.1. O servidor de VPN encapsulará todo o pacote original, o criptografará e o transmitirá como dados do novo pacote através da internet, conforme a **Figura 5**.

Ao chegar ao servidor de VPN da rede 2 o processo é revertido de maneira que a máquina (B) irá receber o pacote original de (A) achando que tem comunicação direta com este. A **Figura 6** ilustra esta etapa final.

Desta maneira as máquinas (A) e (B) poderão trafegar os dados através da Internet sem que o conteúdo seja exposto, por estar criptografado, e sem necessitar de configurações especiais nelas, apenas nos servidores de VPN.

Host a rede

No cenário de host a rede temos o ambiente mais comum existente no trabalho

remoto, no qual você tem uma estação (host) que acessa a rede corporativa – observe a **Figura 7**.

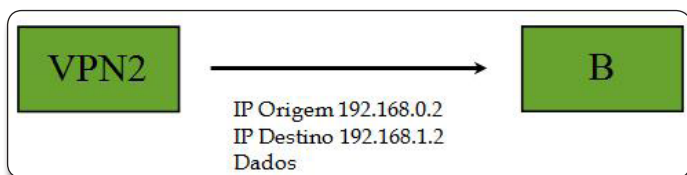


Figura 6. Transmissão entre o servidor de VPN e o destino final

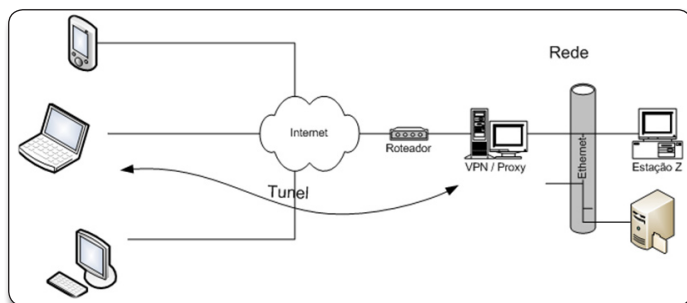


Figura 7. VPN host a rede

De forma similar ao que vimos no cenário rede a rede, os dados são encapsulados e criptografados antes de serem transmitidos.

O que acontece de diferente em relação ao cenário apresentado anteriormente é que neste será necessário instalar na máquina do usuário o software para o estabelecimento da VPN. Com isso ela deve ser configurada para estabelecer a VPN, não acontecendo da forma transparente como na configuração rede a rede.

O ambiente de teste

O cenário mais comum em um ambiente de VPN é aquele no qual temos uma estação remota acessando os recursos da rede interna. Neste artigo iremos realizar uma configuração de forma a habilitar este tipo de acesso. Para referência, utilizaremos os seguintes parâmetros:

1) Servidor

Sistema operacional Linux (distribuição CentOS 5.6);
Duas placas de rede (uma para a Internet e outra para a rede local);
Endereço de rede local 192.168.0.1/24;
Endereço da internet 200.243.68.1.

2) Cliente

Sistema operacional Windows 7;
Conexão à Internet.

Nesse ambiente iremos ilustrar como o Cliente poderá acessar remotamente os recursos da rede local ligada ao servidor. Assim será possível fazer com que o Cliente se comunique com qualquer IP da rede local do servidor como se estivesse ligado diretamente a ela.

Instalando o servidor

A instalação do software OpenVPN para o servidor pode ser feita de várias maneiras, dependendo da distribuição Linux que

você utilize. Em nosso caso, utilizaremos o CentOS 5 e a instalação será feita pelo gerenciador de pacotes *yum*.

Deste modo, o primeiro passo é, como root, habilitar o repositório *rpmforge*, que disponibiliza versões binárias (já compiladas) do OpenVPN.

Importante: você necessitará fazer o download do pacote de acordo com a arquitetura utilizada (32bits ou 64bits). Levando em consideração esta questão, digite:

- Para 32 bits: `wget http://packages.sw.be/rpmforge-release/rpmforge-release-0.5.2-2.el5.rf.i386.rpm;`
- Para 64 bits: `wget http://packages.sw.be/rpmforge-release/rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm.`

Em seguida você irá importar a chave GPG¹ usada pelo *rpmforge* para assinar seus pacotes, conforme o comando:

```
rpm --import http://apt.sw.be/RPM-GPG-KEY.dag.txt
```

Agora você irá instalar o pacote que foi obtido (mude de acordo com a arquitetura usada), digitando:

```
rpm -Uvh rpmforge-release-0.5.2-2.el5.rf.i386.rpm
```

A partir deste momento seu servidor está configurado para acessar e instalar os pacotes providos pelo repositório *rpmforge*.

A instalação do OpenVPN é realizada utilizando-se o gerenciador de pacotes do CentOS, *yum*, que baixará todas as dependências:

```
yum install -y openvpn
```

Feito isso, você pode conferir se a instalação ocorreu com sucesso através do comando `rpm -qi openvpn`, que deve mostrar o resultado da **Listagem 1**.

Listagem 1. OpenVPN instalado.

```
Name       : openvpn  Relocations: (not relocatable)
Version    : 2.1.4   Vendor: Dag Apt Repository, http://dag.wieers.com/apt/
Release    : 1.el5.rf  Build Date: Thu 02 Dec 2010 01:24:13 PM AMT
Install Date: Mon 07 Mar 2011 02:57:40 PM AMT
Build Host : lisse.hasselt.wieers.com
Group      : Applications/Internet
Source RPM : openvpn-2.1.4-1.el5.rf.src.rpm
Size       : 984420
License    : GPL
Signature  : DSA/SHA1, Thu 02 Dec 2010 01:40:13 PM AMT,
              Key ID a20e52146b8d79e6
Packager   : Dag Wieers <dag@wieers.com>
URL        : http://openvpn.net/
Summary    : Robust and highly flexible VPN daemon
```

¹ GPG – Gnu Privacy Guard é uma implementação de criptografia de chave pública usada para garantir a origem de software, ou seja, quem é o responsável por sua compilação.

Na **Listagem 4** é possível ver o arquivo completo.

Listagem 4. Configuração do servidor.

```
local 200.243.68.1
port 1194
proto udp
dev tun

ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh /etc/openvpn/dh1024.pem

server 10.0.0.0 255.255.255.0
comp-lzo

keepalive 10 120

max-clients 3

status /var/log/openvpn-status.log

log-append /var/log/openvpn.log

verb 3

push "route 192.168.0.0 255.255.255.0"
```

Como podemos notar, existem várias diretivas no arquivo de configuração. O funcionamento das principais será visto a seguir:

1) local 200.243.68.1

A diretiva indica qual dos IPs do servidor será usado para escutar conexões (*bind*). Informe sempre o IP configurado na placa de rede externa, ou seja, aquela na qual a conexão com a Internet do seu servidor está ligada.

2) port 1194

Indica qual a porta na qual o servidor de VPN aguardará as conexões. A porta padrão do OpenVPN é a 1194, mas você pode escolher outra de sua conveniência.

3) proto udp

O OpenVPN suporta tanto TCP quanto UDP como protocolos de transmissão.

4) ca /etc/openvpn/ca.crt

Indica o nome e o local no qual o certificado do CA está localizado. Em nosso caso, criamos em passos anteriores este arquivo.

5) cert /etc/openvpn/server.crt

Indica o nome e o local no qual o certificado do servidor está localizado. Este foi criado quando executamos o comando *build-key-server*.

6) key /etc/openvpn/server.key

Indica o nome e o local no qual a chave do servidor está localizada. Esta foi criada quando executamos o *build-key-server*.

7) dh /etc/openvpn/dh1024.pem

Indica o nome e o local no qual o arquivo com os parâmetros do servidor está localizado. Este foi criado através do comando *build-dh*.

8) server 10.0.0.0 255.255.255.0

Quando um cliente se conectar ao servidor ele irá criar uma interface virtual. Para esta interface o servidor irá alocar um IP da faixa indicada por esta diretiva. Em nosso exemplo serão IPs da faixa 10.0.0.0.

9) max-clients 3

Indica o número máximo de conexões simultâneas (clientes) que podem se conectar. É importante que o número indicado não seja superior ao número de IPs definidos na diretiva *server*.

10) push "route 192.168.0.0 255.255.255.0"

Este indica que quando um cliente se conectar ele irá receber um comando para criar uma rota para a rede 192.168.0.0/24. Isso faz com que o servidor possa mandar comandos para o cliente de maneira que a configuração do cliente seja simples.

É possível ter várias linhas dessas *push* no mesmo arquivo, uma para cada configuração que você deseja que o Cliente receba. É possível, por exemplo, colocar novas rotas ou indicar o endereço IP do servidor Wins (recurso utilizado na resolução de nomes para redes Microsoft).

Instalando o cliente

Uma das vantagens do OpenVPN é a sua natureza de código aberto que facilita que ele seja portado para diversas plataformas. Além de ser possível obtê-lo sob a forma de código fonte, você o encontra já compilado para Windows, Mac OS X e diversas distribuições do Linux. Na **Figura 8** vemos a ferramenta instalada em um sistema operacional Windows.

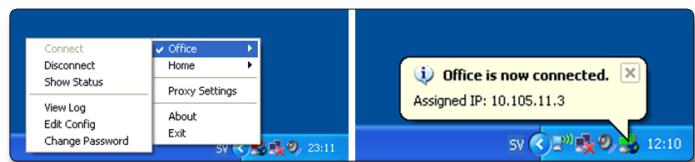


Figura 8. Ferramenta gráfica para controle da VPN em ambiente Windows

Em um ambiente Windows a instalação do OpenVPN é extremamente simples. Para isso, você deve realizar o download da última versão em <http://openvpn.net/index.php/open-source/downloads.html> e seguir o processo de *Install, Next, Next*.

Além da instalação dos arquivos que darão suporte ao software, o instalador para Windows vem com uma ferramenta gráfica que fica disponível na barra de tarefas e lhe permite iniciar e encerrar conexões com OpenVPN de maneira simplificada.

Configurando o cliente

Como parte do processo de estabelecimento da VPN, o cliente e o servidor trocam certificados antes de iniciar a transmissão dos dados criptografados. Deste modo, é preciso criar um certificado para o cliente e sua respectiva configuração. Para isso, execute os comandos descritos a seguir:

1. Criar a chave e certificado para o cliente

No servidor, execute o comando *build-key-pass*:

```
sh build-key-pass cliente
```

Substitua o cliente pelo nome (ou e-mail) do usuário para o qual você estará gerando a chave.

Em seguida o script irá criar a chave e pedir que você coloque uma senha, conforme a **Listagem 5**. Nesse momento, preferencialmente, o usuário da chave deverá estar presente para definir a sua senha.

Listagem 5. Criando a chave do cliente.

```
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'cliente.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Listagem 6. Especificando os parâmetros do certificado do cliente.

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter ', the field will be left blank.
-----
Country Name (2 letter code) [BR]:
State or Province Name (full name) [EE]:
Locality Name (eg, city) [CIDADE]:
Organization Name (eg, company) [SUA EMPRESA]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:email.suaempresa.
com.br
Email Address [adm@suaempresa.com.br]: cliente@suaempresa.com.br
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Feito isso, o script irá solicitar algumas informações específicas do cliente (tais como o e-mail) para incorporar no certificado a ser gerado. Na **Listagem 6** vemos que o script já vem preenchido com alguns dados padrão e na prática só precisamos alterar dois valores: Common Name e Email Address.

O Common Name deverá ser, apenas por questões de padronização, igual ao e-mail do cliente sem o @. Logo, se o e-mail dele for *joao@suaempresa.com.br*, o Common Name será *joao.suaempresa.com.br*.

Na sequência, o próprio software irá assinar o certificado com a chave do CA que foi gerada logo no começo do processo. Na

Listagem 7 o script repete os dados entrados e solicita a sua confirmação.

No final desse processo o script terá criado dois arquivos chamados de *cliente.key* e *cliente.crt*, ambos no diretório *keys* do servidor.

1. Copiar os arquivos para a máquina do cliente

Nas etapas anteriores foram criados vários arquivos que serão usados pelo cliente. Como estes foram gerados no servidor, será necessário copiar os arquivos *ca.crt*, *cliente.key*, *cliente.crt* e *dh1024.pem* do diretório *keys* do servidor para a máquina do cliente.

Você deverá colocá-los no diretório do OpenVPN. Dependendo da versão do Windows instalado, ele poderá mudar, mas o local padrão é *C:\Program Files\OpenVPN\config*.

2. Criar o arquivo de configuração

A etapa final do processo consiste em criar o arquivo de configuração para a sua VPN. Para tanto, basta usar o bloco de notas e criar um arquivo em *C:\Program Files\OpenVPN\config\empresa.ovpn*.

O nome em si não é importante, desde que a extensão *.ovpn* seja mantida. O programa que controla a VPN lê todos os arquivos *.ovpn* do diretório acima e os exibirá como opção para conexão.

Em nosso caso, criaremos o arquivo conforme a **Listagem 8**.

Listagem 7. Assinando o certificado do cliente.

```
Using configuration from /root/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'BR'
stateOrProvinceName     :PRINTABLE:'EE'
localityName            :PRINTABLE:'CIDADE'
organizationName        :PRINTABLE:'SUA EMPRESA'
commonName               :PRINTABLE:'cliente.suaempresa.com.br'
emailAddress            :IA5STRING:'cliente@suaempresa.com.br'
Certificate is to be certified until Jun 13 01:50:04 2012 GMT (365 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
```

Listagem 8. Arquivo de configuração do cliente.

```
client
dev tun
proto udp
remote 200.243.68.1 1194
resolv-retry infinite
nobind
ca "C:\Program Files\OpenVPN\config\ca.crt"
cert "C:\Program Files\OpenVPN\config\cliente.crt"
key "C:\Program Files\OpenVPN\config\cliente.key"
cipher BF-CBC
verb 3
comp-lzo
```

O arquivo do cliente é mais simples que o do servidor, repetindo-o em alguns pontos, como as diretivas *proto* e *dev*.

A primeira diferença entre os arquivos de configuração do cliente e do servidor é que estamos configurando o OpenVPN para atuar em modo cliente (*client*).

Logo em seguida é informado onde o servidor estará localizado e qual a porta que devemos conectar (*remote 200.243.68.1 1194*). Note que você usará o IP (ou nome, caso exista) público do servidor e a mesma porta definida nele.

Em seguida precisamos informar onde o software poderá encontrar os arquivos contendo o certificado do CA (*ca.crt*), o certificado do cliente (*cliente.crt*) e sua chave correspondente (*cliente.key*). Diferentemente do ambiente Linux, você deverá usar aspas duplas e barras duplas.

Agora é só salvar o arquivo e iniciar a conexão escolhendo a opção **Connect** da barra de tarefas. Com isso, uma janela semelhante à **Figura 9** aparecerá e o cliente deverá informar a mesma senha usada na criação de sua chave.

Uma vez conectado à VPN você poderá, por exemplo, acessar os servidores da rede local da mesma maneira que faria se estivesse conectado diretamente a ela.

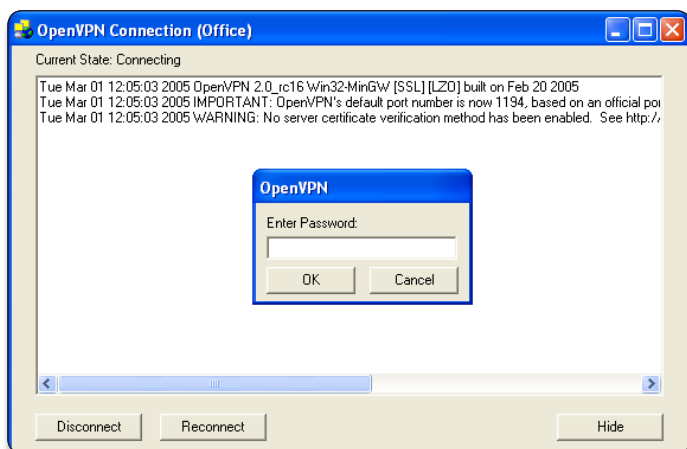


Figura 9. Informando a senha do certificado para iniciar a VPN

Conclusão

Ao longo deste artigo vimos como é possível criar um ambiente seguro para permitir a comunicação entre pontos remotos e sua rede corporativa usando um ambiente GNU-Linux e software livre.

Os conceitos vistos aqui podem ser utilizados tanto para a comunicação entre pontos remotos (host-rede), como no caso de consultores atuando remotamente, ou ainda redes remotas (rede-rede), como na ligação entre a matriz e suas filiais.

Existem outras formas de configuração de sua VPN que podem se adequar à realidade de sua rede ou necessidade de segurança. O OpenVPN tem suporte, por exemplo, a dispositivos de autenticação (e-token) similares aos usados em autenticação bancária ou ainda a associar configurações de IP e firewall específicas a um certificado. Esperamos que este artigo sirva de ponto de partida para a sua configuração.



Mário de Mello Bittencourt Neto

mbneto@gmail.com

Diretor técnico da Argo Internet desde 1996, atuando na área de redes e desenvolvimento de aplicativos Web, eCommerce e segurança. Engenheiro eletrônico e Mestre em informática. Zend Certified Engineer



OpenVPN

<http://openvpn.net>

IPSEC

<http://pt.wikipedia.org/wiki/IPsec>

Iptables

<http://www.frozentux.net/documents/iptables-tutorial/>



Com quantas
mentes se
revoluciona
o mundo?

Campus
Party™



6 a 12 de fevereiro de 2012
Anhembi (SP)

Inovação
Cultura Digital
Ciência
Entretenimento Digital

Unimos talento · Criamos futuro

www.campus-party.com.br

@CampusPartyBRA
www.facebook.com/campuspartybrasil