ESPECIAL - Tecnologias Verdes: Hora de implementá-las

O meio ambiente também se torna um pré-requisito

infra MAGAZINE

Edição 13 :: Ano I

DevMedia

Border gateway protocol

Conheça o protocolo padrão da Internet

Autoconfiguração stateless de endereços

Configure roteadores para gerar endereços IPv6 automaticamente

SEGURANÇA NA NUVEM

Novos desafios para assegurar a confiabilidade dos dados



VOCÊ É ASSINANTE MVP?

ENTÃO PODE TER CERTEZA: O MERCADO PREFERE VOCÊ!



DESENVOLVEDOR ATUALIZADO É O MAIS VALIOSO DO MERCADO!

Muitos profissionais estão acomodados, não se atualizam, não leem livros e não vão a eventos. Acham que é a empresa que deve mantê-los atualizados. Gastam dinheiro com tudo, mas acham caro investir menos de R$60,00 por mês em suas carreiras.

Mas você não! Você é MVP! Parabéns!

TENHA ACESSO A:

- +DE 260 CURSOS ONLINE
- 09 REVISTAS MENSAIS
- 7.850 VÍDEO-AULAS

POR APENAS 59,90 MENSAIS

ASSINATURA MVP MOST VALUABLE PROFESSIONAL

QUEM TEM ESTÁ TRANQUILO.

DevMedia

Acesse: www.devmedia.com.br/mvp

infra MAGAZINE

Ano 2 • Edição 13 • 2013

DevMedia

MVP

Assine agora e tenha acesso a todo o conteúdo da DevMedia: **www.devmedia.com.br/mvp**

EXPEDIENTE

Editor

Eduardo Spínola (eduspinola@gmail.com)

Sub Editores

Marco Antônio Pereira Araújo (maraujo@devmedia.com.br)

Rodrigo Oliveira Spínola (rodrigo.devmedia@gmail.com)

Consultora Técnica

Daniella Costa (daniella@devmedia.com.br)

Jornalista Responsável Kaline Dolabella - JP24185

Capa e Diagramação Romulo Araujo

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 Infra Magazine, entre em contato com o editor, informando o título e mini-resumo do tema que você gostaria de publicar:



EDUARDO OLIVEIRA SPÍNOLA

eduspinola.wordpress.com

@eduspinola / @Java_Magazine

Sumário

04 – Tecnologias Verdes: hora de implementá-las

[*Anderson Vieira Veloso Nunes*]

10 – Segurança na nuvem

[*Leandro de Carvalho Machado e Marco Antônio Pereira Araújo*]

Artigo do tipo Novidades

18 – Autoconfiguração stateless de endereços via Router Advertisement

[*Eduardo Barasal Morales*]

24 – Border gateway protocol: o protocolo padrão da Internet

[*André Koide da Silva*]

Tecnologias Verdes: Hora de Implementá-las

Como as tecnologias que agridem menos o meio ambiente estão se tornando cada vez mais comuns

É inegável, nos dias de hoje, a importância que a tecnologia tem na humanidade. Nossa vida foi e é completamente modificada por conta das incríveis evoluções que vivenciamos ao longo do tempo, e temos que admitir que nossas vidas ficaram muito mais fáceis com ela. Divertidas, até. Através desta tecnologia podemos ter acesso a inúmeros conteúdos que jamais teríamos a oportunidade de conhecer, seja pelo acesso, seja pela distância ou mesmo pela falta de oportunidade; podemos nos conectar a pessoas que estão fisicamente distantes, mas trabalhando juntas com o mesmo objetivo, ao mesmo tempo (real-time); podemos conhecer pessoas, nos divertir, trabalhar, opinar, protestar. A chamada Tecnologia da Informação e Comunicação (TIC), ou simplesmente Tecnologia da Informação (TI), que pode ser definida como o conjunto de todas as atividades, recursos e soluções provenientes da Informática, veio para ficar.

Mas, como tudo na vida, os efeitos desta evolução sem precedentes no mundo estão sendo mostrados nos últimos anos: estamos consumindo demais. O crescimento cada vez mais rápido da população mundial, juntamente com o aumento da expectativa de vida, acabou por gerar uma grande dependência humana no consumo de energia fóssil. E não estamos utilizando em demasia apenas os recursos naturais do planeta (como especialistas ao redor do mundo alertam há tempos), mas também estamos "consumindo" muita tecnologia. Se antes equipamentos tecnológicos eram caros (chegando a custar milhões de dólares) e pesados (computadores simples pesavam mais que automóveis), hoje a facilidade de aquisição de dispositivos e a mobilidade fazem com que seja cada vez mais comum adquirir novos computadores, telefones, vídeo games e *gadgets* em geral. O resultado, para a economia mundial, é extremamente animador e próspero. Mas para o planeta, pode ser desastroso.

Resumo DevMan

Para que serve este artigo:

Neste artigo serão explorados os motivos e as causas que levaram a população mundial a se preocupar cada vez mais com o descarte, a poluição e o consumo que os produtos de tecnologia atualmente podem produzir, estabelecendo-se então uma ponte entre o que efetivamente pode ser feito para que o impacto ambiental seja o menor possível sem afetar demasiadamente o crescente uso de tais produtos tecnológicos.

Em tempos de aquecimento global, ao saber da existência de empresas que utilizam tecnologias limpas, o usuário e consumidor de produtos tecnológicos poderá optar por produtos que agridam menos o meio ambiente, sem abrir mão do seu conforto e do que a tecnologia pode lhe oferecer.

Esta última afirmação é atual e urgente, e no nosso dia a dia uma constante e péssima lembrança do caminho que estamos tomando e que pode afetar negativamente nosso futuro próximo. O planeta pode não conseguir dar conta de tanto lixo eletrônico gerado e acumulado pelo homem, tendo em vista que, até alguns anos, o descarte de um equipamento tecnológico era algo raro, pois a reposição total deste era muito custosa (era sempre preferível "consertar" algo que estava quebrado). Atualmente, funciona-se no esquema: "quebrou, compra outro". Vale lembrar também que não existe o chamado "jogar fora". Para o planeta, não existe "o fora", pois o lixo não desaparece no ar – ele continua armazenado e acondicionado no mesmo planeta que vivemos. Segundo dados da ONU, divulgados no início do ano, o Brasil é o 4° no ranking dos países que mais produzem lixo eletrônico no mundo, e o 1° entre os países emergentes.

A crise econômica global dos últimos anos, que afetou a todos os países no mundo, inclusive o Brasil, acabou por colocar um pequeno freio no consumo em geral. Nos EUA e na Europa, muitas empresas tiveram quedas bruscas nas vendas de seus produtos

tecnológicos, mas ainda assim isso não foi suficiente para diminuir a sede de consumo por novidades tecnológicas da população mundial. A economia vem se recuperando aos poucos no mundo, e especialmente no Brasil a crise econômica não chegou a afetar gravemente o consumo, tanto que a venda de computadores, celulares e *gadgets* em geral só tem crescido nos últimos anos.

Observando-se o lado ambiental da questão, são diversos os problemas presentes: emissão desenfreada de gases poluentes, efeito estufa, aquecimento global, buracos na camada de ozônio, entre muitos outros. A lista é grande para um planeta só. E a tecnologia, infelizmente, contribui para tais problemas, uma vez que ela é uma das grandes responsáveis pelo consumo dos recursos naturais do planeta. Entra na conta a energia consumida durante o processo de produção de um determinado produto, bem como o desperdício de energia causado principalmente pelos aparelhos eletrônicos (computadores mais antigos, sem recursos de economia de energia, chegam a desperdiçar metade da energia que consomem). Também entram na conta o consumo e tráfego de dados na Internet. A maioria dos datacenters das empresas de tecnologia ainda funciona sem uma preocupação verde, pois costumam consumir vastos montantes de energia, algumas vezes de forma irresponsável (funcionando na capacidade máxima sem necessidade, 24 horas por dia, não importando qual seja a real demanda). Esse desperdício pode chegar a números da ordem de 90% da energia consumida, de acordo com estudos recentes na área.

Para dar conta de toda a demanda mundial atual, as empresas de tecnologia tendem a consumir cada vez mais energia. As centrais de processamento norte-americanas, por exemplo, são responsáveis por ¼ (um quarto) do consumo mundial de energia de todos os datacenters do mundo. O número é assustador: juntas, elas consomem 30 bilhões de watts (veja **BOX 1**) de eletricidade, o equivalente em números a 30 usinas nucleares juntas. No Vale do Silício, a meca mundial da tecnologia e inovação, muitas das centrais de processamento de dados hospedadas ali estão incluídas no Inventário de Contaminantes Tóxicos do Ar, que consiste em um documento governamental americano que lista os principais causadores de poluição, em função do uso de diesel para os geradores que protegem os datacenters de quedas de energia.

BOX 1. Watt

Uma medida de consumo total, independente da voltagem e da amperagem. A potência elétrica é medida em watts. Num sistema elétrico, a potência (P) é igual à tensão (V) multiplicada pela corrente (I). Normalmente a conta de luz vem em kilowatt/hora, ou KWh, que corresponde a 1000 watts

Os usuários também têm sua parcela de responsabilidade. Atualmente, todo tipo de dispositivo eletrônico (como televisores, videogames, reprodutores de blu-ray, decodificadores de TV por assinatura, dentre muitos outros) possuem o chamado modo *Stand-by*, que deixa o equipamento com baixo consumo e pronto para uso mais rapidamente do que se não estivesse ligado na tomada. Estudos no Brasil mostram que uma família pode economizar até 18% em sua conta somente desligando os equipamentos da tomada quando não utilizados. Diversas práticas do dia a dia mostram que nossa rotina contribui para esse consumo, a saber: deixar o monitor ligado sem estar na frente do computador; deixar equipamentos no *Stand-by*, conforme citado anteriormente; e deixar o carregador ligado na tomada, mesmo com o celular já carregado, ou mesmo sem o celular conectado a ele. Ainda que mínima, estudos recentes mostram que deixar cerca de 10 dispositivos plugados simultaneamente durante todo o mês (quantidade média de uma família de cinco pessoas), como carregadores de celulares ou aparelhos em *Stand-by*, chega-se a gerar desperdícios diários de cerca de 0,84 kWh, ou aproximadamente 25 kWh por mês. Considerando os valores atuais do KWh no Brasil (R$ 0,40), aproxima-se do valor de R$ 10,00 por mês a mais na conta de luz – ou R$ 120,00 por ano. Além disso, outras práticas não muito recomendáveis são constantemente executadas, como não fazer a correta configuração do computador, de modo que ele possa funcionar com melhor desempenho e economizando energia, além de evitar realizar impressões desnecessárias, quando se poderiam salvar determinados documentos em PDF, gerando economia de tinta, papel e energia.

Por conta desse problema, diversas empresas, cientistas, grupos, organizações não governamentais (ONGs) e até mesmo pessoas comuns têm apostado suas fichas na chamada "Tecnologia Verde", que engloba um grupo de métodos, técnicas e práticas em constante evolução, para que sejam gerados produtos que causem menos impacto ambiental. Também chamada de "TI Verde", essa visão da tecnologia com respeito ao meio ambiente está se tornando uma tendência mundial, e envolve desde a utilização mais eficiente e consciente de energia, recursos e insumos na produção de equipamentos tecnológicos, bem como a criação de produtos que não agridam o meio ambiente e que impactem o menos possível ao final de sua vida útil e consequente descarte. Se vamos continuar consumindo, então que seja de modo mais consciente e com menor agressão ao planeta. Para que consigamos nos beneficiar dos avanços tecnológicos mantendo o respeito ao meio ambiente, este artigo irá apresentar o que as empresas têm feito para poder impactar cada vez menos o planeta e o que você pode fazer para contribuir com essa nova visão de consumo.

A onda da Tecnologia Verde

Assim como todas as atividades humanas, a TI também provoca impactos no meio ambiente, seja pela demanda de materiais a serem utilizados ou pela quantidade de energia elétrica a ser empregada na fabricação de equipamentos. Neste aspecto, podemos observar um crescente número de empresas cada vez mais preocupadas em empregar ações que impactem menos no planeta. Daí surge o conceito de Tecnologia Verde.

A Tecnologia Verde, ou TI Verde, tem ganhado bastante espaço nas discussões sobre o meio ambiente no mundo inteiro. Ela está ligada, primordialmente, aos processos de administração, fabricação de componentes, utilização de equipamentos e

descarte do lixo eletrônico produzido. Assim, a TI Verde pode estar presente na fabricação do produto, tentando evitar a utilização de metais pesados para sua criação, ou ainda que determinado equipamento consuma mais energia. Além disso, a Tecnologia Verde pode garantir que, durante o processo de fabricação, o produto apresente menos componentes químicos. Ela preocupa-se também em regular a quantidade de gases poluentes emitidos durante este processo. Ou seja, tudo o que puder ser feito para reduzir o impacto no meio ambiente durante a fabricação de um determinado equipamento ou produto.

Esse assunto é tão importante que o Centro de Estudos em Sustentabilidade (GVCes) da Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas (FGV-EAESP) criou o Índice de Sustentabilidade Empresarial (ISE) – endereço disponível na seção **Links** –, que consiste em uma "ferramenta para análise comparativa da *performance* das empresas listadas na BM&FBOVESPA sob o aspecto da sustentabilidade corporativa, baseada em eficiência econômica, equilíbrio ambiental, justiça social e governança corporativa.". As empresas que detém ações mais líquidas na bolsa foram convidadas a participar do projeto, que pretende ser um painel de como tais empresas estão lidando com as questões do desenvolvimento sustentável. Dentre as empresas convidadas, algumas responderam ao chamado e utilizaram a ferramenta, como a CCR (Concessionária de Rodovias), EDP Energias do Brasil, Eletropaulo e Natura. Além desta, outra iniciativa que prova que este assunto tem sido tratado com extrema importância é o fato de que, desde 2009, a TI Verde é tema inserido no currículo do Curso Tecnológico de Redes de Computadores na Universidade Cidade de São Paulo (UNICID), com o objetivo de formar profissionais sob a ótica da responsabilidade socioambiental.

Grandes empresas sabem que esta questão, além de lidar diretamente com o planeta, pode influenciar diretamente nos negócios (positivamente quando tratada com transparência e seriedade, e negativamente quando deixada de lado). Tanto que algumas delas executam o chamado **Deep IT** (algo como TI Verde a Fundo) nas suas práticas empresariais. Este conceito indica estratégias de redução de consumo bem antes da construção de um edifício, por exemplo. Estratégia mais ampla de respeito à natureza, incorpora no projeto a implementação de uma estrutura na qual o seu parque tecnológico maximize ao máximo seu desempenho com o menor gasto elétrico possível – e isto inclui implementação de projetos de sistemas de refrigeração e iluminação, além do projeto de disposição dos equipamentos no local. O Google é um exemplo de empresa que pratica de forma maciça estes conceitos, pois costuma executar ações que incluem a construção de seus datacenters seguindo os preceitos indicados anteriormente, além de outras iniciativas, como o deslocamento de seus funcionários em veículos híbridos e captação de energia alternativa, como a energia solar, para alimentação de seus escritórios e datacenters (na foto da **Figura 1**, o datacenter da Bélgica). E o Google precisa mesmo buscar alternativas verdes. Dados revelados recentemente na Internet mostram que as centrais de processamento de dados do Google consumem aproximadamente 300 milhões de watts. Apenas para fins de comparação, o Facebook consome, segundo o mesmo estudo, 60 milhões de watts.

Outra empresa que também adota este tipo de postura é o Yahoo!, que incentiva o consumo consciente de seus funcionários, usa a virtualização de seus servidores, implanta gestão do consumo elétrico baseado no resfriamento de seus equipamentos, e sempre procura criar planos ambientais completos na implantação de datacenters, desde sua elaboração até a sua execução, de acordo com as normas ambientais locais.



Figura 1. Data Center do Google na Bélgica, que utiliza o próprio clima local para esfriar a água sem energia elétrica

Em tecnologia, um dos recursos mais utilizados nas empresas citadas anteriormente, e também amplamente adotada por diversas empresas de TI e que definitivamente se caracteriza como uma das ações que mais trazem benefícios para o consumo consciente é a virtualização. Podemos defini-la rapidamente como a criação de um ambiente virtual que faz a simulação de um ambiente real, como outra máquina ou outro sistema operacional, por exemplo. Com a crescente necessidade de se reduzir os custos e evitar o desperdício de energia, pode-se utilizar um software que emule uma máquina virtual como um servidor físico (criando, assim, um ambiente isolado e independente da máquina "real"), ou seja, podem-se executar diversos sistemas operacionais em um único equipamento, comportando-se como um computador independente. Assim, elimina-se o consumo energético de diversas máquinas físicas, pois com a virtualização, um servidor pode manter vários sistemas operacionais em uso, inclusive reduzindo-se a quantidade de mão de obra técnica.

Outra tecnologia recente que contribui para frear o alto consumo de matérias primas e energia é o *Cloud Computing* (Computação na Nuvem). Um dos atuais "mantras" das empresas de TI, com ela pode-se armazenar uma grande quantidade de arquivos e documentos, de forma segura, em servidores alocados em grandes *datacenters* criados especialmente para este fim. Além de proporcionar uma enorme redução no consumo de energia

(afinal, são usados menos máquinas no parque de TI), os gastos com TI serão menores, uma vez que se pode contratar o serviço pronto sem a necessidade da montagem de todo um ambiente para guardar os dados.

Bons exemplos de Tecnologia Verde

O consumo de energia fóssil, como o petróleo, é uma das principais preocupações mundiais entre os especialistas. Extremamente dependente deste tipo de combustível, países desenvolvidos como os Estados Unidos, Japão e outros lideram estudos para criar alternativas para ter outras fontes de energia para o seu consumo. Algumas iniciativas, ao que parece, estão saindo do papel e virando realidade para o consumo em massa, e não apenas restrito a testes de laboratório. Um exemplo são os chamados carros híbridos e/ou elétricos, que funcionam com vários tipos de combustíveis, conforme mostra a **Figura 2**. Segundo a consultoria PricewaterhouseCoopers (PwC), dados indicam que até 2020 um em cada 16 carros vendidos no mundo será um "carro verde", projetando um crescimento acentuado nos automotivos com selo verde. Até o final da década, afirma a PwC, os carros verdes vão representar 6,3% do mercado mundial automotivo. Embora o número pareça pequeno, é um crescimento muito grande em relação aos anos anteriores.



Figura 2. Estação de recarga, fundamental para a popularização da tecnologia de carros ecológicos

Boas notícias sobre o assunto estão sendo mostradas a todo o momento. Uma startup britânica que está incubada na Universidade de Oxford, na Inglaterra, criou um produto genial que pode ser determinante nos próximos anos para a geração de energia solar, um dos pilares da Tecnologia Verde: um vidro transparente e colorido, que possui a capacidade de gerar energia elétrica a partir da luz solar. Com isso, cientistas da Oxford Photovoltaics (como Henry Snaith, na **Figura 3**) mostram que será possível cobrir toda a fachada de um prédio para que ela possa gerar energia suficiente para a edificação se manter autônoma no consumo de energia.



Figura 3. Henry Snaith, da Oxford Photvoltaics

Outra boa iniciativa vem de uma conhecida escola de inglês. A partir deste ano, os alunos do curso não usarão mais os CDs com aulas e exercícios que acompanham os livros didáticos, mas sim uma ferramenta chamada de CyberFisk, uma plataforma onde poderão ter acesso a todo o conteúdo dos antigos CDs, inclusive os conteúdos de estágios anteriores – ou seja, além das aulas do período/etapa que estão cursando, os alunos poderão voltar às etapas anteriores para revisar seu conteúdo, por exemplo. Com isso, a empresa deixará de produzir 16 toneladas de plástico, com a redução à zero de 500 mil CDs/ano para os cursos de inglês, espanhol e português para estrangeiros.

Iniciativas por parte do governo também existem. No Rio de Janeiro, por exemplo, foi criada em outubro de 2011 a primeira Fábrica Verde, um projeto da Secretaria de Estado do Ambiente para áreas carentes do estado, que consiste em transformar lixo eletrônico em inclusão digital, através do reaproveitamento de computadores, monitores e impressoras. Atualmente, a Fábrica Verde está em funcionamento em duas unidades no estado: uma no Complexo do Alemão e outra na Rocinha. Os alunos do projeto aprendem conceitos de montagem e manutenção de microcomputadores e também a reciclar equipamentos e peças que são doados pelos moradores, empresas públicas e privadas. A cada três máquinas doadas, os jovens produzem um computador em condição de uso, que normalmente é doado para tele centros comunitários e outros espaços. Como incentivo, os jovens recebem uma bolsa de ajuda de custo durante o período do curso, e ao final dele, alguns podem ser escolhidos para trabalhar como monitores do projeto. De acordo com o governo, depois de reaproveitar cerca de 2.000 computadores, o Estado irá economizar cerca de 6 milhões de reais, só na não aquisição de novas máquinas.

Em pleno século XXI, com a tecnologia evoluindo mais rápido a cada dia e com os preços mais acessíveis, é bastante comum que um usuário possua diversos *gadgets* eletrônicos. E definitivamente um dos maiores pesadelos para esse grupo de pessoas consiste em ficar longe de uma tomada para poder carregar seus

dispositivos, sempre ávidos por uma recarga. Para este grupo de pessoas, já existe um carregador universal que permite carregar diversos dispositivos eletrônicos usando apenas energia solar. Portátil e ecologicamente correto, o Universal Solar Charger (ver **Figura 4**) também permite a carga através da energia elétrica em dispositivos de 4.5 até 9V quando a carga por energia solar não for possível.



Figura 4. Carregador universal movido a energia solar

Outro bom exemplo de inovação verde vem de um produto muito consumido entre profissionais de TI: o café. Ele está sendo utilizado não somente para o consumo, mas também como fonte de energia em projetos inovadores e até mesmo inusitados. Um dos mais curiosos é o projeto do coreano Jeon Hwan Ju, que inventou uma impressora que funciona com borra de café, e sem eletricidade! Batizada de RITI Coffee e criada em 2009, é um dispositivo eletrônico totalmente *eco-friendly*. Em vez de jogar fora a borra de café ou o resto do chá, o usuário deposita em um cartucho especial acoplado em cima da impressora. Ao movimentar o cartucho de um lado para o outro de forma rápida (**Figura 5**), a impressora imprime documentos, inclusive com imagens. A RITI Coffee participou da Greener Gadgets Design Competition (Competição de Design de Bugigangas Verdes) e, embora não tenha ganhado a competição, ficou entre os finalistas e atraiu milhares de comentários no mundo todo. Infelizmente a RITI Coffee não entrou em escala de produção para venda, mas só a criação do conceito e do método demonstra que boas ideias estão a todo momento sendo criadas para ajudar o meio ambiente.

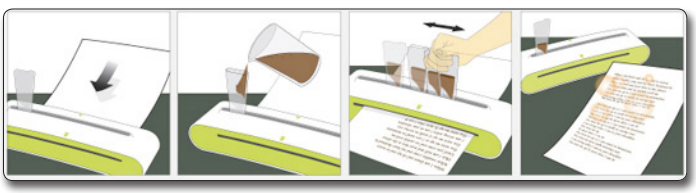


Figura 5. Impressora que imprime documentos utilizando borra de café ou chá

A tecnologia verde também está presente nos softwares. Antes desconectados da realidade ambiental, os programas agora tentam ajudar o usuário através de pequenas ações que podem fazer a diferença para o planeta. Neste cenário, existem diversos aplicativos para computadores e dispositivos móveis que prometem economizar energia, evitando desperdícios com ajustes simples no sistema. Um deles é o Granola, da empresa MiserWare, que é "capaz de economizar a energia consumida pelo computador desnecessariamente sem alterar a performance do sistema". É uma ferramenta de gestão de energia que promete reduzir o consumo a partir de um complexo algoritmo de gerenciamento de energia da CPU. O software pode ser usado em servidores, desktops, notebooks e roda tanto em Windows quanto em Linux.

Conclusão

As empresas de TI atualmente têm um papel central nas discussões sobre a questão ambiental e em projetos voltados à redução do consumo de energia e liberação de CO2 – um dos principais gases causadores do efeito estufa – no mundo. Em geral, os departamentos de tecnologia das empresas correspondem a 10% do consumo total de energia e da emissão de gases das mesmas. Por isso, as empresas estão correndo atrás. O Itaú-Unibanco, por exemplo, elegeu em 2010 o consumo de energia como um dos pilares do projeto de TI Verde da empresa. Com a modernização dos seus parques e datacenters, eles economizam cerca de 500 mil reais em custos gerais.

Existem diversas iniciativas que as empresas podem implantar para contribuir com um impacto menor ao meio ambiente, tais como: reuniões feitas à distância (menos deslocamentos, menos gastos com combustíveis, menos poluição), uso de lixeiras para coleta seletiva (estima-se que, em média, 500 quilos por ano de material reciclável de boa qualidade é jogado fora por cada funcionário de escritórios), utilização de iluminação natural ou a troca de lâmpadas incandescentes para fluorescentes, instalação de softwares para economia de impressão (que fazem o gerenciamento das impressões e permitem economizar tinta e toner), melhorar o ambiente da sala de descanso/café (trocando, por exemplo, copos plásticos por canecas e eliminando máquinas de lanche e café por lanches mais saudáveis) e até a eliminação da máquina de fax (que ficou completamente obsoleta desde o advento do PDF e os softwares que permitem escanear, editar e gerar estes tipos de arquivos).

Mas o que em geral um consumidor pode fazer para dar sua contribuição? Uma pessoa que tenha consciência do meio ambiente e que queira colaborar para a eficácia dos projetos verdes precisa ter paciência e muita disposição. O chamado "Consumo Verde" infelizmente ainda cobra caro do consumidor. Os problemas podem começar ainda na embalagem. Segundo levantamentos da PROTESTE, produtos do mesmo fabricante com a mesma composição, mas com a palavra "ECO" na embalagem, costumam ser mais caros. Já outros podem trazer dados irrelevantes, como os inseticidas que indicam na embalagem que não possuem CFC (clorofluorcarbono) na sua composição, sendo que este componente há muito tempo foi proibido de ser utilizado no Brasil. Também

não vale dizer que a embalagem é reciclável, uma vez que aço e alumínio são matérias primas que possuem esta característica inerentemente. Portanto, é preciso ficar atento para não pagar mais por produtos que, de fato, não são verdes ou simplesmente já estão adequados às leis locais.

Na área tecnológica, a ONG Green Electronics Council criou um selo verde, um padrão de qualidade para certificar produtos que apresentem o menor consumo de energia na sua categoria. O selo, batizado de EPEAT (*Electronic Product Environmental Assessment Tool*), certifica empresas com práticas verdes, para que o consumidor possa ter certeza de que está consumindo sem agredir o meio ambiente. Dentre as mais diversas empresas que possuem o selo está a Amazon.com.

Até mesmo o ato de comprar um computador pode fazer de você um grande emissor de poluentes. Segundo um estudo coordenado pelo professor Ruediger Kuehr, da Universidade das Nações Unidas, uma empresa, ao fabricar um computador simples (desktop com monitor), gasta em média 1.800 Kg de materiais, sendo cerca de 240 Kg de combustíveis fósseis, 22 Kg de componentes químicos dos mais diversos e, absurdos 1.500 litros de água extremamente pura. Esta quantidade imensa de água consumida se explica pelo fato de que durante o processo de produção dos circuitos integrados, das pastilhas de silício e do microprocessador, são necessárias diversas lavagens utilizando-se de água pura, para eliminar toda e qualquer impureza dos componentes.

Por isso, é preciso refletir acerca da real necessidade de aquisição de uma máquina nova. Uma atualização de sistema operacional, de memória RAM e/ou de processador pode fazer com que sua máquina possa atender às suas novas necessidades, sem precisar gastar mais do que o necessário. Quando perceber que a máquina está realmente obsoleta, o descarte deve ser feito de maneira adequada, sempre priorizando a reciclagem. Diversos fabricantes, centros de tecnologia e ONGs recebem máquinas antigas e reciclam, como o exemplo da Fábrica Verde citada anteriormente. Assim, além de dar um destino adequado ao produto que não se deseja mais, ainda contribui para que outras pessoas possam aproveitar o material em uma nova máquina reciclada.

Duas excelentes iniciativas para aumentar a visibilidade da TI Verde estão sendo feitas nos sites Software Verde e Iniciativa Verde. O primeiro deles, (veja a seção **Links**) tem como objetivo certificar empresas que se comprometem em não agredir o meio ambiente, aumentando a sua contribuição com a redução ou mesmo anulando a emissão de carbono na atmosfera, tudo feito a partir de auditorias elaboradas e realizadas pela Software Verde. Ao conseguir o certificado, a empresa será qualificada e terá o direito de figurar na Lista de Empresas Certificadas e de usar a Marca de Conformidade do Software Verde, durante o período de dois anos.

Já no site do Iniciativa Verde (disponível na seção **Links**), você pode saber quantas árvores precisará plantar para neutralizar a sua emissão de carbono com base no seu consumo de energia elétrica, consumo de gás de cozinha, de combustível do seu carro e das viagens aéreas que faz durante um ano. Caso seja difícil plantar a quantidade de árvores que o site indicar, você pode pagar para que o próprio site realize o plantio, fazendo com que sua vida seja considerada "Carbon Free".

Existem diversas outras possibilidades para tentar amenizar o impacto ambiental do nosso consumo tecnológico. Aqui estão listadas apenas algumas delas. Sem extremismos para um lado ou outro, é possível viver e conviver bem com nosso planeta, agredindo menos e aproveitando ao máximo o que a tecnologia tem para nos oferecer. Ao consumir a tecnologia com responsabilidade, o meio ambiente e o planeta agradecem!

Links:

BioVita – Empresas consomem muita energia.
http://www.biovita.com.br/noticias-detalhes/28-empresas-buscam-imagem-ecologicamente-correta-mas-consomem-muita-energia.html

ISE - Índice de Sustentabilidade Empresarial – BM&FBovespa.
https://www.isebvmf.com.br/

EPEAT (Electronic Product Environmental Assessment Tool) – Registro de Produtos Eletrônicos e Fabricantes Verdes.
http://www.epeat.net/

Exame.com – Tecnologias Verdes.
http://exame.abril.com.br/topicos/tecnologias-limpas

Fábrica Verde – Secretaria de Estado do Ambiente (SEA).
http://www.stcambiente.com/

Hardware – Estudo da Fabricação de Computadores
http://www.hardware.com.br/comunidade/computador-fabricacao/704112/

Inovação Tecnológica – Estudo da Fabricação de Computadores
http://www.inovacaotecnologica.com.br/noticias/noticia.php?artigo=010125070309

Iniciativa Verde. Organização dedicada a reduzir os impactos ambientais.
http://www.iniciativaverde.org.br/__novosite/#institucional

Software Verde. Certificação para empresas ambientalmente responsáveis.
http://www.softwareverde.com.br/paginas/

TechMundo – Seção Tecnologia Verde.
http://www.tecmundo.com.br/1588-tecnologia-verde.htm

TI Verde. Blog sobre tecnologias verdes.
http://tecnoinfoverde.blogspot.com.br/

Autor



Anderson Vieira Veloso Nunes
andersonvieirarj@gmail.com



Professor de Tecnologia da Informação e Comunicação há 15 anos. É Tecnólogo em Redes de Computadores pela Universidade Castelo Branco (UCB-RJ), pós-graduado em Docência do Ensino Superior pela Universidade Cândido Mendes (UCAM-RJ) e Mestre em Educação pela Universidade Estácio de Sá (UNESA-RJ). Atualmente é Coordenador de Curso Técnico na rede estadual pública pela FAETEC-RJ, Professor Assistente no Curso de Análise e Desenvolvimento de Sistemas da UniverCidade-RJ, leciona disciplinas ligadas à Informática na Pós-Graduação em Tecnologia Educacional na UCAM e leciona Informática Técnica em Cursos Técnicos na rede pública estadual.

Segurança na Nuvem

A importância da confiabilidade para o armazenamento de dados

A computação em nuvem (*Cloud Computing*) é atualmente uma tecnologia amplamente difundida. Esse novo paradigma da computação é uma tendência que permite utilizar as mais variadas aplicações via *Internet*, em qualquer lugar e independente de plataforma, com a mesma facilidade de tê-las instaladas no próprio computador.

A principal característica da computação em nuvem é que a sua aplicação, ou um conjunto de aplicativos e recursos, serão hospedados em outra empresa, que o isentará de instalações de programas, compra de equipamentos ou obtenção de recursos para armazenamento de dados. Tudo ficará a encargo do *Data Center* que proverá o serviço ao cliente.

Essa nova tecnologia traz benefícios em relação à economia com equipamentos de tecnologia, instalação de aplicações, treinamento de pessoal e segurança. Tudo é feito e configurado pelo provedor de hospedagem. Para isto, é fundamental a existência de uma relação de confiança entre o cliente e o prestador do serviço, que pode ser obtida pela transparência na implementação, desenvolvimento e gerenciamento da segurança.

Porém, a nuvem traz um nível adicional de riscos, diretamente associados à terceirização de serviços essenciais (serviços em nuvem). Isso exige atenção especial na observância aos princípios da segurança da informação: disponibilidade, integridade, confidencialidade e autenticidade, bem como na privacidade, no suporte e na conformidade.

Uma composição topológica simplificada de uma solução de computação em nuvem pode ser observada na **Figura 1**, que mostra os principais elementos integrantes desta estrutura: clientes, servidores distribuídos e *Data Center*.

No âmbito da computação em nuvem, o *Data Center* consta de um conjunto de servidores que serão responsáveis pelo armazenamento dos aplicativos. Sua disposição física pode estar disposta tanto no ambiente de trabalho quanto em qualquer outra parte do mundo, permitindo seu controle pela Internet.

Resumo DevMan

Para que serve este artigo:

Visto que para cada nova tecnologia emergente nasce também novas ameaças e desafios, este artigo aborda a questão da segurança em Cloud Computing, focando na área mais crítica quando o assunto é armazenamento de dados na nuvem: a confidencialidade dos dados.

Este tema é útil para usuários e empresas que desejam implementar ou contratar um serviço de armazenamento de dados em nuvem e queiram saber quais tipos de serviços existem, quais os principais provedores dos serviços existentes, qual o nível de confidencialidade os provedores fornecem para proteger os dados do cliente, como os dados são tratados em caso de crimes envolvendo o ambiente de armazenamento e como a confidencialidade é tratada à luz da Constituição Federal.

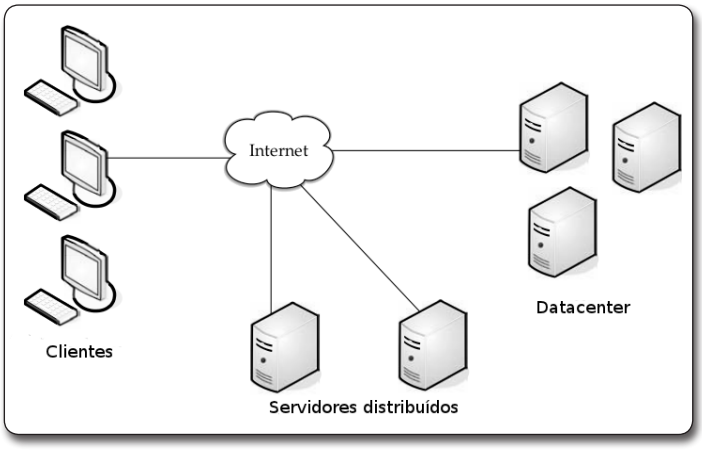


Figura 1. Os elementos que compõem uma solução de computação em nuvem

Cloud computing vs Grid computing

Duas áreas muito confundidas frequentemente são a *grid computing* e a computação em nuvem, porém, são áreas completamente distintas. A *grid computing* aplica os recursos de vários computadores em uma rede de trabalho em um único problema ao mesmo tempo. Isso é feito geralmente para identificar um problema científico ou técnico.

Ainda, a *grid computing* necessita do uso de software que possa se dividir e então enviar partes do programa aos milhares de

computadores. Esse processo de fragmentação pode ser feito em todos os computadores de uma empresa, ou como uma forma de colaboração pública.

A ideia defendida pela *grid computing* é a difusão de um projeto que exija grande quantidade de processamento e recursos os quais serão empregados e compartilhados por múltiplos computadores. Esse recurso é exatamente o oposto ao que a *cloud computing* vem propondo, pois essa permite que muitos aplicativos menores funcionem ao mesmo tempo.

Uma ferramenta que disponibiliza essa utilidade proveniente da *grid computing* é a pesquisa referente ao projeto *Search For Extra-terrestrial Intelligence* (SETI@Home). Segundo o próprio site SETI (2012), este é um experimento científico que utiliza computadores conectados à *Internet* na Busca por Inteligência Extraterrestre. Qualquer pessoa pode participar executando um programa gratuito que baixa e analisa os dados de um radiotelescópio.

Uma visão geral sobre cloud computing

A computação em nuvem pode ser considerada uma metáfora da *Internet* e sua função consta em cortar custos operacionais e permitir que os setores de TI se concentrem em tomadas de decisões estratégicas em vez de se preocupar com o *Data Center.*

É comum encontrar o termo "serviços" na nuvem para caracterizar a utilização de componentes reutilizáveis. Esses serviços são mais conhecidos como "*as a service*" (como serviço) e apresentam características como: alta taxa de disponibilidade, grande escalabilidade, recursos compartilhados por muitos usuários (multilocação) e acesso aos sistemas em diferentes *hardwares* (dispositivos independentes).

Os tipos de serviços existentes podem ser divididos da seguinte forma:

1. Storage-as-a-service: envolve recursos de armazenamento em disco remotamente. Serviço que permite alugar um espaço de armazenamento sem a necessidade de comprar ou requisitar que alguém compre equipamentos. Esse tipo de serviço é geralmente visto como uma alternativa para empresas de médio ou pequeno porte que não possuem orçamento de capital ou pessoal técnico capaz de manter e implementar sua própria infraestrutura. Também é uma boa alternativa para a recuperação de desastres, visando à continuidade do negócio e a disponibilidade;

2. Application-as-a-service ou Software-as-a-service: um aplicativo ou um conjunto de aplicativos são fornecidos como serviço para os clientes que os acessam pela *Internet*. O processo de manter os programas e sistemas atualizados e garantir o funcionamento da infraestrutura ficam a encargo do provedor de serviço;

3. Database-as-a-service: acesso remoto a bancos de dados. A ideia do banco de dados como um Serviço (DaaS) é proporcionar a economia com o custo de execução do banco de dados e evitar sua complexidade. Alguns dos benefícios constam em:

- Facilidade de utilização, uma vez que o cliente não precisa se preocupar com a compra, instalação e manutenção de hardware para a base de dados;
- Potência: os provedores podem fornecer dados de forma personalizada a fim de assegurar a disponibilidade de informações exatas;
- Integração: fornece a capacidade de integrar a base de dados com os demais serviços a fim de agregar mais valor e poder às informações.

4. Security-as-a-service: dispositivos de segurança como gerenciamento de usuários, disponibilizados através da "nuvem". É um modelo de terceirização no que se refere à gestão de segurança. Geralmente, a Segurança como um Serviço envolve *softwares* de antivírus disponíveis na *Internet*. Os benefícios desse tipo de serviço envolvem:

- Atualizações constantes de definições de vírus que não dependem da conformidade do usuário;
- Maior experiência com segurança do que normalmente é disponível dentro da organização;
- Provisionamento de contas de usuários de forma mais rápido;
- Terceirização de ferramentas administrativas como gerenciamento de *logs*, economizando tempo e dinheiro, permitindo que a empresa foque em suas competências principais;
- Interface *Web* que permite o gerenciamento de ferramentas e atividades em execução além das configurações de segurança pré-configuradas.

5. Testing-as-a-service: fornece mecanismos para testes de aplicações. Tipo de serviço que permite a execução de testes complexos que requerem um conjunto de habilidades especializadas, ferramentas de teste caras ou uma grande quantidade de recursos;

6. Infrastructure-as-a-service: toda a infraestrutura de *Data Center* disponibilizada ao contratante. Modelo de disposição em que o cliente contrata os serviços de armazenamento, equipamentos necessários para sua atividade, hardware, servidores e componentes de rede. O provedor do serviço tem os equipamentos e é o responsável por instalá-los, executá-los e prover a manutenção em seu ambiente de nuvem. Os serviços de infraestrutura podem incluir:

- Um conjunto de *APIs* que permite a gestão e interação com a infraestrutura por parte dos consumidores;
- Automação de tarefas administrativas;
- Escalonamento dinâmico;
- Virtualização de *desktops*;
- Conectividade com a *Internet*;
- Serviços baseados em políticas.

Confidencialidade dos dados – Políticas de privacidade e criptografia

Para assegurar a confidencialidade dos dados de um cliente, os fornecedores de *cloud computing* têm políticas de privacidade rigorosas empregando métodos comprovados de criptografia para autenticar usuários em seus ambientes. Uma medida ainda mais

segura seria criptografar os dados antes de armazená-los em um provedor de nuvem.

Antes de contratar algum serviço de nuvem, os usuários devem estar cientes de que a partir do momento em que os dados saem de suas mãos para serem armazenados nas nuvens, perde-se uma camada de controle, uma vez que, como toda tecnologia, a computação em nuvem também apresenta suas limitações.

Para fins de exemplo, pode-se pegar uma empresa que pretende usar a nuvem como meio de armazenar uma lista do número do seguro social de seus funcionários. A partir do momento em que os dados não estão armazenados apenas na empresa, a preocupação em manter esses dados protegidos contra invasões ou roubos de informações passa a ser também do provedor do serviço. No entanto, o provedor pode se absolver de tal responsabilidade através de um acordo. Para os consumidores da tecnologia de nuvem a complexidade é ainda maior, uma vez que não se tem a garantia de que a forma como as informações confidenciais foram armazenadas estão realmente seguras. Como os dados estão armazenados em um local distinto do ambiente tecnológico do cliente, perde-se uma camada de segurança, e outro agravante neste cenário é que as informações estarão dispostas para possíveis investigações do governo sem que o cliente tenha um prévio conhecimento de que os dados estão sob análise.

Para o governo, tornou-se muito mais fácil obter informações de terceiros do que de um servidor de propriedade privada. Em alguns casos, se os provedores receberem citações judiciais, eles são proibidos à luz da Constituição Federal de informar aos clientes que os dados foram fornecidos ao governo.

Porém, existem meios de aumentar o nível de segurança dos dados armazenados em nuvem utilizando ferramentas de criptografia. Assim, os dados terão uma camada maior de segurança antes de serem enviados a terceiros. Programas como PGP e TrueCrypt são capazes de criptografar os dados a fim de que somente aqueles que possuam a senha possam acessá-los.

Privacidade, normas e ferramentas de segurança para a nuvem

O primeiro e maior interesse relacionado à nuvem refere-se às considerações quanto à segurança; constatação comprovada segundo dados de uma pesquisa realizada pelo IDC no gráfico da **Figura 2**, que lista dentre outros, três fatores principais que influenciam na escolha de um serviço de nuvem: segurança, disponibilidade e desempenho. Isto é, se outra empresa armazena os dados de um cliente, como ele sabe se estão seguros e protegidos? Para tanto, é necessário que o cliente analise como o provedor do serviço trata a privacidade e segurança de seus ativos e faça os seguintes questionamentos:

- Existe criptografia dos dados?
- O provedor passa por processos de auditoria?
- O fornecedor do serviço obedece a algum tipo de padronização ou utiliza tecnologias de segurança da informação?

Para subsidiar estas questões, existem algumas normas, padrões e ferramentas de segurança para a cloud computing, que serão tratados adiante, tais como:

- **Auditoria:** SAS 70, SSAE16, ISAE 3402, NBC TO 3402 (norma brasileira baseada na ISAE 3402);
- **Normas:** ISO 27001, PCI DSS;
- **Tecnologias e serviços:** SysTrust, Identity and Access Management (IAM), Multi-factor Authentication (MFA), token e criptografia.

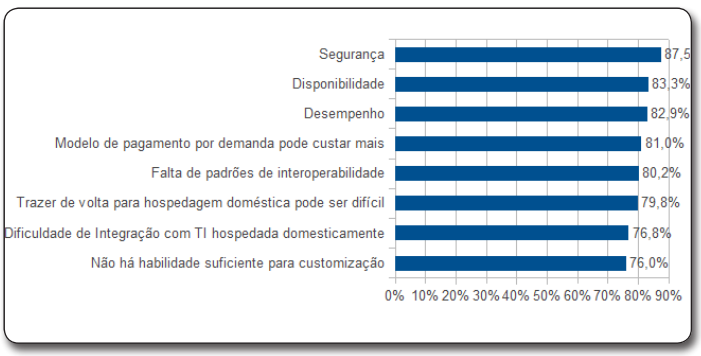


Figura 2. Fatores que influenciam na escolha de um serviço em nuvem (IDC)

Para assegurar que os serviços de nuvem oferecidos tenham um nível aceitável de segurança para seus clientes, os fornecedores dispõem de diversos recursos e tecnologias para atender a essa necessidade dos usuários. Estes elementos são relacionados a seguir como normas, padrões, auditorias e ferramentas para auxiliar cada provedor:

- **Certificação ISO 27001:** norma preparada para prover um modelo capaz de estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). A adoção de um SGSI deve ser uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados, tamanho e estrutura da organização. A certificação se aplica tanto para pequenas, médias e grandes empresas independentemente do setor em que atuam. A norma se aplica fundamentalmente àquelas empresas que apresentam nível de criticidade elevada de informação em áreas como finanças, contabilidade, setores públicos e de TI;
- **SAS 70:** padrão de auditoria desenvolvido pelo Instituto Americano de Contadores Públicos Certificados (AICPA). O foco dos serviços deste padrão de auditoria está nas empresas que prestam serviços de processamento de dados, geração de folha de pagamento, contabilidade e outros processos específicos de negócio. O SAS 70 é um dos tipos de certificações voltadas para uma organização fornecedora de serviços, como um provedor de serviços em nuvem;
- **SysTrust:** tipo de serviço de garantia desenvolvido em conjunto pelo Instituto Americano de Contadores Públicos Certificados (AICPA) e o Instituto Canadense de Revisores Oficiais de Contas (CICA). Destinado a avaliar e testar se um sistema específico é confiável ou não, mediante a observância de três princípios básicos: disponibilidade, segurança e integridade;

• **PCI DSS:** Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI) desenvolvido para incentivar e aprimorar a segurança dos dados e facilitar a ampla adoção de medidas de segurança de dados consistentes no mundo todo. Oferece a base de requisitos técnicos e operacionais projetados para proteção de dados. Ele se aplica a todas as entidades que armazenam, processam ou transmitem os dados de um cliente;
• **SSAE 16:** padrão de atestado emitido como norma de certificação voltada para resolução de compromissos por auditores de serviço. Os compromissos do SSAE 16 conduzidos por auditores nos serviços de uma organização resultarão na emissão de relatórios que podem ser de dois tipos: o Tipo 1, designado de Relatório sobre Descrição do Sistema de Gestão de uma Organização de Serviços e o Tipo 2, que é o Relatório sobre Descrição do Sistema de Gestão de uma Organização de Serviços e Adequação do Projeto e Eficácia Operacional dos Controles;
• **ISAE 3402:** fornece um processo de auditoria dos processos executados na oferta de serviços a clientes, além de opções de padronização internacional para assegurar a entrega de relatórios com dois objetivos fundamentais: obtenção de um nível aceitável de segurança, mediante os aspectos mais relevantes e critérios adequados, e criar relatórios com as conclusões encontradas pelo auditor;
• **Identity and Access Management (IAM):** O Gerenciamento de Acesso e Identidade é uma tecnologia da informação relacionada a processos para gerenciamento de quem tem acesso ao sistema de informação em questão. É um conjunto de processos de negócios, serviços, informações e tecnologias para gerenciamento e uso de identidades digitais;
• **Multi-factor Authentication (MFA):** sistema de segurança caracterizado pela presença de mais de uma forma de autenticação, implementado para verificar a legitimidade de uma transação. O objetivo é criar um sistema de defesa em camadas e tornar seu acesso mais difícil para uma pessoa não autorizada;
• **Token:** tecnologia baseada na autenticação fundamentada em dispositivos pertencentes ao usuário. É um *hardware* comumente utilizado como mecanismo adicional de autenticação provendo segurança de mais alto nível. Esse tipo de dispositivo apenas armazena as informações e não as processa. Possui a característica de ser quase sempre utilizado em conjunto com as senhas (combinação de algo que o usuário sabe com algo que o usuário tem);
• **Criptografia:** ciência que serve de base para as diversas tecnologias e protocolos. É a ciência de manter as mensagens seguras. Suas propriedades – sigilo, integridade, autenticação e não repúdio – garantem o armazenamento, as comunicações e as transações seguras (Nakamura; Geus, 2010). A característica do processo de cifragem se dá pelo processo de disfarçar a mensagem original de modo que sua substância é escondida em uma mensagem com texto cifrado.

Provedores de cloud computing

O NIST (2011) define a computação em nuvem como um modelo de serviço que apresenta cinco características essenciais: serviço sob demanda, acesso a rede, pool compartilhado de recursos computacionais (redes, servidores, armazenamento, aplicações e serviços), elasticidade rápida e serviço mensurado. Estes elementos podem ser rapidamente provisionados e liberados com um esforço mínimo de gestão ou interação com um provedor de serviços. Dentre os fornecedores mais capacitados, estão aqueles que já são dominantes de outros serviços de tecnologia para atenderem as necessidades das organizações. A seguir, são listados os principais provedores, bem como os serviços de nuvem que cada um oferece.

Google

O Google é uma das empresas que destinam parte de suas atividades ao ambiente de nuvem. Dentre os serviços tecnológicos que a empresa oferece, estão os produtos caracterizados como ambientes redundantes e alocação dinâmica de recursos. Esses permitem aos clientes o acesso de forma virtual independente de horário ou localização geográfica a partir de um dispositivo que tenha acesso à *Internet*. Seu ambiente de nuvem permite que os recursos de CPU, memória e armazenamento possam ser compartilhados e utilizados por outros clientes. Dentre seus serviços, destacam-se:
• **Google App Engine:** O Google App Engine é uma solução de computação em nuvem que permite o rápido desenvolvimento, implementação e administração de aplicativos *Web* sem a necessidade de que o usuário se preocupe com o *hardware* e *backup*. O serviço suporta aplicativos criados em várias linguagens de programação. O ambiente de execução presente nesta solução permite a criação de um aplicativo usando tecnologias Java padrão ou qualquer outra linguagem que usa um interpretador ou compilador com base na JVM;
• **Google Web Toolkit:** Essa é uma ferramenta de código-fonte aberto que permite aos desenvolvedores a criação de aplicativos utilizando a tecnologia Ajax em linguagem de programação Java. É uma ferramenta que pode contornar os problemas mais comuns envolvendo a compatibilidade dos navegadores, obtendo ganhos significativos de produtividade e desenvolvimento.

Microsoft

A solução oferecida pela Microsoft como resposta ao ambiente de *Cloud Computing* é o *Azure Service Platform*. A plataforma Windows Azure apresenta-se como um grupo de tecnologias da computação em nuvem que fornece um conjunto de serviços hospedados nos *data centers* da Microsoft. Alguns componentes da plataforma Azure Services serão abordados a seguir:
• **Windows Azure:** O Windows Azure é um sistema operacional baseado em nuvem que permite o desenvolvimento e hospedagem. Esta solução fornece um ambiente de gerenciamento para serviços baseados na plataforma *Azure* que pode ser usado individualmente ou com o auxílio de aplicações *Web*. O Windows Azure pode ser usado para as seguintes finalidades:
- Aumentar a capacidade dos serviços rodando em ambiente *Web* para as aplicações existentes;

- Criar, manipular e modificar aplicações permitindo uma posterior migração para a *Web*;
- Criar, testar, depurar e distribuir serviços *Web* de forma acessível;
- Reduzir os custos de gerenciamento de TI.

• **SQL Services:** Esse é um serviço baseado em nuvem da Microsoft que oferece o armazenamento de dados estruturados, semiestruturados e não estruturados. A capacidade do SQL Services é similar ao Amazon S3 e Amazon Relational Database Service, que será abordado mais adiante. Dentre os serviços oferecidos pelo SQL Services destacam-se consultas relacionais, pesquisa, elaboração de relatórios, análises, integração e sincronização de dados;

• **Windows Intune:** Solução que reúne serviços em nuvem para usuários do Windows para auxiliar na segurança e gerenciamento dos computadores. Essa ferramenta é destinada principalmente a pequenas e médias empresas que desejam gerenciar até 500 computadores que utilizam os sistemas operacionais Windows. A distribuição deste serviço se dá através de um sistema de assinatura com custo mensal fixo. Essa é uma iniciativa da Microsoft como incentivo à mudança do Windows XP, cujo apoio será interrompido em abril de 2014;

• **Business Productivity Online Suite:** Conjunto de serviços para empresas projetados como *Software as a Service* permitindo que as organizações acessem os recursos do seu software através de servidores locais, como serviços online, de acordo com as necessidades da cada uma. Os serviços oferecem a opção de adicionar capacidades complementares dos servidores locais e simplificam a gestão e manutenção do sistema. O pacote inclui serviços como Exchange Online, Office SharePoint Online, Office Communications Online, Forefront Online Protection for Exchange e o Office Live Meeting;

• **Microsoft Dynamics CRM Online:** Serviço integrado de CRM que permite criar e manter uma visão clara dos clientes, do primeiro contato até a pós-venda. Oferece ferramentas para melhorar os processos de vendas, marketing e serviços de atendimento ao cliente. É integrado ao Microsoft Office Outlook e permite melhorias consistentes e mensuráveis em processos de negócios rotineiros;

• **Microsoft Exchange Online:** serviço disponibilizado na nuvem para acessar contas de e-mail, correios de voz, calendário e contatos;

• **Microsoft Office Live Meeting:** solução baseada em nuvem a fim de prover treinamento, eventos e conferências online para permitir a comunicação entre pessoas e empresas;

• **Microsoft Office SharePoint Online:** plataforma de colaboração voltada para a criação de bibliotecas de documentos, wikis, blogs, locais de trabalho compartilhado e ambientes de Intranet.

Amazon

Os serviços de nuvem da *Amazon*, mais conhecidos como *Amazon Web Services*, são disponibilizados como alternativa para as empresas investirem em infraestrutura de TI por meio de serviços *Web*. Um dos benefícios fundamentais oferecidos é a substituição dos gastos com a infraestrutura principal por preços ajustáveis a cada cliente.

A Amazon oferece serviços de nuvem que variam desde soluções de infraestrutura até armazenamento de dados e são listados logo a seguir:

• **Amazon Elastic Compute Cloud (Amazon EC2):** plataforma de computação em nuvem da Amazon que permite a usuários e empresas alugarem computadores virtuais a fim de executarem suas próprias aplicações. O Amazon EC2 é um serviço Web que fornece uma capacidade de computação redimensionável na nuvem. Foi desenvolvido para facilitar a escalabilidade de aplicações web para os desenvolvedores. Esta solução oferece um controle completo dos recursos computacionais e possibilita a execução de tarefas na infraestrutura computacional da Amazon. Possui ainda como característica a redução do tempo exigido para obter e inicializar novas instâncias do servidor, proporcionando o rápido escalonamento da capacidade, para mais ou para menos, à medida que os requisitos de computação forem alterados;

• **Amazon Simple DB:** essa é uma plataforma de armazenamento na nuvem de alta disponibilidade, além de ser flexível e escalável. Possui ainda a característica de minimizar o trabalho de administração do banco de dados por ser um armazenamento não relacional. Os usuários apenas armazenam e consultam os dados por meio de aplicativos web e o Amazon Simple DB se encarrega de fazer o restante;

• **Amazon Simple Storage Service (Amazon S3):** O Amazon S3 é a solução em nuvem que fornece uma interface simples de serviço web que pode ser usada para armazenar e recuperar qualquer quantidade de dados, a qualquer momento, de qualquer lugar na web. Concede acesso aos desenvolvedores para a mesma infraestrutura que a Amazon utiliza para executar sua própria rede global de sites da web. O serviço visa maximizar os benefícios de escala e pode passar esses benefícios para os desenvolvedores;

• **Amazon CloudFront:** rede de distribuição de conteúdo (CDN) da Amazon que proporciona um sistema distribuído de servidores alocados em vários *data centers*. Integrando-se com outros serviços da Amazon, oferece a desenvolvedores e empresas uma maneira fácil de distribuir conteúdos aos clientes, oferecendo para isso, baixa latência e altas velocidades de transferência de dados sem maiores gastos;

• **Amazon Simple Queue Service (Amazon SQS):** a utilização desta solução implica em permitir a comunicação entre os *hosts* da Amazon utilizando a *message-passing* API (sistema de transmissão de mensagens padronizadas para funcionar com uma ampla variedade de computadores paralelos). Oferece o recurso de hospedagem para armazenar mensagens conforme forem trafegando entre os computadores. Os usuários podem mover os dados entre os computadores que armazenam seus aplicativos e que executam diversas tarefas, sem perda ou disponibilidade das mensagens;

• **Elastic Block Store (Amazon EBS):** com o EBS, volumes de armazenamento podem ser criados de forma programada, com a

utilização de dispositivos que podem enviar ou receber dados em blocos de tamanho fixo. Desta forma, os dados são transmitidos de forma fragmentada e são armazenados em dispositivos de comunicação paralela como discos rígidos, drives ou partições. Os volumes são construídos de forma replicada e possuem utilidades específicas para aplicativos que exijam bancos de dados, sistemas de arquivos ou acesso a armazenamento de bloco (ver **BOX 1**).

BOX 1. Armazenamento de bloco

Recurso que apresenta segmentação de dados em blocos geralmente realizada por um sistema de arquivos ou um sistema gerenciador de banco de dados (SGDB) para ser usado por um aplicativo ou usuário. O armazenamento se dá em volumes físicos ou lógicos que podem ser dispositivos internos do servidor conectados via SCSI ou Fibre Channel, ou ainda, a dispositivos remotos acessados via Rede de Área de Armazenamento (Storage Area Network – SAN).

Salesforce.com

Este fornecedor de serviços em nuvem oferece uma plataforma de gestão de relacionamento com o cliente (CRM) e outras soluções de aplicativos na forma de Software como Serviço (SaaS) distribuído pela *Internet*, característica oposta àquela apresentada pelos usuários que compram seus aplicativos e os instalam localmente em seus computadores.

Os serviços oferecidos por esse provedor abrangem os variados tipos de computação em nuvem e são listados a seguir:

- **Force.com:** plataforma de computação em nuvem criada para automatizar e estender os negócios de uma empresa e desenvolver o empreendimento social. Essa é uma Plataforma como Serviço (PaaS) projetada para simplificar o desenvolvimento e implementação de aplicativos e *sites* baseados em nuvem. Os desenvolvedores podem criar aplicativos e *sites* através da nuvem em um ambiente de desenvolvimento integrado, e implantá-los de forma mais rápida. O usuário se concentra na criação de aplicativos, deixando as preocupações com servidores ou software a cargo do provedor;
- **Visualforce:** *framework* que permite a criação de interfaces que podem ser hospedadas nativamente na plataforma Force.com. A estrutura do Visualforce inclui uma linguagem de marcação semelhante ao HTML. Nessa linguagem, cada *tag* corresponde a um componente de interface de usuário, seja uma seção de uma página, uma lista relacionada, ou um campo;
- **Salesforce.com CRM:** solução da Salesforce.com para atender à gerência de relacionamento com o cliente (*Customer Relationship Management* – CRM). Consiste nas vendas e serviços de *cloud computing* e é dividido basicamente em cinco aplicações centrais: vendas, marketing, serviço, colaboração entre empresas e clientes, relatório em tempo real dos negócios e das aplicações personalizadas;
- **AppExchange:** plataforma de serviços que permite a construção, desenvolvimento, customização e comercialização de aplicativos. Permite também o acesso instantâneo a aplicativos desenvolvidos por outras pessoas. Para o desenvolvimento de aplicações é utilizada a tecnologia PaaS (Plataforma como Serviço), não havendo a necessidade de comprar e instalar programas.

Segurança da informação na nuvem

Um dos maiores benefícios da computação em nuvem é a centralização dos dados. Porém, há uma grande preocupação das empresas em relação à proteção e segurança de seus ativos, uma vez que grande parte de seus dados são armazenados em vários dispositivos, como *laptops* e *thick clients* (ver **BOX 2**).

BOX 2. Thick Client

Tipo de cliente que executa tanto processamento quanto possível, direcionando ao servidor os dados necessários para a comunicação e armazenamento de arquivos. Assim, o computador se apresenta inserido em uma rede de arquitetura cliente-servidor, caracterizada pela presença de recursos para realização de operações de forma a depender o mínimo possível de um servidor.

A infraestrutura apresentada pela computação em nuvem compõe-se pelos clientes comumente presentes em uma rede local (LAN), as estações de trabalho. Porém, existem outros tipos de clientes que, com a evolução tecnológica, passaram a fazer parte desse cenário atual, como os *Laptops*, *Tablets*, *Smartphones*, *PDAs* e outra série de dispositivos capazes de se conectarem a rede.



Em geral, esses clientes são dispositivos utilizados pelos usuários para acessar os serviços da nuvem.

Os dados processados, bem como os aplicativos executados na nuvem pública, podem requisitar diferentes níveis de segurança do que geralmente é encontrado no ambiente de hospedagem local. A criticidade presente neste ambiente tecnológico apresenta alguns fatores que podem afetar a segurança dos dados armazenados na nuvem e seu sistema, a saber: a qualidade da implementação, a superfície de ataque, o provável número de atacantes, a complexidade do sistema e o nível de conhecimento que os administradores possuem.

A seguir, serão abordados alguns dos principais problemas relacionados à segurança em um ambiente de computação em nuvem.

Risco não intencional de divulgação de dados

Em um cenário típico, um usuário armazena informações tanto sensíveis quanto não sensíveis em diferentes diretórios de um sistema ou em diferentes mensagens de e-mail em um servidor. Ao fazer isso, a informação sensível deverá ser cuidadosamente gerenciada para evitar sua divulgação não intencional. Se um cliente pretende usar a computação em nuvem como uma computação não sensível, mantendo as vantagens de segurança de instalações de recursos para a computação sensível, o cuidado de armazenar as informações de forma criptografada deve ser tomado.

Privacidade e integridade dos dados

A privacidade está diretamente relacionada à confidencialidade dos dados, seja de um usuário, seja de um ambiente corporativo, e destina-se à proteção dos ativos que contenham informações sensíveis.

A privacidade agrega aspectos legais e questões referentes a responsabilidades, e deve ser vista não apenas como um desafio técnico, mas como uma preocupação ética e legal. A proteção da privacidade em qualquer sistema de computação é de responsabilidade técnica; em um ambiente de configuração em nuvem, esse processo é complicado devido à distribuição natural das nuvens e a possível falta de conscientização dos usuários a respeito do local de armazenamento dos dados, e quem pode acessá-los.

Integridade do sistema

A nuvem exige uma camada de proteção visando à prevenção contra a indisciplina e a capacidade dos usuários de impedir as funcionalidades do ambiente. Dentro da nuvem existem muitas partes envolvidas: consumidores, fornecedores e uma variedade de administradores. A capacidade de dividir os direitos de acesso de cada um desses grupos, enquanto estiver sofrendo ataques maliciosos, é um atributo chave para manter a integridade da nuvem. Nesse ambiente, qualquer falta de

CURSOS ONLINE

A Revista Java Magazine oferece aos seus assinantes
uma série de Cursos Online de alto padrão de qualidade.



CONHEÇA ALGUNS DOS CURSOS:

- Curso de noSQL (Redis) com Java
- Curso Básico de JDBC
- Java Básico: Aplicações Desktop
- JSF com Primefaces
- Conhecendo o Apache Struts

Para mais informações :
www.devmedia.com.br/curso/javamagazine
(21) 3382-5038

visibilidade dos mecanismos que envolvem sua estrutura, torna mais difícil para os consumidores checarem a integridade das aplicações hospedadas.

Conclusão

Com a análise realizada pelo presente artigo, foi possível focar os aspectos da computação em nuvem voltados para a segurança da informação. O trabalho foi centrado nos aspectos conceituais da computação em nuvem e computação em grade, observando as características particulares de seus serviços. Para analisar os serviços existentes, os principais provedores e o que eles oferecem para seus clientes como soluções de SaaS, PaaS e IaaS serviram como fontes de estudo.

Os aspectos relacionados à privacidade, às normas e auditorias e às ferramentas de segurança existentes para garantir a qualidade dos serviços prestados na nuvem, são elementos indispensáveis que também se fizeram presentes neste trabalho.

Os desafios desta nova tecnologia se fazem presentes no âmbito da segurança da informação, principalmente no que envolve questões referentes à confidencialidade dos dados, como foi abordado.

Com os tópicos e estudos levantados, pôde-se ter uma visão geral dos desafios da segurança e confidencialidade dos dados em um ambiente de *Cloud Computing*. Apesar de este ambiente trazer benefícios em relação à economia com equipamentos de tecnologia, instalação de aplicações, treinamento de pessoal e segurança, é necessário que o usuário analise a viabilidade de contratação dos serviços de um provedor, verificando o nível de privacidade, disponibilidade e confidencialidade oferecido para melhor atender a seus clientes.

Autor



Leandro de Carvalho Machado
leandro.cvm@gmail.com
Bacharel em Sistemas de Informação - Faculdade Metodista Granbery. É Especialista em Segurança da Informação - FMG. É Especialista em Docência para a Educação Profissional pela Faculdade Senac Minas. Atua como Orientador de Cursos no Senac Juiz de Fora -MG e pesquisador na área de Segurança da Informação.

Autor



Marco Antônio Pereira Araújo
maraujo@devmedia.com.br
É Doutor e Mestre em Engenharia de Sistemas e Computação pela COPPE/UFRJ, Especialista em Métodos Estatísticos Computacionais e Bacharel em Informática pela UFJF, professor do Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais - Campus Juiz de Fora, professor do curso de Bacharelado em Ciência da Computação da FAGOC, professor dos Cursos de Bacharelado em Sistemas de Informação do Centro de Ensino Superior de Juiz de Fora e da Faculdade Metodista Granbery, Analista de Sistemas da Prefeitura de Juiz de Fora, Editor da Engenharia de Software Magazine.

Links e Referências:

Amazon Simple DB
http://aws.amazon.com/pt/simpledb//188-7509643-3256513/

PGP
www.pgp.com

TrueCrypt
www.truecrypt.org

Windows Intune
https://partner.microsoft.com/brasil/productssolutions/40136477

Business Productivity Online Suite
https://partner.microsoft.com/brasil/productssolutions/40053541.

Microsoft Dynamics CRM Online
http://crm.dynamics.com

IDC, New IDC IT Cloud Services Survey: Top Benefits and Challenges
http://blogs.idc.com/ie/?p=730

NIST, National Institute of Standards and Technology, U.S. Department of Commerce - The NIST Definition of Cloud Computing. 2011.

NAKAMURA, E. T.; GEUS, P. L. Segurança de Redes em Ambientes Cooperativos. São Paulo: Novatec, 2010. 482 p.

PAGLIUSI, Paulo Sergio, A Segurança da Geração que voa na Nuvem.
http://www.decisionreport.com.br/publique/cgi/cgilua.exe/sys/start.htm?infoid=9448&sid=15

PCI DSS, Payment Card Industry Data Security Standard (PCI DSS), Versão 2.0 de 2010
https://www.pcisecuritystandards.org/security_standards/index.php.

PORUS, Ajay, Coud Computing and Its Security Benefits, IT Security Magazine, 2011.
SETI, Search for Extraterrestrial Intelligence.
http://setiathome.berkeley.edu/

VELTE, Antony T., VELTE, Toby J., ELSENPETER, Robert., Cloud Computing: Computação em Nuvem Uma Abordagem Prática, Rio de Janeiro, Alta Books. 2011.

Autoconfiguração stateless de endereços via Router Advertisement

Aprenda a configurar roteadores para gerar endereços IPv6 automaticamente

Com o iminente esgotamento do IPv4, a cada dia que passa, mais e mais o assunto IPv6 fica em evidência. As pesquisas de medição mais recentes demonstram um crescente aumento no número de dados trafegados neste protocolo. A conscientização das empresas provedoras de serviços na *web*, em conjunto com os provedores de acesso a internet, tem acelerado o processo de implantação. Há, portanto, uma grande demanda de profissionais, tais como administradores de rede, técnicos de TI e professores que possuam conhecimento na área. Assim, estar atualizado neste cenário do IPv6 significa ter um diferencial no mercado de trabalho.

Tendo isso em vista, este artigo se propõe a explanar uma das funcionalidades essenciais do IPv6, a autoconfiguração de máquinas. Desta forma, a partir de uma única configuração no roteador, todas as máquinas que estiverem conectadas à rede configurar-se-ão a si mesmas. Evita-se, com isso, o problema de ter que digitar, repetidamente, todas as informações em cada uma das máquinas.

O método de autoconfiguração de máquinas que será descrito é o *stateless*, que significa ausência de armazenamento de estado. Desse modo, nenhuma máquina saberá das informações configuradas nas outras máquinas, além da sua própria configuração. É diferente do DHCP, que mantém as informações centralizadas em um servidor.

Por motivos didáticos, o artigo foi dividido em duas partes: uma teórica, que explicará como a autoconfiguração *stateless* via *router advertisement* funciona; e uma prática, na qual o leitor poderá seguir o passo a passo para implementar a funcionalidade numa rede qualquer.

Resumo DevMan

Para que serve este artigo:

O presente artigo tratará da autoconfiguração stateless via router advertisement, ou seja, uma das técnicas que permite configurar os computadores automaticamente, sem que haja armazenamento das configurações no roteador, no atual cenário do Protocolo Internet versão 6 (IPv6).

As informações contempladas neste artigo ampliam o conhecimento de redes IPv6, mostrando uma das maneiras de se configurar endereços nos computadores. Deste modo, um administrador de redes poderá se atualizar e assim julgar qual é a melhor técnica para se alocar endereços em diversas situações.

Revisão sobre IPv6

Antes de entrar no assunto do artigo, alguns conceitos elementares sobre IPv6 precisam estar bem consolidadas na mente do leitor. Para isso, uma pequena revisão foi escrita para ajudar. Caso já tenha lido o artigo sobre DHCPv6 ou já possua conhecimento básico sobre IPv6, a leitura da revisão será desnecessária para a compreensão geral do texto.

Endereço IPv6

O endereço IPv6 é composto por 128 bits, dispostos em oito campos separados pelo caractere dois pontos (":"). Cada campo possui quatro dígitos hexadecimais, que por sua vez são compostos por quatro bits (multiplicando oito campos com quatro hexadecimais e quatro bits, chega-se ao valor total de 128 bits). Um exemplo de endereço IPv6 é:

2001:0DB8:0000:F0F0:CA00:0ADA:00E0:B100

Sobre os números hexadecimais utilizados no endereço IPv6, convém lembrar que estes podem variar entre 0 a 9 e de A a F (independente se for maiúscula ou minúscula).

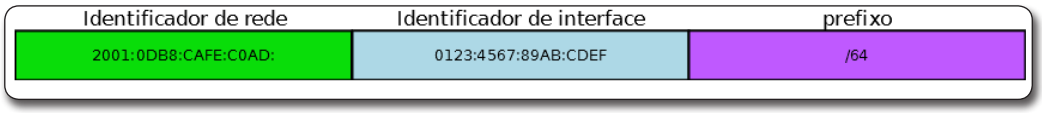


Figura 1. Endereço IPv6 com prefixo

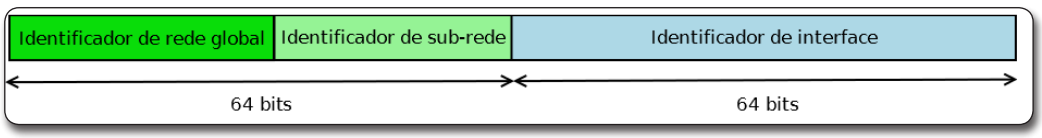


Figura 2. Recomendação de utilização de 64 bits para o identificador de interface

Regras de abreviação

Três regras de abreviação podem ser aplicadas para melhorar a legibilidade dos endereços. A primeira expõe que devem ser omitidos todos os casos de zeros à esquerda. A segunda fala que é possível representar quatro zeros, pertencentes ao mesmo campo, com apenas um único zero. Por fim, a terceira permite substituir uma única sequência continua de zeros, relativos a um ou mais campos, por "::" (dois pontos, dois pontos). Para ilustrar melhor como estas regras operam, a seguir apresentamos um exemplo:

Sem regras: 2001:0DB8:0000:0000:C0CA:DA00:0000:D0CE

Com regras: 2001:DB8::C0CA:DA00:0:D0CE

Prefixo IPv6

Todo endereço IP pode ser separado em duas partes: uma que identifica a rede e outra que identifica uma interface de uma máquina na rede. O que delimita essa separação é o valor chamado prefixo. O prefixo é constituído por um número decimal que varia de 0 a 128 (tamanho máximo do endereço). Esse número representa uma simples contagem de bits, da esquerda para a direita, que compõe a identificação da rede. O resto dos bits forma a identificação da interface de uma máquina. A **Figura 1** expõe como o endereço IPv6 é formado com um prefixo.

Nesta figura, a rede é composta pelos 64 primeiros bits (2001:DB8:CAFE:C0AD:), enquanto que o resto identifica a máquina (0123:4567:89AB:CDEF).

Classificação dos endereços

Os endereços IPv6 podem ser categorizados em três tipos: *unicast*, *anycast* ou *multicast*. O endereço *unicast* serve para designar uma única interface de uma máquina. Já os endereços *anycast* e *multicast*, por sua vez, são utilizados para identificar um grupo de interfaces. A diferença entre os dois é que se um pacote é enviado com o destino *anycast*, somente a máquina mais próxima da origem receberá e responderá o pacote, enquanto que se o destino for *multicast*, todas as máquinas do grupo receberão e responderão o pacote.

Autoconfiguração Stateless de endereços IPv6

Após a compreensão dos conceitos básicos sobre o endereço IPv6, podemos iniciar a explicação sobre a autoconfiguração stateless de endereços via router advertisement. Para tal, será detalhado o protocolo que transmitirá as informações e o procedimento que as máquinas envolvidas realizarão.

Pré-condição

Como se sabe, os endereços IPv6 possuem inúmeros bits em sua composição. Este número excessivo foi criado devido ao esgotamento de endereços da versão anterior, que não conseguiu acompanhar o crescimento da internet. Agora, com o novo endereço de 128 bits, é possível não só prover identificação para as máquinas já existentes, como também para mais de um undecilhão de novas máquinas distribuídas pelo mundo todo.

Todavia, novas recomendações do *Internet Engineering Task Force* (IETF) sugerem que sejam reservados 64 bits para identificação das interfaces de máquina. Isto significa que sobrarão outros 64 bits para serem usados na geração de identificadores de redes e sub-redes. A **Figura 2** mostra como ficará essa separação no endereço IPv6.

Refletindo sobre esta recomendação, percebe-se que uma rede, de um enlace qualquer, terá a possibilidade de conter 2^64 dispositivos conectados. É um número enorme para um enlace comum atualmente e, portanto, o leitor deve ter percebido que nem todos os endereços disponibilizados serão utilizados. Haverá, portanto, um enorme desperdício de endereços, mas isso não é um problema. É um novo paradigma que os administradores de redes terão que assimilar!

Tendo em vista a recomendação do IETF, novas aplicações e funcionalidades surgiram utilizando este conceito de separação do endereço IPv6 pela metade (64 bits para o identificador de rede e outros 64 para o identificador de interface). Uma delas é o assunto desse artigo, a autoconfiguração stateless via router advertisement. Para que as máquinas se configurem automaticamente, é preciso trabalhar com identificadores de interface com exatos 64 bits (nem mais, nem menos).

Identificador de interface

O identificador de interface, como já foi dito, é uma das duas partes que compõem o endereço IPv6. Num determinado enlace, ele serve para diferenciar as interfaces das máquinas com o mesmo prefixo. Ademais, o mesmo identificador pode ser reutilizado em mais de um endereço na mesma interface. Todavia, os dois precisam obrigatoriamente estar em sub-redes diferentes (ou seja, prefixos distintos).

Normalmente com 64 bits, o identificador de interface pode ser gerado de diferentes maneiras: manual, randômica, tempo-

rária ou algorítmica. A autoconfiguração stateless, na maioria dos sistemas operacionais, utiliza o algoritmo baseado no endereço MAC (camada de enlace) EUI-64. Por causa disso, ele é essencial para a compreensão da parte prática mais adiante. Seu funcionamento está detalhado a seguir:

1. Obtém-se o endereço MAC, padrão IEEE 802, que é composto por 48 bits, como por exemplo, A9:BD:12:87:0C:EF;
2. Inverte-se o sétimo bit, da esquerda para a direita, desse endereço (lembre-se que cada hexadecimal é formado por quatro bits). No exemplo A9:BD:12:87:0C:EF, o sétimo bit se localiza dentro do campo A9, que convertido em binário é 10101001. Invertendo o bit em vermelho, o resultado fica 10101011, que em hexadecimal é representado por AB. Então, após o término desse passo, teremos AB:BD:12:87:0C:EF;
3. Adiciona-se os dígitos hexadecimais FF:FE entre o terceiro (em verde) e o quarto byte (em azul) do resultado do passo anterior (AB:BD:12:87:0C:EF). Logo, o exemplo ficaria assim: AB:BD:12:FF:FE:87:0C:EF;
4. Por fim, transforme o resultado do passo antecedente usando o padrão do endereço IPv6, onde cada campo é composto por quatro hexadecimais. Para isso, é preciso concatenar os campos dois a dois do endereço AB:BD:12:FF:FE:87:0C:EF (para melhorar a compreensão, diferentes cores foram utilizadas para demonstrar os campos que devem ser concatenados) para formar o identificador de interface ABBD:12FF:FE87:0CEF.

A partir daí, ao adicionar o identificador gerado no último passo com um prefixo, cria-se um endereço IPv6. Isto posto, se fosse acrescentado o prefixo 2001:DB8:B010:D0CE::\64, ter-se-ia o endereço mostrado a seguir:

Prefixo: 2001:DB8:B010:D0CE::\64 + **Identificador:** ABBD:12FF:FE87:0CEF
Forma o endereço IPv6: 2001:DB8:B010:D0CE:ABBD:12FF:FE87:0CEF

Protocolo ICMPv6 (Internet Control Message Protocol version 6)

O ICMPv6 é um dos novos protocolos que surgiram para trabalhar com o IPv6. Baseado na versão anterior, o ICMPv4, ele apresenta as mesmas funcionalidades antigas, porém com algumas modificações adicionais. Isto é, além de informar características da rede, realizar diagnósticos e relatar erros de processamento, ele também possui novas funcionalidades como o mapeamento de endereços da camada 3 para a camada 2 (e vice-versa) e o gerenciamento de grupos multicast. No cenário do IPv4, estas funcionalidades pertenciam a protocolos distintos, como o ARP, RARP e o IGMP. No IPv6, eles não são mais necessários!

Este protocolo é essencial, ou melhor, vital para a comunicação via IPv6. Sem ele, não existe troca de mensagens entre quaisquer dispositivos. Além de realizar funções básicas que possibilitarão que pacotes encontrem seu próximo destino no enlace, este protocolo também permite que outros protocolos escrevam sobre ele. Esse é o caso do Neighbor Discovery Protocol, que possui a mensagem Router Advertisement utilizada na autoconfiguração stateless. A **Figura 3** mostra o formato do cabeçalho ICMPv6.

Protocolo NDP (Neighbor Discovery Protocol)

O Neighbor Discovery Protocol é um protocolo desenvolvido para ser a base da arquitetura do IPv6. Ele é escrito sobre o protocolo ICMPv6, com o objetivo de transmitir informações a respeito da vizinhança, como configurações da rede e das máquinas. Seus dados atuam em nível de enlace e, portanto não podem ser repassados pelos roteadores.

Ele é composto por cinco tipos de mensagens: Neighbor Solicitation, Neighbor Advertisement, Redirect, Router Solicitation e Router Advertisement. Cada uma possui suas próprias particularidades e objetivos distintos, sendo assim utilizadas em diversas funcionalidades básicas. Nesse artigo, explicaremos somente as duas últimas, pois só estas participam da autoconfiguração stateless via router advertisement.



Figura 3. Cabeçalho ICMPv6

Router Solicitation

Essa mensagem serve para um dispositivo localizar os roteadores que estiverem presentes no enlace. Em outras palavras, ele solicita que os roteadores se apresentem ao receber esta mensagem. Os demais dispositivos ignorarão o seu recebimento e continuarão com seus próprios processamentos.

Ela é enviada quando a interface de um dispositivo for habilitada (no momento em que ele se conecta na rede). Ao chegar ao roteador, este enviará uma resposta Router advertisement.

Router Advertisement

Essa mensagem serve para um roteador anunciar sua presença no enlace. Ou seja, ela informa aos dispositivos que roteador está presente e operante. Logo, todos os dispositivos que receberem a mensagem Router Advertisement a interpretarão e adicionarão em seus caches as informações transmitidas.

Ela é enviada em três ocasiões. Uma é em resposta à mensagem router solicitation enviada por um dispositivo qualquer no enlace. A segunda é quando existe uma nova modificação na configuração do roteador que precisa ser informada aos outros dispositivos no enlace. E a terceira, que é enviada de tempos em tempos, serve para atualizar o cache de todos os dispositivos do enlace, atuando como uma espécie de mensagem "keep alive" (aviso de que o roteador continua operante).

Em seus campos, ela carrega diversas informações de configuração, como prefixo para geração de endereços, MTU, DNS, entre outras. Ao se configurar o roteador, este replicará todas essas informações, e as divulgará para que todas as máquinas conectadas se configurem.

Procedimento: detalhando a Autoconfiguração Stateless

Após a explicação das duas mensagens, Router Solicitation e Router Advertisement, falta explicar como elas se juntam para realizar a autoconfiguração de endereços.

Para ingressar em uma rede, a máquina precisa ter o mínimo de conhecimento sobre ela. Para adquirir essas informações, a máquina utiliza mensagens. Ela as envia como uma forma de pergunta para os roteadores, que armazenam os dados da rede, responderem com as informações desejadas.

Essa mensagem "pergunta" é a Router Solicitation, que procura os roteadores presentes e ativos no enlace. Ela é enviada com o destino multicast ALL Routers (identificado pelo endereço IPv6 ff02::2), que atinge todos os roteadores. Estes, então, interpretarão e processarão a mensagem, enquanto que todas as demais máquinas simplesmente ignorarão seu recebimento.

A mensagem Router Solicitation ocasiona a criação de uma mensagem de resposta, chamada Router Advertisement. Tal mensagem, gerada no roteador, é enviada com diversas informações sobre a rede para a máquina se autoconfigurar e assim poder se comunicar. Dentre os dados transmitidos, um que merece destaque é o prefixo de rede. Ao ser mandado em conjunto com o flag AdvAutonomous setado na mensagem, faz com que a máquina receptora elabore um endereço IPv6 próprio (juntando o prefixo recebido com a identificação da interface da própria máquina). Nesse momento, dependendo do dispositivo, um algoritmo para formar o identificador de interface é utilizado, sendo o mais comum o baseado no MAC Address.

A mensagem Router Advertisement pode ser enviada para dois tipos de destino: o unicast da máquina solicitante, ou para o grupo de máquinas pertencentes ao multicast ALL Nodes (identificado pelo endereço IPv6 ff02::1, que atinge todos os nós do enlace). Isso depende da implementação de cada roteador, uma vez que ambas estão corretas de acordo com a Request for Comment (RFC4861). Em roteadores comerciais, normalmente se encontra a segunda opção, uma vez que essa mensagem também serve para informar que o roteador está ativo e operante (ou seja, algo parecido com um Keep Alive) e assim evitar novas trocas de mensagens.

Exemplo prático

Nesse tópico eremos como configurar o roteador para trabalhar com a autoconfiguração stateless via router advertisement. Como existem diversas aplicações e roteadores no mercado, com diferentes sistemas operacionais, que podem realizar esta funcionalidade, para o exemplo a seguir demos preferência a uma opção gratuita que permita implementar adequadamente o protocolo IPv6.

Radvd é uma aplicação daemon open-source, gratuita, que implementa o envio de Router Advertisements. Ele funciona tanto em sistemas operacionais Linux como BSD. Sua instalação e configuração básica são bem simples, o que ajuda ainda mais no aprendizado. Uma de suas principais vantagens é a sua integração com a ferramenta Dibbler, exposta no artigo sobre DHCPv6. Ao se trabalhar com os dois em conjunto, é possível fazer com que o DHCP distribua prefixos (ao invés de endereços) para que sejam repassados via router advertisement. Esta é uma funcionalidade nova do IPv6 chamada prefix delegation, porém esse é um enfoque para outro artigo.

Equipamentos

Para realizarmos o exemplo prático, precisaremos de dois tipos de equipamentos: um computador e um roteador, ambos utilizando o sistema operacional Ubuntu na versão 11.10. O Radvd será instalado somente no roteador, na versão 1.7. Na **Figura 4** estão apresentados os diagramas esquemáticos que representam cada equipamento que será utilizado nas experiências.



Figura 4. Equipamentos do exemplo prática

Instalação do radvd

Antes de começar a instalação é preciso verificar se a ferramenta já está instalada e qual é a respectiva versão. Para isso, no roteador, digite o seguinte comando no terminal:

```
$ radvd -v
```

No exemplo utilizaremos o Radvd na versão 1.7. Acredita-se que em outras versões da ferramenta (pouco antigas) a autoconfiguração stateless também funcione corretamente.

Caso o Radvd não esteja instalado no sistema, basta digitar o seguinte comando no terminal:

```
$sudo apt-get install radvd
```

Na seção **Links** é indicada a URL do site que possui o fonte do Radvd para download. Dessa maneira, se houver algum problema com o comando informado, é possível se obter o código fonte e instalá-lo.

Implementação

Neste exemplo, montaremos uma topologia simples composta por um roteador e um computador. Ambos precisam estar conectados por algum meio de comunicação, podendo ser Wi-Fi, cabo ethernet ou outro qualquer. A **Figura 5** mostra um desenho da rede que deverá ser criada.

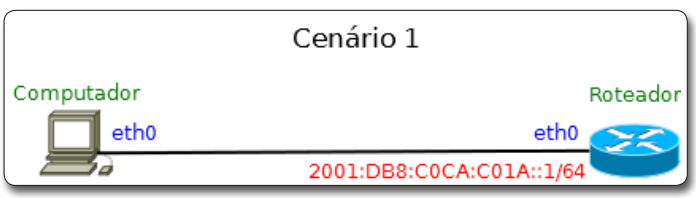


Figura 5. Cenário do exemplo da autoconfiguração stateless

Depois de criada a topologia da rede, é importante observar as configurações de cada uma das máquinas. Repare nas características das interfaces conectadas entre si. Desta forma, fica fácil entender a troca de mensagens e saber quando o endereço foi adicionado na interface do computador. Para isso, em cada uma das máquinas, digite o seguinte comando:

```
$ ip addr show
```

Após a execução desse comando, descubra qual interface está conectada em cada máquina e anote para utilizar nas configurações subsequentes.

Máquina roteador

Nesta etapa, trabalharemos com a configuração do Radvd no roteador. Em seguida, veremos a configuração do computador. Portanto, em um terminal do roteador, edite o arquivo que se encontra no caminho */etc/radvd.conf* (caso ele não exista, crie-o e remova a permissão dos outros, com o comando: *$ sudo chmod o-w /etc/radvd.conf*). Um editor fácil de operar é o "nano", mas existem outros, como o vi, vim, emacs, pico, etc. A escolha sobre qual ferramenta de edição utilizar deve ser feita de acordo com o conhecimento que o administrador de rede possui. Para abrir o arquivo de configuração em modo de edição com o nano, digite o seguinte comando no terminal do roteador:

```
$ sudo nano /etc/radvd.conf
```

Feito isso, coloque as linhas da **Listagem 1** dentro do arquivo.

Listagem 1. Arquivo de configuração do Radvd no roteador.

```
interface eth0
{
   AdvSendAdvert on;
   prefix 2001:DB8:C0CA:C01A::/64
   {
        AdvOnLink on;
        AdvAutonomous on;
   };
};
```

A seguir, explicaremos o motivo do uso de cada uma das linhas presente no arquivo de configuração da **Listagem 1**:

• interface eth0: determina o nome da interface na qual se definirá um escopo de configuração. A partir deste escopo, o administrador de rede poderá tanto delimitar as funções que serão habilitadas na interface como também escolher os tipos de dados que serão transmitidos. No nosso caso, trabalharemos com a eth0, mas o leitor deverá colocar a interface previamente anotada (usando o comando ip addr show);

• AdvSendAdvert on;: habilita um flag para indicar que o roteador deverá enviar mensagens router advertisements através da interface definida, independentemente se o motivo for o envio periódico ou em resposta à mensagem router solicitation;

• prefix 2001:db8:1::/64: determina um escopo para o prefixo de rede que será divulgado nas mensagens router advertisement. Escolha o prefixo do endereço da sua interface no roteador. Dessa forma, o computador, ao se configurar, poderá se comunicar com o roteador utilizando o endereço gerado. Não se esqueça de utilizar um prefixo do tamanho de 64 bits, que é o necessário para a autoconfiguração funcionar;

• AdvOnLink on: habilita um flag que indica se o prefixo divulgado pertence ao enlace. É a partir dessa configuração que a máquina saberá para onde enviar os dados de determinado destino, se é diretamente para a máquina que está presente no enlace ou para um roteador. Como queremos que a funcionalidade de autoconfiguração de endereço IPv6 no enlace ocorra, convém setar esse flag para que, dessa maneira, todos os computadores conectadas saibam que o prefixo enviado está sendo utilizado em endereços no enlace;

• AdvAutonomous on: habilita um flag que indica que as máquinas receptoras da mensagem devem realizar a autoconfiguração de endereços utilizando o prefixo enviado.

Outras linhas de configuração podem ser adicionadas para transmitir mais informações sobre a rede, como por exemplo: **AdvLinkMTU 1280;**, que serve para informar as máquinas sobre o tamanho máximo de MTU (1280) dos pacotes que podem trafegar no enlace; e **RDNSS 2001:DB8:1:1::1 {};**, que informa o endereço da máquina de DNS (nesse caso foi utilizado um endereço fictício). Para adicionar novos comandos, veja na seção **Links** o manual do Radvd.

Depois de gerado o arquivo de configuração, podemos iniciar o Radvd no roteador. Para isso, digite o seguinte comando no terminal:

```
$ sudo radvd -C /etc/radvd.conf
```

Máquina cliente

Finalizada a inicialização do Radvd do roteador, podemos observar a interface da máquina conectada para ver o novo endereço configurado. Portanto, digite o seguinte comando na máquina do cliente e repare no endereço IPv6 que possui o mesmo prefixo enviado pelo Router Advertisement (2001:DB8:C0CA:C01A::/64, configurado no Radvd anteriormente):

```
$ ip addr show
```

Caso nenhum endereço apareça, convém analisar se o computador está configurado para aceitar o anúncio de router advertisements. No Linux, a regra é que esta configuração venha "setada", mas vale a pena conferir! Para isso, digite o comando a seguir e observe se aparece o valor 1 na tela:

```
$ sudo nano /proc/sys/net/ipv6/conf/eth0/accept_ra
```

Vale ressaltar que *eth0* corresponde à interface conectada no enlace. Caso a interface seja outra, esta deve ser trocada nesse comando.

Se aparecer o valor 0, edite para o valor 1 e salve. Repita o mesmo processo para o arquivo */proc/sys/net/ipv6/conf/eth0/accept_dad*, que determina se a máquina deve ou não realizar a funcionalidade de detecção de endereços duplicados. Antes de um endereço IPv6 ser adicionado a uma interface de uma máquina, esta precisa ter certeza que o endereço é único no enlace. Sendo assim, a máquina precisa executar essa funcionalidade.

Por fim, reinicie as configurações da interface da máquina com o comando:

```
$ sudo service networking restart
```

Resultado

Para entender melhor a troca de mensagens e observar as informações que estão sendo transmitidas, pode ser utilizado o programa Wireshark. Dessa maneira, o administrador de rede conseguirá observar os erros nas mensagens trafegadas e propor soluções. No sistema operacional que estamos trabalhando no exemplo, o Ubuntu, a instalação do Wireshark é bem simples, basta digitar no terminal:

```
$ sudo apt-get install wireshark
```

Feito isso, aproveite o programa para iniciar a captura dos pacotes que estão passando pela interface de rede da máquina. Assim, poderá observá-los e estudá-los para compreender melhor a funcionalidade autoconfiguração stateless de endereços.

Como conseguir um endereço IPv6?

Caso o leitor não possua endereço IPv6 do seu provedor para reproduzir o exemplo prático, é possível conseguir através de um tunnel broker. Existem algumas opções desse serviço na internet, contudo citaremos duas que são gratuitas e que possuem boa reputação. A primeira delas é a Hurricane Eletric, uma empresa que possui o maior backbone IPv6 do mundo, medido em quantidades de redes conectadas. A outra é a SixXs, que oferece serviços de forma colaborativa para várias organizações e possui o enfoque de prover uma boa conectividade IPv6. Ambas fornecem blocos de endereços mediante um simples cadastro; basta preencher os formulários nos endereços expostos na seção **Links**.

Ao receber o bloco IPv6 é preciso garantir que o prefixo possua exatamente 64 bits. Para isso, o leitor pode utilizar um divisor de sub-redes, como o demo do NIC.br ou o aplicativo Android chamado Subnet6 do SimpleBit. Os dois utilizam algoritmos padronizados pela RFC 3531 para a divisão de redes e suas URLs também se encontram na seção Links. Dessa forma, não haverá dificuldades em se trabalhar com o novo protocolo.

Conclusão

Com a crescente migração para o IPv6, os profissionais ligados à área de redes devem estar sempre atualizados para trabalhar com as funcionalidades do novo protocolo. Neste cenário, o presente artigo trouxe uma das configurações possíveis que facilitarão o processo de sua implantação. Além dos conceitos básicos de IPv6, que já foram abordados em outro artigo, foi apresentada a técnica de autoconfiguração stateless via router advertisement.

Enfim, espera-se que todos os ensinamentos transmitidos neste artigo ajudem o leitor a implementar IPv6 na sua rede. Quanto maior o número de computadores operando com o novo protocolo, melhor será o futuro da internet.

Links:

Site da ferramenta Radvd
http://packages.ubuntu.com/lucid/radvd

Guia de uso do Radvd
http://manpages.ubuntu.com/manpages/hardy/man5/radvd.conf.5.html

RFC 4861 – Neighbor Discovery for IP version 6
http://tools.ietf.org/html/rfc4861

Apostila "Curso IPv6 básico" do NIC.br
http://ipv6.br/download/

Núcleo de Informação e Coordenação do Ponto BR
www.nic.br

Autor



Eduardo Barasal Morales
ed.barasal@gmail.com



É Engenheiro de computação graduado e mestrando pela Escola Politécnica da Universidade de São Paulo e trabalhou com desenvolvimento de softwares para transferência eletrônica de fundos, gestão de saúde e tarifação de telefonia. Atualmente, no NIC.br, é Analista de Projetos, ministra cursos do projeto IPv6.br e também participa do desenvolvimento de seu material didático para a disseminação de conhecimento do protocolo pelo país.

Border gateway protocol: o protocolo padrão da Internet

Como um único protocolo de roteamento suporta a comunicação entre todas as redes de computadores conectadas à Internet?

No início dos anos 1970, quando a primeira rede de computadores entrou em operação, era inimaginável que esta chegaria às proporções atuais da Internet. A administração da comunicação entre todos os roteadores que faziam parte deste embrião precisava ser realizada de maneira dinâmica e necessitava suportar a rápida expansão da infraestrutura. Neste cenário, surgiu o protocolo BGP para padronizar e organizar a comunicação entre as diferentes entidades que se interligavam a rede mundial de computadores. Responsável por superar as deficiências de seu antecessor (o protocolo EGP), o BGP evoluiu até sua quarta versão, denominada BGP-4. Atualmente, este é o padrão que guia a comunicação de dados entre todos os sistemas autônomos da Internet.

Nos dias de hoje, para que seja possível acessar qualquer um dos segmentos de rede disponíveis na Internet são necessárias mais de 440.000 rotas de endereços IPv4 (*Internet Protocol version* 4, neste artigo doravante denominado IP). Este número corresponde aos prefixos (agrupamentos de endereços) em uso nas organizações espalhadas por todos os continentes que acessam a rede mundial. Para que exista comunicação entre estas entidades, é importante que haja um único conjunto de regras que oriente como os dados serão compartilhados. Analogamente às relações humanas, nas quais existe um idioma predominante, o qual permite que pessoas de qualquer parte do planeta Terra possam partilhar mensagens, os provedores de conteúdo, as operadoras de telecomunicações, as instituições financeiras, os órgãos de ensino e pesquisa, entre outros, também precisam de um padrão para que suas redes de computadores estejam acessíveis, possibilitando o envio e o recebimento de pacotes IP.

O protocolo BGP foi criado em meados de 1989 com o intuito de reger este diálogo entre os roteadores e de suportar as diferentes infraestruturas já existentes, provendo escalabilidade, flexibilidade e redundância, além de possibilitar a criação de políticas de roteamento que respeitassem as particularidades e os anseios de cada uma das organizações que se conectavam a Internet.

Resumo DevMan

Para que serve o artigo:

Este artigo apresenta os conceitos fundamentais de operação do border gateway protocol (BGP), componente que torna possível a comunicação de dados IP entre as organizações que se interligam por meio da Internet. Dentre as razões para sua adoção, será destacado seu suporte às diferentes topologias lógicas das redes de computadores, o qual impede loops no envio dos pacotes IP e possibilita a configuração de arquiteturas que atendem às diferentes necessidades das políticas de roteamento.

A administração de redes de computadores com suporte ao BGP é uma tarefa complexa, pois este protocolo permite a configuração de políticas díspares de roteamento para cada um de seus provedores de acesso à Internet. Erros na operação do protocolo BGP podem gerar indisponibilidades no acesso aos serviços da rede mundial de computadores, tanto para a organização interna quanto para os usuários de outros sistemas autônomos. Neste contexto, observa-se a importância da compreensão da terminologia e do funcionamento deste protocolo entre os profissionais da área de redes de computadores, permitindo a contenda e o aprofundamento técnico no tema.

Entretanto, estas características tornaram o gerenciamento deste protocolo mais complexo, pois foi necessária a inclusão de diversos recursos que sustentassem a pluralidade de seus usuários.

Em seu início, este artigo mostra a definição dos sistemas autônomos, que são as unidades fundamentais da rede mundial de computadores, interligados pelo BGP-4. A seguir, são apresentadas as características principais da operação deste protocolo e destacados os três cenários básicos de roteamento observados nas infraestruturas de comunicação de dados. Também são descritas as diferentes mensagens que são empregadas pelos roteadores configurados com BGP-4 a fim de estabelecer sessões internas e externas, abordando a máquina de estados finitos do BGP – a qual auxilia na compreensão dos diferentes estados pelos quais o protocolo transita antes do efetivo envio e recebimento dos prefixos de roteamento. Por fim, são contextualizados os distintos atributos que conferem ao BGP uma forma flexível de influenciar a escolha do melhor caminho para um determinado destino remoto.

Sistemas autônomos

Os sistemas autônomos (em inglês, *autonomous system* – AS) são compostos por uma ou mais redes de computadores gerenciadas de acordo com uma política de roteamento única, que define as regras para o encaminhamento dos pacotes de dados IP à *Internet*. Cada AS pode determinar o protocolo de roteamento interno – IGP (*interior gateway protocol*) que realizará a integração entre os componentes de sua infraestrutura baseado em seus próprios critérios operacionais, administrativos, e técnicos. Por outro lado, para que seja viável a troca de dados entre os diferentes sistemas autônomos, é necessário que todos optem por um único protocolo de roteamento externo – EGP (*exterior gateway protocol*).

Os protocolos de roteamento internos (IGPs) suportam os roteadores instalados em um mesmo AS. São agrupados em duas principais categorias, conforme o processo utilizado para determinar como os pacotes serão encaminhados: vetor de distâncias e estado de enlaces. Na primeira, os roteadores possuem uma tabela que armazena as menores distâncias para os destinos conhecidos e por onde os pacotes deverão ser enviados, a fim de determinar as melhores rotas. *Routing Information Protocol* (RIP), *Interior Gateway Routing Protocol* (IGRP) e *Enhanced Interior Gateway Routing Protocol* (EIGRP) são alguns dos protocolos inseridos neste grupo. Já na segunda categoria, todos os roteadores mapeiam a topologia lógica da rede e se baseiam nesta para determinar os melhores caminhos. *Open Shortest Path First* (OSPF) e *Intermediate System to Intermediate System* (IS-IS) são os protocolos mais conhecidos neste subconjunto.

Criados com o intuito de subsidiar o crescimento estruturado da rede mundial de computadores e de estabelecer um padrão de comunicação, os protocolos de roteamento externos suportam a transferência de dados entre os sistemas autônomos. Atualmente, o *Border gateway protocol version* 4 (BGP-4) é o protocolo padrão para a integração entre as redes de computadores espalhadas por todos os continentes.

Para identificar os ASs, um número global e único (*Autonomous System Number* – ASN) é atribuído às organizações por um registro regional da Internet (*Regional Internet Registry* – RIR), órgão responsável pela alocação e reserva dos recursos de numeração da Internet em uma determinada região do mundo. Inicialmente, o ASN foi definido como um número inteiro de 16 *bits* (2 *bytes*), possibilitando associar números desde 1 a 65.535. Posteriormente, esta faixa foi ampliada para 32 *bits* (4 *bytes*), expandindo para 4.294.967.295 ASNs.

As instituições públicas e privadas que desejam se tornar um sistema autônomo devem apresentar suas justificativas técnicas ao RIR e descrever sua infraestrutura de comunicação de dados. Além disso, precisam disponibilizar: uma equipe técnica habilitada para projetar, implantar e operar sua política de roteamento; *software* e *hardware* compatíveis com o protocolo BGP-4; e, condições financeiras para a manutenção dos recursos de numeração (ASN e endereços IP). Operadoras de telecomunicações, provedores de conteúdo, empresas de tecnologia da informação, fornecedores de *hardware* e *software*, órgãos de ensino e pesquisa, instituições financeiras, entre outros, são alguns exemplos de sistemas autônomos (**Figura 1**). Entre as diversas vantagens de se tornar um AS, destacam-se:

- **Disponibilidade:** remove a restrição de conexão em um único provedor de acesso à Internet, ou seja, possibilita o encaminhamento dos dados para múltiplas operadoras de telecomunicações;
- **Espaço de endereçamento IP próprio:** os endereços IP podem ser atribuídos diretamente aos clientes, reduzindo o uso das traduções de endereços IP (*Network Address Translation* – NAT) e facilitando a rastreabilidade dos eventos na rede;

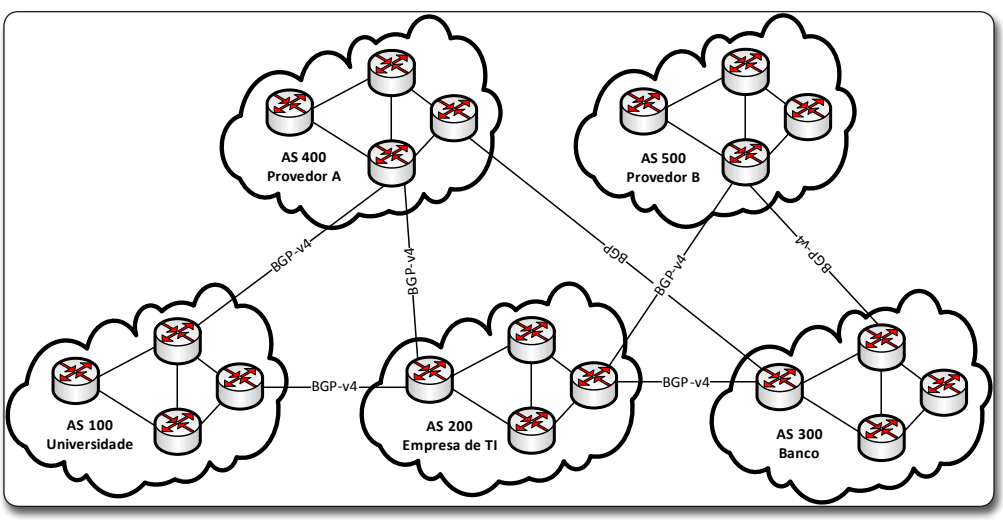


Figura 1. Relações entre os sistemas autônomos

• **Portabilidade de endereços IP:** independência do provedor de acesso, permitindo a manutenção das configurações IP mesmo quando ocorrerem mudanças nos fornecedores de acesso à Internet;
• **Políticas de roteamento:** a engenharia de tráfego determina a melhor opção técnica-financeira para o encaminhamento de dados IP aos diversos destinos na rede mundial de computadores.

Border gateway protocol version 4

No início dos anos 1970, quando a primeira rede de computadores entrou em operação nos EUA, existiam poucas instituições de pesquisa conectadas àquela que seria o embrião da Internet: a ARPANET (*Advanced Research Projects Agency Network*). Inicialmente, o gerenciamento das tabelas de rotas era feito manualmente, configurando quais redes IP poderiam ser acessadas a partir de cada roteador da infraestrutura. Entretanto, o célere crescimento da Internet mostrou que a atualização destas informações seria inviável; logo, seriam necessários mecanismos dinâmicos para sua manutenção. Neste contexto, surgiram os protocolos de roteamento externos: o *exterior gateway protocol* – EGP representou a primeira tentativa de comunicação entre sistemas autônomos distintos (observe que este protocolo possui a mesma denominação da categoria na qual está inserido). Todavia, segundo *Alex Soares de Moura*, em seu artigo *O protocolo BGP-4*, este não se mostrou flexível para a configuração das políticas de roteamento e para suportar diferentes topologias, evitando *loops* no encaminhamento dos pacotes IP.

Assim o protocolo BGP surgiu em meados de 1989 (RFC 1105) com o objetivo de substituir o EGP e suplantar suas deficiências. A proposta inicial sofreu diversas alterações até a versão atual, apresentada na RFC 4271. Entre suas características principais, destacam-se:
• Suporte às diferentes arquiteturas de comunicação de dados, permitindo flexibilidade na concepção dos projetos de infraestrutura;
• Atualização incremental dastabelas de roteamento (apenas no momento inicial são enviados todos os dados);
• Uso de um protocolo confiável (*Transmission Control Protocol* – TCP) na troca das mensagens de controle;
• Disponibilização do *Classless Interdomain Routing* (CIDR), recurso que possibilita a agregação ou sumarização de rotas IP;
• Opção de autenticação da conexão entre os roteadores envolvidos (chamados de BGP *speakers*) por meio de senhas.

Os três cenários fundamentais de roteamento suportados pelo protocolo BGP-4 são: intersistemas autônomos, intrassistemas autônomos e trânsito entre ASs. Definem o relacionamento entre os roteadores, as regras que serão utilizadas para propagação das tabelas de roteamento e as políticas que serão implantadas por cada um dos sistemas autônomos.

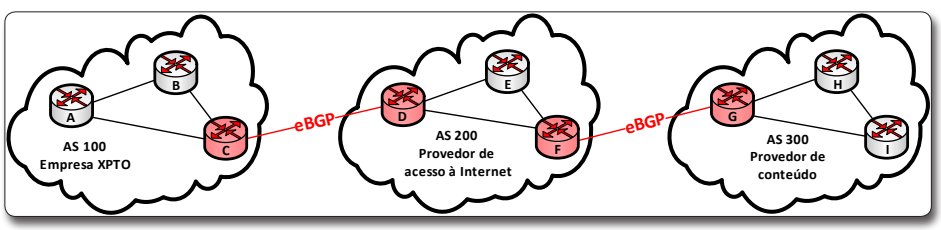


Figura 2. Roteamento intersistemas autônomos

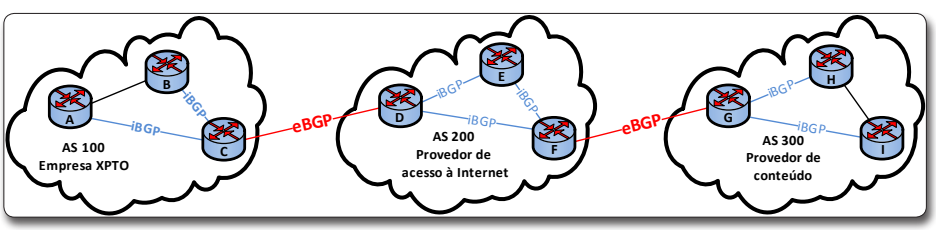


Figura 3. Roteamento intrasistemas autônomos

Dois ou mais roteadores em ASs distintos se comunicam pelo roteamento intersistemas autônomos, que gera uma relação de vizinhança *external* BGP (eBGP). Esta é a aplicação mais comum do protocolo BGP-4 e o alicerce de funcionamento da Internet, que em última instância pode ser definida como uma coleção de ASs interconectados. A **Figura 2** ilustra relações eBGP entre os roteadores C (AS 100) e D (AS 200), e, entre F (AS 200) e G (AS 300). Portanto, os dados de um usuário conectado ao segmento de rede do roteador A da empresa XPTO, direcionados a um servidor *web* localizado no provedor de acesso à Internet, necessariamente serão encaminhados pela rede interna do AS 100 ao roteador C, segundo sua política interna de roteamento, pois esta é a única interface entre os ASs 100 e 200.

Já a comunicação intrassistemas autônomos ocorre quando o protocolo BGP-4 é configurado entre dois ou mais roteadores pertencentes ao mesmo AS. Comumente chamada de vizinhança *internal* BGP (iBGP), esta aplicação permite o compartilhamento das tabelas de rotas entre os roteadores do AS que possuem conexões com outros sistemas autônomos e aqueles localizados internamente. No exemplo apresentado na **Figura 3**, destacam-se em azul as relações iBGP entre os roteadores internos dos ASs 100, 200, e 300. É possível observar também que os roteadores C (AS 100), D (AS 200), F (AS 200) e G (AS 300) possuem ambos os tipos de vizinhanças: iBGP e eBGP. São estes os roteadores responsáveis pela propagação das rotas externas aos demais dispositivos de seus sistemas autônomos.

O trânsito entre os sistemas autônomos é realizado por ASs que não possuem relação direta com o remetente ou destinatário dos pacotes IP, ou seja, que apenas encaminham os dados de terceiros. A **Figura 4** destaca o AS 200 como uma entidade de trânsito, que conecta os usuários da empresa XPTO (AS 100) ao provedor de conteúdo (AS 300). Tipicamente, os provedores de acesso à Internet e as operadoras de telecomunicações são organizações que oferecem trânsito IP aos seus clientes, criando uma malha de interconexão

entre os diferentes sistemas autônomos espalhados pela região geográfica na qual possuem cobertura.

Por padrão, três importantes regras devem ser consideradas no projeto de uma topologia de rede com suporte ao protocolo BGP-4:

1. As rotas recebidas por uma conexão eBGP podem ser propagadas para vizinhanças eBGP e iBGP. Entretanto, para evitar *loops* de roteamento, por padrão, as rotas aprendidas por iBGP não são encaminhadas para outros roteadores em sessões iBGP. Portanto, necessariamente um sistema autônomo sempre empregará um IGP para o compartilhamento interno das tabelas de roteamento de seus dispositivos;
2. Todos os roteadores configurados com o protocolo BGP-4 devem estar conectados logicamente entre si (vizinhanças iBGP), formando uma topologia com malha completa (*full-mesh*). Esta arquitetura é necessária para atender a restrição imposta pelo comportamento descrito no item anterior. Por exemplo, suponha que o AS 200 ilustrado na **Figura 5** é de uma operadora de telecomunicações que provê trânsito para os sistemas autônomos 100, 300, 400 e 500. No cenário (a), as rotas na conexão eBGP com o AS 300 serão propagadas aos roteadores A e D via iBGP; mas estes não as encaminharão ao roteador C. Por outro lado, A e D enviarão para C, respectivamente, as rotas dos ASs 100 e 400, pois estas foram recebidas por meio de sessões eBGP. Destarte, para que os sistemas autônomos possam se comunicar, é necessário que todos os roteadores BGP do AS 200 estejam conectados logicamente em topologia *full-mesh* (b);
3. Somente são propagadas para os BGP *peers* (vizinhos) rotas que estejam na tabela de roteamento dos dispositivos, sejam redes diretamente conectadas, prefixos IP configurados estaticamente ou aprendidos por intermédio de protocolos dinâmicos.

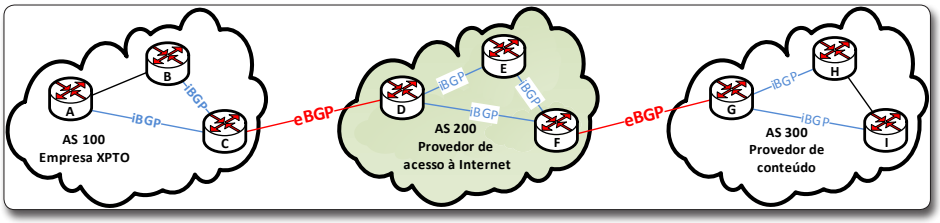


Figura 4. Sistema autônomo com função de trânsito IP

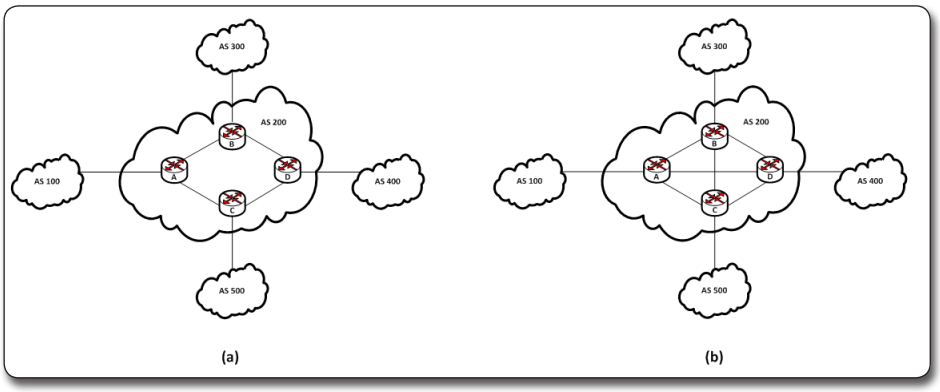


Figura 5. Topologia BGP parcial-mesh (a) e full-mesh (b)

Mensagens BGP-4

O protocolo BGP-4 utiliza um conjunto de mensagens para estabelecer a comunicação com os demais roteadores, monitorar as sessões ativas, enviar atualizações de roteamento e notificar erros. Cada uma destas mensagens é empregada para um tipo específico de ação, a saber:

- ***OPEN*:** enviada por cada roteador BGP (também chamado BGP *peer*) envolvido no estabelecimento da vizinhança, após a abertura da conexão TCP na porta 179. Entre outras informações, indica a versão do protocolo, o número do sistema autônomo e a identificação do roteador;
- ***UPDATE*:** uma vez estabelecida a sessão BGP, os roteadores iniciam a trocam de seus prefixos IP por intermédio de mensagens *UPDATE*, as quais detalham cada uma das rotas propagadas para o BGP *peer*. Estes prefixos IP também são comumente denominados informações de alcançabilidade da camada de rede – NLRI (*Network Layer Reachability Information*). As mensagens *UPDATE* transportam atualizações das tabelas de roteamento, tais como: rotas que devam ser removidas (inalcançáveis) e adicionadas (alcançáveis), atributos dos caminhos pelos quais os pacotes IP serão encaminhados (BGP *path atributes*), etc.;
- ***NOTIFICATION***: mensagens que indicam um erro que resultará no encerramento da sessão BGP. Entre os principais eventos notificados, destacam-se as conexões não sincronizadas, as falhas na autenticação, na identificação do BGP *peer* e do ASN, e os erros na escolha dos BGP *path atributes* mandatórios;
- ***KEEPALIVE***: após o estabelecimento da vizinhança e da troca de mensagens *UPDATE*, os BGP *peers* enviam periodicamente *KEEPALIVES* para assegurar que a conexão esteja ativa entre os roteadores.

Estados de uma conexão BGP-4

O estabelecimento de uma sessão BGP passa por seis passos distintos antes da efetiva troca dos prefixos IP entre os BGP *peers*: *idle*, *connect*, *active*, *open sent*, *open confirm* e *established*. A **Figura 6** ilustra uma máquina de estados finitos, representação habitualmente adotada para indicar os estados e a transição entre cada um deles. Em todas as etapas, os roteadores enviam e recebem mensagens, processam os dados e reservam os recursos, antes de iniciarem a próxima fase. Quando ocorrem falhas, os BGP *peers* retornam ao ponto inicial (*idle*) e repetem o processo novamente. A lista a seguir descreve detalhadamente os diferentes passos:

- *Idle*: estágio inicial, observado após a configuração do BGP-4 em um roteador. Neste momento, o protocolo aguarda a inicialização de uma conexão TCP com um *peer* remoto. Quando esta ocorrer, há a transição para a etapa *connect*; em caso

contrário, a vizinhança permanece na fase inicial. Filtros de segurança, restrições de conectividade e configurações incorretas do IP/ASN nos BGP *peers* são as principais causas de problemas neste estado;

• *Connect*: neste passo, o protocolo aguarda a conclusão da conexão TCP entre os roteadores para enviar uma mensagem *OPEN*. A seguir, o BGP *peer* efetua a transição para *open sent*. Se ocorrerem falhas no TCP, o protocolo passa para o estágio *active*;

• *Active*: analogamente à etapa anterior, o roteador aguarda a conclusão da comunicação TCP. Caso seja bem sucedida, o protocolo envia uma mensagem *OPEN* e passa para a fase *open sent*. Se ocorrer uma nova falha, o BGP *peer* efetua a transição para *connect*. Quando o administrador do sistema autônomo realiza alguma intervenção manual, o protocolo retorna ao estado *idle*. Intermitências entre *connect* e *active* geralmente indicam problemas na conexão TCP entre os BGP *peers*;

• *Open sent*: o *peer* BGP aguarda uma mensagem *OPEN*. Após recebê-la, valida a versão do protocolo, o número do sistema autônomo, a identificação do roteador e os demais campos da mensagem; se forem identificados erros, envia uma mensagem *NOTIFICATION* e retorna ao estado *idle*. Em caso contrário, o roteador inicia o envio de mensagens *KEEPALIVE* e negocia o intervalo de espera (*hold time*) entre as mensagens *KEEPALIVE* e *UPDATE*. Neste momento também determina se a relação será *internal* BGP ou *external* BGP, por intermédio da comparação do AS informado pelo *peer* remoto com aquele configurado localmente. A seguir, o protocolo BGP-4 efetua a transição para *open confirm*. Se ocorrerem desconexões na camada TCP, a vizinhança retorna para *active*. Outras falhas resultarão na passagem para o estágio inicial;

• *Open confirm*: nesta fase, o protocolo BGP-4 espera o *KEEPALIVE* para efetuar a transição para *established* e finalizar a negociação entre os BGP *peers*. Mensagens *NOTIFICATION*, falhas no recebimento do *KEEPALIVE* periódico, intervenções do administrador do sistema autônomo e outros eventos resultarão na transição para o ponto inicial;

• *Established*: os roteadores BGP enviam e recebem mensagens *UPDATE* ou *KEEPALIVE* conforme o *hold time* negociado anteriormente. Quaisquer falhas resultarão no envio de uma *NOTIFICATION* e no retorno para o estágio *idle*.

A máquina de estados finitos do protocolo BGP-4 permite identificar em qual estágio encontra-se uma vizinhança entre dois BGP *peers*, auxiliando na resolução de problemas na ativação destas sessões. Comumente, os usuários não familiarizados com esta terminologia atribuem o correto funcionamento ao estágio *active*; entretanto, conforme descrito nesta seção, a troca dos prefixos de roteamento é realizada apenas no estado *established*. Portanto, resumidamente, a comunicação entre os roteadores BGP-4 envolve as seguintes ações:

1. Inicialização e estabelecimento de uma sessão TCP entre os dispositivos;
2. Criação da vizinhança entre os roteadores: para tanto, o protocolo BGP-4 utilizará as mensagens abordadas anteriormente para efetuar a transição entre seus diversos estados até o estágio *established*;
3. Envio de um fluxo inicial de dados, correspondentes à tabela completa dos prefixos IP conhecidos pelos roteadores;
4. Atualizações posteriores serão enviadas de forma incremental, à medida que as alterações ocorrerem na topologia da rede;
5. Propagação periódica de mensagens *KEEPALIVE* para manter a sessão *established*;
6. Manutenção da tabela de roteamento recebida do BGP *peer* enquanto a sessão com o mesmo estiver no estado *established*;
7. Encaminhamento de mensagens *NOTIFICATION* em qualquer condição de erro e encerramento da conexão BGP-4, retornando ao estágio inicial.

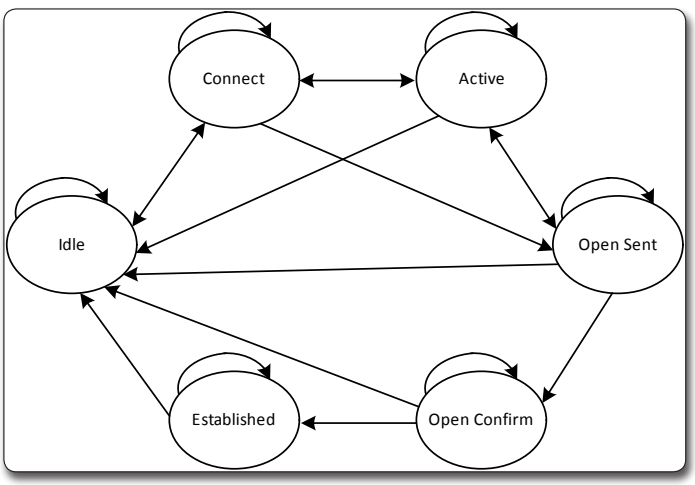


Figura 6. Estados de uma conexão BGP-4

Atributos do BGP-4

O protocolo BGP-4 é sustentado pelo algoritmo vetor de caminhos (*path vector*), no qual, a partir de dados recebidos dos demais sistemas autônomos, cria-se um vetor que armazena os ASNs que formam o caminho até cada uma das redes remotas. Considerando que as diversas vizinhanças BGP divulgam estas informações, é possível calcular o menor caminho para uma determinada rede IP (*as-path*). Por exemplo, suponha a topologia ilustrada na **Figura 7**, na qual a empresa B pode acessar o prefixo 7.7.7.0/8 (empresa A) por intermédio das operadoras Y (AS 300) ou Z (AS 400). É importante notar que a operadora Z possui uma conexão eBGP direta com a empresa A (AS100), enquanto que a operadora Y depende do serviço de trânsito BGP prestado pela operadora X (AS 200). Neste cenário, a rota de menor caminho seria pela operadora Z, pois os dados passam somente por um sistema autônomo até o destino final.

Uma importante melhoria introduzida no algoritmo vetor de caminhos está relacionada à prevenção dos *loops* de roteamento, pois os roteadores verificam no *as-path* de cada prefixo se o mesmo foi originado ou propagado pelo seu próprio sistema autônomo, descartando-o quando esta observação for verdadeira.

Cabe destacar também, que a escolha da melhor rota não é ne-

cessariamente baseada no menor caminho, pois outros atributos podem ser avaliados. Estes descrevem um conjunto de propriedades dos prefixos IP e são empregados na decisão da melhor opção para o encaminhamento dos pacotes quando há múltiplos caminhos. Os atributos podem ser agrupados nas categorias indicadas a seguir:

• ***Well-known mandatory*** **(mandatório):** atributos suportados por todas as implementações BGP e necessariamente incluídos nas mensagens *UPDATE*;

• ***Well-known discretionary*** **(discricionário):** atributos suportados por todas as implementações BGP, mas opcionalmente incluídos nas mensagens *UPDATE*;

• ***Optional transitive*** **(opcional transitório):** atributos opcionais que são reencaminhados de forma transparente pelos roteadores, mesmo quando não suportados, para seus BGP *peers*;

• ***Optional non-transitive*** **(opcional não transitório):** atributos opcionais que, quando não suportados, são removidos pelos roteadores ao encaminhá-los para outras vizinhanças BGP.

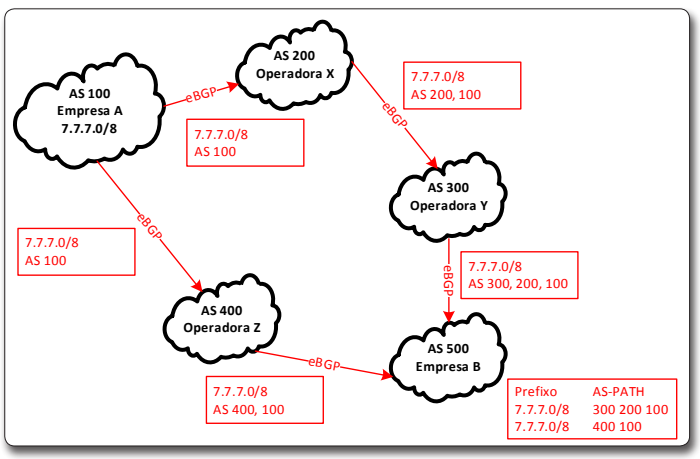


Figura 7. Diferentes caminhos (as-paths) entre as empresas A e B

Entre os atributos definidos como *well-known mandatories*, destacam-se:

• ***ORIGIN:*** indica a origem do prefixo IP encaminhado pelo protocolo BGP-4. Pode assumir o valor IGP (aprendido a partir de qualquer BGP *peer*), EGP (gerado pelo protocolo de roteamento externo) e *INCOMPLETE* (rota manualmente configurada, redistribuída por outros protocolos ou configurada diretamente na interface do roteador);

• ***AS_PATH:*** lista dos sistemas autônomos pelos quais o prefixo IP passou desde sua origem até o BGP *peer* que o recebeu. Para tanto, todos os ASs adicionam seu número no início do *AS-PATH;* roteadores com vizinhanças iBGP não alteram este atributo;

• ***NEXT_HOP***: identifica o próximo roteador (*hop*) para se alcançar a rede de destino. Por padrão, o roteador que anuncia uma rota repassa como *NEXT_HOP* seu próprio endereço IP, exceto nas vizinhanças iBGP. Nestas, é mantido o endereço IP da vizinhança eBGP na qual o prefixo foi recebido.

A lista a seguir detalha os atributos *well-known discretionaries*:

• ***LOCAL_PREF***: utilizado localmente para indicar o melhor caminho de saída para um determinado destino, não sendo repassado por sessões eBGP. Configurado pelo administrador do sistema autônomo quando há múltiplos caminhos para um mesmo destino: quanto maior o valor atribuído, mais prioritária será aquela rota;

• ***ATOMIC_AGGREGATE:*** indica aos BGP *peers* que os prefixos foram sumarizados no roteador de origem.

Já entre os atributos denominados *optional transitives*, devem ser citados:

• ***AGGREGATOR***: empregado em conjunto com o *ATOMIC_AGGREGATE*, informa o ASN e a identificação do roteador que agregou as rotas;

• ***COMMUNITY:*** associa um marcador (*tag*) aos prefixos IP que compartilham características comuns, tais como aqueles que não serão anunciados externamente (identificados com *NO_EXPORT*), os que não devem ser reencaminhados para outros BGP *peers* (*community NO_ADVERTISE*) ou outros definidos pelo administrador do sistema autônomo.

Por fim, os atributos a seguir pertencem à última categoria, chamada *optional non transitives*:

• ***MULTI_EXIT_DISCRIMINATOR (MED):*** permite ao AS divulgar para seus vizinhos por qual conexão eBGP o tráfego deverá ser preferencialmente encaminhado, quando há duas ou mais sessões ativas. O MED tem por objetivo influenciar o tráfego de entrada no sistema autônomo por meio da configuração de uma métrica, que terá maior preferência à medida que seu valor se aproxima de zero;

• ***ORIGINATOR_ID***: utilizado em uma topologia particular do protocolo BGP-4, conhecida como *route reflector*, para indicar o roteador que originou as rotas localmente; é empregado para detecção de *loops* de roteamento;

• ***CLUSTER_LIST***: apresenta a lista de grupos (*clusters*) de *route reflectors* pelos quais o prefixo foi anunciado, também com o objetivo de evitar *loops* de roteamento.

A escolha da melhor rota baseia-se nos atributos de cada prefixo IP. Nos sistemas autônomos com duas ou mais saídas para a Internet, existem múltiplas alternativas para uma mesma rede. Neste cenário, o algoritmo de decisão do protocolo BGP-4 determina o caminho que será utilizado por meio da seguinte análise (segundo *Karl Solie* e *Leah Lynch*, em seu artigo *BGP-4 Theory*):

1. Verificar se o *NEXT_HOP* é alcançável. Em caso contrário, desativar o prefixo;
2. Selecionar a alternativa com o maior *LOCAL_PREF*;
3. Caso as opções possuam o mesmo *LOCAL_PREF*, escolher aquela com o menor *AS-PATH*;
4. Em caso de empate, avaliar o atributo *ORIGIN* (prioridade para os anúncios do tipo IGP, EGP e *INCOMPLETE*, respectivamente);

5. Preferir a rota com o menor MED;
6. Se o MED for igual ou não utilizado, eleger os caminhos eBGP (comparando-os com os iBGP);
7. Caso ambos sejam iguais, selecionar a alternativa com a menor métrica IGP;
8. Preferir os anúncios que foram recebidos primeiro (mais antigos);
9. Em caso de empate, selecionar o BGP *peer* com a menor identificação (IP).

Conclusão

O célere crescimento da Internet impulsionou a ampliação da infraestrutura de redes que suportava seus diversos serviços. Quando foi criada, esta interligava poucas instituições dos EUA na década de 1970; hoje, apenas 43 anos depois, conecta algumas centenas de milhares de entidades. Para que esta expansão fosse possível, os componentes das redes de computadores foram agrupados em sistemas autônomos, organizações que possuem liberdade para determinar como seus recursos internos são configurados e gerenciados, conforme seus critérios técnicos, administrativos e operacionais. No entanto, ainda existia a necessidade de um protocolo de comunicação padrão, que suportasse a pluralidade de cada um destes ambientes, além de oferecer escalabilidade, flexibilidade e redundância da infraestrutura. Desta demanda, foi concebido o protocolo BGP em meados de 1989, o qual evoluiu e encontra-se em sua quarta versão (BGP-4).

Seus três cenários básicos de roteamento sustentam: (1) a comunicação entre roteadores internos por meio de vizinhanças iBGP; (2) o envio e o recebimento das tabelas de roteamento entre sistemas autônomos distintos, desde que estes possuam conexões eBGP estabelecidas; e, por fim, (3) o transporte de dados por organizações que não estejam diretamente relacionadas à origem ou ao destino dos pacotes IP, por intermédio dos sistemas autônomos de trânsito.

Para a operação do protocolo são necessárias apenas quatro mensagens, as quais são compartilhadas entre os BGP *peers*. Estas alicerçam os diferentes estados que uma sessão BGP pode se apresentar: *idle*, *connect*, *active*, *open sent*, *open confirm* e *established*. A troca dos prefixos de roteamento é realizada apenas na última etapa que, inicialmente, contempla a tabela completa. A seguir, apenas as alterações são compartilhadas entre os roteadores que estabeleceram a vizinhança. Justapostos aos prefixos, também são encaminhados diversos atributos que possibilitam a determinação da melhor rota para cada um dos destinos, não somente baseada no menor caminho, mas por meio de outros critérios que conferem ao administrador do sistema autônomo a flexibilidade necessária para criação de suas políticas de roteamento.

Links:

Artigo "BGP", escrito por Aaron's Wiki.
http://trouter.co.uk/wiki/index.php/BGP.

Artigo "BGP-4 Theory", escrito por Karl Solie e Leah Lynch.
http://www.informit.com/library/content.aspx?b=CCIE_Practical_Studies_II&seqNum=73.

Artigo "O Protocolo BGP4", escrito por Alex Soares de Moura.
http://www.rnp.br/newsgen/9903/bgp4.html.

Autor



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 e na Universidade Gama Filho. 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 treze anos na área de redes de computadores e tecnologia da informação, além de sete 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), ITIL v3 Release, Control and Validation (RCV) e ISO/IEC 20000 - IT Service Management.

Somos tão apaixonados por tecnologia que o nome da empresa

diz tudo.

Porta 80 é o melhor que a Internet pode oferecer para sua empresa.

Já completamos 8 anos e estamos a caminho dos 80, junto com nossos clientes.

Adoramos tecnologia.
Somos uma equipe composta de gente que entende e gosta do que faz,

assim como você.





Estrutura

100% NACIONAL. Servidores de primeira linha, links de alta capacidade.



Suporte diferenciado

Treinamos nossa equipe para fazer mais e melhor. Muito além do esperado.



Serviços

Oferecemos a tecnologia mais moderna, serviços diferenciados e antenados com as suas necessidades.



1-to-1

Conhecemos nossos clientes. Atendemos cada necessidade de forma única.
Conheça!

Porta 80
WEB HOSTING

Hospedagem | Cloud Computing | Dedicados | VoIP | Ecommerce | Aplicações | Streaming | Email corporativo

porta80.com.br | comercial@porta80.com.br | twitter.com/porta80

SP 4063-8616 | RJ 4063-5092 | MG 4063-8120 | DF 4063-7486