



Edição 07 :: Ano I



**ESPECIAL:**  
**As novidades do Windows Server 2012**  
Saiba o que esperar da nova versão

**SNMP**

Um estudo sobre o padrão  
de gerência para redes IP

**Segurança da Informação X Redes Sociais**

O ser humano é o elo mais  
fraco na corrente da segurança

**Introdução à Content Delivery Network**

O que é e que vantagens ela pode trazer para sua empresa



# SEGURANÇA em redes Wi-Fi

**Infraestrutura de Data Centers:** Conheça as características de infraestrutura dos DC's

# TENHA ACESSO ILIMITADO A TODO CONTEÚDO DO SITE DEVMEDIA

## SEJA UM ASSINANTE **MVP!**

Tenha acesso garantido a qualquer tema  
que você possa necessitar!



### VIDEOS - AULAS

O assinante MVP acessa todas as vídeo-aulas do site DevMedia. Nenhum outro produto dá essa possibilidade. São mais de **7.000 vídeo-aulas**.



### CURSOS

Nosso site possui atualmente **+ de 250 cursos online** com a qualidade que você já conhece e confia. Com o MVP você terá acesso a todos eles.



### REVISTAS

Assinante MVP acessa todas as nossas revistas na versão digital, incluindo todas as edições anteriores. Quando pintar aquela dúvida você terá mais de **3.500 artigos para consultar!**



A assinatura MVP te dá a oportunidade de aumentar seu conhecimento em diversos assuntos, com qualidade e economia.

**Invista na sua carreira se torne um profissional ainda mais completo!**



DevMedia

POR APENAS  
**R\$59,90** POR MÊS

Acesse: [www.devmedia.com.br/mvp](http://www.devmedia.com.br/mvp)

# Sumário

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



Segurança, Web

## 06 – Segurança da Informação X Redes Sociais

O ser humano é o elo mais fraco na corrente da segurança  
[ Érika Priscila Pereira Santana Santos ]

Redes

## 12 – Infraestrutura de Data Centers

Conheça as características de infraestrutura dos Data Centers  
[ André Koide da Silva ]

Segurança, Web

## 20 – Segurança em Redes IEEE 802.11

Podemos nos sentir seguros nas redes IEEE 802.11?  
[ Bruno Bogaz Zarpelão ]

Segurança

## 27 – Monitorando ativos de rede e serviços

Saiba como controlar sua infraestrutura de TI  
[ Thiago Nache ]

Sistema Operacional

## 32 – As novidades do Windows Server 2012

O que esperar da nova versão?  
[ Josué Vidal ]

Redes

## 39 – SNMP – Simple Network Management Protocol

O padrão de gerência para redes IP  
[ Bruno Bogaz Zarpelão ]

Redes

## 45 – Introdução à CDN – Content Delivery Network

O que é e que vantagens ela pode trazer para sua empresa  
[ Alex Felipelli ]

**[Redes]** Artigo que apresenta tecnologias relacionadas a criação e manutenção de redes.

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

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

## Edição

### Editor

Eduardo Spínola ([eduspínola@gmail.com](mailto:eduspínola@gmail.com))

### Sub Editores

Marco Antônio Pereira Araújo ([maraujo@devmedia.com.br](mailto:maraujo@devmedia.com.br))

Rodrigo Oliveira Spínola ([rodrigo.devmedia@gmail.com](mailto:rodrigo.devmedia@gmail.com))

## Produção

**Jornalista Responsável** Kaline Dolabella - JP24185

## Atendimento ao leitor

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

## Publicidade

[publicidade@devmedia.com.br](mailto:publicidade@devmedia.com.br) – 21 3382-5038

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

### Fale com o Editor!

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

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

Eduardo Spínola - Editor da Revista  
[eduspínola@gmail.com](mailto:eduspínola@gmail.com)

# Editorial

Você já percebeu que a quantidade de redes Wi-Fi que sua placa de rede wireless detecta só faz aumentar? Em busca, principalmente, da facilidade de acesso, famílias e empresas cada vez mais investem nas redes sem fio. Com certeza é muito mais fácil (e barato) instalar um dispositivo no canto de uma sala para fornecer acesso à rede, do que espalhar os tão conhecidos e tradicionais cabos de rede em todo um ambiente, o que é quase uma obra de engenharia. Apesar destas vantagens, não podemos nos esquecer da segurança. Estamos realmente seguros nas redes IEEE 802.11?

**Segurança em Redes IEEE 802.11** apresenta as principais questões relacionadas à segurança em redes IEEE 802.11. Primeiramente, serão apresentadas as redes IEEE 802.11 e os fatores que fazem delas inseguras. Então, serão apresentados o WEP e o WPA, que são arquiteturas de segurança desenvolvidas para as redes IEEE 802.11. Também serão apresentadas vulnerabilidades descobertas no WEP e no WPA1. Por fim, serão apresentadas outras ameaças à segurança das redes sem fio.

**Segurança da Informação X Redes Sociais** faz uma abordagem sobre a segurança da informação, os riscos corridos, o alvo de ataques, como implementar a segurança e mantê-la em pleno funcionamento, além de alertar sobre o impacto que o mau uso das redes sociais pode causar nas organizações.

**Infraestrutura de Data Centers** descreve os principais tipos de Data Centers e os serviços frequentemente oferecidos pelas empresas de telecomunicações que disponibilizam estas infraestruturas para seus clientes. Serão apresentadas as topologias e os padrões recomendados pela norma TIA-942 para o projeto de instalações com alta confiabilidade e disponibilidade. Também será exposta a classificação dos DC's conforme o nível de redundância previsto na concepção de seus elementos. Por fim, será abordada a relação entre estas infraestruturas e a computação em nuvem.

Na matéria **Monitorando ativos de rede e serviços**, abordaremos aspectos de monitoramento de ativos de redes utilizando as principais ferramentas open source. Perceberemos que estas ferramentas são ricas em recursos, possuindo diferentes abordagens que garantem o total controle da infraestrutura de redes.

**As novidades do Windows Server 2012** apresenta as novas funcionalidades e recursos do Windows Server 2012, bem como as melhorias introduzidas em relação ao Windows Server 2008 R2. Serão abordadas as diversas novidades do Hyper-V 3.0. Também veremos as novidades no Active Directory, BitLocker, DHCP, WSUS, BranchCache, DirectAccess.

O artigo **SNMP – Simple Network Management Protocol** retrata os principais conceitos relacionados ao padrão de gerência de redes IP, denominado SNMP. Primeiramente, serão apresentados aspectos básicos do modelo gerente-agente adotado pelo SNMP, das operações suportadas pelo SNMP e das MIBs, que são responsáveis por armazenar os dados gerenciais dos equipamentos. Em seguida, serão analisadas as três versões do SNMP.

Para encerrar, **Introdução à CDN – Content Delivery Network** destaca as principais características das CDNs – Content Delivery Networks. Será explicado como elas funcionam, assim como as vantagens técnicas e de negócios no uso desse tipo de rede. Também será apresentada uma comparação das CDNs tradicionais com Cloud Computing. Por fim, será analisado um estudo de caso da rede da Akamai e como ela funciona.

Eduardo Oliveira Spínola  
[eduspínola@gmail.com](mailto:eduspínola@gmail.com)  
[twitter.com/Java\\_Magazine](https://twitter.com/Java_Magazine)



# Seu conhecimento vale muito na DevMedia

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

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



Para saber mais acesse:  
[www.devmedia.com.br/paycontent](http://www.devmedia.com.br/paycontent)



# Segurança da Informação X Redes Sociais

## O ser humano é o elo mais fraco na corrente da segurança

A necessidade que o ser humano possui de expor informações sobre seu cotidiano vem desde sua existência e é perceptível desde as figuras gravadas nas paredes das cavernas a toda essa disseminação de informação graças às redes sociais.

Com as novas formas de comunicação, e armazenamento de dados lidados hoje no cotidiano, há uma necessidade de adaptação e discernimento sobre quais tipos de dados disponibilizar na rede.

Há pouco tempo atrás era bastante comum a utilização do papel para transcrever informações pessoais, públicas ou empresariais, sendo esses armazenados de formas adequadas para evitar perda das informações contidas nesses documentos. Agora com as novas possibilidades de armazenamento, existe uma grande demanda do setor corporativo em digitalizar seus documentos e realizar a importação desses para seus sistemas.

Vê-se que a utilização do papel para armazenamento de informações ainda é bastante comum em algumas situações, porém, cada vez mais essa prática vem sendo reduzida, dando lugar ao acesso de informações no ambiente virtual.

É devido às novas formas de armazenamento de dados e comunicação que se torna cada vez mais comum e imprescindível o interesse das empresas em investir na segurança da informação.

É natural que surjam vários questionamentos quando o assunto é segurança da informação e, principalmente por tratar-se de uma área desafiadora, que segundo Nakamura e Geus (2010, p. 52) “uma solução de segurança é imensurável e não resulta em melhorias nas quais todos podem notar que alguma coisa foi feita. Pelo contrário, a segurança tem justamente o papel de evitar que alguém perceba que alguma coisa está errada. O fato é que ninguém percebe a existência da segurança, apenas a inexistência dela, quando um incidente acontece e resulta em prejuízos gigantescos”.

A prática da segurança visa mitigar vulnerabilidades que algo ou alguém estejam sujeitas, com o intuito de

### Resumo DevMan

#### *De que se trata o artigo:*

Compreender os riscos que as informações correm, como evitar perdas, manter o ambiente protegido, saber o quanto investir mesmo assumindo os riscos que norteiam a segurança da informação e olhar a divulgação de informações via redes sociais observando os pontos positivos e negativos são fundamentais para uma maior efetivação da proteção de conteúdo.

#### *Em que situação o tema é útil:*

Indicado para estudantes, professores, profissionais da área de tecnologia da informação, e até mesmo empresários que desejam ampliar seus conhecimentos e que queiram obter mais informações a cerca da segurança da informação e os impactos que o mau uso das redes sociais pode gerar.

#### *Segurança da Informação X Redes Sociais:*

Este artigo faz uma abordagem sobre a segurança da informação, os riscos corridos, o alvo de ataques, como implementar a segurança e mantê-la em pleno funcionamento, além de alertar sobre o impacto que o mau uso das redes sociais pode causar nas organizações.

proteger o mesmo, e para que isso aconteça, é interessante e recomendado que os procedimentos tomados para reduzir os riscos não sejam ditos ou divulgados.

A exposição do procedimento de segurança reduz a eficiência da operação, uma vez que o inimigo possuirá mais recursos para planejar melhor sua ação.

Sabe-se que há várias medidas de segurança que são visíveis pelo indivíduo, como é o caso da instalação de câmeras, sensores, chips, senhas, entre inúmeros outros procedimentos que são usados com a finalidade de proteção, seja de um ambiente, das pessoas ou da informação.

Porém, ainda com a utilização desses recursos, não há uma garantia de segurança, justamente porque as câmeras podem não estar sendo monitoradas e os sensores podem não estar postos em locais estratégicos como deveriam, entre tantas e tantas situações

como a própria falta de energia que podem tornar o investimento em segurança um grande fracasso.

Devido a todas essas circunstâncias é que se pode dizer que a segurança não se vê, uma vez que o visível não é a garantia de segurança, mas é possível senti-la devido a vários procedimentos os quais um indivíduo é submetido em prol da segurança, ou pelo histórico de um ambiente ou empresa. Deve-se ter o cuidado para que não seja uma falsa sensação de segurança, o que é mais arriscado que a total ausência dela.

Primeiro é interessante compreender o que o termo “segurança” está associado, o que corresponde às medidas tomadas para evitar prejuízos de um modo geral.

Já a “segurança da informação” aborda o assunto com um foco mais específico. Sendo assim, trata-se de um conjunto de precauções que tem o objetivo de proteger as informações, estejam elas armazenadas em servidores, trafegadas na rede, comentada dentro ou fora da organização ou de uma residência, dos comentários realizados nas redes sociais, contidas nos papéis que são dispensados no lixo, da conversa no fim de semana com os amigos, da ligação telefônica que fizeram erroneamente, entre outras situações possíveis em que a informação pode ser obtida ou transmitida.

### Analizando os riscos corridos pelas informações

Vários são os riscos que as informações correm a todo instante. A quantidade de ameaças continua crescendo exponencialmente e os sistemas de proteção seguem implementando novas vacinas, porém as vacinas não conseguem mais acompanhar o ritmo de crescimento das ameaças, o que incide na necessidade de fazer uso também de outros métodos de proteção e que serão abordados mais adiante. Por hora, são listadas algumas das várias ameaças que norteiam as informações:

- Acesso indevido à rede ou ambiente, abrindo um leque de vulnerabilidades que podem ser utilizadas para o ataque;
- Alteração e manipulação dos dados afetando a integridade desses;
- Perda ou roubo de equipamentos onde está armazenado algum tipo de informação;
- Perda de conexão com os provedores de serviços da rede, como a cloud, VPN ou servidor local;
- Perdas decorrentes de eventos envolvendo fenômenos da natureza, ou da probabilidade de ataque terrorista em algumas regiões do mundo decorrente de questões políticas ou religiosas;
- Disponibilização de informações via redes sociais sem o mínimo de cuidado com as consequências dos comentários e da forma como eles podem ser utilizados;
- Os riscos da engenharia social que busca obter informações de forma bem planejada e inteligente através de uma boa conversa convincente onde o indivíduo que está sendo atacado na maioria das vezes não percebe o perigo no diálogo, e acaba respondendo às questões levantadas seja por autoconfiança, vaidade ou simplesmente pela possibilidade de novas amizades;
- Intercepção de comunicações de dados, voz ou vídeo.

Entre os diversos tipos de ataques e infiltrações possíveis em uma rede de computadores, é interessante observar que as informações correm riscos físicos e virtuais que podem ocorrer intencionalmente ou não intencionalmente:

- **Físico:** é quando um espião (indivíduo mal intencionado) pode obter informações tendo acesso indevido a um ambiente onde até mesmo as informações postas em quadros de avisos e orientações de procedimentos podem ser utilizadas de forma contrária. Ainda há a possibilidade de roubo de equipamento, obtenção de informações via dispositivos móveis e falhas de comunicação por problemas relacionados a nível físico, o que pode ser um evento ou intencional, ou ainda a obtenção de informação por meio de um bom papo via engenharia social;
- **Virtual:** equivale à intercepção de comunicação de voz, vídeo e dados pela rede.

### Tornando as informações mais seguras

É preciso fazer uma verificação da rede para saber quais métodos de segurança são mais adequados para o ambiente. Isso porque quanto mais valioso o conteúdo com que se está trabalhando, mais investimento pode ser necessário. O mesmo vale para o contrário. Aqui são apresentadas opções de implementação da proteção da informação:

- Configuração de *firewall*;
- Configuração de DMZ, ou *DeMilitarized Zone*, procedimento usado para proteger a rede interna dos acessos externos. Sendo assim, caso um servidor que esteja em uma DMZ seja atacado, isso em nada afetará a rede interna. Para tanto é necessário que a implementação seja realizada alinhada com as políticas de segurança, além de bem planejada;
- Configuração de antivírus;
- Fazer uso de chaves criptográficas;
- Definir normas de segurança;
- Realizar a autenticação quando for utilizar qualquer serviço da rede;
- Fazer o monitoramento da rede, corrigindo os problemas apresentados de forma imediata e ficando atento a qualquer anormalidade;
- Lidar com a segurança em camadas, o que dificulta o ataque de *crackers*;
- Aplicação de campanhas de conscientização dos usuários, as quais podem alertar sobre a importância da alteração das senhas a cada no máximo 90 dias, incentivar a não reutilização da mesma senha para outros acessos e ainda abordar a composição da senha, onde é recomendado que possua letras, números e caracteres especiais. Esses são pequenos exemplos de orientações que podem fazer parte da campanha;
- Aliar a segurança da informação e patrimonial evita o acesso físico indevido e roubo de equipamentos, o que é uma consequência de falha no setor de segurança patrimonial. A integração desses dois segmentos oferece uma maior satisfação, eficiência e eficácia dos procedimentos de segurança.

## Realizando a manutenção da segurança após as ações de proteção

A área da segurança da informação, ao mesmo tempo em que retrata uma zona de conforto, também deve ser associada a um estado de alerta constante, para que não venha a existir a falsa sensação de segurança, como já abordado anteriormente.

Então, para que a manutenção desse serviço seja efetiva, é importante que constantemente sejam tomadas algumas providências, a saber:

- Sempre fazer testes na rede com o intuito de identificar as possíveis vulnerabilidades que nela possam vir a existir de forma que não venham a impactar no desempenho e funcionamento da rede, realizando as correções necessárias. Isso porque o universo da segurança é muito dinâmico, onde sempre surgem novos métodos de ataque e novas vulnerabilidades;
- Sempre que possível reforçar as boas práticas de segurança com os usuários, lembrando que o ser humano é o elo mais fraco nessa corrente de métodos relacionados à segurança;
- Aplicar as vacinas do antivírus;
- Manter os sistemas atualizados;
- Continuar realizando o monitoramento da rede;
- Permanecer atento às novas formas de intrusão, a fim de trabalhar na defesa do ambiente.

## Alvo dos ataques

Os objetivos são vários para o ataque feito por *crackers*. Esse é o termo genericamente usado para identificar os realizadores de ataques às informações, porém conforme as ações do atacante, esse termo pode variar bastante. Segue os possíveis termos que podem ser usados para casos específicos:

- **Script kiddies** – atacantes iniciantes que possuem pouco conhecimento sobre as ferramentas de ataques e suas consequências às organizações;
- **Cyberpunks** – atacantes mais velhos e antissociais. Eles são motivados muitas vezes pelo desafio e diversão, mas em geral são grandes conhecedores de segurança e obcecados por ela;
- **Insiders** – colaboradores insatisfeitos com a empresa. Esse tipo de atacante é um dos mais comuns;
- **Coders** – exibicionistas que comentam suas conquistas como atacante. Em geral gostam de compartilhar seus conhecimentos;
- **White hat** – profissionais contratados, também conhecidos como “hackers do bem” e “éticos”. Buscam vulnerabilidades e as corrigem, evitando que seja explorada por atacantes;
- **Black hat** – também chamados de *crackers* ou ainda de “hackers do mal”. Esses utilizam os seus conhecimentos para roubar informações, manipular dados, vender informações e estão sempre em busca de obter um retorno financeiro com suas ações;
- **Gray hat** – corresponde a um *Black hat* que trabalha como um *White hat*. Na verdade um perigo para a empresa, uma vez que esse pode tranquilamente se aproveitar da sua função para obter informações sigilosas e fazer delas o que achar conveniente.

Há várias motivações para que um atacante escolha um alvo e inicie seus procedimentos de invasão a um sistema de comunicação. A seguir são listadas as situações mais comuns:

- Conseguir informações com a intenção de roubar, modificar ou usufruir das informações para obtenção de lucro;
- Ataque de negação de serviço, também conhecido como *Denial-of-Service Attack* – DoS, trata-se de técnicas invasivas que exploram o sistema por meio de uma enxurrada de solicitações de serviços causando o estouro da memória do hardware em questão. Consequentemente o serviço prestado por esse dispositivo ficará paralisado, impedindo que os usuários do mesmo possam utilizá-lo. Esse tipo de invasão pode levar muitas empresas e sistemas ao descrédito;
- Invasões motivadas pelo ego e exibicionismo, onde o desafio impulsiona a prática e, geralmente, a intenção é simplesmente a exposição das habilidades ao mundo *cracker*.

Nas redes sociais, há algumas vulnerabilidades mais específicas, como:

- Divulgação de *links* falsos, maliciosos, que podem ser clicados caso não se tenha atenção ou não conhecimento sobre o assunto. Esses *links* podem causar danos bastante diversificados;
- Perfis falsos, onde se podem disponibilizar informações relevantes para pessoas não autorizadas.

## Retorno de investimento em segurança da informação

Devido ao pequeno orçamento disponível para o setor de TIC que muitas empresas dispõem para atender a todas as necessidades relacionados aos seus serviços prestados, é que acaba dificultando o investimento em segurança da informação.

Uma maneira interessante de propor um maior investimento nessa área seria fazer uma breve comparação entre o valor a ser investido contra os prejuízos que a ausência da segurança pode causar.

Para poder fazer a comparação proposta, primeiramente é importante mensurar o valor das informações que se quer proteger, para saber quanto se pode investir. É necessário ter em mente de que não é viável investir mais do que o valor que as informações representam.

O valor das informações é difícil de ser obtido, justamente porque nesse processo de avaliação faz-se uma abordagem baseada em incertezas e dúvidas, e que envolve os recursos tangíveis e intangíveis, onde o resultado não é preciso, apenas estimado:

- **Recursos tangíveis:** corresponde a horas de trabalho, equipamentos e softwares necessários para a recuperação dos dados;
- **Recursos intangíveis:** faz referência ao valor do conhecimento, quebra de sigilo e a imagem da organização.

## Segurança e a produtividade

As questões relacionadas às restrições de acesso aos serviços da rede e recursos de hardware e dispositivos em geral deve possuir certo equilíbrio para não vir a comprometer o desempenho das atividades dos usuários.

O aconselhável é que seja levado em consideração as atividades desempenhadas por cada usuário e o departamento em que trabalha, de forma que sejam disponibilizados apenas os serviços dos quais necessita para a realização de suas funções.

É importante que haja bons procedimentos e cuidado na implementação das restrições de acesso. Isso porque os equipamentos e softwares existem na organização para que possam ser utilizados para facilitar as atividades dos usuários em suas funções, porém se os bloqueios forem excessivos podem afetar e, até mesmo, irritar os usuários por não conseguirem realizar seu trabalho a contento.

### **Não subestime o poder das redes sociais**

A disponibilização de informações via redes sociais pode funcionar como aliado ou como um inimigo de uma organização. Portanto, o cuidado com os dados que estão sendo disponibilizados nas redes vai desde o que pode estar sendo exposto na rede social da empresa, ao conteúdo disponibilizado pelos colaboradores, sócios, investidores e clientes.

É muito complexo, ou até mesmo cansativo e desafiador, controlar todos esses meios de comunicações e administrar todas as informações disponibilizadas nas redes. Quando se faz referência ao conteúdo disponibilizado pela organização, sócios e colaboradores, há uma possibilidade maior de orientação e acompanhamento do que se é publicado.

A boa orientação sobre qual tipo de informação é inofensiva ou perigosa pode variar conforme o segmento da empresa ou cargo ocupado pelo colaborador. Os comentários negativos a uma empresa realizados por um funcionário ou cliente podem afetar a reputação da empresa, além de fornecer um conteúdo valioso para concorrentes, hackers e reduzir a porcentagem de vendas de produtos e serviços oferecidos pela organização em questão.

As informações são disseminadas rapidamente na Internet e disponíveis a qualquer um que fizer consultas sobre os produtos e serviços da empresa. Da mesma forma como os consumidores buscam informações sobre a qualidade, fazem reclamações relativas à empresa por meio da internet, fazendo imprescindível um retorno da organização a essas questões levantadas na rede, de forma que venha a ter respostas positivas, o que reflete em maior confiança na marca.

O poder que as redes sociais representam na atualidade é bastante relevante. Em decorrência desse fato é que as organizações as veem como um grande obstáculo a ser enfrentado, uma vez que um cliente possivelmente dará mais crédito a um comentário realizado por um amigo que por um desconhecido.

### **Criação de regras e estratégias específicas para utilização das redes sociais**

A resistência para que empresas entrem no mundo das redes sociais é bem mais comum do que se possa imaginar. Essa é uma questão de cultura e que está sendo mudada gradativamente com o passar no tempo.

O fato de uma empresa não ter aderido às mídias sociais para se comunicar com seus clientes é bastante relativo ao seu

segmento, à visão que possui, aonde ela quer chegar, entre outras variáveis.

Uma vez que há outras formas de comunicação com o cliente, fica difícil dizer que quem está fora das redes sociais não terá um futuro bem definido e promissor.

Mas uma coisa é certa: se abraçou as redes sociais, é necessário lhe dar uma atenção especial para que a empresa não venha a se tornar vulnerável nesse campo cada vez mais diversificado e poderoso, onde os passos falsos podem comprometer a reputação e o futuro da organização com muita facilidade.

Primeiro vamos às regras. Se há um profissional responsável por monitorar a rede social da empresa, esse precisa se concentrar em suas atividades e ser bastante consciente de suas ações e as consequências delas.

As regras devem ser publicadas e conhecidas por todos que compõem a empresa. O mais indicado nesse caso é a realização de uma campanha de conscientização com os funcionários para orientá-los nesse processo.

Algumas regras bastante comuns aos profissionais das mídias sociais são:

- Definir um tempo máximo aceitável para responder a um diálogo de um cliente;
- Ser cauteloso no momento de publicar qualquer que seja a informação;



**Não perca tempo reinventando a roda!**

**COBREBEMX**

**Componente completo para sua Cobrança por Boleto Bancário e Débito em Conta Corrente**

**Mais de 40 exemplos em diversas linguagens de programação**

**Geração e leitura de arquivos (remessa e retorno) nos padrões FEBRABAN e CNAB**

**Testes e Downloads gratuitos em nosso site**

**ACESSE E CONHEÇA O COMPONENTE EM:**  
**WWW.COBREBEM.COM**

- Estar atento à veracidade das informações;
- As informações publicadas devem ter sempre uma relação ao segmento da empresa;
- Demonstrar simpatia e atenção principalmente nos casos de atendimento ao cliente;
- Caso cometa algum erro, é imprescindível que o assuma e faça o que for possível para corrigi-lo da forma mais breve possível.

Nas poucas regras listadas já dá para perceber que, se pelo menos algumas delas forem seguidas, a empresa estará mais imune às vulnerabilidades de sua reputação.

As estratégias envolvem muito a interação entre o profissional responsável pelas redes sociais e o marketing, que definiram o que será publicado, quando, porque, qual o público alvo e como gerenciar a resposta do público.

## Monitorando as redes sociais

Há uma grande disponibilidade de ferramentas de monitoramento das redes sociais, as quais podem ser gratuitas ou não, mas em geral, as ferramentas gratuitas, ou as versões gratuitas, não dão suporte a muitas redes sociais ao mesmo tempo, ou seja, não são tão completas.

Para as empresas que não querem gastar com software de monitoramento, a opção gratuita é sim uma boa recomendação, porém, tendo em vista que essa alternativa não abrange muitas redes sociais em uma mesma plataforma, é indicado que esta trabalhe articulando entre várias ferramentas, onde cada uma terá um papel importante na missão de verificar seu *status* na rede.

As ferramentas pagas, por outro lado, costumam oferecer serviços de monitoramento entre várias redes sociais, criação de relatórios, gráficos estatísticos e são mais confiáveis.

A seguir, serão apresentados alguns dos vários softwares de monitoramento com breves comentários a seu respeito. Para começar, listaremos as ferramentas gratuitas:

- **TweetLevel:** Essa ferramenta mede a influência de um perfil do Twitter na rede. Para isso, faz uma associação da quantidade de contatos e a interação que o usuário possui com eles, seja *retweetando*, respondendo e a frequência com que realiza suas postagens, além de verificar o alcance das publicações realizadas.

Para fazer a busca, basta informar o ID do Twitter que se deseja consultar e, caso queira, pode especificar a localidade e *tags* relacionadas ao perfil em questão. Feito isso, é só aguardar o resultado da análise, que pode ser visualizado via gráficos. O TweetLevel é uma ferramenta gratuita e pode ser acessada via <http://tweetlevel.edelman.com>;

- **Klout:** É um serviço gratuito que possibilita o monitoramento de várias redes sociais. Ele faz uma análise da repercussão das publicações realizadas e quais pessoas são influenciadas por elas.

O grau de influência é medido de 0 a 100 entre os seguidores, se utilizando de várias métricas para chegar a esse resultado e exibindo-os por intermédio de gráficos. Para utilizar seus recursos, basta acessar <http://klout.com> e logar pelo Twitter ou Facebook,

podendo ainda monitorar o Google+, LinkedIn, Instagram, entre outros;

- **PeerIndex:** Possui características bem parecidas com o Klout, visto anteriormente, sendo que de uma forma mais enxuta e objetiva. O PeerIndex não suporta muitas redes sociais. O resultado da análise é fundamentado em três componentes bem definidos: autoridade, audiência e atividade.

O nível de influência é medido de 0 a 10, é uma ferramenta gratuita e, para conhecê-la, basta acessar <http://www.peerindex.com/>;

- **Whos Talkin:** Essa ferramenta faz uma análise sobre o assunto de interesse do usuário, retornando uma lista de opiniões ou diálogos em torno do assunto pesquisado, podendo ainda ser filtrado por tipo de mídia social. Para conhecer o Whos Talkin, acesse <http://www.whostalkin.com>;

- **socialmention\*:** Possibilita a realização de filtros por palavras-chave ou frases, onde o usuário pode escolher qual tipo de busca deseja realizar, que pode ser por vídeos, imagens, blogs, microblogs, entre outras opções, ou ainda todas as opções de busca disponíveis ao mesmo tempo, e tudo em tempo real.

Após a filtragem dos dados, é possível verificar as postagens, opiniões e seus respectivos autores, além de obter dados sobre quando a informação foi publicada. Ainda é possível ativar alertas que são encaminhados por e-mail caso alguma notificação adicional venha a ser registrada.

Como resultado dos filtros, tem-se também as porcentagens da pesquisa realizada, o que corresponde a uma comparação entre os comentários positivos e negativos postados na web.

Socialmention\* trata-se de uma ferramenta gratuita e que pode ser acessada via <http://www.socialmention.com>;

- **Likester Affinities:** É um aplicativo que analisa apenas o Facebook, é gratuito e lista os contatos seguidos dos *links* curtidos por eles. Por meio dessas informações é possível saber quais os interesses dos contatos e sugerir *links* que podem ser de gosto comum entre o usuário e seus contatos.

Para conhecer e testar as funcionalidades do Likester deve-se acessar <http://www.likester.com> e fazer *login* no Facebook;

- **Topsy:** Também faz o monitoramento em tempo real, podendo aplicar filtros por imagens e vídeos, entre outras opções. A busca pode seguir a ordem de publicação, ou ainda por informações mais relevantes. Além disso, é possível verificar quem, quais e quantas publicações foram feitas em torno da palavra ou frase pesquisada, e ainda obter informações sobre essas pessoas, se elas são influentes ou não.

O Topsy realiza o monitoramento apenas do Twitter e do Google Plus, mas o interessante é que, por meio dele, é possível responder a um comentário e *retweetar*, entre outras opções. Ademais, a consulta pode ser por idiomas diferentes ou realizar uma busca por todos os idiomas e ainda visualizar *hashtags* relacionadas.

Assim como as ferramentas citadas até o momento, Topsy também é uma ferramenta gratuita e, para acessá-la, basta informar o endereço <http://topsy.com> no browser.

A partir de agora serão abordadas as ferramentas pagas e suas características principais. Algumas delas permitem testar sua versão *free* ao acessar o site, já outras apenas entrando em contato com a empresa prestadora do serviço para que se possa fazer uma análise da mesma. Vamos à análise:

- **Seekr:** É um software que, assim como os listados anteriormente, faz a verificação da saúde da empresa nas redes. Um das suas principais características é a grande disponibilidade de criação de filtros entre várias redes sociais, de forma personalizada.

Além disso, destacam-se a criação de *blogs* que armazenam o histórico dos resultados das campanhas, discussões e desempenhos relacionados, relatórios avançados dos resultados obtidos, e o monitoramento da interação entre a marca e o cliente por meio da própria ferramenta – tudo em tempo real.

Para dispor dos recursos do Seekr basta acessar [www.seekr.com.br](http://www.seekr.com.br). É possível realizar um *Trial Free* fazendo um breve cadastro e, caso queira contratar seus serviços, a empresa dispõe de vários planos de forma que se adeque às necessidades do contratante;

- **SismoWeb:** Esse sistema possui, além das opções tradicionais da categoria, um serviço de alerta via SMS e e-mail. Outra opção interessante é a disponibilidade de relatórios analíticos que avaliam a presença da marca na rede.

Para conhecer melhor esse software é necessário se cadastrar e solicitar uma apresentação do mesmo. Mais informações podem ser obtidas em [www.sismoweb.com.br](http://www.sismoweb.com.br);

- **PostX:** Faz a verificação do status da marca na rede por meio de palavras-chave, checa o *ranking* de influenciadores, contabiliza os *retweets*, possibilita a interação com o cliente, dispara alarmes de emergência, entre outras funcionalidades como relatórios, análise do humor com que um comentário foi divulgado e outras avaliações mais específicas.

Como diferencial, há o serviço de cruzamento das informações sobre a marca e produtos concorrentes, possibilita conhecer tendências do mercado, identificar vulnerabilidades que os comentários sujeitam a marca da empresa e identificam influenciadores das redes sociais. Esse último pode tanto contribuir como também levar muitas pessoas a descreditarem em um serviço ou produto pela influência de seus comentários. Com base nas informações obtidas, pode realizar um planejamento consolidado e contar com uma equipe de analistas do PostX para que avaliem e categorizem o conteúdo capturado, vislumbrando emitir alertas de urgência em tempo real, a fim de informar a empresa caso alguma notícia não conveniente seja publicada para que essa tome as medidas cabíveis à situação. Os planos de contratação são bem diversificados, de forma que venham a atender melhor o perfil da empresa. Essa e outras informações podem ser obtidas via [www.postx.com.br](http://www.postx.com.br).

Aqui foram listados apenas alguns dos inúmeros sistemas de monitoramento de redes sociais. Ao realizar uma breve comparação é possível notar que os serviços pagos são realmente mais completos e detalhistas, mas no geral todos contribuem bastante para saber como anda a saúde da marca na rede.

O software mais adequado pode variar de empresa para empresa conforme suas necessidades e possibilidades de investimento. Uma boa dica é analisar com calma o que cada uma das opções tem a oferecer e qual delas pode realmente atender às expectativas.

## Conclusão

Como vimos, a segurança da informação envolve questões físicas e virtuais, sendo recomendada uma ação combinada entre o setor de segurança da informação e patrimonial para obter uma maior proteção dos dados.

Não se deve esquecer que o ser humano é o elo mais fraco nessa corrente de segurança, podendo ser manipulado e não corresponder às boas medidas de proteção sugeridas pela organização. Uma campanha de conscientização é fundamental para que se tenha bom retorno nas atitudes dos colaboradores.

O uso das redes sociais de forma indevida pode resultar em impactos de nível igual ou superior à falta de implementação da segurança de informação, porque a propagação do problema é muito mais rápida que em outras situações.

A segurança é uma área bastante desafiadora, requer bastante esforço, atenção e investimento. Os procedimentos de segurança não são muito perceptíveis quando executados. Em contrapartida, a ausência destes é bastante notável aos usuários envolvidos, provocando a sensação de insegurança no ambiente.

Não é de uma hora para a outra que a cultura das empresas irá mudar dando mais atenção a esse segmento, mas a análise dos orçamentos, levando em consideração os prejuízos que a organização pode ter com a ausência de segurança, é uma boa estratégia para ajudar a conscientizar as empresas da necessidade de se investir na segurança da informação.



**Érika Priscila Pereira Santana Santos**

[priscila.erika@gmail.com](mailto:priscila.erika@gmail.com)

Pós graduanda em Gerenciamento de Redes de Computadores, Complementação em Docência no Ensino Superior e Bacharel em Sistemas de Informação, experiência com suporte a help-desk, políticas de segurança, criação de procedimentos, documentação e controle de custos da área de TIC. Professora do curso Técnico em Redes de Computadores na ETENERB.



# Infraestrutura de Data Centers

## As características de infraestrutura dos Data Centers podem variar conforme a disponibilidade demandada pelas aplicações e sistemas

Os Data Centers são estruturas complexas que abrigam as aplicações e os sistemas de informação de uma empresa. Idealmente, suas instalações devem contemplar os componentes redundantes e sobressalentes necessários para eliminar os pontos de falha e aumentar seu nível de disponibilidade e confiabilidade. Diversos fatores têm impulsionado o surgimento de novos Data Centers, entre eles: o célere aumento das transações comerciais na Internet (comércio eletrônico), o avanço do processamento comercial de alto desempenho através da computação em nuvem e o crescimento dos provedores de software como serviço (SaaS – Software as a Service).

Atualmente, muitas das aplicações Web estão hospedadas em DCs: os sistemas de troca de mensagens instantâneas, as redes sociais, as aplicações de comércio eletrônico e os buscadores de conteúdo. Cada vez mais, os aparelhos domésticos (televisores, telefones, tablets, videogames, entre outros) acessam dados disponibilizados em um Data Center. Diferentes segmentos da atividade humana igualmente estão controlados por servidores instalados em Data Centers pulverizados em várias localidades, tais como: energia, iluminação, telecomunicações, tráfego urbano, instituições financeiras, sistemas de saúde, serviços de entretenimento e meios de transporte público e privado.

Estes oferecem aos seus usuários diversas vantagens, entre elas: a redução dos investimentos em recursos humanos e materiais, serviços de tecnologia da informação aderentes às necessidades do negócio, economias de escala em serviços de telecomunicações e redes de computadores, além da flexibilidade e rapidez na implantação e disponibilização de novos sistemas de informação.

Neste artigo, serão expostas as definições habitualmente encontradas para os Data Centers, bem como as

### Resumo DevMan

#### *De que se trata o artigo:*

Neste artigo serão descritos os principais tipos de Data Centers e os serviços frequentemente oferecidos pelas empresas de telecomunicações que disponibilizam estas infraestruturas para seus clientes. Serão apresentadas as topologias e os padrões recomendados pela norma TIA-942 (Telecommunications Infrastructure Standard for Data Centers) para o projeto de instalações com alta confiabilidade e disponibilidade. Também será exposta a classificação dos Data Centers conforme o nível de redundância previsto na concepção de seus elementos. Por fim, será abordada a relação entre estas infraestruturas e a computação em nuvem.

#### *Em que situação o tema é útil:*

Os tópicos abordados serão fundamentais para a compreensão dos principais componentes e dos aspectos de redundância que devem ser observados na avaliação da infraestrutura de um prestador de serviços de telecomunicações que disponibiliza Data Centers. Estes são essenciais para os profissionais que necessitam determinar qual tipo de instalação atenderá às características particulares das aplicações e sistemas de informação de sua empresa, sobretudo ponderando os requisitos de confiabilidade e disponibilidade.

#### *Infraestrutura de Data Centers:*

Os Data Centers são instalações que abrigam as salas de computadores e suas áreas de suporte. Disponibilizam a infraestrutura de condicionamento de ar, de sistemas elétricos, de telecomunicações, de combate e prevenção de incêndio, e de segurança física e lógica para os equipamentos e sistemas de tecnologia da informação 24 horas por dia, 7 dias na semana e 365 dias por ano. Os Internet Data Centers, mantidos por prestadores de serviços de telecomunicações, oferecem diversos tipos de serviços agrupados em duas principais classes: Colocation e Hosting. Dependendo das características e necessidades do modelo de negócios de cada empresa, infraestruturas distintas podem ser utilizadas. Com a finalidade de auxiliar nesta escolha, os Data Centers são classificados em quatro níveis, com diferentes especificações e interrupções anuais permitidas aos serviços ofertados.

diferenças entre as instalações mantidas por empresas privadas ou agências governamentais, e aquelas ofertadas por prestadores de serviços de telecomunicações. Serão contextualizados os serviços oferecidos pelos Internet Data Centers agrupados como Colocation e Hosting. Também serão abordadas as topologias e os padrões recomendados pela norma TIA-942, enfocando os principais componentes e seus aspectos de redundância para o dimensionamento de Data Centers com estruturas típicas, reduzidas e distribuídas. Será descrita a classificação comumente empregada nestas instalações, destacando as características consideradas em sua concepção, em termos da arquitetura, sistemas de telecomunicações, elétricos e mecânicos. Por fim, serão apresentadas as infraestruturas que são utilizadas pelos sistemas de computação em nuvem.

### O que são os Data Centers?

Atualmente, existem diversas definições empregadas para descrever um Data Center. Alguns autores afirmam que é uma estrutura utilizada para armazenar todos os sistemas de informação (SI) de uma empresa. Outros contextualizam como uma infraestrutura com alta disponibilidade para os equipamentos e sistemas de tecnologia da informação (TI), a qual assegura seu funcionamento 24 horas por dia, 7 dias na semana e 365 dias por ano. Já a especificação TIA-942, Telecommunications Infrastructure Standard for Data Centers, os delinea como construções ou partes de um edifício cuja função primária é abrigar salas de computadores e suas áreas de suporte.

Os Data Centers podem ser categorizados em dois grupos: Private Data Center (PDC) e Internet Data Center (IDC). Um PDC é mantido por empresas privadas, instituições ou agências governamentais com o objetivo de armazenar os dados processados internamente e as aplicações que servem seus usuários na Internet. Já um IDC geralmente pertence aos provedores de telecomunicações, às operadoras comerciais das redes de telefonia ou a outros tipos de prestadores de serviços de telecomunicações. Segundo Pravin Ganore, em seu artigo How To Build Data Centers, habitualmente esta categoria de DC tem como propósito oferecer diversos tipos de serviços agrupados em duas principais classes: Colocation e Hosting.

Na modalidade de Colocation, os usuários contratam somente o espaço físico onde seus servidores e dispositivos de redes serão instalados. O IDC pode também oferecer racks (gabinetes projetados e padronizados para a montagem modular dos equipamentos), além do fornecimento da infraestrutura de climatização, energia elétrica, telecomunicações, sistemas de combate e prevenção de incêndio, e segurança física e lógica. Opcionalmente podem ser ofertados outros serviços, tais como:

- Monitoração e notificação proativa de eventos relacionados à rede de comunicação de voz e dados;
- Sistemas para resolução de nomes (Domain Name System – DNS), responsáveis pela tradução de nomes, como [www.devmedia.com.br](http://www.devmedia.com.br) para o endereço IP (Internet Protocol) empregado na identificação do servidor onde a página Web está hospedada;
- Suporte técnico de especialistas nas diversas áreas de TI;

- Operadores para realização de tarefas locais, como inserção de mídias removíveis (por exemplo, CDs e DVDs) e reinicialização de servidores, roteadores, switches, firewalls e balanceadores de carga.

Entre as principais vantagens do Colocation, destacam-se: a redução de investimentos na infraestrutura, a economia de escala na compra de serviços de telecomunicações e operações de TI, a agilidade na implantação e disponibilização de novas aplicações de SI, e o suporte de profissionais e consultores altamente especializados e experientes.

Já no serviço de Hosting, toda infraestrutura de hardware e software do IDC é disponibilizada aos usuários que não desejam especializar-se na operação da tecnologia de informação. Assim, é possível escolher os servidores, sistemas operacionais, sistemas de banco de dados e softwares aplicativos conforme as necessidades e características de cada negócio. Diversos serviços com alto valor agregado são ofertados aos clientes, entre eles:

- Planejamento de capacidade e expansão para servidores e dispositivos de rede;
- Sistemas de detecção de intrusos (Intrusion Detection System – IDS) que visam monitorar os acessos não autorizados em uma rede de computadores, os quais podem indicar a ação de um cracker ou funcionários mal intencionados;
- Monitoração e notificação proativa de eventos relacionados à comunicação de dados;
- Controle e disponibilização de novas faixas de endereçamento IP para atribuição aos dispositivos conectados à Internet;
- Relatórios detalhados sobre a utilização e a capacidade total do hardware e do software de servidores, roteadores, switches, firewalls e balanceadores de carga;
- Servidores para relay de mensagens de correio eletrônico (serviço no qual as correspondências são encaminhadas para um servidor intermediário responsável por entregá-las aos destinatários finais);
- Sistemas para resolução de nomes (DNS);
- Suporte técnico de especialistas em TI, 24 horas por dia, 7 dias na semana e 365 dias por ano;
- Ponto único de contato (Service Desk), o qual possibilita o registro e o acompanhamento dos pedidos de suporte e manutenção;
- Operadores para realização de tarefas locais e reinicialização de servidores, roteadores, switches, firewalls e balanceadores de carga;
- Aplicação das correções de segurança (patches) disponibilizadas para os sistemas operacionais;
- Manutenção, substituição e atualização do hardware dos servidores;
- Backup total ou incremental dos dados e dos aplicativos;
- Infraestrutura completa para o armazenamento de grandes volumes de dados, por intermédio de SANs (Storage Area Networks);
- Expansão sazonal da capacidade de escoamento do tráfego para Internet, através da contratação de Gigabytes adicionais.

São os principais benefícios da contratação do Hosting: redução do investimento em ativos fixos e em pessoal técnico especializado em TI, serviços de TI aderentes às necessidades do negócio, atualização constante do software e hardware utilizados, know-how de consultores em TI, agilidade na implantação e disponibilização de novas aplicações de SI, e segurança física e lógica com altos padrões de desempenho e disponibilidade.

## Topologias e padrões para os Data Centers

Segundo José Maurício S. Pinheiro, em seu artigo Ambiente de Data Center, um Data Center robusto é aquele projetado segundo padrões que estabelecem os requisitos que asseguram disponibilidade e confiabilidade. Um DC também deve suportar as tecnologias existentes e os avanços tecnológicos em processamento de dados, telecomunicações e armazenamento. Portanto, a construção de um Data Center depende da integração completa entre diversas áreas e sistemas, entre elas:

- Arquitetura;
- Climatização;
- Gestão das instalações prediais;
- Políticas de manutenção;
- Infraestrutura elétrica;
- Infraestrutura de telecomunicações;
- Segurança física e lógica.

A **Figura 1** ilustra as principais áreas de um Data Center típico e como estas se relacionam entre si e com outros espaços externos, conforme a recomendação TIA-942.

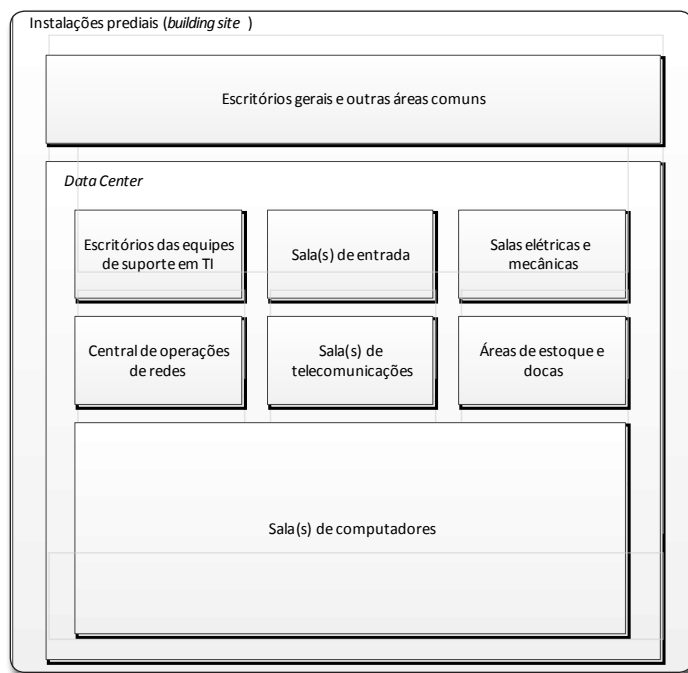
Esta norma também descreve as principais áreas funcionais que compõem a estrutura de um DC (**Figura 2**). São elas:

- **Entrance Room (ER)** – Sala de entrada: área na qual as instalações pertencentes às operadoras de telecomunicações promovem a interface com o cabeamento estruturado do Data Center. A ER abriga todos os equipamentos destas operadoras, que também disponibilizam enlaces de comunicação de dados aos seus clientes. Recomenda-se que esta sala esteja localizada fora do local onde estão os servidores e os dispositivos de rede, denominado sala de computadores (computer room), para aumentar a segurança (evita o acesso físico dos prestadores de serviço terceirizados). Os DCs podem ter múltiplas ERs para prover redundância e para evitar que sejam excedidos os limites de distância do cabeamento estruturado (fibras óticas e pares trançados – metálicos);
- **Main Distribution Area (MDA)** – Área de distribuição principal: este espaço compreende o Main Cross-Connect (MC), que é o ponto central de distribuição do sistema de cabeamento estruturado de um Data Center. Pode incluir também o Horizontal Cross-Connect (HC) para atender equipamentos instalados no local, como as centrais telefônicas, e os roteadores e switches de backbone (principais). A MDA geralmente está localizada dentro da sala de computadores, mas também pode estar em um espaço dedicado, a fim de aumentar a segurança física;
- **Horizontal Distribution Area (HDA)** – Área de distribuição horizontal: conecta as áreas de distribuição de equipamentos.

Frequentemente, a HDA está situada na sala de computadores, porém, por questões de segurança, pode ser instalada em um local dedicado. A área de distribuição horizontal tipicamente inclui os switches LAN (Local Area Network), SAN (Storage Area Network) e KVM (Keyboard/Video/Mouse) usados pelos equipamentos terminais localizados nas EDAs. Os DCs podem ter várias salas de computadores, em diferentes andares, cada qual suportada por sua própria HDA. Já as infraestruturas menores não requerem necessariamente a área de distribuição horizontal, pois a sala de computadores pode ser atendida diretamente pela MDA;

- **Zone Distribution Area (ZDA)** – Área de distribuição da zona: ponto opcional de interconexão. Situado entre as áreas de distribuição horizontal e de equipamentos, possibilita flexibilidade ao Data Center, permitindo alterações rápidas na reconfiguração do cabeamento;

- **Equipment Distribution Area (EDA)** – Área de distribuição de equipamentos: espaço alocado para dispositivos terminais (servidores, unidades de armazenamento de dados, telefones, entre outros) e equipamentos de telecomunicações (roteadores, switches, firewalls e balanceadores de carga).



**Figura 1.** Áreas presentes em um Data Center típico.

## Topologias reduzidas para Data Centers

Segundo a norma TIA-942, as infraestruturas para DCs menores podem ser dimensionadas como uma topologia reduzida. Neste modelo, tanto o ponto central de distribuição do cabeamento estruturado (MC) quanto o cabeamento horizontal (HC) são consolidados na MDA (no extremo, em um único rack); por fim, a sala de entrada também pode ser agregada na área de distribuição principal (**Figura 3**). Esta arquitetura é muito utilizada no projeto de pequenos Data Centers, geralmente mantidos por empresas

privadas. Habitualmente o espaço físico é limitado nestes DCs e as aplicações não justificam os investimentos em elevados níveis de disponibilidade, redundância, escalabilidade e modularidade.

## Topologias distribuídas para Data Centers

Restrições relacionadas ao comprimento máximo do cabeamento podem demandar múltiplas salas de entrada em grandes Data Centers (Figura 4). As ERs estão conectadas às áreas de distribuição principal e horizontal por intermédio de fibras ópticas, pares trançados ou cabos coaxiais. A ER primária não deve ser interligada diretamente às HDAs, somente através da MDA. Já a ER secundária pode ser conectada às HDAs, embora não seja uma prática recomendada. Este modelo é implementado em grandes infraestruturas, frequentemente, Internet Data Centers. Duas salas de entrada possibilitam redundância na interface com as operadoras de telecomunicações, viabilizando a interconexão com diferentes equipamentos e infraestruturas de fibras óticas encaminhadas por caminhos físicos díspares (por exemplo, abordagens de entrada em logradouros distintos). Assim, os IDCs também oferecem aos seus clientes conexões de alta velocidade e capacidade com as principais operadoras de telecomunicações locais, ou seja, o tráfego originado nos servidores hospedados nas suas instalações será encaminhado diretamente para os destinatários finais conectados nestes provedores.

## Classificação dos Data Centers

A recomendação TIA-942 afirma que os pontos únicos de falha devem ser eliminados do projeto de um Data Center para assegurar sua redundância e confiabilidade. Estes podem ocorrer em qualquer componente dos subsistemas de um DC, entre eles:

- Sistemas de climatização: os equipamentos podem sofrer falhas elétricas, hidráulicas ou mecânicas e não suportar o condicionamento do ar conforme as condições de temperatura e umidade dimensionadas; além disso, o sistema pode não suportar condições extremas de temperatura (por exemplo, dias muito quentes e úmidos);

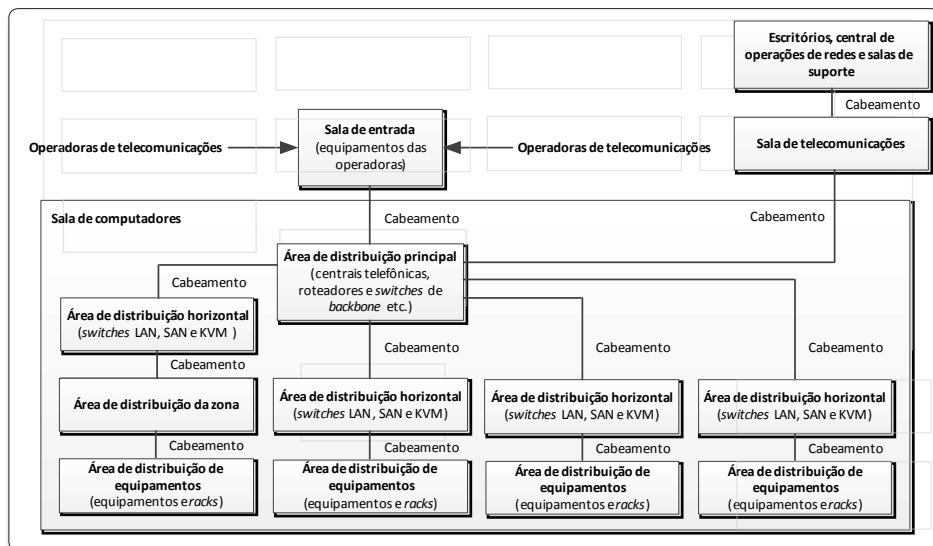


Figura 2. Principais áreas funcionais da topologia de um Data Center típico

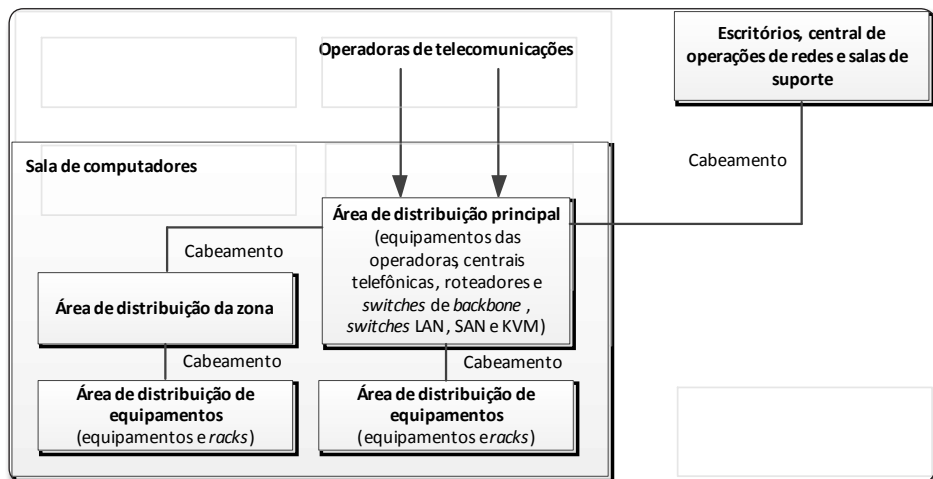


Figura 3. Principais áreas de um Data Center com topologia reduzida

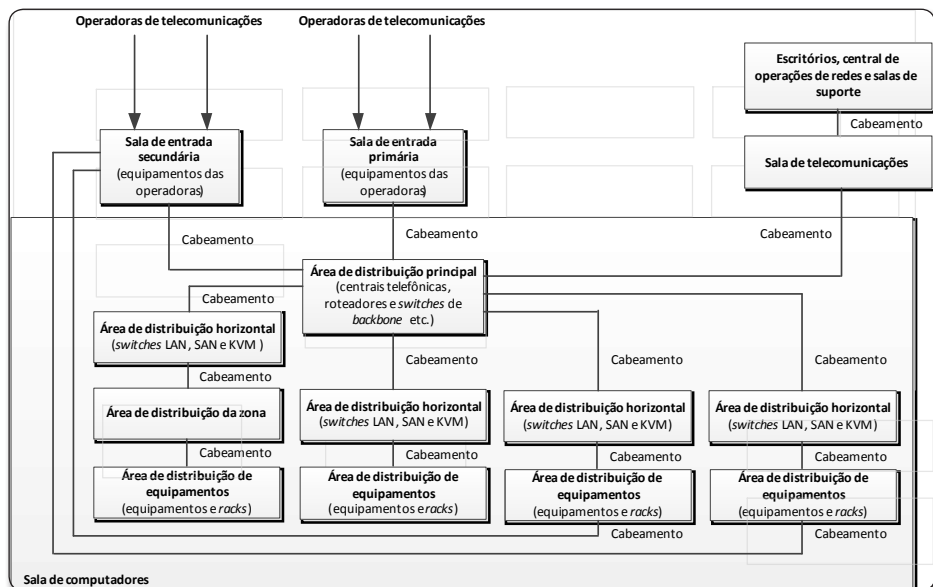


Figura 4. Principais áreas de um Data Center com topologia distribuída

- **Infraestrutura elétrica:** falhas ou manutenções programadas podem causar interrupções no fornecimento de energia elétrica, pois diversos e complexos dispositivos estão envolvidos, como painéis elétricos, redes internas de transmissão, baterias e geradores;
- **Infraestrutura de telecomunicações:** envolve equipamentos especializados e sofisticados para a transmissão dos dados e a interface com as operadoras de telecomunicações. As principais falhas estão relacionadas ao software e ao hardware dos equipamentos, ou seja, podem ocorrer inconsistências na alocação de memória, mau funcionamento nos módulos, nas portas de interconexão, nas fontes de alimentação e nos resfriadores dos gabinetes (ventiladores);
- **Segurança lógica e física:** incidentes de segurança podem causar suspensões no fornecimento dos serviços. Geralmente são provocadas por vírus, cavalos de troia, ataques de negação de serviço, falhas nos protocolos e nos sistemas operacionais. Também são comuns deficiências nas políticas de segurança, que deveriam limitar o acesso físico somente às equipes e usuários que prestam suporte aos dispositivos da infraestrutura do Data Center.

Desta forma, os DCs podem ser classificados segundo aspectos intimamente relacionados à maneira como foram concebidos: (i) arquitetura, (ii) telecomunicação, (iii) elétrico e (iv) mecânico. A partir destas características, foram criados quatro níveis de infraestrutura (também chamados Tiers):

- Tier 1 (Data Center básico);
- Tier 2 (Data Center com componentes redundantes);
- Tier 3 (Data Center que permite manutenção sem paradas);
- Tier 4 (Data Center tolerante a falhas).

As próximas seções descrevem brevemente as principais características de cada uma destas categorias de DCs, destacando o tempo máximo de indisponibilidade da infraestrutura (downtime) e os principais pontos de atenção.

## Tier 1 – Data Center básico

Neste nível, a infraestrutura de telecomunicações será distribuída da sala de entrada para as áreas de distribuição principal e horizontal por meio de um caminho (duto) único, sem rotas alternativas físicas ou lógicas. Também não contempla a redundância na entrada da alimentação elétrica da concessionária fornecedora. Suporta um nível de distribuição de energia que atende somente a demanda prevista, sem carga elétrica adicional. Já o sistema de condicionamento de ar, mantém a temperatura e a umidade relativa das áreas críticas nas condições estabelecidas no projeto, igualmente sem capacidade ociosa.

Os DCs desta categoria são suscetíveis a interrupções planejadas (manutenções preventivas e corretivas, atividades para expansão da infraestrutura, atualizações de software, entre outras) e não previstas (falhas e incidentes). O tempo máximo de indisponibilidade da infraestrutura é de 28,8 horas por ano. Este valor é obtido por meio do cálculo da disponibilidade total prevista, ou seja, 99,671% das 8.760 horas anuais. Os principais pontos de atenção são:

- Falhas de alimentação elétrica no Data Center ou na Central da Operadora de Telecomunicações;
- Falhas nos dispositivos de redes, como roteadores, switches, firewalls, balanceadores de carga, entre outros;
- Eventos catastróficos nos caminhos de interligação ou nas áreas ER, MDA, HDA, ZDA e EDA.

## Tier 2 – Data Center com componentes redundantes

Neste grupo, os equipamentos de rede e de telecomunicações possuem seus principais módulos de hardware redundantes, tais como:

- Fontes de energia;
- Placas processadoras de dados;
- Placas de gerenciamento;
- Portas para conexão com outros dispositivos.

O cabeamento das áreas de distribuição horizontal para os equipamentos de backbone deve ser composto por fibras ópticas ou pares trançados redundantes, suportando a interconexão com diferentes módulos dos dispositivos de redes e telecomunicações. Deve disponibilizar também duas caixas de acesso de telecomunicações e dois caminhos de entrada até a ER (separados minimamente por 20 metros e conectados a pontos opostos da sala de entrada).

Os DCs denominados Tier 2 ainda não contemplam a redundância na entrada da alimentação elétrica da concessionária fornecedora. Entretanto, os nós de baterias (Uninterruptible Power Supply – UPS) que suportam a operação até o acionamento dos geradores elétricos devem estar configurados como N+1. Neste cenário, N representa a quantidade de nós necessária para atender a carga elétrica total planejada; já na redundância N+1, existe um nó sobressalente que será ativado quando qualquer outro estiver indisponível. Também não há necessidade de geradores de energia elétrica redundantes. Por fim, os equipamentos condicionadores de ar devem ser projetados para operação contínua, 24 horas por dia, 7 dias na semana e 365 dias por ano, em configuração N+1.

A indisponibilidade máxima permitida é de 22,0 horas por ano (disponibilidade total prevista de 99,749%). Os principais pontos de atenção são relacionados às falhas nos sistemas de energia elétrica e climatização, que podem gerar incidentes em todos os demais componentes do Data Center.

## Tier 3 – Data Center que permite manutenção sem paradas

Estes DCs são atendidos por duas ou mais operadoras de telecomunicações, que provisionam seus enlaces de dados por intermédio de infraestruturas totalmente independentes. Estas estarão distribuídas em duas salas de entrada, minimamente separadas por 20 metros, em lados opostos do Data Center. Estas ERs devem possuir sistemas de condicionamento de ar, energia elétrica, proteção contra incêndios e equipamentos de telecomunicações distintos.

Também estarão disponíveis caminhos redundantes entre as ERs, MDAs e HDAs, por intermédio de fibras ópticas ou pares

trançados. Todos os dispositivos de rede e de telecomunicações estarão configurados em modo redundante, seja ativo-ativo (quando todos os nós estão operando simultaneamente e dividindo as transações a serem processadas) ou ativo-backup (neste modelo, um nó ocioso está disponível para entrar em operação somente no momento da ocorrência de um incidente). Desta maneira, poderão ocorrer manutenções e alterações no layout sem nenhuma indisponibilidade para os serviços do Data Center.

O sistema elétrico também deverá operar com contingenciamento N+1. Finalmente, os equipamentos condicionadores de ar serão dimensionados com equipamentos redundantes suficientes para suportar falhas ou manutenções planejadas em até um painel elétrico (neste caso, haverá interrupção no fornecimento de energia elétrica para todos os dispositivos do sistema de climatização conectados em circuitos alimentados por este quadro de distribuição elétrica), mantendo as condições de temperatura e de umidade relativa.

Neste nível, os DCs possuem downtime anual máximo de 1,6 horas (disponibilidade total prevista de 99,982%). O ponto crítico da infraestrutura são as áreas de distribuição principal e horizontal, pois qualquer incidente nestas poderá resultar na interrupção da operação.

#### Tier 4 – Data Center tolerante a falhas

Analogamente aos Data Centers do Tier 3, as instalações desta camada serão atendidas por duas ou mais operadoras de telecomunicações, que utilizam infraestruturas distintas. Estas estarão distribuídas em duas ERs, separadas por 20 metros, em lados opostos do DC. Ambas terão sistemas de climatização, energia elétrica, proteção contra incêndios e equipamentos de telecomunicações independentes.

Toda infraestrutura de cabeamento estruturado deverá ser redundante e instalada em dutos fechados. Além disso, é recomendada uma MDA secundária (em uma zona de proteção contra incêndio separada). O cabeamento das HDAs deverão seguir caminhos diferentes, um até a MDA principal, e outro até a MDA secundária. Os dispositivos de rede serão redundantes e serão alimentados por circuitos elétricos distintos, possibilitando o chaveamento automático para os equipamentos backup.

A instalação também deverá possuir duas alimentações de energia elétrica das concessionárias fornecedoras, conectadas em diferentes subestações para assegurar a redundância no fornecimento. O sistema elétrico estará configurado como 2 (N+1), onde além de um componente sobressalente, toda estrutura elétrica será duplicada.

Já o sistema de climatização será concebido com os componentes redundantes necessários para suportar falhas ou manutenções planejadas em até um painel elétrico, mantendo as condições de temperatura e de umidade relativa. Estes equipamentos devem possuir duas ou mais fontes de energia elétrica, conectadas em circuitos independentes.

Os Data Centers deste Tier têm indisponibilidade anual máxima de 0,4 hora (disponibilidade total prevista de 99,995%). Nota-se

que a probabilidade de interrupções nos serviços é baixa, desde que seguidas as recomendações de disponibilização das áreas de distribuição principal e horizontal secundárias.

#### Sumário dos níveis de infraestrutura dos Data Centers

Conforme exposto nas seções anteriores, os DCs podem ser classificados em diferentes tiers. A infraestrutura elétrica, os sistemas de condicionamento de ar e a arquitetura de cabeamento são mais complexos nas instalações em conformidade com os tiers mais altos. Além disso, os equipamentos de rede e telecomunicações também utilizam mais componentes redundantes e robustos, resultando em um maior índice de disponibilidade. Abaixo, estão sumarizados os principais aspectos apresentados previamente. Por fim, a **Figura 5** ilustra graficamente o downtime anual para as instalações em diferentes tiers.

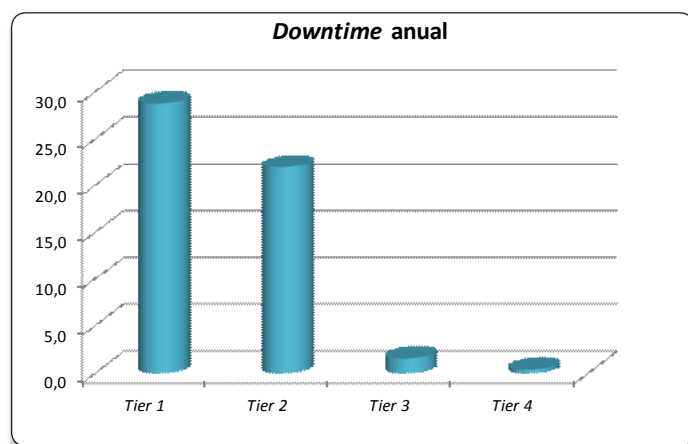


Figura 5. Downtime anual para cada um dos Tiers

- **Tier 1:** a infraestrutura deste grupo possui numerosos pontos de falha, pois não dispõe de redundância elétrica, de climatização, de cabeamento e de equipamentos de rede e telecomunicações;
- **Tier 2:** equipamentos de rede e telecomunicações com módulos de hardware redundantes. Cabeamento encaminhado por caminhos distintos. Os sistemas de UPS e condicionamento de ar estão configurados com contingenciamento N+1. Não há abordagem dupla no fornecimento de energia elétrica pela concessionária, geradores redundantes e circuitos elétricos independentes para os equipamentos;
- **Tier 3:** dispositivos de rede e telecomunicações redundantes. Duas ou mais operadoras de telecomunicações instaladas em salas de entrada totalmente independentes, com cabeamento encaminhado por dutos distintos para as áreas de distribuição principal e horizontal. Sistema elétrico configurado com contingenciamento N+1. Já o sistema de climatização suporta falhas e manutenções planejadas em até um painel elétrico. Por fim, as MDAs e HDAs não são duplicadas, ou seja, incidentes nestas áreas podem causar a interrupção nos serviços;
- **Tier 4:** todos os equipamentos de rede e telecomunicações são redundantes e conectados em diferentes circuitos elétricos.

O DC tem duas ou mais operadoras de telecomunicações instaladas em ERs independentes, com cabeamento redundante e encaminhados por dutos fechados. Existem áreas de distribuição principal e horizontal primárias e secundárias. A alimentação elétrica é fornecida a partir de subestações diferentes e o sistema elétrico está configurado como 2 (N+1).

## Qual o melhor Data Center?

Segundo Sri Chalasani, em seu artigo TIA-942: Data Center Standards, dependendo das características do modelo de negócios da empresa, diferentes infraestruturas podem ser utilizadas. Assim, o critério mais relevante na escolha de um Data Center é a dependência que uma empresa ou organização apresenta em relação aos sistemas de informação. Portanto, empresas que não realizam seus negócios diretamente pela Internet e cujas operações não necessitam ser processadas em tempo real, podem optar por investimentos em infraestruturas menos robustas e com menor disponibilidade. Já as companhias que possuem forte vínculo com a tecnologia da informação, como aquelas que praticam comércio eletrônico ou as instituições financeiras, devem escolher DCs com os menores índices de downtime. A lista abaixo ilustra alguns exemplos conforme os níveis descritos nas seções anteriores:

- **Tier 1:** Companhias pequenas, com presença limitada na Internet, pouca dependência da tecnologia da informação e que toleram a indisponibilidade momentânea dos serviços;
- **Tier 2:** Organizações que vendem alguns de seus produtos pela Internet, com sistemas de informação instalados em múltiplos servidores, dependentes de aplicações de correio eletrônico e voz sobre IP. Suportam apenas a indisponibilidade planejada de seus serviços;
- **Tier 3:** Empresas com presença mundial na Internet e amplamente conhecidas, com páginas Web de comércio eletrônico. Possuem alta dependência da tecnologia e dos sistemas de informação. Portanto, a interrupção dos serviços pode gerar um prejuízo significativo;
- **Tier 4:** Instituições e companhias que realizam transações de alto valor monetário através da Internet. Totalmente dependentes da TI e não tolerantes a nenhuma indisponibilidade na operação de seus serviços online.

## Infraestrutura para computação em nuvem (cloud computing)

A computação em nuvem (cloud computing) é um tema atual e fortemente relacionado à infraestrutura dos Data Centers, pois estes últimos são a sua manifestação física. Segundo Fábio Verdi, Christian Rothenberg, Rafael Pasquini e Maurício Magalhães, em seu artigo Novas Arquiteturas de Data Center para Cloud Computing, a computação em nuvem é um conjunto de recursos virtuais facilmente usáveis e acessíveis, tais como hardware, plataformas de desenvolvimento e serviços. Sua estrutura é modular e flexível, possibilitando ser dinamicamente reconfigurada para se ajustar a uma carga variável, otimizando o uso dos recursos. Este conceito é ilustrado graficamente pela **Figura 6**.



**Figura 6.** Componentes da computação em nuvem

Dependendo da infraestrutura física e da sua localização, os Data Centers que suportam a computação em nuvem podem ser classificados como mega, micro, nano ou baseados em contêineres:

- **Mega Data Centers:** são instalações com dezenas de milhares de servidores. Estas são construídas em locais próximos às subestações de fornecimento de energia elétrica, e com boa conectividade à Internet (oferecida por diferentes operadoras de telecomunicações). Habitualmente, são empregadas para aplicações em nuvem que analisam bases de dados ou outros sistemas que requeiram grandes volumes de memória, ciclos de processamento e espaço para armazenamento dos dados;
- **Micro Data Centers:** possuem milhares de servidores e geralmente são conhecidos como instalações satélites, pois estão localizadas em pontos próximos aos grandes centros populacionais para oferecer uma diversidade geográfica que minimiza a latência (atrasos na transferência dos dados) e os custos das comunicações com as operadoras de telecomunicações. Suportam aplicações interativas, como correio eletrônico, compartilhamento de documentos e distribuição de conteúdos;
- **Nano Data Centers:** este conceito surgiu da possibilidade de considerar os equipamentos dos usuários finais como uma extensão do Data Center, utilizando seus recursos para execução de tarefas de processamento e armazenamento de dados. Este novo paradigma evidencia os desafios de gerenciar um sistema com natureza distribuída e assegurar desempenho, confiabilidade e segurança;
- **Data Centers baseados em contêineres:** modelo que disponibiliza instalações modularizadas em contêineres com até 2.000 servidores, formando um bloco computacional que necessita apenas de energia elétrica, água (para refrigeração) e conectividade à Internet para iniciar sua operação. Este tipo de infraestrutura é uma opção para implantação em locais remotos ou temporários, como nas proximidades dos eventos culturais e esportivos.

É importante notar que, independentemente da classificação adotada pelas instalações que suportam a computação em nuvem, sua infraestrutura deve seguir a recomendação TIA-942 para assegurar que sejam reduzidos os pontos únicos de falha, especialmente aqueles relacionados aos aspectos elétricos, aos sistemas de climatização, à arquitetura de cabeamento, e aos equipamentos de redes e telecomunicações. Somente desta forma, será possível atingir os índices de disponibilidade, escalabilidade e confiabilidade apresentados para cada um dos tiers.

## Conclusões

Os Data Centers são estruturas complexas porque envolvem a integração entre diversas áreas e sistemas, tais como: climatização,

sistemas elétricos, infraestrutura de telecomunicações, dispositivos de combate e prevenção de incêndio, e políticas de segurança física e lógica. Suas instalações devem abrigar os equipamentos e os sistemas de tecnologia da informação de uma empresa 24 horas por dia, 7 dias na semana e 365 dias por ano. Podem ser Private Data Centers (mantidos por empresas privadas ou públicas) ou Internet Data Centers (providos por prestadores de serviços de telecomunicações). Estes últimos agrupam seus serviços em duas modalidades básicas: Colocation (fornecem somente o espaço físico a fim de permitir a instalação dos equipamentos de seus clientes) e Hosting (ofertam a infraestrutura completa de hardware e software).

A infraestrutura dos Data Centers deve suportar as tecnologias existentes e os avanços tecnológicos nas áreas de processamento de dados, telecomunicações e armazenamento. Para tanto, uma instalação típica é composta por cinco principais áreas funcionais: sala de entrada, área de distribuição principal, área de distribuição horizontal, área de distribuição da zona e área de distribuição de equipamentos. Também existem versões reduzidas e distribuídas, para acomodar infraestruturas menores e mais complexas, respectivamente.

Por fim, conforme o nível de disponibilidade e confiabilidade requerido pelo modelo de negócio de uma empresa, Data Centers em diferentes níveis ou Tiers podem ser selecionados. As instalações no primeiro nível possuem numerosos pontos de falha e atendem organizações pequenas, com presença limitada na Internet e pouca dependência de tecnologia da informação. Já os Data Centers classificados como Tier 4 empregam sofisticados e modernos componentes de redundância que resultam em uma indisponibilidade anual máxima de 0,4 hora. Com obviedade, tal infraestrutura tem um custo compatível somente com empresas que realizam um alto volume de negócios através da Internet, ou seja, que não toleram nenhum tipo de interrupção em seus serviços, pois haveria um prejuízo inestimável em transações perdidas e a sua própria imagem.



#### **André Koide da Silva**

*andre@aksilva.com*

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

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



#### **Artigo “Ambiente de Data Center”, escrito por José Maurício S. Pinheiro.**

[http://www.projetederedes.com.br/aulas/unifoa\\_topicos/unifoa\\_topicos\\_aula1.pdf](http://www.projetederedes.com.br/aulas/unifoa_topicos/unifoa_topicos_aula1.pdf)



#### **Artigo “How To Build Data Centers?”, escrito por Pravin Ganore.**

<http://www.esds.co.in/blog/how-to-build-data-centers>

#### **Artigo “Novas Arquiteturas de Data Center para Cloud Computing” escrito por Fábio Verdi, Christian Rothenberg, Rafael Pasquini e Maurício Magalhães.**

<http://www.dca.fee.unicamp.br/~chesteve/pubs/MC-DATA-CENTER-NETWORKS-SBRC2010.pdf>

#### **Artigo “TIA-942: Data Center Standards” escrito por Sri Chalasani.**

[http://www.merit.edu/events/mmc/pdf/2010\\_chalasani.pdf](http://www.merit.edu/events/mmc/pdf/2010_chalasani.pdf)

#### **Artigo “TIA-942 – Telecommunications Infrastructure Standard for Data Centers”, escrito por Telecommunications Industry Association.**

<http://www.tiaonline.org>

# Segurança em Redes IEEE 802.11

## Podemos nos sentir seguros nas redes IEEE 802.11?

**A**s redes sem fio estão por toda parte. Cada vez mais as pessoas utilizam dispositivos móveis para navegar na Internet, trabalhar, realizar chamadas telefônicas e assistir vídeos. Segundo pesquisa realizada recentemente pela fabricante de equipamentos de telecomunicações Cisco, o tráfego global de dados móveis deve aumentar em 18 vezes entre 2011 e 2016, quando atingirá um total de 10,8 exabytes por mês. As redes sem fio são bastante utilizadas devido a sua facilidade de instalação, já que dispensam a instalação de cabeamento. Além disso, elas conferem maior independência ao usuário, que pode utilizar os serviços de comunicação em diferentes lugares com facilidade. Um dos principais atores desta nova realidade é o padrão IEEE 802.11.

O padrão IEEE 802.11 tem sido largamente utilizado para construção de redes sem fio. Pesquisa recente publicada na revista Network World aponta que 25% das residências do mundo têm uma rede IEEE 802.11. Segundo a Wi-Fi Alliance, um terço das residências americanas que possuem acesso à Internet tem uma rede IEEE 802.11. É comum encontrarmos hot spots IEEE 802.11 em ambientes variados como cafés, bares, restaurantes, hotéis e academias. Ambientes públicos também têm utilizado a tecnologia IEEE 802.11 para oferecer serviço de Internet aos seus frequentadores. A INFRAERO anunciou recentemente que os principais aeroportos brasileiros oferecerão acesso grátis à Internet aos passageiros por meio de redes sem fio IEEE 802.11. Na praia de Copacabana, no Rio de Janeiro, os banhistas podem acessar a Internet a partir de seus dispositivos móveis gratuitamente por meio de conexões IEEE 802.11. Cidades nos Estados Unidos, Europa e Brasil oferecem Internet grátis aos cidadãos por meio de redes IEEE 802.11.

A tendência é que as redes IEEE 802.11 continuem sendo o padrão *de facto* para redes locais sem fio por um longo tempo, já que a tecnologia continua evoluindo de forma a proporcionar taxas de transmissão cada vez mais altas. O IEEE já está trabalhando no novo padrão IEEE 802.11, que será denominado IEEE 802.11ac e promete oferecer taxas de transmissão superiores a 1 Gbps.

### Resumo DevMan

#### *De que se trata o artigo:*

Este artigo apresenta as principais questões relacionadas à segurança em redes IEEE 802.11. Primeiramente, serão apresentadas as redes IEEE 802.11 e os fatores que fazem delas inseguras. Então, serão apresentados o WEP e o WPA, que são arquiteturas de segurança desenvolvidas para as redes IEEE 802.11. Também serão apresentadas vulnerabilidades descobertas no WEP e no WPA1. Por fim, serão apresentadas outras ameaças à segurança das redes sem fio que não estão diretamente relacionadas com a exploração de vulnerabilidades do WEP e do WPA1 como war driving, negação de serviço, spoofing e APs mal configurados.

#### *Em que situação o tema é útil:*

As redes sem fio estão presentes em diversos lugares como aeroportos, cafés, residências, restaurantes, universidades e grandes corporações. A utilização de redes sem fio é atrativa, pois elas oferecem praticidade ao dispensar a instalação de cabos e permitir a mobilidade das estações cliente. Entretanto, estes benefícios das redes sem fio são acompanhados por riscos relacionados à segurança, já que os dados transmitidos nestas redes são propagados pelo ar e facilmente interceptados. Os usuários têm acessado as redes sem fio para utilizar diversas aplicações, incluindo aquelas que manipulam informações sensíveis como os aplicativos de Internet Banking. Portanto, conhecer e fazer bom uso das soluções de segurança disponíveis para as redes sem fio é necessário para que seja garantida a tranquilidade dos usuários ao acessar estes ambientes.

#### *Segurança em Redes IEEE 802.11:*

A adoção das redes sem fio tem apresentado uma forte expansão nos últimos anos. Pesquisas mostram que o tráfego de dados móvel deve crescer 18 vezes até 2016 e que 25% das residências do mundo possuem uma rede IEEE 802.11. Esta forte tendência de aumento de utilização das comunicações sem fio é acompanhada pela preocupação com a segurança da informação nestas redes. Este artigo mostra as diferentes soluções de segurança adotadas nas redes IEEE 802.11 e as vulnerabilidades presentes nestas soluções. Além disso, são apresentadas diversas formas de ataques que podem atingir as redes IEEE 802.11. O objetivo é mostrar que as redes IEEE 802.11 podem ser confiáveis do ponto de vista de segurança mantendo a praticidade que tem feito delas um grande sucesso de mercado.

Mesmo com todos os benefícios provenientes da utilização das redes sem fio, há uma preocupação sempre presente quando tratamos da utilização desta tecnologia: a segurança. A propagação do sinal pelo ar torna as redes sem fio propensas à interceptação de dados. Além disso, as redes sem fio são utilizadas frequentemente por dispositivos móveis que não estão sob o controle das políticas de segurança e proteção determinadas pela administração da rede. Logo, eles podem atuar como vetores de transmissão de pragas virtuais como vírus e worms. No caso das redes IEEE 802.11, o uso massivo desta tecnologia a torna ainda mais atrativa para agentes maliciosos, que podem conseguir atingir grandes quantidades de usuários descobrindo apenas uma vulnerabilidade. Neste cenário, a aplicação de técnicas que garantam privacidade aos usuários e a integridade das informações é essencial.

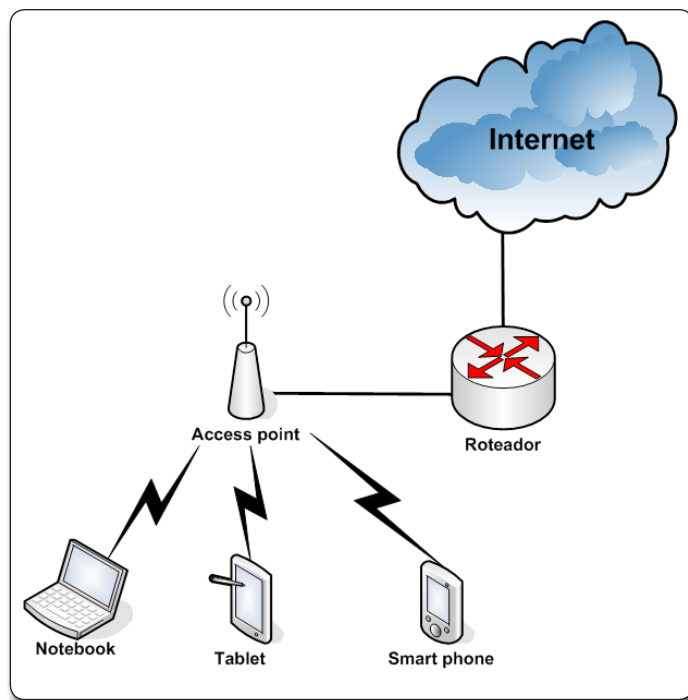
### As Redes IEEE 802.11

O grupo de trabalho responsável pelo padrão IEEE 802.11 foi criado em 1990. O objetivo da criação do grupo foi desenvolver protocolos de controle de acesso ao meio e especificações de camada física para redes locais sem fio. Os principais padrões publicados pelo grupo ao longo dos últimos 20 anos são os seguintes: 802.11a, 802.11b, 802.11g e 802.11n. Todos estes padrões constroem quadros com o mesmo formato e utilizam o mesmo protocolo de acesso ao meio, denominado CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*). O primeiro padrão a atingir uma parcela significativa do mercado foi o IEEE 802.11b. Com o crescente domínio deste padrão, a indústria começou a se preocupar em garantir que haveria interoperabilidade entre equipamentos IEEE 802.11b de diferentes fabricantes. Diante desta necessidade, foi formada em 1999 a Wi-Fi (*Wireless Fidelity*) Alliance. A entidade desenvolveu um conjunto de testes dedicados a verificar a interoperabilidade para produtos IEEE 802.11 e passou a batizar as redes construídas segundo o padrão.

A maneira mais comum de implantar uma rede IEEE 802.11 é a seguinte: há um Access Point (AP) conectado à Internet ou ao núcleo da rede corporativa. Todas as estações sem fio se conectam a este AP, responsável por diversas funções como coordenar as transmissões e realizar a autenticação de usuários. O alcance do sinal emitido pelo AP determina a área de abrangência da rede. A **Figura 1** ilustra um cenário comum de rede IEEE 802.11.

Apesar de proporcionarem praticidade aos usuários ao permitir a mobilidade e dispensar a instalação de cabeamento, as redes sem fio, incluindo as redes IEEE 802.11, despertam desconfiança por estarem mais expostas a problemas de segurança. Os seguintes fatores fazem com que estas redes sejam inseguras:

- Redes sem fio são naturalmente expostas à interceptação de dados, já que todos os pacotes trocados entre transmissores e receptores se propagam pelo ar;
- Redes sem fio devem oferecer certa facilidade de acesso, pois são utilizadas frequentemente para proporcionar conforto a usuários móveis ou em trânsito, que devem se aproximar da área de cobertura da rede e se conectarem sem maiores dificuldades. Esta facilidade de acesso pode ser explorada por agentes mal intencionados;



**Figura 1.** Cenário comum de rede IEEE 802.11.

- Redes sem fio são utilizadas comumente por dispositivos que não estão sujeitos às políticas de segurança das corporações. Em cenários nos quais os usuários acessam a rede sem fio por meio de seus tablets, smartphones e notebooks pessoais, é impossível garantir que eles possuem dispositivos de segurança como softwares antivírus, por exemplo;
- Dispositivos móveis utilizam diferentes redes sem fio. Um mesmo notebook ou tablet pode ser utilizado na rede sem fios doméstica, na rede sem fios do escritório e na rede sem fios de um aeroporto, por exemplo. Desta forma, um notebook infectado pode agir como o vetor de transmissão de vírus e worms. Ao ingressar em diferentes redes, este notebook está levando os vírus e outras pragas virtuais que ele carrega a diferentes lugares.

Para aumentar o nível de segurança nas redes sem fio, há dois pontos principais que devem ser atacados:

- **Autenticação:** verificação da identificação das estações que estão participando da rede. Nas redes cabeadas, o simples fato de permitir a conexão física já sinaliza uma autorização de uso. Nas redes sem fio isto não é válido. Portanto, elas fazem uso de mecanismos de autenticação para que a estação possa se identificar e ser autorizada a transmitir e receber dados;
- **Privacidade:** usada para prevenir que dados transmitidos na rede sem fio a um determinado receptor possam ser lidos por terceiros.

As redes sem fio IEEE 802.11 utilizam dois esquemas de segurança. O primeiro é o WEP (*Wired Equivalence Privacy*), mais antigo e comprovadamente inseguro. O segundo é o WPA (*Wi-Fi Protected Access*), mais utilizado atualmente e desenvolvido para substituir o WEP.

## WEP (Wired Equivalence Privacy)

O WEP (*Wired Equivalence Privacy*) é um algoritmo incluído na especificação original do padrão IEEE 802.11 para prover, principalmente, privacidade às comunicações realizadas nestas redes sem fio. O WEP utiliza criptografia simétrica baseada no algoritmo RC4. Na criptografia simétrica, apenas uma chave é usada para cifrar e decifrar a informação. Desta forma, temos uma informação que é cifrada na origem utilizando uma chave  $k$ . Somente utilizando a mesma chave  $k$ , o destinatário vai poder decifrar esta informação. O ponto crítico deste algoritmo é o compartilhamento da chave secreta, que precisa ser realizado antes do início da sessão segura.

No WEP, a chave de criptografia é formada por dois elementos: uma chave secreta conhecida pelo AP e pelas estações e um IV (*Initialization Vector*) de 24 bits. A chave secreta é cadastrada manualmente no AP e nas estações, pois não há protocolos para distribuição de chaves no WEP. A chave secreta compartilhada tem 40 bits ou 104 bits. O IV é utilizado para evitar um ataque de criptoanálise, já que a chave secreta compartilhada raramente é modificada. A autenticação de uma estação que deseja se comunicar com um AP é executada pelos seguintes passos:

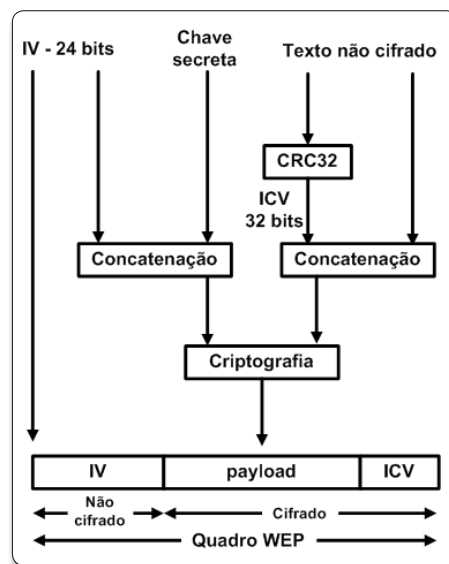
1. A estação cliente requisita ao AP autorização para acesso à rede;
2. O AP responde com uma palavra não cifrada;
3. A estação cliente escolhe um IV;
4. Utilizando o IV e a chave secreta compartilhada, a estação cliente cifra a palavra enviada no passo 2 pelo AP;
5. O cliente envia a palavra cifrada e o IV para o AP;
6. Utilizando o IV, o AP cifra a palavra enviada por ele no passo 2;
7. Se a palavra cifrada enviada pelo cliente for igual à palavra cifrada produzida no passo 6 pelo AP, o AP autoriza a estação cliente a ingressar na rede.

A partir da autenticação, o cliente está apto a enviar quadros para o AP. De forma a permitir o controle da integridade do quadro durante a transmissão, é computado um ICV (*Integrity Check Value*) para cada quadro a ser transmitido. Para calcular o ICV, o WEP utiliza o algoritmo CRC32. O ICV é incluído no final do quadro que será transmitido. Quando o quadro chega ao destino, o receptor calcula novamente o ICV para o conteúdo do quadro. Caso haja alguma alteração no conteúdo do quadro, o AP poderá detectá-la, pois o ICV do quadro que chegou ao destino não será igual ao ICV calculado na origem do quadro.

Cada quadro é cifrado com a chave criada a partir da concatenação da chave secreta compartilhada pela estação e pelo AP e de um IV. Para cada quadro é utilizado um IV novo, que é informado ao receptor do quadro em um campo não cifrado no cabeçalho. A formação do quadro WEP é ilustrada na **Figura 2**.

Infelizmente, o WEP é um algoritmo bastante vulnerável a ataques. Alguns ataques ao WEP se concentram em explorar vulnerabilidades do algoritmo de criptografia RC4. Apesar de o RC4 permitir a utilização de chaves de até 256 bits, o que proporciona um nível de segurança satisfatório, a implementação do RC4 utilizada no WEP utiliza chaves de 64 bits. Desta chave, 24 bits são

utilizados para o IV. Desta forma, temos apenas 16, 7 milhões de vetores possíveis, número insuficiente em situações nas quais a rede está com altos níveis de tráfego. Caso o atacante observe o tráfego por um determinado período, ele pode conseguir capturar a utilização de IVs repetidos. Utilizando estes vetores e as palavras cifradas, o atacante pode fazer o processo inverso ao da criptografia dos dados e acabar descobrindo a chave compartilhada entre os usuários da rede.



**Figura 2.** Construção de um quadro WEP

Este não é o único problema de segurança do WEP. Há diversos ataques que foram discutidos por especialistas e estão documentados com detalhes na literatura. O primeiro destes ataques é o FMS Attack, descoberto em 2001. O nome do ataque tem origem nos nomes dos autores do artigo que publicou esta vulnerabilidade do WEP: Fluhrer, Martin e Shamir. Os autores apresentaram uma série de IVs fracos, que facilitavam ataques. Estes IVs fracos eram descobertos a partir da análise de pacotes cuja parte do conteúdo já conhecemos normalmente de antemão, como os pacotes ARP (*Address Resolution Protocol*). O ataque FMS tem 50% de probabilidade de sucesso e precisa analisar cerca de 9.000.000 de pacotes.

Outro tipo de ataque sobre o protocolo WEP é denominado KoreK. Em 2004, um usuário de um fórum na Internet que utilizava o apelido de Korek publicou um programa que englobava 17 ataques que poderiam ser aplicados sobre o protocolo WEP. Os ataques, que utilizam diferentes estratégias, levam à descoberta das chaves secretas utilizadas pelas estações presentes na rede. Estes ataques são capazes de ter sucesso em 97% das tentativas utilizando apenas 300.000 pacotes. É possível observar que são ataques bem mais perigosos do que o relatado por Fluhrer, Martin e Shamir três anos antes.

O ataque PTW foi criado em 2007 e é mais perigoso que o ataque FMS e que os ataques publicados por KoreK. Assim como o ataque FMS, o ataque PTW também utiliza as iniciais de seus criadores

em seu nome: Pyshkin, Tews e Weinmann. Este ataque otimizou a maneira como é realizada a descoberta da chave no FMS. Desta maneira, ela pode ser realizada mais rapidamente e não depende da utilização de um IV fraco. Os ataques podem alcançar 97% de sucesso utilizando apenas 70.000 pacotes.

O ataque chop chop é outro tipo de ataque que pode ser efetuado contra redes WEP, mas é bem diferente dos ataques FMS, PTW e KoreK. Neste caso, o atacante intercepta apenas um pacote que está sendo transmitido na rede e aproveita uma vulnerabilidade no algoritmo CRC32 para decifrar todos os bytes do pacote que estavam cifrados, mesmo sem descobrir a chave secreta utilizada. O ataque começa pelo último byte do pacote. O atacante tenta adivinhá-lo e envia o pacote ao AP. Caso a tentativa do atacante seja fracassada, o AP detectará por meio do ICV que o pacote foi corrompido e o descartará. Caso o atacante tenha tido sucesso ao adivinhar o byte, o AP vai aceitar o pacote e enviar um pacote de reconhecimento (ACK) ao atacante. Desta forma, o atacante sabe que já adivinhou o último byte do pacote. Esta mesma operação é repetida pelo atacante para todos os bytes restantes do pacote. São necessárias, em média, 128 tentativas para adivinhar cada byte do pacote. Com posse destes dados, o atacante pode, por exemplo, passar a enviar pacotes como se fosse a estação cujos dados foram descobertos.

A única solução para diminuir os riscos causados pelas vulnerabilidades apresentadas pelo WEP é não utilizá-lo, adotando outra solução de segurança. É expressamente recomendado que não se utilize o WEP para conferir segurança a redes sem fio IEEE 802.11. Para cumprir este objetivo, é recomendado que se adote o WPA, que será apresentado na seção a seguir.

## WPA (Wi-Fi Protected Access)

Devido às falhas encontradas no WEP, foi formado um grupo para abordar os problemas de segurança das redes sem fio. Este grupo produziu o padrão de segurança 802.11i. A Wi-Fi Alliance, por sua vez, lançou o WPA (Wireless Protected Access) como o seu padrão de segurança em 2003. O WPA é baseado no padrão 802.11i. O IEEE 802.11i aborda aspectos de autenticação e controle de acesso, além de privacidade e integridade das informações. O padrão inclui a figura de um servidor de autenticação que não existia no WEP. Este servidor permite a geração e o compartilhamento de chaves temporárias e a autenticação mútua.

O controle de acesso segue o padrão IEEE 802.1X, também denominado EAPoL (EAP over LAN), já que é baseado no EAP (Extensible Authentication Protocol) – ver **Notas do DevMan 1 e 2**. Ele é utilizado para a troca de informações entre clientes e o servidor de autenticação. Normalmente, o servidor de autenticação é o RADIUS, que armazena as credenciais (nome de usuário e senha) de todos os clientes em seu banco de dados. A autenticação e troca de chaves ocorre da seguinte forma:

1. Uma estação cliente se conecta a um AP;
2. Todo o tráfego que não seja necessário à autenticação é bloqueado. O tráfego só será liberado quando a autenticação se concluir;

3. O servidor RADIUS envia um número aleatório em aberto para a estação cliente. Este número não se repetirá em futuras comunicações;

4. O cliente concatena a sua senha ao número enviado pelo AP e aplica um algoritmo de hash sobre ambos (ver **Nota do DevMan 3**), resultando em  $H(x)$ , que é enviado para o servidor RADIUS;

5. O servidor RADIUS aplica o algoritmo de hash sobre as senhas que ele tem armazenadas concatenadas ao número aleatório que ele enviou à estação cliente no passo 3. Se um dos resultados for igual ao resultado  $H(x)$  obtido no passo 4, o servidor RADIUS gera uma chave secreta e envia para o AP;

6. A chave secreta é enviada do AP para o cliente usando o protocolo EAP. Uma das implementações do EAP, por exemplo, utiliza TLS (Transport Layer Security), um protocolo que é capaz de estabelecer canais seguros sobre conexões TCP. Desta forma, a troca de chaves é realizada em um canal seguro, requisito que não era atendido no WEP.



### Nota do DevMan 1

#### EAP (Extensible Authentication Protocol)

O EAP é um framework de autenticação definido no documento RFC 3748, que oferece suporte a diversas atividades ligadas a autenticação como, por exemplo, a troca de chaves.



### Nota do DevMan 2

#### EAPoL (Extensible Authentication Protocol over LAN)

O EAPoL ou IEEE 802.1X é um padrão IEEE que define a utilização do EAP em redes locais baseadas em padrões como o IEEE 802.3 (Ethernet) e IEEE 802.11.



### Nota do DevMan 3

#### Algoritmo de Hash

Um algoritmo de hash é uma função  $H(x)$  que produz um código único para cada sequência de dados inseridos na entrada do algoritmo.

É importante observar que o WPA tem duas possíveis abordagens. A primeira delas é o WPA-Enterprise, que implementa o padrão IEEE 802.1X e, consequentemente, faz uso de um servidor de autenticação como o RADIUS. Para facilitar a adoção do WPA em soluções SOHO (Small Office Home Office – ver **Nota do DevMan 4**), também foi lançada a versão WPA-Personal. Esta solução dispensa o uso do servidor de autenticação e permite a utilização de senhas cadastradas manualmente no AP e nas estações.

Resolvida a questão de controle de acesso e troca de chaves, temos de garantir privacidade nas comunicações. A primeira versão do WPA, a WPA1, foi desenvolvida para permitir a solução dos problemas do WEP sem causar a troca dos equipamentos legados. Desta forma, o protocolo de criptografia introduzido no

WPA1, denominado TKIP (*Temporal Key Integrity Protocol*), também utiliza o algoritmo de criptografia RC4.

A primeira solução adotada pelo TKIP para sanar as vulnerabilidades do WEP são as chaves temporárias. Elas são misturadas ao endereço MAC da estação cliente, gerando uma chave intermediária única para cada estação. O IV também é incrementado sequencialmente a cada quadro. Assim, a chave utilizada em cada quadro é única, resultando da união do IV e da chave intermediária. Estas soluções evitam ataques de criptoanálise comuns no WEP.



## Nota do DevMan 4

**SOHO (Small Office Home Office)**

A sigla SOHO designa ambientes domésticos e de pequenas empresas formados por até 10 usuários.

Além disso, o TKIP agrega um código de integridade ao fim das mensagens gerado por um algoritmo de hash denominado Michael. No TKIP, a entrada do algoritmo Michael é a união dos endereços MAC de origem e destino, uma chave secreta conhecida apenas pelo transmissor e pelo receptor e a mensagem para a qual se deseja garantir a integridade. Quando a mensagem chega ao receptor, ele insere os endereços MAC, a senha secreta e a mensagem recebida no algoritmo de hash. Se o resultado encontrado for igual ao código de integridade enviado pelo transmissor, é confirmado que a mensagem não foi modificada por um atacante.

Mesmo sendo mais seguro que o WEP, o WPA1 também pode sofrer ataques. Os atacantes aproveitam o fato de que o WPA1 é uma solução de transição entre o WEP e o WPA2 e ainda mantém o ICV gerado pelo algoritmo CRC32, utilizado no WEP. Logo, é possível realizar um ataque semelhante ao ataque chop chop, que era realizado em redes que utilizavam o WEP.

O TKIP tentou se precaver contra este ataque. Primeiramente, mesmo que o atacante consiga produzir um pacote que não seja dado como corrompido a partir da análise do ICV produzido pelo CRC32, ele será dado como corrompido pelo código de integridade produzido pelo Michael. Neste caso, o receptor do pacote com a falha envia uma resposta reportando a falha e inicia uma contagem de 60 segundos. Se outro pacote com o mesmo problema chegar até o receptor dentro do prazo de 60 segundos, ele assume que um ataque chop chop está em curso e desabilita as comunicações, reiniciando o processo de autenticação e distribuição de chaves aos clientes. Além disso, o AP descarta pacotes que cheguem com o número sequencial menor do que o número sequencial do último pacote recebido.

Apesar destas medidas, o ataque ainda é possível. O primeiro ponto do ataque é escolher um canal com pouco ou nenhum tráfego. Desta forma, evita-se que o AP perceba a atividade maliciosa a partir da checagem do número sequencial. O atacante,

então, intercepta um pacote e começa o processo semelhante ao realizado no ataque chop chop: ele tenta adivinhar o último byte do pacote e o envia para o AP. Se há sucesso, a checagem com o ICV gerado pelo CRC32 dá o pacote como legítimo, mas a checagem com o código de integridade gerado pelo Michael dá o pacote como corrompido e retorna uma falha. Desta forma, o atacante sabe que teve sucesso. Então, ele aguarda 60 segundos para evitar que o AP se defenda e repete o ataque para o próximo byte. Em aproximadamente 12 minutos, ele consegue adivinhar os demais bytes do pacote e pode utilizar estas informações para enviar pacotes fingindo ser outro dispositivo presente na rede. As consequências deste tipo de ataque podem ser evitadas se o período para renovação das chaves for menor, como 120 segundos. Algumas redes utilizam períodos de 3600 segundos, tempo suficiente para que o ataque seja completado e as informações descobertas sejam utilizadas de maneira maliciosa.

A segunda versão do WPA, a WPA2, foi lançada em 2004. Ela utiliza o algoritmo de criptografia simétrica AES (*Advanced Encryption Standard*) no lugar do RC4. O algoritmo AES é bem mais seguro que o RC4. O WPA2 também não utiliza o TKIP, que foi substituído pelo CCMP (*Counter Mode-CBC MAC Protocol*). O CCMP é baseado no modo de operação CCM (Counter with CBC-MAC) definido no AES.

O Counter mode é utilizado para garantir a confidencialidade dos dados. No processo de criptografia baseado no Counter mode, as mensagens a serem transmitidas são divididas em blocos de 128 bits e um contador é iniciado em zero. Para cada bloco processado, o contador é incrementado em 1 e é cifrado utilizando uma chave secreta. O contador cifrado é então aplicado a cada bloco de mensagem para cifrá-los.

O CBC-MAC (*Cipher Block Chaining-Message Authentication Code*) é utilizado para garantir a integridade das mensagens. Assim como no Counter mode, o CBC-MAC também divide a mensagem em blocos de 128 bits. Logo após a divisão, é realizada uma operação de XOR entre um vetor de inicialização e o primeiro bloco. O resultado desta operação é cifrado com a chave secreta. Temos, então, uma mensagem cifrada que vai ser o primeiro código de integridade. Este código de integridade é utilizado como vetor de inicialização para que o mesmo processo seja aplicado ao próximo bloco e assim por diante, produzindo códigos de integridade para cada bloco. Estes códigos são transmitidos junto com a mensagem.

Ao adotar soluções mais sofisticadas, o WPA2 tornou-se uma abordagem bem mais segura que o WPA1. À época de seu lançamento, o principal problema era a falta de suporte dos equipamentos existentes ao WPA2. A atualização dos equipamentos para que eles deixassem de utilizar o WEP e passassem a utilizar o WPA1 era mais simples, pois o WPA1 continuou mantendo os principais atributos do WEP. A migração do WPA1 para o WPA2, por outro lado, não pode ser realizada de maneira trivial. Atualmente, isto não é mais um problema, já que os equipamentos têm sido produzidos com suporte a WPA2.

## Outras ameaças à segurança em redes sem fio

Além dos ataques que exploram diretamente as vulnerabilidades encontradas no WEP e no WPA e permitem, principalmente, que chaves secretas sejam descobertas por agentes maliciosos, temos outras ameaças a redes sem fio como war driving, negação de serviço, spoofing, man in the middle, rogue APs, misconfigured APs, redes ad hoc, end point attacks, evil twin APs, deauthentication attacks e wireless phishing.

O war driving é a atividade de reconhecimento que costuma preceder boa parte dos ataques que são efetuados contra redes sem fio. O war driving pode ser definido como o ato de utilizar um carro para buscar diversas redes sem fio que estejam disponíveis, registrando a localização geográfica e as configurações de segurança de cada uma delas. De posse deste mapeamento, agentes maliciosos podem investir na invasão de redes sem fio que foram mapeadas. O war driving também pode ser utilizado com fins legítimos. O mesmo mapeamento pode ser realizado de forma que o nível de segurança das redes sem fio seja avaliado e possíveis medidas de proteção sejam tomadas. Existem variantes do war driving como o war walking, realizado a pé, e o war cycling, realizado com uma bicicleta.

Outro problema bastante comum é a negação de serviço. As redes sem fio IEEE 802.11 são naturalmente suscetíveis a negação de serviço, já que todos os usuários e redes compartilham e competem no mesmo espectro de frequência não licenciado. Desta forma, o espectro de frequência utilizado pelas redes IEEE 802.11 está sendo cada vez mais populado, o que traz queda na qualidade e maior risco de situações de negação de serviço. A utilização do IEEE 802.11n deve ajudar neste sentido, já que boa parte dos usuários vai migrar para a faixa de 5 GHz, que comporta melhor o grande volume de usuários.

Nas situações de negação de serviço causadas por agentes maliciosos, não há acesso indevido a informações, mas pode ocorrer a interrupção do funcionamento da rede. A maneira mais primária de realizar um ataque de negação de serviço é emitir sinais que causem interferência no sinal da rede sem fio. Porém, este tipo de ataque precisa de dispositivos com alta potência de transmissão e é facilmente rastreável. Como o objetivo dos atacantes é sustentar o ataque pelo maior tempo possível, estratégias que sejam facilmente rastreáveis não são adotadas.

Outra forma de realizar um ataque de negação de serviço aproveita o mecanismo de controle de acesso ao meio das redes IEEE 802.11. O controle de acesso ao meio do IEEE 802.11 permite que um emissor reserve um canal para realizar a transmissão de um pacote durante 0,033 segundos. Se o atacante conseguir transmitir 30 pacotes por segundo, a rede pode ser totalmente ocupada por ele. É relevante observar que o atacante precisa ter permissão de acesso na rede sem fio atacada para enviar estes pacotes.

Uma forma mais sofisticada de negação de serviço é conhecida como Random Packet Destruction e pode ser executada sem que o atacante precise de permissão para transmitir pacotes na rede, além de não ser facilmente rastreável. O ataque se baseia na geração de sinais de interferência por períodos muitos curtos de tempo,

destruindo uma parte dos pacotes que estão sendo transmitidos na rede atacada. Mesmo não destruindo todos os pacotes, este ataque pode causar a degradação de serviços sensíveis a latência como VoIP ou transmissão de vídeos.

Outra ameaça à segurança das redes sem fio é o spoofing, que é normalmente realizado após o atacante explorar vulnerabilidades encontradas nos protocolos de segurança como o WEP e o WPA1. No spoofing, o atacante envia pacotes fingindo ser outra entidade presente na rede, como uma estação cliente ou um AP. A partir do spoofing, o atacante pode realizar outras ações maliciosas. Um exemplo é o ataque de authentication. Neste ataque, o agente malicioso finge ser um determinado cliente e requisita a sua desconexão do AP. A partir disso, todos os pacotes enviados pelo cliente verdadeiro passam a ser descartados pelo AP até que ele se autentique novamente. O ataque man in the middle também é uma possível consequência de um ataque de deauthentication. Após o ataque de deauthentication, quando o cliente tentar se autenticar novamente, o agente malicioso pode fingir que é o AP. Ao fim do processo de autenticação, o agente malicioso vai estar apto a receber todos os pacotes enviados pelo cliente que foi enganado.

Há diferentes ameaças que envolvem diretamente os APs (ver **Nota do DevMan 5**). Eles podem ser instalados nas redes corporativas sem a devida autorização da administração da rede, se tornando um ponto de vulnerabilidade, pois não estão sob o controle das mesmas políticas de segurança que o restante da rede. APs mal configurados também podem representar riscos à segurança das redes. No início, os APs eram configurados individualmente e manualmente, o que trazia maiores riscos de erros na configuração. Atualmente, já existem ferramentas que permitem a gerência centralizada da configuração de diversos APs em uma mesma rede, diminuindo o risco de má configuração. Mesmo assim é necessário sempre manter-se alerta, pois novas tecnologias trazem novidades como priorização de tráfego e reserva de recursos para aplicações sensíveis a latência, demandando operações de configuração com a qual os operadores não estão acostumados.



### Nota do DevMan 5

#### Rogue AP

O AP inserido na rede corporativa sem o conhecimento da administração é conhecido como rogue AP.

Temos também situações nas quais APs implantados por agentes mal intencionados podem divulgar um SSID (*Service Set Identifier*) igual ao de um AP legítimo, fazendo com que usuários se conectem a este AP fraudulento. Este tipo de ataque é comum e pode ser facilitado por ferramentas que permitem que o atacante escute o canal de forma a ver em quais SSIDs os clientes próximos estão se conectando. Depois que os clientes se conectam, os endereços de DNS e default gateway fornecidos pelo AP falso (também denominado evil twin) são utilizados para que o tráfego do cliente seja direcionado pela rede do atacante e ataques de man in the

middle sejam realizados. Neste caso, também podem ser realizados ataques do tipo phishing, pois o agente malicioso pode, por exemplo, levar um cliente a acessar sites falsos de bancos. A melhor saída para este tipo de ataque é utilizar o WPA-Enterprise com servidores de autenticação como o RADIUS.

As redes ad hoc também são um problema para os administradores de rede, pois elas podem ser estabelecidas entre duas estações cliente, desviando-se dos controles de segurança estabelecidos na rede onde estes usuários estão. Em ambientes que utilizam o Windows 7, este tipo de situação é mais provável pois o sistema operacional da Microsoft facilita o estabelecimento de redes ad hoc. Uma possível solução para bloquear a construção destas redes ad hoc é a utilização de Wireless Intrusion Prevention Systems. Estes sistemas monitoram os pacotes que estão trafegando pela rede e bloqueiam comportamentos inadequados.

Com a evolução dos mecanismos de segurança que garantem privacidade e integridade às conexões sem fio em redes IEEE 802.11, os atacantes têm tentado explorar vulnerabilidades presentes nos computadores dos clientes. Eles exploram, por exemplo, defeitos e vulnerabilidades em drivers de placas IEEE 802.11. Os fabricantes das placas tentam solucionar estes problemas lançando patches de correção das vulnerabilidades. Entretanto, estes patches nem sempre são distribuídos juntamente com os patches de atualização dos sistemas operacionais e os clientes acabam não realizando todas as atualizações necessárias. Uma solução possível é utilizar ferramentas como o Wi-FiDenum para rastrear as vulnerabilidades existentes nos dispositivos que estão presentes em uma rede IEEE 802.11.

## Conclusão

As redes sem fio, em especial as redes IEEE 802.11, se tornaram bastante populares por dispensarem a instalação de cabeamento e permitirem a mobilidade dos usuários. Pesquisas mostram que a adoção de redes sem fio deve crescer ainda mais nos próximos anos, principalmente devido à explosão nas vendas de dispositivos móveis como tablets e smartphones. O problema neste cenário é que a praticidade do acesso sem fio vem acompanhada de vulnerabilidades com relação à segurança da informação.

As redes IEEE 802.11 têm demonstrado a preocupação dos especialistas com questões de segurança desde seu primeiro padrão, que incluía o WEP. Atualmente, temos o WPA2, que utiliza técnicas de criptografia e autenticação sofisticadas o suficiente para oferecer um bom nível de segurança às redes IEEE 802.11.

Diferentemente do que ocorreu com o WEP e o WPA1, não houve ainda descobertas de grandes falhas de segurança no WPA2. Juntamente ao WPA2, podem ser utilizados outros dispositivos de segurança como os sistemas de detecção de intrusão para redes wireless e scanners de vulnerabilidades em drivers de placas IEEE 802.11. É importante observar que as soluções de segurança podem ser adotadas sem comprometer a facilidade com que o usuário legítimo acessa a rede sem fio. A figura do servidor de autenticação, por exemplo, facilita o processo de distribuição de chaves e autorização de acesso em redes sem fio de grandes corporações. Desta forma, é possível afirmar que as redes IEEE 802.11 estão aptas a oferecer a praticidade das comunicações sem fio com a segurança desejada pelos usuários.



**Bruno Bogaz Zarpelão**

*brunozarpelao@gmail.com*

Bacharel em Ciência da Computação pela Universidade Estadual de Londrina (UEL) e doutor em Engenharia Elétrica pela Universidade Estadual de Campinas (UNICAMP). Atualmente é pesquisador no Laboratório de Redes de Comunicações da Faculdade de Engenharia Elétrica

e de Computação da UNICAMP. Atua também como pesquisador associado no Next Generation Networks and Applications Group (NetGNA) da Universidade da Beira Interior em Portugal e como professor do curso de especialização em Redes de Computadores da UEL. Possui experiência de sete anos em pesquisa e desenvolvimento de soluções para gerência de redes de computadores, governo eletrônico e cidades digitais.



## Artigo Practical attacks against WEP and WPA, escrito por Martin Beck e Erick Tews

<http://dl.aircrack-ng.org/breakingwepandwpa.pdf>



## Artigo Top Ten Wi-Fi Security Threats, escrito por Lisa Phifer

<http://www.esecurityplanet.com/print/views/article.php/3869221/Top-Ten-WiFi-Security-Threats.htm>

## Cisco Visual Networking Index: Global Mobile Data Traffic Forecast

[http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white\\_paper\\_c11-520862.html](http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html)

## Projetos de redes sem fio municipais

<http://www.muniwireless.com>

## The State of Wi-Fi Security

[https://www.wi-fi.org/sites/default/files/uploads/files/wp\\_State\\_of\\_Wi-Fi\\_Security\\_20120125.pdf](https://www.wi-fi.org/sites/default/files/uploads/files/wp_State_of_Wi-Fi_Security_20120125.pdf)

# Monitorando ativos de rede e serviços

## Saiba como controlar sua infraestrutura de TI

**E**m uma infraestrutura de TI, a função dos equipamentos de rede é imprescindível para o correto funcionamento dos outros componentes. Se a comunicação de rede não estiver funcionando corretamente, os serviços podem se comportar de maneira inesperada e com certeza gerarão problemas.

Neste artigo abordaremos como monitorar os equipamentos de rede de forma abrangente para que o administrador possa agir antes do problema acontecer.

Para monitorar equipamentos de rede podemos fazer uso de recursos disponíveis nos próprios equipamentos. Mas para que você consiga monitorar o equipamento é preciso que o mesmo tenha suporte ao protocolo SNMP (Simple Network Management Protocol). Atualmente, a grande maioria dos equipamentos já possui esta funcionalidade. No entanto, é importante citar que a grande maioria dos equipamentos não possui as configurações necessárias para o monitoramento definidas como padrão, então consulte o administrador de rede ou veja no manual do equipamento como habilitar tais configurações.

O SNMP é um protocolo exclusivo para gerenciar ativos de rede. Ele é quem gerencia as informações do equipamento, ou seja, o protocolo é responsável pela coleta e disponibilização dos valores. Com o protocolo SNMP você pode ler e gravar informações. Porém, para fins de monitoramento, utiliza-se apenas o recurso de leitura das informações, pois quem coleta e grava os valores é o próprio sistema do equipamento. Neste artigo, utilizaremos a versão 3 do protocolo SNMP, que exige autenticação por usuário e senha. Portanto, certifique-se que exista um usuário específico para o monitoramento e apenas com permissão de leitura.

Para que o protocolo saiba o que coletar e onde ele deve gravar cada valor, disponibiliza-se a MIB (Management Information Base). Esta base de dados fornecerá vários identificadores de objetos (OID) que nos dirão a quem pertence aquele valor. Por exemplo: o identificador de objeto 1.3.6.1.4.1.789.1.2.1.4 se refere ao valor de CPU idle (ociosa) de alguns switches Cisco. Certifique-se que esta base de informações foi carregada no equipamento

### Resumo DevMan

#### *De que se trata o artigo:*

Nesse artigo abordaremos aspectos de monitoramento de ativos de redes utilizando as principais ferramentas open source. Perceberemos que estas ferramentas são ricas em recursos, possuindo diferentes abordagens que garantem o total controle da infraestrutura de redes.

#### *Em que situação o tema é útil:*

Esse artigo é interessante para todas as empresas que utilizam infraestrutura de TI. Com o conteúdo aqui exposto consegue-se garantir que a infraestrutura de redes esteja funcional. Veremos que através das abordagens apresentadas neste artigo o administrador poderá controlar o crescimento da utilização da infraestrutura e prever seu crescimento antes da ocorrência de problemas.

#### *Monitorando ativos de rede e serviços:*

Neste artigo discutiremos o monitoramento de ativos de redes utilizando o protocolo SNMP e abordaremos alguns aspectos em servidores Linux como, por exemplo, instalar módulos através do CPAN e gerenciar pacotes RPM. Explicaremos como funciona o monitoramento de uma infraestrutura de redes e demonstraremos algumas configurações. Para isso, utilizaremos pacotes do Linux para simular os equipamentos de rede e criaremos o monitoramento baseado em Nagios.

que se quer monitorar. Como cada equipamento possui sua própria MIB, deve vir junto com o equipamento ou estar disponível no site do fabricante.

A MIB de estatísticas de utilização da rede é a mais comum entre todos os ativos de rede. Ela é organizada através de índices chamados ifIndex. Durante o monitoramento, cada porta do seu ativo de rede receberá um ID sequencial para que você consiga localizar a informação de cada porta separadamente.

forma ativa de monitoramento do SNMP é feita através de requisições que podem ser GetRequest, GetNextRequest ou GetBulkRequest. Para minimizar o impacto gerado pelo monitoramento, utilize o GetRequest, pois se utilizadas muitas requisições GetNextRequest ou poucas requisições GetBulkRequest, você consumirá muito recurso do ativo de rede e isto não é bom.

Além da forma ativa de monitoramento, o SNMP também disponibiliza o SNMPTrap. Um trap consiste no envio de um identificador (OID) quando ocorrer determinado evento no equipamento. Por exemplo: para o evento de queda de conectividade (link down) e restabelecimento de conectividade (link up), é enviado um identificador X para o servidor de monitoramento. Dado esta informação, entende-se que o servidor de monitoramento precisará de um sistema que entenda o que significa este identificador e envie a mensagem para o sistema de monitoramento.

## SNMP Trap Translator

O SNMP Trap Translator ou SNMPTT é um projeto de código aberto para integrar o daemon snmptrapd com o sistema de monitoramento Nagios (explicado mais adiante).

O projeto consiste em diversos scripts Perl (ler **Nota do DevMan 1**) para realizar diversas tarefas, entre elas a de ser o traphandle, ou seja, quem recebe a saída do daemon snmptrapd e as traduz para o Nagios. O daemon snmptrapd é um binário do pacote net-snmp do Linux.



## Nota do DevMan 1

### Perl

Conforme definido no portal [www.perl.org.br](http://www.perl.org.br), Perl é uma linguagem de programação estável e multiplataforma, usada em aplicações de missão crítica em todos os setores, e tem sido bastante usada para desenvolver aplicações web de todos os tipos.

## Nagios

O Nagios é definido como sendo um conjunto de projetos para monitoramento de infraestrutura de TI. Estes projetos são: Nagios core, Nagios plug-ins, Nagios Frontends e Nagios Config Tools. Por se tratar de quatro projetos, percebe-se que o Nagios é um grande e completo sistema de monitoramento, além de ser totalmente open source. Existe também uma versão do Nagios paga chamada Nagios XI. Porém, não iremos considerar esta versão neste artigo.

## Nagios Core

O Nagios core é o projeto inicial do Nagios e consiste no sistema de monitoramento em si, ou seja, o sistema responsável por todas as funções de monitorar. Como exemplos de atividades desempenhadas pelo Nagios Core, temos: gerenciar a agenda de monitoramento, realizar o monitoramento ativo, gerar alertas, etc.

Existem diversas formas de se implementar o Nagios, tudo vai depender de quantos servidores serão monitorados e qual o nível de detalhamento de monitoramento que você quer. Se você tiver até 100 servidores, você pode utilizar o NRPE (Nagios Remote Plugin Executor) e fazer o monitoramento ativo no mesmo servidor que gera os alarmes. Porém, se sua infraestrutura for maior que isso ou tiver probabilidade de crescer, recomenda-se que você utilize o collectd para coletar os valores nos servidores monitorados,

crie um serviço no Nagios para ler os valores do collectd e gere os alarmes. É importante também separar a função de acompanhar a situação da rede da função de realizar o monitoramento ativo. Assim, recomenda-se ter servidores Nagios específicos para fazer o monitoramento ativo, pois com o aumento da quantidade de servidores, a concorrência entre os serviços de monitoramento poderá trazer problemas.

## Tutorial



## Hands on

A partir de agora, trabalharemos em um estudo de caso considerando o monitoramento de ativos de rede nas formas ativa e passiva.

O sistema operacional que utilizaremos será o Mac OS X 10.6.8 e o Parallels Desktop para criar a máquina virtual do laboratório. Durante a instalação, escolha o tipo *minimal*, ou seja, não será personalizado nenhum pacote do sistema operacional.

Na seção de downloads da Infra Magazine disponibilizamos dois arquivos para instalação do sistema operacional. Se o usuário possuir o software *kickstart*, deve utilizar o arquivo *anaconda-ks.cfg*, senão deve usar o *rpm-qa.txt*. Se o usuário seguir esses passos, é importante que o sistema operacional tenha os mesmos pacotes instalados conforme o arquivo *rpm-qa.txt*.

A **Tabela 1** apresenta as informações para instalação e configuração do servidor.

| Nome     | Sistema operacional | Proc | Mem | Endereço IP  | Máscara de rede |
|----------|---------------------|------|-----|--------------|-----------------|
| Nagios01 | CentOS 6.3 x86_64   | 1    | 1G  | 10.211.55.11 | 255.255.255.240 |

Tabela 1. Informação da máquina virtual

## Banco de dados

Para este estudo de caso, utilizaremos um banco de dados para algumas funcionalidades. Assim, instale um banco de dados no *nagios01*. Ambas as ferramentas de monitoramento que faremos uso suportam o MySQL e o PostgreSQL. Para instalar o banco de dados MySQL, execute o comando `yum install -y mysql-server`, e para instalar o PostgreSQL, execute o comando `yum install -y postgresql84-server postgresql84-plperl`.

## SELinux

O SELinux é uma facilidade de segurança disponível no CentOS. Recomenda-se que você deixe-o habilitado. Para que tudo funcione corretamente com o SELinux, você deve ativá-lo conforme os passos descritos na **Listagem 1**.

Caso você tenha problemas para utilizar o SELinux, desabilite-o com o comando `setenforce 0`.

## Nagios

Como o foco deste estudo de caso não é a instalação do Nagios (mas seu uso), utilizaremos um RPM (*RPM Package Manager*)

fornecido pelo repositório do Fedora (distribuição Linux para a comunidade da Red Hat). Recomenda-se que o Nagios seja compilado pelo próprio administrador.

Para proceder com a instalação do Nagios, execute a sequência de comandos apresentados na **Listagem 2**.

#### Listagem 1. Habilitando o módulo SELinux.

```
module mypol 1.0;

require {
    type snmpd_t;
    type var_spool_t;
    class dir { write add_name };
    class file { write ioctl create open getattr };
}

#===== snmpd_t =====
#!!!! This avc is allowed in the current policy

allow snmpd_t var_spool_t:dir { write add_name };
allow snmpd_t var_spool_t:file { ioctl getattr };
#!!!! This avc is allowed in the current policy

allow snmpd_t var_spool_t:file { write create open };
```

#### Listagem 2. Comandos para instalação do Nagios.

```
# rpm -ihv http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-7.noarch.rpm
# yum install -y httpd
# chkconfig httpd on
# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
# service iptables save
# yum install -y nagios nagios-plugins-all
# htpasswd -c /etc/nagios/htpasswd.users nagiosadmin
# chkconfig nagios on
```

O comando *rpm* é utilizado para gerenciar pacotes RPM. Neste caso, instala-se o pacote do EPEL que adicionará o repositório do Fedora às configurações do *YUM*. Perceba que o pacote não está hospedado no servidor local, o *rpm* utiliza o protocolo HTTP para baixar o arquivo e depois segue o procedimento de instalação.

O comando *yum* é utilizado para gerenciar os pacotes do sistema operacional. Na **Listagem 2**, o empregamos para instalar o Apache HTTPD, Nagios e Nagios Plugins.

Na sequência, utilizamos o comando *iptables* para liberar a regra de *firewall* da porta 80 (HTTP). Em nosso exemplo não utilizaremos HTTPS. Portanto, não foi realizada a regra para a porta 443. Se você pretende usar SSL, crie a regra também para a porta 443, conforme o parâmetro *--dport* do comando *iptables*.

Já o comando *chkconfig* é utilizado para gerenciar os serviços que são iniciados no processo de inicialização do sistema operacional. O aproveitamos em nosso estudo para indicar que o Apache deve ser iniciado nos *run levels* padrões.

O script de inicialização do Nagios fornecido pelo pacote RPM utiliza o *sh* como Shell. Em nosso estudo, alteramos para ele adotar o *bash*. Para isso, informamos o comando *sed*.

Por fim, o comando *htpasswd* é um binário que foi instalado no pacote *httpd*. Com ele foi criada a autenticação do usuário *nagiosadmin* para o Apache (*htpasswd.users*).

## Monitoramento passivo

O monitoramento passivo de equipamentos de rede é feito através de *traps*. Trap é o resultado de um evento gerado no equipamento, sendo o mais conhecido o de perda e restabelecimento de conectividade da porta de rede. Quando conectamos o cabo de rede, o estado da porta é alterado de *down* para *up*. Este evento gera um trap com OID correspondente ao evento de *link up*. Quando desconectamos o cabo, o procedimento é o mesmo, mas trocam-se os estados.

## NetSNMP

O *snmptrapd* é o serviço que recebe os *traps* dos ativos de rede e realiza um *pipe* para o *script* do *SNMPTT*. Para utilizá-lo, execute a sequência de comandos da **Listagem 3** para instalar o pacote *Net-SNMP* com suporte ao Perl, pois conforme dito anteriormente, nossos plugins utilizam-se da linguagem de programação Perl.

## SNMPTT

O *SNMPTT* é o script que iniciará o tratamento do trap e enviará os dados coletados ao sistema de monitoramento Nagios. Como os scripts são escritos na linguagem Perl, precisamos instalar alguns plugins, e para isto faremos uso do CPAN. Sendo assim, execute o comando *cpan* e responda no para a pergunta “Are you ready for manual configuration? [yes]”. Em seguida, no shell do CPAN, digite *quit*. Feito isso, execute o comando *cpan* para que sejam realizadas as configurações iniciais do acesso ao CPAN. As configurações são muitas e não abordaremos neste artigo, pois não são necessárias para este exemplo.

Agora execute a sequência de comandos da **Listagem 4**, para instalar os módulos Perl necessários. Estes módulos são as bibliotecas necessárias para que os scripts funcionem.

#### Listagem 3. Comandos para instalação do NetSNMP.

```
# yum install -y net-snmp net-snmp-perl net-snmp-utils
# chkconfig snmptrapd on
# echo 'OPTIONS="-On -Oa -Lsd -p /var/run/snmptrapd.pid"'
>> /etc/sysconfig/snmptrapd
# service snmptrapd start
```

#### Listagem 4. Instalando módulos Perl.

```
# yum install -y perl-CPAN perl-Time-HiRes make
# perl -MCPAN -e 'install Perl::OSType, ExtUtils::MakeMaker'
# perl -MCPAN -e 'install Module::Build::Compat, Config::IniFiles'
Responda yes para confirmar a instalação dos módulos dependentes.
Basta apertar a tecla Enter, pois já é a resposta padrão.
```

Nosso próximo passo é instalar o *SNMPTT*. Para isso, execute a sequência de comandos da **Listagem 5**. O comando *groupadd* é utilizado para criar grupos e o comando *useradd* para criar usuários. Perceba que criamos o grupo *snmptt* e o usuário *snmptt* dentro desse grupo.

Após isso, utilizamos o *sed* para alterar os arquivos de inicialização do *SNMPTT*. Na sequência, o comando *mkdir* é especificado para criar diretórios. Criamos os diretórios para armazenar os logs e o *spool* do *SNMPTT*.

## Listagem 5. Comandos para instalação do SNMPPTT.

```
# yum install -y wget
# wget http://downloads.sourceforge.net/project/snmpptt/snmpptt/snmpptt_1.3/
snmpptt_1.3.tgz
# tar xzvf snmpptt_1.3.tgz
# cd snmpptt_1.3
# cp snmpptt.logrotate /etc/logrotate.d/snmpptt
# cp snmpptt-init.d /etc/init.d/snmpptt
# cp snmpptthandler /usr/sbin
# cp snmpptt /usr/sbin
# cp snmppttconvert /usr/sbin
# cp snmppttconvertmib /usr/sbin
# cp snmpptt.ini /etc/snmp/snmpptt.ini
# chkconfig --add snmpptt
# chkconfig snmpptt on
# groupadd snmpptt
# adduser -g snmpptt snmpptt
# sed -i "s/^\\snmp\\snmpptt.conf\\/etc\\snmp\\snmpptt.conf.if-mib/g" /etc/
snmp/snmpptt.ini
# sed -i "s/log_system_enable = 0/log_system_enable = 1/g" /etc/snmp/snmpptt.ini
# sed -i "s/^net_snmp_perl_enable = 0/net_snmp_perl_enable = 1/g" /etc/snmp/
snmpptt.ini
# mkdir /var/spool/snmpptt/
# mkdir /var/log/snmpptt/
# chown -R snmpptt: /var/spool/snmpptt/ /var/log/snmpptt /etc/snmp/snmpptt.ini
# chcon system_u:object_r:var_spool_t:s0 /var/spool/snmpptt
```

Em seguida, criamos os arquivos de logs em branco a partir do comando `touch`. Por fim, com o comando `chown`, alteramos o proprietário dos arquivos e diretórios. Perceba que definimos também o tempo de vida do log e a inicialização automática do serviço. Com isso, todas as configurações necessárias para o serviço do SNMPPTT estão finalizadas.

Para finalizar a configuração do monitoramento via traps, devemos criar o arquivo de tradução da MIB para o SNMPPTT utilizando o script `snmppttconvertmib`. Este é responsável por ler o arquivo `MIB` e gerar o arquivo de configuração do SNMPPTT. O parâmetro `out` é onde o arquivo do SNMPPTT será gerado, e o parâmetro `exec` é o `script` que envia o resultado ao Nagios. O `script` do parâmetro `exec` (`submit_check_result`) é provido pelo pacote do Nagios.

```
# snmppttconvertmib --in=/usr/share/snmp/mibs/IF-MIB.txt --out=/etc/snmp/snmpptt.conf.
if-mib --exec="/usr/lib64/nagios/plugins/eventhandlers/submit_check_result $r TRAP 2"
```

Para facilitar o uso, cada plugin do Nagios trabalha com códigos de saída. Se o código de saída for 0, significa que o plugin foi executado e o serviço está normal; se for 1, significa que você deve ficar alerta (WARNING); se for 2, significa que existe um problema no ambiente; e se for 3, significa que ocorreu algum erro na execução do plugin.

O número 2 após a palavra `TRAP` é o código de saída para o Nagios. Em nosso estudo de caso, estamos utilizando apenas o Trap de perda de conectividade, portanto o código de saída será 2, que significa `CRITICAL`. Quando um link perde a conectividade, significa que existe um problema no ambiente, portanto o código de retorno deve ser 2.

## SNMPTrapd

O `snmptrapd` é o daemon que recebe o trap do ativo de rede e o envia para que o SNMPPTT faça a tradução e depois a envie ao Nagios. Na seção de downloads da revista você encontrará o arquivo `snmptrapd.conf`. Copie-o para a pasta `/etc/snmp`. Já o arquivo `TRAP-TEST-MIB.txt` deve ser copiado para o diretório das MIBs (`/usr/share/snmp/mibs/`). Por último, copie o script `submit_check_result` para `/usr/lib64/nagios/plugins/eventhandlers/` e execute o comando `chmod +x /usr/lib64/nagios/plugins/eventhandlers/submit_check_result`.

O comando a seguir adiciona uma linha no arquivo de configuração do Nagios para criar o serviço do Trap:

```
# echo 'cfg_file=/etc/nagios/objects/snmp.cfg' >> /etc/nagios/nagios.cfg
```

Na seção de downloads da Infra Magazine você também encontrará o arquivo `snmp.cfg`. Copie-o para o diretório `/etc/nagios/objects/`. Este arquivo de configuração representa a configuração do serviço do Nagios para receber os traps.

O comando a seguir adiciona a configuração do serviço do Trap no servidor localhost. Com isto, o Nagios passa a monitorar o serviço de traps para o servidor localhost.

```
# echo -e "define service{\n\tuse\t\ttsnmptrap-service\n\tthost_name\tlocalhost\n\t}" >>
/etc/nagios/objects/localhost.cfg
```

Agora execute a sequência de comandos da Listagem 6 para iniciar os serviços configurados.

## Listagem 6. Iniciando os serviços configurados.

```
# service snmpptt start
# service snmptrapd start
# service nagios start
# service httpd start
```

Com os serviços rodando, todas as configurações e dependências estão prontas. Agora execute o próximo comando para enviar um trap idêntico ao que o ativo de rede enviará, a fim de verificarmos o funcionamento do monitoramento.

```
# snmptrap -v 1 -c public localhost TRAP-TEST-MIB::demotraps localhost 2 0 "IF-
MIB::ifIndex i 1
```

Atenção: a resolução de nome precisa estar idêntica a localhost. Portanto, a linha dos hosts para localhost deve estar conforme o trecho:

```
127.0.0.1 localhost localhost.localdomain
```

Após a execução desse comando, o `snmptrapd` receberá um trap que será encaminhado para o script `snmptraphandler`. O script fará a tradução e utilizará o script `submit_check_result` para enviar o resultado para o `nagios.cmd`. Após a escrita do resultado no `nagios.cmd`, o alarme surgirá no monitoramento.

Prosseguindo com a configuração dos nossos serviços de monitoramento, destacaremos um item muito importante e que muitas vezes não é considerado: a porta do switch ou roteador. É muito importante que se monitore o tráfego da porta de rede além do seu status de conectividade, ou seja, não basta saber se a porta está UP ou DOWN, precisamos verificar também qual é o tamanho do tráfego. A recomendação é que o tráfego fique entre 60% e 70% da capacidade da porta.

Para esta etapa de nosso estudo de caso, faremos uso do memcached. Este é um banco de dados não relacional volátil, ou seja, é um banco de dados baseado em chave e valor armazenado em memória. Assim, execute o comando a seguir para instalar o memcached:

```
# yum install -y memcached
```

Para facilitar a configuração de nosso exemplo, utilizaremos o daemon SNMPD para representar o papel do ativo de rede. Como o daemon possui a mesma MIB do ativo de rede, aplicam-se as mesmas configurações. Deste modo, execute o comando a seguir para criar um acesso apenas de leitura para o service:

```
# echo 'rocommunity public' > /etc/snmp/snmpd.conf
```

Feito isso, execute os comandos a seguir para iniciar o serviço e testá-lo:

```
# service snmpd start  
# snmpwalk -v 1 -c public localhost system
```

No arquivo `snmp.cfg` baixado anteriormente, existe a configuração do serviço para monitorar se a porta está Up ou Down via SNMP com `ifIndex 1`. Agora, você precisa configurar um service para cada porta. Portanto, execute o comando abaixo para configurar o monitoramento da porta 1 para o host localhost:

```
# echo -e "define service{\n\tuse\tlink-status-1\n\tthost_name\tlocalhost\n\t}" >> /etc/nagios/objects/localhost.cfg
```

Para completar o monitoramento, é preciso monitorar o tráfego das portas dos ativos de redes. Para isso, novamente na seção de downloads da Infra Magazine, disponibiliza-se um script para coletar os dados e disponibilizá-los no memcached que configuramos anteriormente. O nome do arquivo é `get_bandwidth.pl`. Grave-o no diretório `/opt/`.

O arquivo de configuração para o script `get_bandwidth.pl` deve ser criado pelo administrador em `/etc/get_bandwidth.conf`.

O conteúdo deste arquivo é separado por “;”, sendo o primeiro campo o nome do servidor ou endereço IP, o segundo a community SNMP e os próximos campos são os índices das portas a coletar. Exemplo: `localhost;public;1;2;3`.

Como apresentado no comando a seguir, nota-se que o script precisa da permissão de execução e da lib do Perl para o memcached:

```
# chmod +x /opt/get_bandwidth.pl  
# yum install -y perl-Cache-Memcached
```

Para finalizar, colocamos o script no cron para coletar os valores a cada minuto:

```
# echo "*/1 * * * * /opt/get_bandwidth.pl" >> /var/spool/cron/root  
# service crond restart
```

## Conclusão

O monitoramento de redes é essencial para a infraestrutura de TI. Deste modo, visando segurança e confiabilidade, deve-se aplicar o monitoramento ativo e passivo para garantir o seu correto funcionamento.

Baseado em soluções open source, mostramos neste artigo como é possível monitorar de forma eficiente e eficaz toda a infraestrutura da rede, garantindo assim o bom funcionamento de todos os outros componentes.

Agora seu ambiente já está pronto para receber as notificações de perda e reestabelecimento de conectividade, além de qualquer outro trap enviado pelo ativo de rede. Com as configurações efetuadas, também é possível monitorar ativamente o status de cada porta.



### Thiago Nache

[thiagonbcarvalho@gmail.com](mailto:thiagonbcarvalho@gmail.com)

Atua na área de infraestrutura há mais de 8 anos, tem grande experiência em sistema de alta disponibilidade e alta performance. Kursou ensino médio técnico em processamento de dados, graduação em Tecnologia em Redes de Computadores na FIAP e possui certificações Red Hat e ITIL. Tem experiência em empresas de grande porte.



### Site do Collectd

<http://collectd.org>

### Wiki do Collectd

[http://collectd.org/wiki/index.php/Main\\_Page](http://collectd.org/wiki/index.php/Main_Page)

### Documentação do Nagios

<http://library.nagios.com/library/products/nagioscore/manuals/>

### Site do CPAN

<http://www.cpan.org>



# As novidades do Windows Server 2012

## O que esperar da nova versão?

A Microsoft anunciou em abril de 2012 o nome da próxima versão do Windows Server, que será o Windows Server 2012. No lançamento de produtos, a Microsoft sempre traz grandes novidades:

- No Windows Server 2000, o Active Directory foi o grande marco, visto que no Windows NT não existia Active Directory (ler **Nota do DevMan 1**);
- O Windows Server 2003 apresentou significativas melhoras no Active Directory, além de incluir novas funcionalidades;
- No Windows Server 2008, o grande marco foi a plataforma de virtualização Hyper-V (ler **Nota do DevMan 2**).



### Nota do DevMan 1

O Active Directory é um serviço de diretório, o qual identifica todos os recursos disponíveis em uma rede mantendo informações sobre estes dispositivos (contas de usuários, grupos, computadores, recursos, políticas de segurança etc.) em um banco de dados. Além disso, torna estes recursos disponíveis para usuários e aplicações.

Afinal, o que é Diretório? Um diretório nada mais é do que um cadastro ou, melhor ainda, um banco de dados com informações sobre usuários, senhas e outros elementos necessários ao funcionamento de um sistema, quer seja um conjunto de aplicações no Mainframe, um grupo de servidores da rede local, o sistema de e-mail ou outro sistema qualquer.



### Nota do DevMan 2

A virtualização permite particionar um único sistema computacional em vários outros denominados de máquinas virtuais. Cada máquina virtual oferece um ambiente completo muito similar a uma máquina física. Com isso, cada máquina virtual pode ter seu próprio sistema operacional, aplicativos e serviços de rede (Internet). É possível ainda interconectar (virtualmente) cada uma dessas máquinas através de interfaces de redes, switches, roteadores e firewalls virtuais.

Para o Windows Server 2012, o grande marco é uma plataforma estruturada para trabalhar com computação em nuvem. Além disso, teremos também a nova console conforme demonstrado na **Figura 1**. O objetivo é estabelecer uma console única entre os produtos, ou seja, a console do Windows Server 2012 será similar à console do

## Resumo DevMan

### De que se trata o artigo:

Neste artigo apresentaremos as novas funcionalidades e recursos do Windows Server 2012, bem como as melhorias introduzidas em relação ao Windows Server 2008 R2. Serão abordadas as diversas novidades do Hyper-V 3.0. Também destacamos as novidades no Active Directory, BitLocker, DHCP, WSUS, BranchCache, DirectAccess. Serão descritos também os inúmeros aspectos que fazem desta nova versão do Windows Server uma plataforma estruturada para trabalhar e suportar computação em nuvem.

### Em que situação o tema é útil:

Os fatores apresentados neste artigo serão úteis para esclarecer as novidades presentes no Windows Server 2012, bem como suas melhorias em relação ao Windows Server 2008 R2.

### As novidades do Windows Server 2012:

A Microsoft irá lançar o Windows Server 2012 para atender às demandas mais preocupantes do departamento de Tecnologia da Informação das empresas: custo e agilidade nos processos. Através do Windows Server 2012 será possível implementar computação em nuvem dentro das empresas, ou seja, nuvem privada. Neste contexto, destacaremos neste artigo as principais novidades do Windows Server 2012.

Windows 8, Windows Phone e até mesmo à console do Xbox 360. Neste contexto, este artigo tem como objetivo apresentar os recursos e as novas funcionalidades introduzidas no Windows Server 2012. O Windows Server 2012 é um produto que irá oferecer um melhor suporte para trabalhar com computação na nuvem, seja ela pública ou privada. Além disso, inúmeras novidades foram adicionadas neste novo produto como, por exemplo, a nova console do Server Manager, Hyper-V 3.0, Active Directory Clone, DirectAccess, DHCP, BranchCache, entre outras novidades. Vamos conhecer algumas delas a partir de agora.

### Server Manager

Uma das principais novidades do Server Manager é a console apresentada na **Figura 2**. Nesta console foi adicionado um

Dashboard que permite uma visualização de todas as funções instaladas no servidor.

O Server Manager ainda permite adicionar e criar grupos de outros servidores da rede, ou seja, gerenciar outros servidores, instalar e remover funções a partir de uma única console.

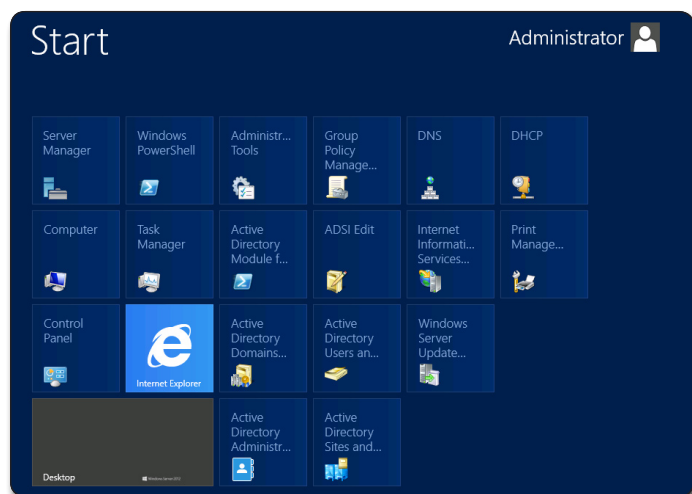


Figura 1. Console do Windows Server 2012 Release Candidate

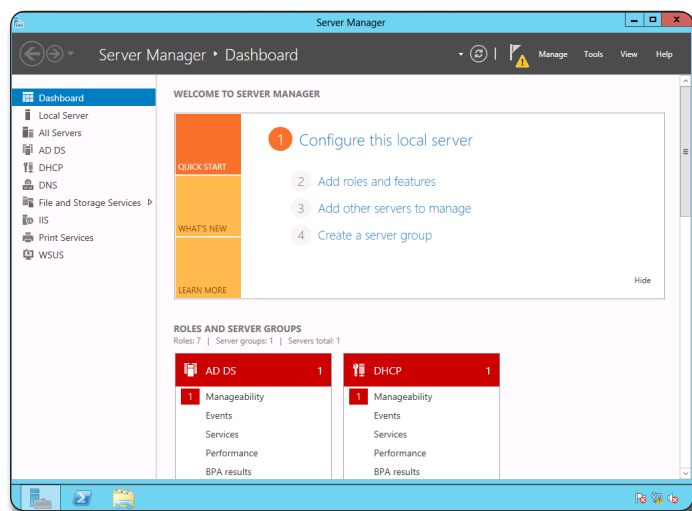


Figura 2. Console Server Manager

## Hyper-V 3.0

O Windows Server 2012 disponibilizou uma nova versão do Hyper-V, agora conhecido como Hyper-V 3.0. O Hyper-V é a tecnologia que virtualiza hardware para proporcionar um ambiente no qual você possa executar vários sistemas operacionais ao mesmo tempo em um computador físico. Ele permite que você crie e gerencie máquinas virtuais e seus recursos, sendo cada máquina virtual um recurso isolado, ou seja, um sistema de computador virtualizado que pode executar seu próprio sistema operacional.

Seguem algumas melhorias desta nova versão:

- Processadores lógicos do host: 160;

- Memória do host: 2 TB;
- Processadores virtuais: 2048;
- Máquinas virtuais por host: 1024;
- Processadores por VM: 32;
- Memória por VM: 1 TB;
- VMs em cluster: 4000.

## Hyper-V Cliente

Uma das grandes novidades do Hyper-V 3.0 é estar disponível em uma versão para desktop, ou seja, o Hyper-V está disponível no Windows 8. Assim, agora é possível virtualizar sistemas operacionais no Windows para desktop. Entretanto, vale informar que não são todas as funcionalidades que estão disponíveis na versão para Windows Cliente.

Os seguintes recursos não estão disponíveis no Hyper-V 3.0 no Windows 8:

- Remote FX capability to virtualize GPUs: Permite virtualizar uma instância do Graphical Processing Unit (GPU) em várias máquinas virtuais do Windows 7. Isso proporciona VMs com acesso à GPU física, permitindo aceleração por hardware para cenários gráficos de alta performance, tais como renderização 3D e jogos;
- Live VM migration: Permite mover uma máquina virtual em execução de um host físico de origem para um host físico de destino o mais rápido possível, ou seja, a máquina virtual está sendo acessada enquanto ocorre a movimentação entre os hosts;
- Hyper-V Replica: Permite mover uma máquina virtual em execução de um host físico de origem para um host físico de destino através somente do cabo de rede, ou seja, a máquina virtual é transferida para outro host sem a necessidade de uma área comum de armazenamento;
- SR-IOV networking: Permite que máquinas virtuais acessem diretamente a placa de rede que dá suporte ao single-root I/O virtualization (SR-IOV). Isto diminui a latência da rede e maximiza o throughput da rede;
- Synthetic fibre channel: Permite acesso a recursos de armazenamento em alta velocidade, ou seja, cargas de trabalho e aplicativos que exigem acesso direto ao armazenamento baseado em canais de fibra.

## Memória dinâmica

Novidades referentes à memória dinâmica incluem suporte para configuração de memória mínima e de memória de paginação, que é uma técnica de gerenciamento de memória para fornecer uma experiência segura para a reinicialização de máquinas virtuais configuradas com pouca memória de inicialização.

Estas mudanças irão ajudar a melhorar a utilização do hardware, tornando-o mais prático para executar mais máquinas virtuais em um único computador físico ao mesmo tempo. Desta forma, recursos de memória podem ser alocados para máquinas virtuais de forma mais eficiente, uma vez que você pode configurar uma

máquina virtual com o mínimo de memória de inicialização sem ter que planejar a memória suficiente para reiniciar a máquina virtual.

## Módulo do Hyper-V para Windows PowerShell

O módulo do Hyper-V para Windows PowerShell inclui mais de 160 cmdlets para gerenciar o Hyper-V, máquinas virtuais e discos rígidos virtuais. A disponibilidade de built-in Hyper-V cmdlets torna mais fácil automatizar várias operações. Além disso, os nomes dos cmdlets são semelhantes aos de outros cmdlets do Windows PowerShell (usando verbos como 'Get' e 'Set'), tornando mais fácil para usuários familiarizados com o Windows PowerShell aprender a usar os novos cmdlets.

## Hyper-V Replica

Esta é uma das melhores novidades. Este recurso permite replicar as máquinas virtuais entre sistemas de armazenamento, clusters e entre localidades para proporcionar a continuidade do negócio e a recuperação de desastres. Ou seja, esta característica torna mais fácil e menos dispendioso o planejamento e implementação de soluções de continuidade de negócios e recuperação de desastres para suas máquinas virtuais.

## Importação de máquinas virtuais

Algumas melhorias foram implementadas no processo de importação de máquinas virtuais. Com a nova versão é possível, por exemplo, importar uma máquina virtual somente com a cópia do arquivo de VHD (Virtual Hard Disk).

## Live Migration

Agora é possível realizar uma migração a quente em um ambiente sem cluster, bem como executar mais de uma migração em tempo real ao mesmo tempo. Estas melhorias oferecem maior flexibilidade na movimentação de uma máquina virtual em execução, tornando mais fácil e mais rápido executar migrações a quente. Enfim, agora só com um cabo de rede é possível realizar o Live migration, sem a dependência de storage e cluster.

## Monitoração de recursos

Outra novidade importante é monitorar dados sobre o processador físico, memória, armazenamento e uso da rede por máquinas virtuais específicas. Com esta nova facilidade, poderemos determinar o uso de recursos específicos de máquinas virtuais e usar esses dados para, por exemplo: realizar o planejamento de capacidade, monitorar o consumo por diferentes unidades de negócios ou clientes, ou para capturar os dados necessários para ajudar a redistribuir os custos da gestão de uma carga de trabalho. Enfim, podemos configurar uma máquina virtual e medir, periodicamente, o processador físico, memória, armazenamento e uso da rede.

## Maior escalabilidade e melhor resiliência

Com certeza esta versão do Hyper-V oferece significativamente maior capacidade de computação e recursos de armazenamento,

além de melhorar o tratamento de erros de hardware. Esses recursos ajudam a garantir a configuração de máquinas virtuais de alto desempenho para suportar cargas de trabalho que podem precisar ser incrementadas de forma significativa.

Um dos grandes diferenciais é o computador que executa o Hyper-V. Este pode ser configurado com até 160 processadores lógicos e 2 Terabytes (TB) de memória. As máquinas virtuais podem ser configuradas com 32 processadores virtuais e 1 TB de memória. Além disso, o tratamento melhorado de erros de hardware aumenta a resiliência e estabilidade do ambiente de virtualização (ler **Nota do DevMan 3**).



### Nota do DevMan 3

Resiliência é a capacidade do ambiente virtualizado se recuperar normalmente de situações de alta sobrecarga onde há um aumento de processamento. Desta forma, permite que o ambiente possa alocar de forma eficaz todos os recursos disponíveis, criando assim ambientes resistentes que possam se recuperar destas situações.

## Autorização simplificada

O grupo de administradores Hyper-V foi introduzido e implementado como um grupo de segurança local. Desta forma, este grupo pode reduzir o número de usuários que pertencem ao grupo Administradores local, proporcionando aos usuários acesso ao Hyper-V.

## SR-IOV

Outra grande novidade é atribuir uma placa de rede que suporte single-root I/O Virtualization (SR-IOV) diretamente para uma máquina virtual. Assim, o uso de SR-IOV maximiza o throughput da rede, minimizando a latência da rede, bem como a sobrecarga de CPU necessária para processar o tráfego da rede.

## Migração de Storage (armazenamento)

A migração de armazenamento é uma excelente notícia, pois facilita muito a migração, ou seja, mover os discos rígidos virtuais usados por uma máquina virtual para outro armazenamento físico diferente enquanto a máquina virtual permanece em execução. Com isso, esta nova funcionalidade torna mais fácil gerenciar os subsistemas de armazenamento físicos usados por máquinas virtuais. Isto faz com que não seja mais necessário ter uma máquina virtual off-line para fazer a migração de discos rígidos.

## Armazenamento em compartilhamentos SMB2

O Hyper-V agora suporta o uso de compartilhamentos SMB2 para oferecer armazenamento para máquinas virtuais. Esse novo recurso oferece uma nova maneira de fornecer máquinas virtuais com armazenamento compartilhado sem o uso de um Storage Area Network (SAN) – ler **Nota do DevMan 4**.

Você pode especificar um compartilhamento de arquivos como o local de armazenamento para máquinas virtuais.



## Nota do DevMan 4

### Storage Area Network

Storage Area Network (SAN) é uma rede de armazenamento dedicada que oferece acesso a informações com alta velocidade de leitura e gravação. As SANs são usadas principalmente para unir dispositivos de armazenamentos como array de discos, ficando acessíveis a servidores, e estes dispositivos aparecem como se estivessem conectados localmente ao sistema operacional. Uma SAN normalmente tem sua própria rede de dispositivos de armazenamento que geralmente são acessíveis através da rede por meio dos dispositivos tradicionais.

## Virtual Fibre Channel

Esta nova funcionalidade permite que você conecte diretamente ao armazenamento Fibre Channel a partir do sistema operacional que é executado em uma máquina virtual (ler **Nota do DevMan 5**). Esta característica torna possível virtualizar cargas de trabalho e aplicativos que exigem acesso direto ao armazenamento baseado em canais de fibra. Também torna possível configurar cluster diretamente no sistema operacional da máquina virtual, ou seja, cluster entre máquinas virtuais utilizando Fibre Channel no sistema operacional da máquina virtual para armazenamento direto no storage.



## Nota do DevMan 5

Fibre Channel é a arquitetura mais utilizada para implementações de SANs. Trata-se de um padrão tecnológico alternativo à Ethernet, que permite a transferência de dados de um nó para outro nó da rede em velocidades extremamente altas. Implementações atuais podem atingir taxas de transferência de dados de 10Gbps ou mais e alcançar distâncias de até 10 km quando a fibra ótica é utilizada como o meio físico.

## Formato de disco rígido virtual

O novo formato foi introduzido para atender às necessidades em evolução e tirar proveito das inovações em hardware de armazenamento. O novo formato aumenta o tamanho máximo de armazenamento por disco rígido virtual, bem como melhora a estabilidade e eficácia desses discos.

O novo formato de disco rígido virtual (VHDX) suporta até 64 Terabytes de armazenamento. Ele também oferece proteção embutida contra a corrupção decorrente de falhas de energia e evita a degradação do desempenho em alguns discos de grande setor físico.

## Snapshots de máquinas virtuais

Snapshot é a técnica que permite salvar o estado da máquina virtual no momento desejado. Nessa nova versão do Windows Server o snapshot também foi melhorado. Agora, depois que um snapshot foi excluído, o espaço de armazenamento que antes ficava bloqueado agora é disponibilizado enquanto a máquina virtual está executando. Deste modo, já não é necessário desligar ou colocar a máquina virtual em um estado salvo para recuperar o espaço de armazenamento.

## Virtual NUMA

A topologia virtual Non-Uniform Memory Access (NUMA) está disponível para o sistema operacional em uma máquina virtual.

O recurso NUMA permite um processador acessar sua memória local diretamente, otimizando com isso o desempenho de aplicações e sistemas operacionais.

## Switch virtual

A arquitetura do switch virtual foi atualizada para fornecer uma estrutura aberta, permitindo que terceiros adicionem novas funcionalidades ao switch virtual. Essa alteração permite que os parceiros da Microsoft estendam o switch virtual, oferecendo novas funcionalidades tais como o monitoramento, encaminhamento e filtragem.

## Dynamic Host Configuration Protocol (DHCP)

No Windows Server 2012, como já foi possível observar até aqui, foram adicionadas novidades significativas. A **Figura 3** exemplifica a console do DHCP. Direcionando o foco do artigo para este recurso, a partir de agora analisaremos algumas das suas novidades introduzidas no Windows Server 2012.

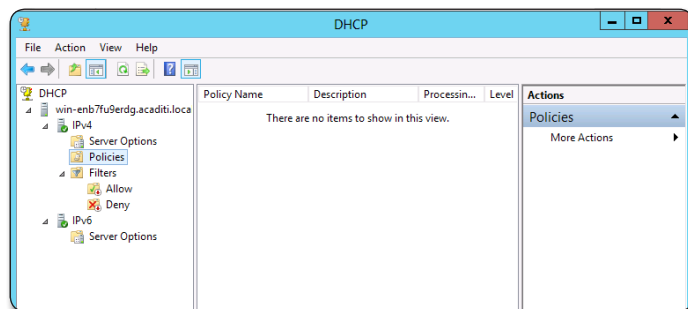


Figura 3. Console do Dynamic Host Configuration Protocol (DHCP)

## DHCP Policy Based Assignment

Agora é possível atribuir políticas baseadas em assignment (PBA), o que permite ao administrador agrupar clientes DHCP por atributos específicos baseados em campos contidos no pacote de solicitação de cliente DHCP. Esta característica permite a administração direcionada e um maior controle dos parâmetros de configuração fornecidos para dispositivos de rede.

A necessidade de administração centralizada de endereços IP está aumentando devido ao crescimento da computação móvel, virtualização e dispositivos IP que continuam a consumir mais endereços.

## DHCP Failover

Outro recurso interessante é o DHCP Failover. Este permite aumentar a disponibilidade do serviço de DHCP. Nas versões anteriores era possível estabelecer uma alta disponibilidade do DHCP, mas agora ficou ainda mais fácil, ou seja, o DHCP Failover fornece a capacidade dos administradores implantarem um

serviço de DHCP em alta disponibilidade para suportar uma grande empresa.

Agora é possível que dois servidores DHCP entreguem endereços IP da mesma sub-rede, ou seja, dois servidores DHCP entregando IP no mesmo intervalo de IPs, proporcionando, deste modo, alta disponibilidade para o serviço de DHCP. Os dois servidores DHCP replicam informações entre eles, permitindo um servidor assumir a responsabilidade pela manutenção de clientes para a sub-rede enquanto o outro não estiver disponível. Também é possível configurar failover em uma configuração de balanceamento de carga com pedidos de clientes distribuídos entre os dois servidores.

## Active Directory Domain Services

O Active Directory é o serviço de diretório que permite uma administração centralizada dos recursos da rede. No Windows Server 2012, ele recebeu significantes melhorias. Vamos a elas.

## Clone de controlador de Domínio

Uma grande novidade é o clone de controladores de domínio virtualizado. Com a clonagem de controlador de domínio virtualizado, os administradores podem agora promover um controlador de domínio virtual adicional rapidamente. Os administradores não têm repetidamente que implantar uma imagem do servidor Sysprep, promover o servidor a um controlador de domínio e em seguida completar os requisitos adicionais de configuração para cada controlador de domínio de réplica. Assim, o procedimento de adicionar controladores de domínio no mesmo domínio se tornou mais simples.

## Gerenciamento da topologia e replicação com Windows PowerShell

O Windows PowerShell para o Active Directory (AD) agora inclui suporte para replicação e gerenciamento de topologia. Deste modo, ele permite que seja feito o gerenciamento de replicação, trusts, sites, domínios e florestas, controladores de domínio e partições. Além disso, as ferramentas de gestão anteriores, como Active Directory e Repadmin.exe, agora estão disponíveis a partir do Windows PowerShell.

## BitLocker

O BitLocker é um recurso de segurança que permite a criptografia do sistema de arquivos, ou seja, é possível criptografar todo o C:. Com isso, ao ligar o computador, o BitLocker irá solicitar a senha para acesso, e somente com esta senha será possível descriptografar o disco e depois efetuar o login.

## Habilitar o BitLocker para volumes em cluster

No Windows Server 2012 o BitLocker Drive Encryption pode ser ligado por volumes em um cluster de failover, tanto no padrão de discos em cluster quanto no Cluster Shared Volumes (CSVs). Como o BitLocker criptografa no nível de volume, se um disco de cluster é composto por mais de um volume e você quiser

proteger todo o disco, a proteção do BitLocker deve ser ativada para cada volume do disco.

A seguir destacamos as novidades do BitLocker:

- É possível ativar e criptografar o disco antes da instalação do Windows, ou seja, agora, durante o processo de instalação do Windows, é possível criptografar o disco e depois instalar o Windows no disco já criptografado;
- Melhor velocidade para criptografar o disco;
- São oferecidos dois métodos de criptografia: criptografar somente o espaço utilizado ou criptografar todo o disco;
- Desbloqueio automático a partir da rede sem a necessidade de digitar o PIN. O Windows Server 2012 permite gerenciar dispositivos com o BitLocker habilitado, como desktops e servidores, ou seja, caso o dispositivo venha acessar um domínio com o BitLocker ativo, o Windows Server 2012 irá reconhecer que é um dispositivo confiável e irá desbloquear automaticamente, permitindo acesso ao computador;
- Mais fácil de implantar e gerir uma organização, possibilitando que o PIN do BitLocker possa ser alterado por um usuário padrão.

## Windows Server Update Services – WSUS

O WSUS já é bem conhecido pelo administrador de rede. No Windows Server 2012 também temos diversas novidades para ele. O WSUS agora é uma função de servidor embutida que pode ser adicionada e removida usando o Gerenciador do Servidor. Além desta mudança, há também algumas novas melhorias:

- Inclusão de cmdlets do Windows PowerShell para gerenciar as 10 mais importantes tarefas administrativas do WSUS;
- Melhoria de segurança com capacidade de SHA256 hash;
- Separação de cliente/servidor, novas versões do Windows Update Agent (WUA);
- Novo pacote de gerenciamento para o SCOM.

## Administração do WSUS usando o Windows PowerShell

Agora é possível gerenciar o WSUS através do PowerShell. Com isso, diversas atividades rotineiras serão automatizadas por meio de scripts. Ao expor as operações fundamentais do WSUS através do Windows PowerShell, os administradores de rede serão capazes de experimentar as seguintes vantagens:

- Aumento da produtividade;
- Redução da curva de aprendizado para novas ferramentas;
- Redução de erros.

Para que os administradores de sistema possam automatizar suas operações, eles precisam da linha de comando para realizar esta automação. O objetivo principal é facilitar a administração do WSUS, permitindo que os administradores de rede possam automatizar o dia-a-dia das operações. As tarefas que estão disponíveis para serem executadas com o uso de cmdlets do Windows PowerShell são:

- Listar computadores no ambiente WSUS;
- Adicionar um computador a um determinado grupo e criar esse grupo em tempo real;

- Obter uma atualização;
- Ver uma atualização;
- Aprovar uma atualização;
- Recusar uma atualização;
- Configurar tipo de classificação de atualização;
- Configurar tipo de produto de atualização;
- Configurar fonte de atualização;
- Executar o assistente de limpeza.

### Gerenciamento de Impressão

O gerenciamento de impressão no Windows Server 2012 permite que você compartilhe impressoras em uma rede e centralize o servidor de impressão e as tarefas de gerenciamento de rede da impressora usando o gerenciamento de impressão Microsoft Management Console (MMC). O gerenciamento de impressão permite, entre outras coisas, migrar servidores de impressão e implementar conexões de impressora usando a Diretiva de Grupo.

Além disso, os administradores também podem usar o novo módulo de gestão de impressão do PowerShell para gerenciar completamente uma infraestrutura de impressão a partir da linha de comando. Usar o poder e a flexibilidade do PowerShell permite que o administrador escreva scripts personalizados para gerenciar

e configurar a impressão sem usar a console de gerenciamento de impressão.

### BranchCache

Outro recurso que ganhou melhorias é o BranchCache. O serviço BranchCache reduz o uso de WAN (Wide Area Network) e o tempo necessário para usuários de filiais abrirem arquivos na rede. Ele nunca disponibiliza dados obsoletos e protege a segurança do seu conteúdo. O BranchCache foi introduzido pela primeira vez no Windows 7 e no Windows Server 2008 R2.

Destacamos aqui algumas novidades:

- O desempenho do banco de dados foi melhorado. O BranchCache agora usa o mecanismo extensível de armazenamento, o mesmo utilizado no Microsoft Exchange Server e Active Directory. Isso permite que um único servidor de cache hospedado possa atender às demandas de mais pessoas ao mesmo tempo usando o mesmo hardware. Também permite que um servidor de cache hospedado possa armazenar dados significativamente maiores (na ordem de Terabytes);
- Existem novas ferramentas e um novo modelo de implantação simplificado. Isso faz do BranchCache mais eficaz, mais fácil de implementar e simples de gerenciar;

# DÊ UM SALTO EM CONHECIMENTO!



Acesse o maior portal para desenvolvedores da América Latina!

**17**  
mil  
posts

**280**  
mil  
cadastrados

**5**  
milhões de  
page-views  
por mês

- O BranchCache não requer configuração em todos os escritórios. A implantação se tornou simplificada porque não há mais exigência de uma Diretiva de Grupo (GPO) separada para cada local. Apenas uma única GPO que contém um pequeno grupo de configurações é necessária para implantar BranchCache em organizações de qualquer tamanho;
- A configuração do computador do cliente é automática. Os clientes podem ser configurados através de Diretiva de Grupo (GPO) como modo cache distribuído por padrão. No entanto, em busca de um servidor de cache hospedado, e se for descoberto, os clientes automaticamente irão se autoconfigurar como cliente modo cache hospedado;
- Os dados de cache são mantidos criptografados e os servidores de cache hospedado não necessitam de certificados de servidor. A segurança do BranchCache oferece melhor criptografia de dados, proporcionando a segurança de dados sem a necessidade de uma infraestrutura de chave pública;
- O BranchCache fornece ferramentas para manipular dados e pré-carregar o conteúdo em locais remotos. Agora, você pode enviar conteúdo para filiais para que ele esteja imediatamente disponível quando o usuário solicitar o acesso. Isso permite que você possa distribuir o conteúdo durante os períodos de baixa utilização do link da WAN;
- O BranchCache agora possibilita administração com o Windows PowerShell e Windows Management Instrumentation (WMI).

## DirectAccess

O DirectAccess foi implementado no Windows Server 2008 R2 e no Windows Server 2012 ganhou algumas melhorias. Através do DirectAccess é possível realizar o acesso remoto a recursos da rede corporativa sem a necessidade de Virtual Private Network (VPN). Ele também fornece várias atualizações e melhorias para lidar com políticas de implantação e que proporcionam uma gestão simplificada.

Vejamos agora mais alguns benefícios e melhorias em relação ao DirectAccess do Windows 7:

- DirectAccess coexistente com o serviço de VPN do RRAS;
- Gerenciamento simplificado do DirectAccess para administradores de rede;
- Não é pré-requisito a implantação de PKI (Public Key Infrastructure) para implementar o DirectAccess;
- Suporte a NAT64 e DNS64 para acessar recursos IPv4;
- Simplificação da política de segurança de rede;
- Suporte de balanceamento de carga;
- Suporte para vários domínios;
- Integração com NAP (Network Access Protection);
- Suporte para OTP (autenticação baseada em token);
- Suporte para Server Core;
- Suporte a PowerShell.

## Conclusão

Tendo em vista as inúmeras novidades apresentadas neste artigo, podemos observar que esta nova versão do Windows Server irá mudar alguns procedimentos de administração e gerenciamento da infraestrutura de rede. Devemos estar preparados para estas novidades e, para isso, a certificação ajuda bastante. Caso você tenha uma certificação Microsoft Windows Server 2003 ou Windows Server 2008, lembre-se que agora será necessário atualizá-la.



**Josué Vidal**

*josuevidal2003@yahoo.com.br*

Trabalha na área de Tecnologia da Informação desde 2001, como consultor especializado na plataforma Microsoft, com experiência em infraestrutura e arquitetura de soluções de segurança, deployment e gerenciamento. Atualmente trabalha como consultor numa empresa de consultoria. Ministra palestras e webcasts nas comunidades de infraestrutura e é colunista da comunidade TechNet da Microsoft. Possui as seguintes certificações: MCP / MCSA / MCSE / MCTS / MCITP / MCT, MCITP – Windows Server 2008 R2, Virtualization Administrator, MCITP – Enterprise Administrator, MVP – Active Directory de 2009 a 2011.



# SNMP – Simple Network Management Protocol

## O padrão de gerência para redes IP

**A**s redes IP e seus serviços formam ambientes heterogêneos e complexos, nos quais conjuntos de software e hardware de diferentes fabricantes interagem constantemente para atender os usuários com rapidez e precisão. Atualmente, as redes IP são capazes de suportar diversos serviços simultâneos como acesso à Internet, telefonia, transmissão de vídeo, transmissão de TV, telemedicina, etc, e se tornaram essenciais para seus usuários. Problemas decorrentes de falhas ou paradas nestas redes representam perdas enormes. A solução para diminuir os riscos de perdas decorrentes de falhas nas redes é a adoção de práticas eficientes de gerência de redes, que incluem o monitoramento, a avaliação, a configuração e o controle de elementos de software e hardware. Dentro desta solução, o desafio passa a ser encontrar ferramentas que permitam a gerência de tantos elementos heterogêneos, com funções, propriedades e fabricantes diferentes. No caso do gerenciamento de redes IP, a resposta para este desafio é o SNMP (Simple Network Management Protocol).

O SNMP é um padrão de gerência de redes definido pelo IETF (Internet Engineering Task Force) que inclui um protocolo para comunicação entre estações de gerência e dispositivos gerenciados e especificações relacionadas à modelagem, à disponibilização e ao armazenamento de informações sobre os dispositivos gerenciados. O SNMP foi introduzido pelo IETF em 1988 por meio do RFC 1067 e sua principal característica era a simplicidade. Inicialmente, o SNMP foi tratado como uma solução provisória que seria substituída em longo prazo pelo CMIP (Common Management Information Protocol), que era mais complexo e sofisticado. Justamente por esta razão, tanto o SNMP quanto o CMIP são baseados no mesmo modelo gerente-agente. Entretanto, a indústria passou a adotar o SNMP massivamente,

### Resumo DevMan

#### *De que se trata o artigo:*

O SNMP (Simple Network Management Protocol) é um padrão de gerência para redes IP criado pelo IETF (Internet Engineering Task Force) em 1988. Ele opera segundo o modelo gerente-agente, no qual uma estação de gerência é responsável por controlar e monitorar recursos de diversos elementos da rede gerenciada por meio da interação com agentes implantados nos elementos desta rede. As informações gerenciais de cada um destes elementos são armazenadas em MIBs (Management Information Base), que são implantadas juntamente com os agentes nos elementos gerenciados.

#### *Em que situação o tema é útil:*

As redes IP têm sido utilizadas como plataforma para diversos serviços que envolvem a transmissão de dados, vídeo e voz. Desta forma, estas redes têm crescido em complexidade e importância, fazendo com que seja fundamental gerenciá-las com eficácia para garantir tranquilidade aos usuários e organizações. O SNMP é um dos principais pilares deste cenário, pois ele é amplamente adotado pelos fabricantes de equipamentos e definido pelo IETF como o padrão para gerência de redes IP.

#### *SNMP – Simple Network Management Protocol:*

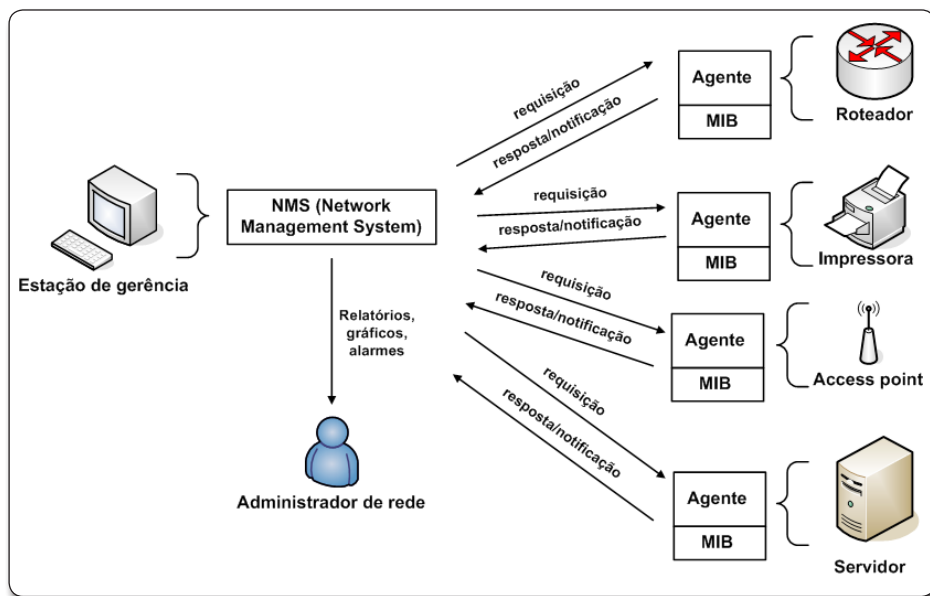
Para que as redes IP proporcionem a confiabilidade desejada pelos seus usuários, os administradores de rede devem implementar práticas eficazes de gerência. No caso das redes IP, o padrão para gerência é o SNMP. A primeira versão do SNMP foi lançada em 1988 e rapidamente adotada por grande parte dos fabricantes de equipamentos de rede. A segunda versão e a terceira versão foram lançadas em 1993 e em 1998, respectivamente, solucionando problemas de desempenho e segurança que ficaram evidentes na primeira versão, quando ela passou a ser usada em ambientes de rede mais complexos. Atualmente, o SNMP ainda é amplamente utilizado na gerência de redes IP e a perspectiva para o futuro é que este cenário permaneça, mesmo que a utilização do SNMP seja complementada pela adoção de outros padrões como o IPFIX.

justamente por sua simplicidade. Desta forma, em poucos anos, grande parte dos equipamentos de rede passaram a dar suporte ao SNMP, que passou a ser, de maneira concreta, um padrão de gerência. Ainda hoje, mais de duas décadas depois de sua criação, o SNMP continua sendo o padrão de gerência mais utilizado nas redes IP.

## Aspectos básicos do SNMP

O padrão SNMP é baseado no modelo gerente-agente, ilustrado na **Figura 1**. Primeiramente, temos a estação de gerência com um NMS (Network Management System) implantado. O NMS é responsável por reunir os dados coletados sobre a rede monitorada e apresentar ao administrador de rede. Para que o administrador compreenda melhor o que está ocorrendo com a rede, é desejável que o NMS seja capaz de gerar relatórios e gráficos sobre os dados coletados na rede. Por meio do NMS, o administrador também pode enviar comandos de forma a configurar parâmetros de funcionamento da rede. Por fim, o NMS repassa ao administrador de rede alarmes que o notificam sobre a ocorrência de eventos importantes como interrupções, falhas, falta de energia elétrica, etc. Uma única estação de gerência pode ser utilizada para monitorar vários elementos na rede. Em resumo, o NMS e a estação de gerência são a interface de controle entre o administrador e a rede que está sendo monitorada.

Do outro lado da arquitetura, temos agentes que são implantados nos dispositivos gerenciados. Cada agente é responsável por coletar os dados sobre o elemento gerenciado e armazená-los em uma base de dados local, conhecida como MIB (Management Information Base). Quando a estação de gerência requisita um determinado dado sobre o elemento gerenciado, o agente coleta este dado no respectivo objeto e responde ao gerente enviando o dado requisitado. O agente também é responsável por receber e processar requisições de alteração de dados da MIB enviadas pela estação de gerência e por enviar notificações sobre eventos



**Figura 1.** Visão geral da arquitetura gerente-agente

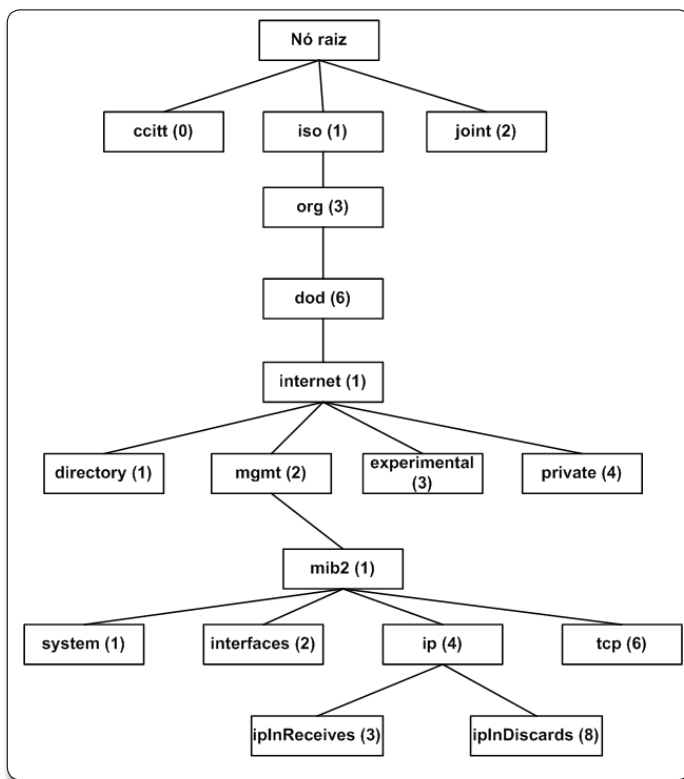
importantes para o gerente. Na MIB, são armazenadas informações como a quantidade de pacotes IP que ingressaram e partiram do equipamento, a quantidade de bytes que ingressaram e partiram das interfaces do equipamento, a quantidade de conexões TCP que estão ativas, quantos pacotes foram descartados, o nome do equipamento, a localização física do equipamento, etc.

As MIBs são organizadas de maneira hierárquica, segundo especificação documentada no RFC 1155 – Structure of Management Information. Os criadores do SNMP padronizaram a estruturação das informações de gerência na MIB para garantir que haveria interoperabilidade entre equipamentos de diferentes fabricantes. A **Figura 2** ilustra esta organização. No topo da organização hierárquica temos um nó raiz. Logo abaixo dele, temos três divisões principais: *ccitt*, *iso* e *joint*. Todos os nós posicionados hierarquicamente abaixo do nó *ccitt* (0) são administrados pela International Telegraph and Telephone Consultative Committee (CCITT). Os nós posicionados abaixo do nó *iso* (1) são administrados pela International Organization for Standardization (ISO). Por fim, os nós posicionados abaixo do nó *joint* (2) são administrados conjuntamente pela CCITT e pela ISO. Logo abaixo do nó *iso* (1), a ISO reservou um

nó a ser usado por outras organizações internacionais: o nó *org* (3). Abaixo do nó *org* (3), foi reservado um nó para o departamento de defesa dos Estados Unidos: o nó *dod* (6). O departamento de defesa, por sua vez, designou um nó para o Internet Activities Board (IAB), que foi nomeado de *internet* (1). Abaixo deste nó, temos quatro nós. Os principais são o *mgmt* (2), sob o qual são alocadas as informações aprovadas em documentos do IAB e o *private* (4), sob o qual podem ser incluídas informações definidas por fabricantes e desenvolvedores de equipamentos de rede. As informações incluídas abaixo do nó *mgmt* (2) devem estar presentes nas MIBs de todos os equipamentos que seguem o padrão SNMP.

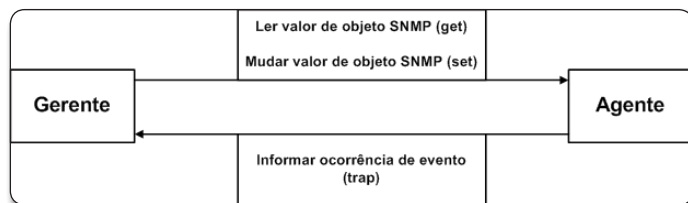
O último nível hierárquico da MIB traz os nós que realmente contêm dados sobre os equipamentos que estão sendo gerenciados. O termo apropriado para designar o nó que contém um dado sobre o equipamento gerenciado é objeto de gerência. O objeto *ipInReceives*, por exemplo, é responsável por registrar quantos pacotes IP ingressaram nas interfaces do equipamento monitorado até o momento. Há objetos para os mais diversos atributos, que cobrem desde medidas de desempenho como a quantidade de bytes e pacotes que ingressaram no equipamento até dados descritivos como

identificação e localização do equipamento. Para acessar um determinado objeto, seja para consultar ou para modificar seu conteúdo, o gerente deve informar ao agente toda a cadeia hierárquica de nós que leva ao objeto em questão. Desta forma, se o gerente deseja conhecer o valor atual do objeto *ipInReceives*, ele deve requisitar esta informação passando o identificador do objeto: 1.3.6.1.2.1.4.3. Cada número do identificador corresponde ao número de um nó que deve ser percorrido pelo agente na hierarquia da MIB para chegar ao objeto *ipInReceives*.



**Figura 2.** Estrutura hierárquica das MIBs

Para atender a questão da interação entre os gerentes e os agentes, o SNMP especifica um protocolo que opera na camada de aplicação da arquitetura TCP/IP. O protocolo utilizado na camada de transporte é o UDP, uma vez que este protocolo, ao contrário do TCP, dispensa o estabelecimento de conexão lógica entre os dois pontos finais de comunicação, proporcionando maior agilidade no transporte dos dados. A porta normalmente utilizada pelo SNMP é a 161. O SNMP disponibiliza três operações básicas de interação entre agente e gerente, conforme é apresentado na **Figura 3**. A operação *get* permite que o gerente requisite um determinado dado disponível na MIB do agente. A operação *set* é utilizada para que o gerente requisite que um novo valor seja atribuído a um determinado objeto presente na MIB do elemento gerenciado. Por fim, a operação *trap* permite que o agente notifique o gerente sobre a ocorrência de algum evento importante no elemento monitorado.



**Figura 3.** Operações básicas do SNMP

## SNMP v1

A primeira versão do padrão SNMP foi especificada em 1988 e ainda é amplamente utilizada. Sua principal característica é a simplicidade, que é a razão pela qual esta versão é tão popular. Os seguintes documentos especificam a primeira versão do SNMP:

- RFC 1155, que define como devem ser especificados os objetos contidos na MIB;
- RFC 1213, que define a MIB padrão para gerenciamento de redes IP, denominada MIB-II. Este documento especifica quais objetos de gerência devem estar presentes em uma MIB de um equipamento TCP/IP;
- RFC 1157, que define o protocolo utilizado para comunicação entre os gerentes e os agentes.

O SNMPv1 segue estritamente a arquitetura gerente-agente, na qual um único gerente é responsável por gerenciar todos os elementos da rede. O SNMPv1 permite as seguintes operações de interação entre o gerente e o agente:

- *GetRequest*: este comando é utilizado pelo gerente para requisitar o valor de um determinado objeto ao agente;
- *GetNextRequest*: este comando é uma variação do *GetRequest*, utilizada para percorrer a hierarquia da MIB;
- *SetRequest*: este comando permite que o gerente atribua um novo valor para um determinado objeto. O objeto *sysLocation*, por exemplo, é utilizado para que seja cadastrada a localização do equipamento gerenciado. Caso o equipamento seja mudado de lugar, o gerente pode enviar um comando *SetRequest* para o agente pedindo que a nova localização seja atribuída ao objeto *sysLocation*;
- *GetResponse*: é a resposta dada pelo agente para os comandos *GetRequest*, *GetNextRequest* e *SetRequest* enviados pelo gerente;
- *Trap*: é uma notificação enviada pelo agente para o gerente que informa a ocorrência de algum evento não esperado como uma falha em um enlace ou um *reboot* do equipamento.

Na primeira versão do SNMP, os objetos da MIB podem assumir os seguintes tipos:

- *NetworkAddress*: tipo utilizado para objetos que vão receber endereços IPv4;
- *Counter*: representa um número inteiro não negativo que pode ser incrementado, mas não pode ser decrementado. O objeto *ifInOctets*, que registra a quantidade de bytes que ingressaram em uma determinada interface, é do tipo *Counter*;

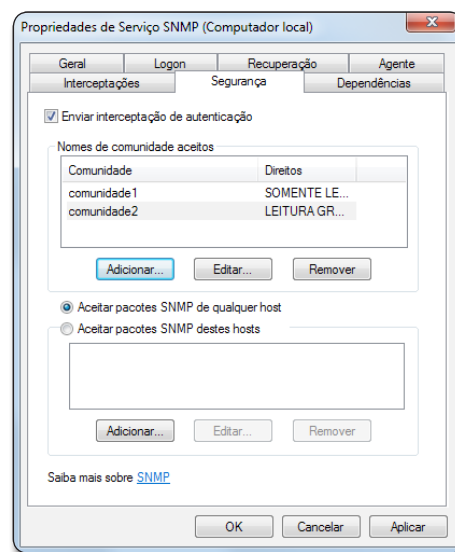
- *Gauge*: representa um número inteiro não negativo que pode ser incrementado ou decrementado. O objeto *tcpCurrEstab*, que registra a quantidade de conexões TCP ativas no momento, é do tipo *Gauge*;
- *Timeticks*: representa um inteiro não negativo que conta o tempo em centésimos de segundo a partir de um determinado momento. O objeto *sysUpTime*, que registra o tempo percorrido desde quando o equipamento foi ligado pela última vez, é do tipo *Timeticks*;
- *Opaque*: permite a atribuição de formatos binários específicos a um determinado objeto.

É importante fazer mais uma observação com relação a objetos do tipo *Counter*. Iniciantes em SNMP frequentemente apresentam dificuldade em tratar estes objetos para obter séries temporais, as quais são bastante importantes quando queremos acompanhar indicadores de desempenho. Ao medir o tráfego em bytes de uma determinada interface para construir a série temporal, por exemplo, o administrador pode desenvolver uma rotina que busque o valor do objeto *ifInOctets* de 10 em 10 segundos. O problema é que, muitas vezes, a rotina é programada para coletar o valor presente no objeto e assumir que ele representa o tráfego nos últimos 10 segundos, o que não é correto. Um objeto do tipo *Counter* é incrementado continuamente com os novos valores que são medidos. Se às 10:50:15 o *ifInOctets* retornou um valor igual a 1.200.560 bytes e às 10:50:25, em uma nova coleta, o *ifInOctets* retornou um valor igual a 1.300.000 bytes, isso quer dizer que 99.440 bytes ingressaram na interface no intervalo de 10 segundos. O gerente pode então registrar que, neste momento, o tráfego de ingresso da interface era de 9.944 bytes/s.

Uma das principais críticas realizadas ao SNMPv1 tem relação com a segurança. Para que um gerente possa acessar os dados de um agente, basta que ele conheça um atributo do agente denominado comunidade. O Windows 7, por exemplo, tem um agente SNMP implantado. Por meio deste agente, é possível que um gerente monitore diversos objetos do equipamento no qual o Windows 7 está instalado. A **Figura 4** mostra a tela na qual é possível configurar a segurança do agente SNMP no Windows 7. Podemos observar que há comunidades cadastradas com os respectivos direitos de acesso de cada uma delas. O gerente que fizer uma requisição ao agente utilizando a *comunidade1*, por exemplo, poderá apenas ler valores dos objetos do agente. Em resumo, para que um gerente envie uma requisição a um agente SNMP, ele precisa conhecer apenas o endereço IP do elemento monitorado, a porta que está sendo utilizada pelo serviço e o nome da comunidade. A solução para este problema de segurança está implantada no SNMPv3, que será apresentado mais adiante neste artigo.

## SNMP v2

A primeira versão do SNMP foi proposta no final da década de 80 como uma solução provisória que seria substituída posteriormente pelo CMIP. Entretanto, a transição entre o SNMP e o CMIP não seria simples, pois as especificações da SMI e da MIB não eram compatíveis com a estrutura complexa de objetos que havia sido projetada para o CMIP.



**Figura 4.** Tela de configuração de segurança de agente SNMPv1 no Windows 7

Quando o SNMP passou a ser utilizado em larga escala, alguns problemas começaram a ser detectados. O primeiro problema estava relacionado à segurança. Não era possível autenticar a estação que tinha enviado a requisição ao agente. O conceito de comunidade utilizado para prover segurança era bastante vulnerável. Como o tráfego SNMP não era cifrado, um atacante poderia interceptar os pacotes que trafegavam sem qualquer proteção e descobrir o nome da comunidade. De posse deste nome de comunidade, o atacante poderia passar a acessar o agente SNMP legitimamente. Consequentemente, muitos fabricantes não implementaram a operação *set* em seus equipamentos. Outro problema do SNMPv1 tinha relação com o desempenho. A busca por dados realizada por meio da operação *GetRequest* era ineficiente em situações nas quais o gerente necessitava de vários dados de uma única vez, já que era necessário enviar uma requisição para cada dado que se desejava buscar. Tendo em vista estes problemas e o fato de que o SNMP tinha deixado de ser um protocolo provisório para se tornar um padrão amplamente adotado por toda a indústria, os pesquisadores passaram a trabalhar em uma nova versão do SNMP, que foi lançada no início de 1993. Em 1996, o IETF determinou uma revisão no SNMPv2. As soluções de segurança especificadas em 1993 não haviam sido bem recebidas pela indústria e acabaram sendo eliminadas do SNMPv2 nesta revisão. A **Tabela 1** traz a lista de RFCs que compõem o SNMPv2 após a revisão de 1996.

Três mudanças principais foram, então, consolidadas no SNMPv2. A primeira delas é a comunicação entre gerentes. Foi criada uma nova operação denominada *InformRequest*, que permite que um gerente notifique outro gerente sobre eventos inesperados ou importantes que ocorreram em sua rede. A segunda principal mudança é a criação da operação *GetBulkRequest*, que permite que o gerente requisiute um grande volume de dados ao agente sem ter de enviar várias requisições. A terceira mudança tem relação com a SMI. Na SMIV1, o tipo *Counter* era limitado a 32 bits, causando

dificuldades principalmente quando ele era usado em objetos que monitoravam interfaces com tráfego intenso. Na SMIV2, foi introduzido um tipo *Counter* de 64 bits.

| Número do RFC | Título                                                                                            |
|---------------|---------------------------------------------------------------------------------------------------|
| 1901          | Introduction to Community-Based SNMPv2                                                            |
| 1902          | Structure of Management Information (SMI) for SNMPv2                                              |
| 1903          | Textual Conventions for SNMPv2                                                                    |
| 1904          | Conformance Statements for SNMPv2                                                                 |
| 1905          | Protocol Operations for SNMPv2                                                                    |
| 1906          | Transport Mappings for SNMPv2                                                                     |
| 1907          | Management Information Base for SNMPv2                                                            |
| 1908          | Coexistence Between Version 1 and Version 2 of the Internet-Standard Network Management Framework |

Tabela 1. RFCs do padrão SNMPv2

## SNMP v3

Após a revisão do SNMPv2 realizada em 1996, as discussões com relação à segurança do protocolo continuaram. No início de 1998, então, o IETF publicou os RFCs 2271, 2272, 2273, 2274 e 2275, que definem o SNMPv3. O principal destaque da versão 3 do SNMP é a introdução de uma infraestrutura completa de segurança. Além disso, na versão 3, o SNMP foi formalizado como uma arquitetura modular, que teve como objetivo facilitar a implementação do SNMP. Ao definir uma arquitetura modular para o SNMP, os pesquisadores permitiram que ele fosse implementado parcialmente pelos fabricantes, respeitando aqueles que desejam uma solução mais simples sem deixar de atender aqueles que necessitam de uma solução mais complexa.

A infraestrutura de segurança do SNMPv3 é composta por dois elementos: o USM (User-Based Security Model) e o VACM (View-Based Access Control Model).

O USM provê as seguintes funcionalidades:

- **Cifragem dos dados:** o algoritmo DES é utilizado para cifrar os dados que são transmitidos por meio do SNMP, garantindo que um agente mal intencionado, mesmo que intercepte os dados, não consiga interpretá-los;
- **Integridade da mensagem:** o USM permite que o destinatário de uma mensagem SNMP verifique se ela foi modificada no seu trajeto;
- **Autenticação:** o USM permite verificar se um indivíduo mal intencionado está fingindo ser um agente legítimo para enviar mensagens SNMP. Não há mais o conceito de comunidade como havia no SNMPv1. O usuário que pretende acessar um agente SNMP passa a ser identificado por um nome de usuário e senha.

O VACM, por sua vez, permite que seja controlado o acesso aos recursos gerenciados. Por meio do VACM, podem ser criados grupos que têm diferentes permissões de acesso aos objetos da MIB. Além disso, podem ser estabelecidos diferentes níveis de segurança para diferentes grupos que pretendem acessar os recursos gerenciados. Entre os níveis de segurança disponíveis temos:

- *No authentication and no privacy:* neste nível de segurança, as mensagens SNMP não são cifradas e nem autenticadas;
- *Authentication and no privacy:* neste nível de segurança, as mensagens SNMP são autenticadas, mas não são cifradas;
- *Authentication and privacy:* este é o nível de segurança mais alto, no qual as mensagens SNMP são cifradas e autenticadas.

## MIB-II

A MIB-II foi definida no RFC 1213 e é a MIB padrão para o gerenciamento de equipamentos TCP/IP. Esta MIB possui 171 objetos divididos em 10 grupos:

- *system:* agrupa objetos com informações gerais sobre o elemento que está sendo gerenciado;
- *interfaces:* agrupa objetos com informações sobre as interfaces do elemento que está sendo monitorado;
- *at (address translation):* agrupa objetos que trazem a tradução de endereços IP para endereços físicos
- *ip:* agrupa objetos que trazem informações relacionadas à operação do protocolo IP no elemento gerenciado;
- *icmp:* agrupa objetos que trazem informações relacionadas à operação do protocolo ICMP no elemento gerenciado;
- *tcp:* agrupa objetos que trazem informações relacionadas à operação do protocolo TCP no elemento gerenciado;
- *udp:* agrupa objetos que trazem informações relacionadas à operação do protocolo UDP no elemento gerenciado;
- *egp:* agrupa objetos que trazem informações relacionadas à operação do protocolo EGP no elemento gerenciado;
- *dot3:* agrupa objetos que trazem informações sobre os meios físicos de transmissão utilizados pelo elemento gerenciado;
- *snmp:* agrupa objetos que trazem informações relacionadas à operação do protocolo SNMP no elemento gerenciado.

Para evitar que o envio de requisições SNMP sobrecarregue a rede, o administrador de rede deve ser cauteloso quanto à quantidade de objetos SNMP que ele monitorará constantemente. Dentre os 171 objetos disponibilizados na MIB-II, é possível escolher objetos que sejam mais úteis no dia a dia do gerenciamento.

No grupo *system*, há objetos interessantes para apoiar a gerência de configuração da rede como o *sysDescr*, que armazena uma descrição do sistema monitorado, o *sysLocation*, que traz a localização do elemento, o *sysContact*, que traz o contato do responsável pelo elemento e o *sysName*, que armazena o nome do elemento de rede. Ainda no grupo *system*, há o objeto *sysUpTime*, que permite que o administrador de rede verifique há quanto tempo o sistema está operando sem interrupções. Ao monitorar este objeto continuamente, o administrador pode verificar qual é o tempo médio que o sistema opera sem interrupções. A diminuição neste tempo médio pode evidenciar defeitos no elemento monitorado, ajudando o administrador a tratar possíveis problemas de maneira preventiva.

No grupo *interfaces* também há diversos objetos úteis. O objeto *ifOperStatus* pode ser utilizado na detecção de falhas, pois permite que o administrador verifique se uma determinada interface está

operando ou não. Há, também, diversos objetos que podem ser interessantes para monitorar o volume de tráfego de uma determinada interface. Entre estes objetos temos o *ifInOctets*, que mostra a quantidade de bytes recebidos pela interface, o *ifOutOctets*, que mostra a quantidade de bytes que foram enviados pela interface, o *ifInDiscards*, que mostra a quantidade de pacotes ingressantes que foram descartados e o *ifOutDiscards*, que mostra a quantidade de pacotes que foram descartados ao deixar a interface.

O grupo *ip* também traz uma série de objetos que podem ser utilizados para gerência do tráfego no equipamento. O objeto *ipInReceives* mostra quantos pacotes IP foram entregues à camada de rede. O objeto *ipInDelivers* mostra quantos pacotes IP foram processados com sucesso na camada de rede e entregues à camada de transporte. O objeto *ipInDiscards*, por outro lado, mostra a quantidade de pacotes que não puderam ser processados pela camada de rede e foram descartados. Ainda há objetos que trazem informações mais detalhadas, como o *ipHdrErrors*, que mostra a quantidade de pacotes descartados por problemas com o cabeçalho e o *ipAddrErrors*, que traz a quantidade de pacotes descartados por problemas com o endereço IP do pacote.

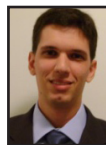
O grupo *tcp*, por sua vez, traz uma série de objetos com informações interessantes para a gerência do tráfego de pacotes TCP e das conexões TCP estabelecidas. Os objetos *tcpInSegs* e *tcpOutSegs* trazem a quantidade de segmentos TCP que ingressaram e deixaram o equipamento, respectivamente. Os objetos *tcpAttemptFails*, *tcpEstabResets* e *tcpRetransSegs* podem indicar a confiabilidade da rede. O *tcpAttemptFails* traz a quantidade de tentativas de conexão que falharam. O *tcpEstabResets* informa o número de conexões estabelecidas que foram reiniciadas. O *tcpRetransSegs* informa a quantidade de segmentos TCP que foram retransmitidos. Há ainda os objetos que monitoram o número de conexões ativas e passivas: *tcpActiveOpens* e *tcpPassiveOpens*. Um crescimento elevado e rápido no número de conexões estabelecidas em um elemento que contém um servidor HTTP, por exemplo, pode indicar uma tentativa de ataque de negação de serviço. O grupo *udp* também reúne objetos que podem prover informações importantes para a gerência do tráfego no elemento monitorado. Os objetos *udpInDatagrams* e *udpOutDatagrams* retornam a quantidade de datagramas UDP que ingressaram e deixaram o equipamento, respectivamente.

## Conclusão

As redes IP têm sido utilizadas para disponibilização de serviços diversificados e importantes para o cotidiano das pessoas e das organizações. Com isso, é fundamental que as redes IP sejam seguras, confiáveis e apresentem alta disponibilidade. Um dos

caminhos para que estes requisitos sejam atendidos é a adoção do padrão de gerência para redes IP, conhecido como SNMP.

O SNMP foi lançado pelo IETF em 1988. Sua principal característica era a simplicidade, pois o objetivo do IETF era que ele fosse implementado com rapidez pelos fabricantes que sentiam falta de um padrão para gerenciar as redes IP. O SNMP foi criado como uma solução provisória, que seria substituída em longo prazo pelo CMIP, um padrão construído pela ISO que era bem mais sofisticado e complexo que o SNMP. Contudo, o SNMP, desde o seu lançamento, foi amplamente adotado pelos fabricantes, que depois não demonstraram desejo de trocá-lo por outro padrão mais complexo como o CMIP. Desde então, foram lançadas mais duas versões do SNMP: a versão 2 foi lançada em 1993 e a versão 3 foi lançada em 1998. Ambas buscaram solucionar questões de desempenho e segurança que não haviam sido bem tratadas na versão 1 e que passaram a merecer mais atenção assim que o SNMP passou a ser adotado em massa pelos fabricantes de equipamentos e softwares de rede. Mesmo com o lançamento das versões 2 e 3, a simplicidade presente na versão 1 nunca deixou de ser a principal característica do SNMP, que ainda hoje é o protocolo de gerência mais utilizado em redes IP. A expectativa para o futuro é que, mesmo que seja acompanhado por outros padrões como o IPFIX (IP Flow Information Export), o SNMP continue sendo um dos principais pilares da gerência de redes IP.



**Bruno Bogaz Zarpelão**

*brunozarpelao@gmail.com*

Bacharel em Ciência da Computação pela Universidade Estadual de Londrina (UEL) e doutor em Engenharia Elétrica pela Universidade Estadual de Campinas (UNICAMP). Atualmente é pesquisador no Laboratório de Redes de Comunicações da Faculdade de Engenharia Elétrica e de Computação da UNICAMP. Atua também como pesquisador associado no Next Generation Networks and Applications Group (NetGNA) da Universidade da Beira Interior em Portugal e como professor do curso de especialização em Redes de Computadores da UEL. Possui experiência de sete anos em pesquisa e desenvolvimento de soluções para gerência de redes de computadores, governo eletrônico e cidades digitais.



## IETF Request for Comments (RFCs)

<http://www.ietf.org/rfc.html>

**Livro “SNMP, SNMPv2, SNMPv3 and RMON 1 and 2”, escrito por William Stallings**

**Editora Addison Wesley, 3.ª edição, 1999.**

**Livro “Essential SNMP”, escrito por Douglas Mauro e Kevin Schmidt**  
**Editora O’Reilly, 2.ª edição, 2001.**



# Introdução à CDN – Content Delivery Network

## O que é e que vantagens ela pode trazer para sua empresa

**C**ontent Delivery Networks (CDNs) estão em uso no mundo há mais de 15 anos e hoje aceleram aplicações para quase todos os usuários da internet, na maioria dos casos, sem que eles saibam. O resultado de tudo isso é que mais de 30% do tráfego da Internet passa pelas CDNs.

Entre 1995 e 1998, o conceito e algoritmo das CDNs foram criados em um projeto acadêmico no Massachusetts Institute of Technology (MIT). Desde então, a internet multiplicou sua importância e hoje ele está presente em todos os aspectos de nossas vidas. Com a demanda dos usuários por desempenho cada vez maior, a CDN tornou-se uma necessidade para grandes empresas na internet.

No Brasil, as CDNs ainda são relativamente desconhecidas do público, mas são largamente utilizadas em alguns ramos como e-commerce, mídia e entretenimento, portais de notícias e grandes empresas em geral, que querem proporcionar uma experiência superior aos clientes e usuários de seus websites. É sobre este assunto que abordaremos neste artigo.

### Mas o que é Content Delivery Network?

Antes de respondermos a essa pergunta, vamos entender um pouco mais sobre o problema de performance da internet.

A internet é uma rede de redes, e para ter acesso a ela, o usuário paga para um provedor de internet, que tem a sua própria rede. O provedor, por sua vez, precisa se conectar com as outras redes da internet, o que é feito através de contratos comerciais, os chamados contratos de peering. Esses contratos, e os termos monetários definidos neles, é o que determinam como o tráfego dos usuários da rede será roteado.

### Resumo DevMan

#### *De que se trata o artigo:*

Content Delivery Network é um grande sistema distribuído de servidores instalados em múltiplos datacenters ao redor do mundo. O objetivo principal das CDNs é prover distribuição de conteúdo online com alta performance, disponibilidade e segurança aos usuários finais.

#### *Em que situação o tema é útil:*

As Content Delivery Networks têm utilidade em diversas áreas: websites em geral (e-commerce, site de notícias etc.), aceleração de aplicações corporativas na internet (Internet Banking, sites B2B, Setor Público etc.), segurança de aplicações web e entrega de vídeo e downloads pela internet.

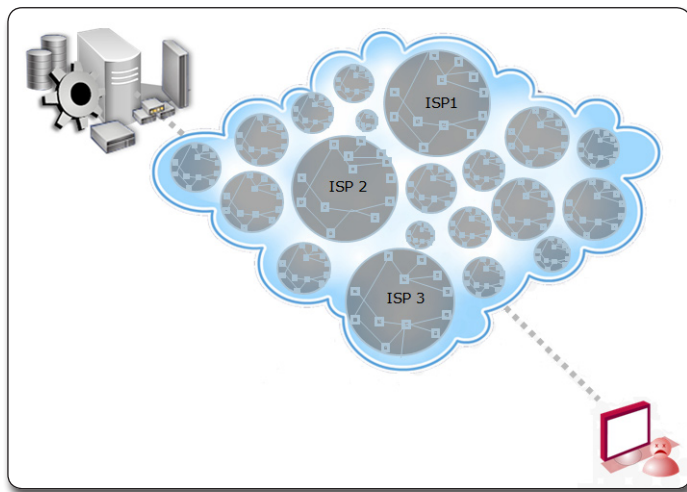
#### *Introdução à CDN – Content Delivery Network:*

Neste artigo serão apresentadas as principais características das CDNs – Content Delivery Networks. Será explicado como elas funcionam, assim como as vantagens técnicas e de negócios no uso desse tipo de rede. Também será apresentada uma comparação das CDNs tradicionais com Cloud Computing. Por fim, será analisado um estudo de caso da rede da Akamai e como ela funciona.

Portanto, além de o usuário poder estar topológica e fisicamente longe do servidor que ele pretende acessar, sua performance será impactada devido ao fato de que os roteadores estão programados para economizar dinheiro para as operadoras no caminho e não necessariamente para melhorar a performance da comunicação.

Esse problema é ainda mais intensificado no Brasil e na América Latina, onde as grandes operadoras fazem contratos de peering muito limitados, e uma grande parte da troca de conteúdo entre elas acontece em redes de interconexão nos Estados Unidos, já que o

custo para as operadoras se conectarem a essas redes é baixo e elas evitam trocar dados diretamente devido à concorrência. A **Figura 1** mostra uma representação mais realista e detalhada da internet e o caminho que os pacotes de dados devem percorrer para chegar do usuário final até o servidor de origem da aplicação.



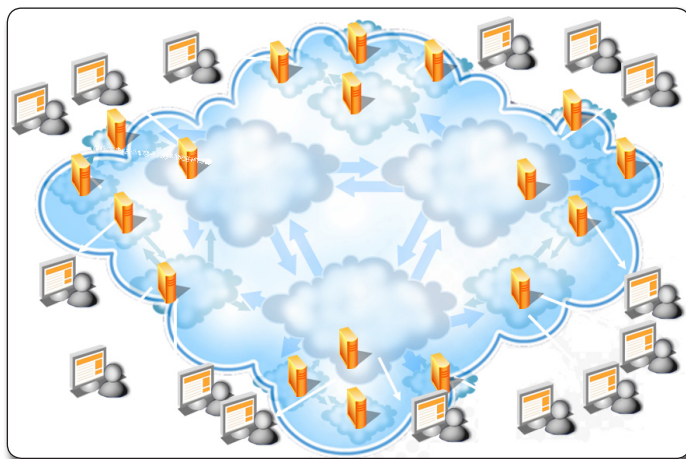
**Figura 1.** Distância e peering não otimizados geram performance insatisfatória

Além do problema de interesse financeiro, o BGP (*Border Gateway Protocol*), criado para uso nos roteadores da internet, não leva em consideração a carga de uma rota. Ou seja, mesmo que a rota esteja extremamente congestionada, o protocolo ainda enviará pacotes por aquele caminho, causando ainda mais congestionamento, perda de pacotes e piora da performance. Além disso, o algoritmo BGP ainda fica sujeito à perda de rotas acidentais ou, efetivamente, a roubos de rotas. Veja na seção **Links** um artigo explicando essa vulnerabilidade do BGP mais detalhadamente.

## Como a CDN resolve o problema de desempenho da internet?

Content Delivery Network é uma rede distribuída, com servidores hospedados dentro dos provedores de internet ao redor do mundo. Assim, quanto maior o número de servidores e mais distribuída for a rede, melhor a qualidade da CDN para os usuários finais (**Figura 2**). A ideia básica desta tecnologia é que o usuário é servido por um servidor próximo e, portanto, com latência, taxa de erros e reenvio muito menores. Para conteúdos transacionais ou individualizados, como um carrinho de compras ou um extrato de conta, o servidor da CDN ainda precisa buscar a informação no servidor de origem da aplicação, mas geralmente usando métodos otimizados para atravessar a internet, como uso de rotas alternativas e otimização da camada TCP.

Todo esse processo acontece de forma transparente para o usuário final, e normalmente é feito no nível de DNS. A empresa que contrata uma Content Delivery Network redireciona os usuários para o servidor de DNS da CDN via um registro **cname** (*canonical name* – ver **Nota do DevMan 1**). A partir daí, o DNS da CDN passa a ser o responsável por eleger o servidor com a melhor performance para servir àquele determinado usuário.



**Figura 2.** CDNs aproximam o usuário dos servidores



## Nota do DevMan 1

CNAME Record, ou Canonical Name Record, é um tipo de registro DNS que especifica que o domínio é um sinônimo de outro domínio. O registro mais comum de DNS é o registro A, que mapeia um hostname a um endereço IP. O registro CNAME mapeia um hostname a outro, permitindo a delegação da resolução do nome a outro servidor DNS.

## Vantagens para a empresa em usar uma CDN

As CDNs melhoram a performance das aplicações web para o usuário, mas o que uma empresa ganha em adotar uma solução como esta? Em suma, a empresa obtém benefícios como aumento de receita, redução de custos e otimização de investimento em tecnologia.

A seguir descrevemos essas vantagens com mais detalhes:

- **Melhor desempenho aumenta o uso do site e a receita.** Qualquer que seja o modelo de negócios da empresa, atrair e reter mais usuários sempre abre a possibilidade de maiores receitas. Para sites de e-commerce, a vantagem é a mais clara possível. Quanto mais satisfeito o usuário estiver, maior será o tempo que ele passará navegando pelo site e maior será a taxa de conversão desses usuários em vendas. A concorrência no mercado de e-commerce está muito acirrada no Brasil e cinco segundos que a página leva para carregar pode ser suficiente para que o usuário abra uma nova janela e busque o produto com a concorrência.

Para sites de mídia, entretenimento e notícias, a melhor performance aumenta, no mínimo, a receita com propaganda. Isso sem falar de sites com modelos de negócios onde os usuários pagam para ter acesso ao conteúdo. Nesse tipo de modelo, os usuários são ainda mais exigentes e não admitem um desempenho ruim. Um bom exemplo desse tipo de conteúdo pago são os sites de streaming de filmes e seriados. Como o usuário paga para assistir esse conteúdo, ele espera um serviço imediatamente disponível e com imagem e som de alta definição;

- **Escalabilidade.** As Content Delivery Networks proporcionam capacidade global sob demanda sem a necessidade de provisionamento exagerado ou de datacenters redundantes. A adoção

de uma solução de CDN permite à empresa atender os picos de acessos, sejam eles diários, semanais, mensais ou periódicos (por exemplo, período de vendas do Natal ou eventos esportivos). Essa escalabilidade é obtida sem a necessidade de hardware extra, que seria subutilizado posteriormente ao período de pico. Novamente, quanto maior e mais distribuída for a rede, mais escalável ela será;

- **Offload.** Cada conteúdo (imagem, JavaScript, HTML etc.) encontrado no cache do servidor da CDN significa um hit a menos no servidor de origem. Isso causa uma grande economia para a infraestrutura da empresa com banda de conexão, servidores, roteadores etc. Além disso, como o servidor de origem é acessado somente pelos servidores da CDN quando necessário, o número de conexões que eles precisam suportar é muito menor. Para tráfego HTTPS, em que uma grande quantidade de recursos é utilizada para criptografar e descriptografar o conteúdo, a CDN ainda provê um offload adicional dessas tarefas;

- **Disponibilidade.** Devido ao fato de ser uma rede distribuída e de grande escala, a CDN dificilmente fica indisponível. Inclusive, algumas CDNs possuem SLAs (*Service Level Agreement*) altíssimos para disponibilidade. No entanto, além da disponibilidade da rede em si, a CDN ainda melhora a disponibilidade do site de seus clientes. Como a CDN contém o cache do website, ainda que esse esteja indisponível em um determinado momento, os usuários ainda podem utilizá-lo sem problemas, desde que não sejam requisitadas partes transacionais do mesmo. Ainda assim, para essas partes, é possível criar mensagens amigáveis de erro, para que o usuário tente novamente mais tarde. Isso ajuda na proteção da marca e das receitas do site;

- **Redução de custos.** Além do offload mencionado acima proporcionar economia com investimento em infraestrutura, a adoção de CDN aumenta a utilização do canal de comunicação com o cliente mais barato para as companhias: a Internet. Empresas como bancos, provedoras de telefonia, utilidades, entre outras, têm diversos canais de atendimento ao cliente. Normalmente, pelo menos três: internet, telefônico e físico. O atendimento pela internet é sempre o que apresenta o menor custo para a empresa, porém, quando o website é muito lento, o usuário se cansa de esperar e acaba ligando ou indo a um posto de atendimento. Com um serviço de Content Delivery Network, a empresa pode diminuir o número de clientes que usam os canais mais caros e permite à empresa crescer sem a necessidade de novos investimentos em estrutura de atendimento;

- **Segurança.** Um dos tipos de ataques mais comuns a propriedades na internet atualmente é o DDoS – *Distributed Denial of Service*. Ele consiste em atacar um site de maneira distribuída com uma quantidade massiva de requisições com o intuito de “indisponibilizar” o sistema. Esse tipo de ataque ficou muito conhecido recentemente com a atividade do grupo Anonymous e similares.

Quando o site está em uma CDN, um ataque irá, na verdade, atingir à CDN. Entretanto, para alguns ataques, somente o fato de a CDN também ser distribuída já resolve o problema, já que cada

servidor absorve parte do tráfego. Mesmo assim, ainda que algum servidor da CDN venha a cair, a rede e o sistema como um todo continuará disponível para os usuários efetivos do sistema.

Além disso, a maioria das CDNs oferece outros serviços de segurança, como firewall de camada três e sete, tráfego via SSL, autenticação etc.

- **Adoção de ferramentas de trabalho.** No mundo atual, muitas empresas têm a sua equipe distribuída geograficamente. Desse modo, usuários espalhados pelo país e pelo mundo necessitam usar aplicações como se estivessem no escritório. Isso se torna ainda mais importante no cenário de SaaS (*Software como um Serviço*), em que a aplicação está hospedada em um provedor na nuvem e todos os usuários do sistema são “remotos”.

A utilização de Content Delivery Network para aceleração de aplicações web permite que as empresas consigam uma maior adoção de suas ferramentas entregues através da internet, melhorando os processos e aumentando a produtividade de seus funcionários.

## CDN é Cloud Computing?

Não exatamente. As CDNs têm algumas características de Cloud Computing, como: contratação como serviço (SaaS), recursos compartilhados e instalação e configuração na nuvem. Entretanto, as CDNs se diferenciam por não serem um substituto para o servidor de origem da aplicação. A ideia principal da CDN é acelerar a aplicação na internet e, portanto, usar a mesma infraestrutura já existente de forma mais inteligente. O Cloud Computing, por outro lado, oferece às empresas a alternativa de hospedar uma aplicação web em datacenters na nuvem, ao invés de próprios.

Inclusive, as CDNs funcionam muito bem com Cloud Computing: SaaS (*Software as a Service*), PaaS (*Platform as a Service*) e IaaS (*Infrastructure as a Service*). Em uma arquitetura conjunta, por exemplo, a aplicação é hospedada em um provedor de Cloud Computing e acelerada com uma Content Delivery Network.

## Estudo de caso: como funciona a solução da Akamai

Para entender a arquitetura de uma CDN com mais detalhes, vamos apresentar e estudar como funciona a rede da Akamai, que foi a empresa pioneira e atualmente é a líder do mercado de CDN no Brasil e no mundo.

A **Figura 3** mostra o fluxo de uma requisição HTTP para um domínio acelerado com a Akamai. Os passos realizados neste processo são:

1. O usuário digita *www.exemplo.com.br* no browser e este requisita o endereço IP de *www.exemplo.com.br* ao servidor de DNS local. Como este domínio tem um CNAME para a Akamai, a requisição é encaminhada ao servidor de DNS da Akamai, que retorna o endereço IP do servidor da Akamai com a menor latência para esse usuário;
2. O browser faz a requisição HTTP ao servidor web da Akamai;
3. O servidor da Akamai monta a página a partir do cache ou acessando o servidor de origem do cliente, se necessário. Por fim, a página HTML é retornada ao usuário.

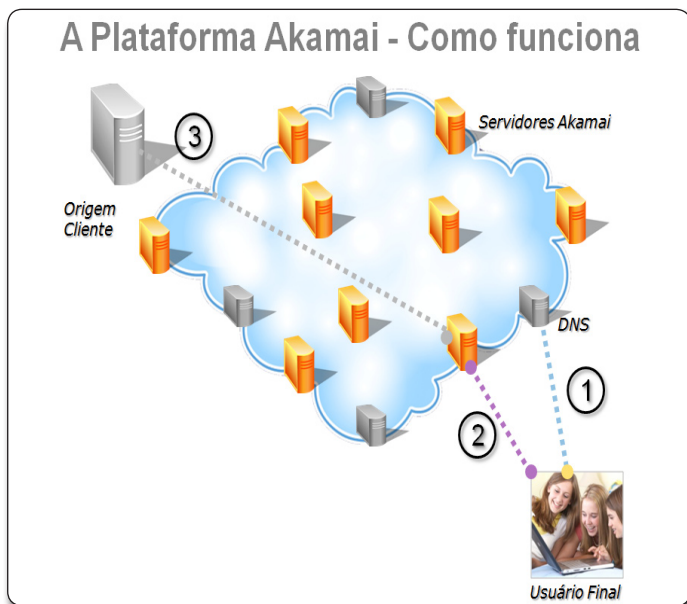


Figura 3. Fluxo de uma requisição HTTP na Akamai

Uma vez que o cname esteja configurado e o tráfego HTTP dos usuários do site esteja passando pela rede da Akamai, otimizações em diversas camadas de rede são possíveis e executadas em favor do cliente, conforme explicado na **Tabela 1**.

| Camada de Rede      | Características                                                                                 |
|---------------------|-------------------------------------------------------------------------------------------------|
| IP/ Roteamento      | Mapeamento Dinâmico<br>Otimização de Rotas - SureRoute                                          |
| TCP / Transporte    | Detecção automática de Falha<br>Offload de conexões<br>Otimização da camada de transporte (TCP) |
| HTTP / Protocolo    | Compressão de dados<br>Cache na Borda                                                           |
| HTML / Apresentação | Busca antecipada (Prefetch) de objetos<br>Leitura e otimização de JavaScript                    |

Tabela 1. Melhorias de performance em cada camada de rede

A seguir, cada uma dessas melhorias de performance é descrita:

- **Mapeamento Dinâmico:** É a funcionalidade de eleger um servidor de borda na rede da Akamai que tenha a melhor performance para um determinado usuário. É o que provê a distribuição característica das CDNs;
- **Otimização de Rotas – SureRoute:** É a rota otimizada para acessar o servidor de origem da aplicação do cliente. De tempos em tempos, a rede da Akamai roda testes entre os servidores de borda e a origem do cliente usando três caminhos: o direcionado pelo BGP (*Border Gateway Protocol*) e outras duas rotas passando por servidores da Akamai em pontos com boa conexão. A melhor dessas rotas é escolhida e usada para comunicação até que outro teste aconteça;
- **Detecção automática de falha:** Se a rota determinada pelo SureRoute passar por algum problema antes que um novo teste seja executado, a rede automaticamente passará a usar o caminho

com a segunda melhor performance, evitando que um problema em alguma rede afete os usuários do site;

- **Offload de conexões:** Os browsers modernos abrem entre seis e oito conexões TCP com o servidor web. Quando o site está com a Akamai, essas conexões são abertas com os servidores de borda e não com o servidor web de origem. A origem vai receber conexão somente dos servidores da Akamai. Além disso, as conexões abertas pela Akamai serão persistentes e reutilizadas para diferentes usuários, diminuindo ainda mais a carga na infraestrutura do cliente;

- **Otimização da camada de transporte (TCP):** O protocolo TCP (*Transmission Control Protocol*) foi criado em 1974, quando a qualidade da internet era muito menor. O TCP controla o estabelecimento de conexões entre máquinas de origem e destino, a taxa de transmissão de pacotes entre as duas, a detecção de perda de pacotes e algoritmos de recuperação. A Akamai é capaz de otimizar janelas de conexão, ajustar timeouts e algoritmos de recuperação de perdas, maximizar o uso de conexões persistentes e controlar outros aspectos do protocolo para melhorar o desempenho do site. Em última análise, estas otimizações maximizam a performance entre os servidores de borda da Akamai e o servidor de origem;

- **Compressão de dados:** Os browsers atuais conseguem receber e interpretar conteúdo compactado, porém a maioria das empresas não tira proveito dessa funcionalidade por falta de conhecimento, falta de recursos de processamento na origem ou devido ao trabalho envolvido para implementar uma lógica que faça a compactação somente para browsers que suportam receber conteúdo compactado. Com o serviço da Akamai, o cliente pode servir o conteúdo sem compactação, o servidor Akamai que recebe esse conteúdo o compacta e o servidor de borda decide se entrega o conteúdo compactado ou não, baseado no tipo e versão do browser que solicitou;

- **Cache na Borda:** É a funcionalidade que permite armazenar o conteúdo de um site no servidor de borda da rede Akamai, ou seja, o mais próximo possível do usuário final. Quando o conteúdo não está no cache, o servidor de borda busca na origem. A partir daí, para as próximas requisições, o conteúdo é servido dos servidores Akamai e a origem fica livre de ter que responder por essas requisições. É importante observar que não só conteúdo estático pode ser cacheado. Páginas dinâmicas, montadas por aplicações com consultas a banco de dados também podem ser cacheadas, desde que não tenham nenhum dado pessoal. Mesmo nesses casos, há formas de cachear partes da página e deixar sem cache somente o conteúdo pessoal. A vantagem de cachear também as páginas dinâmicas é que essas requisições que fazem consultas a banco de dados são as mais “caras” computacionalmente, isto é, não somente se usa banda para responder, mas também recursos dos servidores web, de aplicação e de banco de dados. Sem falar em ataques que exploram URLs que buscam conteúdos dinâmicos justamente para sobrecarregar a origem com processamento. O cache dessas URLs ajuda a amenizar esses tipos de ataques;

- **Busca antecipada (Prefetch) de objetos:** É o mecanismo que se passa no servidor de borda da Akamai quando uma pági-

na HTML é requisitada pelo browser do usuário. Quando o servidor de borda busca a página no servidor de origem, antes de enviar a resposta com a página ao browser, o servidor analisa o HTML e busca por imagens, JavaScripts, Cascade Style Sheets (CSS) etc. Enquanto envia a página ao browser, o servidor busca esses objetos na origem, quando eles não estão em cache. Dessa forma, quando o browser recebe o HTML e começa a pedir pelos objetos internos, o servidor de borda já os tem e pode servir sem necessidade de buscar na origem;

• **Leitura e otimização de JavaScript:** Da mesma forma que o HTML é analisado em busca de links para objetos, os JavaScripts também são. Quando há links para objetos dentro do JavaScript, esses objetos também serão baixados para o servidor de borda da Akamai quando o JavaScript passar pelo servidor.

Todas essas características permitem que a Akamai forneça um *Service Level Agreement* (SLA) de melhora de pelo menos 50% na performance do website, quando comparado com a performance da aplicação servida de maneira centralizada. Esse SLA de performance se soma ao de disponibilidade da rede: 100% disponível por SLA, o que é possível graças à grande escala e distribuição da rede da Akamai.

Essa é a solução para aceleração de websites dinâmicos (*Dynamic Site Accelerator*). Além dela, as CDNs também têm outras aplicações: entrega de vídeo, aceleração de aplicações, segurança, entre outras. A base das outras soluções é a mesma. A diferença está na camada de aplicação, onde há diferentes tratamentos para cada necessidade.

## Conclusão

As CDNs estão aqui para ficar. A demanda por alto desempenho por parte de usuários está mudando a maneira de investir em websites. A escalabilidade, offload e segurança que as CDNs agregam permite um investimento mais inteligente em recursos de TI, bem como garante a disponibilidade do site em momentos de alto tráfego e receita para a empresa.

Do ponto de vista técnico, em uma aplicação web, as CDNs visam otimizar a performance na camada de rede, ao invés do foco usual em aprimorar o desempenho de processamento da aplicação. As CDNs focam na otimização quando o gargalo está na transmissão da informação depois que o conteúdo sai do servidor web até chegar ao usuário. Com sua rede distribuída, as CDNs resolvem esse problema de uma maneira que nenhuma arquitetura de software pode resolver: estando perto – leia-se, com baixa latência – dos usuários.

Essas melhorias são potencializadas nas CDNs que têm uma rede grande e bem distribuída. Todas as vantagens descritas nesse artigo são possíveis graças à proximidade do servidor da CDN ao usuário final. Com o acesso à Internet crescendo no Brasil e no mundo, fornecer uma performance aceitável para aplicações web cada vez mais dependerá de estar próximo, inclusive topologicamente, dos usuários e dos clientes.



**Alex Felipelli**

[alex.felipelli@akamai.com](mailto:alex.felipelli@akamai.com)

Atua no ramo de tecnologia da informação, internet e dispositivos móveis há mais de 15 anos. É Engenheiro de Computação formado na Escola Politécnica da Universidade de São Paulo. Senior Solutions Engineer para a América Latina na Akamai, Líder Global na área de Content Delivery Network e Aceleração de Aplicações na Internet.



## Especificação do registro CNAME

<http://tools.ietf.org/html/rfc1034>

## Home Page da Akamai

<http://www.akamai.com/>

## Artigo sobre a vulnerabilidade do protocolo BGP

<http://www.wired.com/threatlevel/2008/08/revealed-the-in/>



# 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](http://porta80.com.br) | [comercial@porta80.com.br](mailto:comercial@porta80.com.br) | [twitter.com/porta80](https://twitter.com/porta80)

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