Eduardo Fontinelle Pereira de Oliveira

Implementação de redundância de rede usando BGP

Lavras

2014

Eduardo Fontinelle Pereira de Oliveira

Implementação de redundância de rede usando BGP

Relatório de Estágio apresentado ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel em Ciência da Computação.

Universidade Federal de Lavras - UFLA

Departamento de Ciência da Computação

Orientador: Neumar Costa Malheiros

Lavras

2014

EDUARDO FONTINELLE PEREIRA DE OLIVEIRA

IMPLEMENTAÇÃO DE REDUNDÂNCIA DE REDE USANDO BGP

Trabalho de Conclusão de Curso de Graduação apresentado ao Colegiado do Curso de Bacharelado em Ciência da Computação, para obtenção do título de Bacharel.

APROVADA em 21 de novembro de 2014.

Dr. Luiz Henrique Andrade Correia

Lucas Gonçalves Cunha

Neumar Costa Malheiros

Dr. Neumar Costa Malheiros (Orientador)

LAVRAS-MG
Novembro/2014

Agradecimentos

Agradeço à Gerencianet Pagamentos do Brasil por confiar no meu potêncial e me atribuir tarefas com tamanha responsabilidade para os negócios.

Ao senhor Sílvio, meu pai, a senhora Dalva, minha mãe, ao jovem André, meu irmão e a Kênia, minha namorada. Vocês foram fundamentais nesta grande etapa da minha vida e sem o apoio de vocês, certamente eu não teria chegado aqui.

Agradeço também ao Professor Dr. Neumar, que instigou sempre a pesquisa e a busca pelo conhecimento. Considero um grande amigo.

Aos Amigos feitos na UFLA: Túlio Spuri, Alessandro P.O., Marquim, Davizim, Sergio Mira, Galeano Véio, Paulo Fejão, Michel Chécha, Leandro Berdan e Caio Balão pela gigante contribuição nos momentos de estudo e amizade maior. Aos velhos amigos por não deixarem de ser os bons e velhos amigos que sempre foram. Um dia o Bacon disse: *Não há solidão mais triste do que a do homem sem amizades.*

Reconheço que grande parte das reclamações que fiz sobre as aulas foram sem fundamentos e por esta minha falha, agradeço todos os professores que tive. A insistência dos mesmos me fez ter um grande respeito e admiração pela profissão. Agradeço em especial aos professores Luiz Henrique, Joaquim Uchoa e Júlio Bueno. O aprendizado que tive com eles me seguirá por bons tempos.

Agradeço também todos os colaboradores do DGTI, pela oportunidade que me foi dada e que nunca se omitiram nos meus momentos de dúvida.

Resumo

Este relatório de estágio tem como objetivo descrever as atividades desenvolvidas durante a implantação do protocolo de roteamento BGP entre a empresa Gerencianet e os provedores de Internet que fornecem acesso à empresa. O objetivo do projeto foi manter os sistemas da empresa sempre *on-line*, tanto para os funcionários durante o expediente quanto para os clientes, além de reduzir a dependência de um único provedor.

A realização do estágio contribuiu de forma muito significativa no conhecimento em redes de computadores, possibilitando a configuração real do roteamento dinâmico através do protocolo de roteamento BGP desde o começo. As atividades desenvolvidas trouxe conhecimento e experiência com um tipo de conexão à Internet que não é comum encontrar, nem tão pouco ter a oportunidade de implantá-las desde o início.

Palavras-chaves: BGP. Redes de Computadores. Roteamento. Redundância de Rede.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

AS	Autonomous System
B2B	Business-to-business
BGP	Border Gateway Protocol
CEO	Chief Executive Officer
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
ISP	Internet Service Provider
NIR	National Internet Registry
RIR	Regional Internet Registries
SEO	Search Engine Optimization

Sumário

1 Introdução

Este estágio foi realizado na área de redes de computadores realizado na Gerencianet, uma empresa que desenvolve soluções para transações financeiras pela Internet.

O projeto teve como principal objetivo elevar a disponibilidade do acesso à Internet da empresa Gerencianet, tanto para os funcionários, conectados à rede interna da empresa, quanto no acesso dos clientes dos sistemas online que a empresa disponibiliza. O aumento da disponibilidade foi implementado à partir do uso de redundância nos links de acesso a provedores de Internet (ISPs).

Outro objetivo do projeto foi eliminar a dependência do acesso à Internet de um único provedor, através de links de rede com mais de um provedor. Desta forma, quando um dos provedores falhar, a disponibilidade da rede tem impactos mínimos.

Anteriormente, a medida adotada para excluir tal dependência era hospedar todos os serviços da Gerencianet em empresas de hospedagem web, colocando em xeque todos os investimentos em recursos tecnológicos que a Gerencianet fez.

O estagiário participou de todas as atividades do projeto, desde a compra de equipamentos até a escolha e a negociação com os provedores.

Este estágio representou uma oportunidade de desenvolver atividades com alto teor de complexidade e desenvolver maneiras de contorná-las da melhor forma encontrada.

Este relatório está organizado da seguinte forma. No Capítulo 2, é descrito o ambiente de trabalho onde foi realizado o estágio. No Capítulo 3, são apresentados os conceitos básicos sobre os tópicos abordados neste trabalho, com foco em protocolos de roteamento. No Capítulo 4, são descritas as atividades realizadas para implantação de links redundantes com diferentes provedores a fim de aumentar a disponibilidade dos serviços de rede da empresa. Por fim, no Capítulo 5, são apresentadas considerações finais sobre o projeto realizado.

2 Descrição do Local do Estágio

Neste capítulo é apresentado a história da Gerencianet, a descrição física do ambiente de trabalho, o organograma administrativo e a plataforma de produtos da empresa.

2.1 Histórico

A Gerencianet foi fundada em 2007 na cidade de Ouro Preto pelo atual CEO Evanil Rosano de Paula. A empresa oferece soluções em pagamentos, cobranças e gestão de clientes. Tudo começou quando o próprio Evanil, que é formado em Administração pela Universidade Federal de São João Del Rei, desenvolvia sites para seus clientes. Alguns deles começaram a questioná-lo sobre como receber pagamentos via Internet de forma segura. O Evanil então começou a desenvolver alguns mecanismos para fazer esta parte, porém, ainda muito artesanal. Ele e, depois de algumas semanas, a sua irmã Eliana faziam as transações financeiras manualmente, indo direto ao caixa dos bancos e enviando o dinheiro para os vendedores.

Com o tempo o sistema foi crescendo e as transações não puderam mais ser feitas de forma manual. O sistema precisava de uma automatização e de mais pessoas. Desde então, a empresa só vem crescendo.

A Gerencianet hoje tem como objetivo intermediar pagamentos entre compradores e vendedores, com soluções B2B *(Business to Business)* de interface e integração descomplicadas, atendendo mais de 30 mil clientes[1].

2.2 Descrição Física

A Gerencianet está com sede desde a sua fundação na cidade mineira de Ouro Preto. A cidade é um atrativo a mais para os trabalhadores, pois toda a cidade é um ponto turístico, possui uma universidade federal, tem grandes mineradoras ao redor e fica a 90km da capital Belo Horizonte. Tudo isso torna a cidade atrativa para diversos tipos de pessoas.

A empresa utiliza 2 prédios na cidade. O primeiro a ser utilizado foi a residência do CEO da empresa, que mais tarde foi expandindo verticalmente e hoje aloja o *datacenter* da companhia, concentrando toda infraestrutura necessária para funcionamento dos serviços

[1] Dados de 2013

oferecidos. O acesso ao datacenter é controlado pelo setor de infraestrutura e para acessar, o usuário deve ter um cartão e uma senha previamente autorizados.

O segundo prédio foi alocado em 2013 para abrigar o crescimento da empresa. Toda a mão-de-obra (desenvolvedores, administrativo, refeitório, etc) foi movida para esta nova edificação, que é maior e localizada próxima à moradia da maioria dos funcionários.

Cada funcionário que trabalha com computador possui uma mesa com sua estação de trabalho. Cada estação de trabalho possui 2 monitores de 23", um teclado, um mouse, uma doca e cada um destes funcionários recebem da empresa um *laptop* para encaixar na doca e trabalhar. Esta facilidade permite que se leve o trabalho pra casa, quando há necessidade.

Esta sede onde ficam alocadas toda a mão-de-obra está ligada, através de 2 *links* de rádio, à primeira sede, trazendo segurança no desenvolvimento das aplicações uma vez que os servidores de desenvolvimento não precisam de acesso externo para o uso de ferramentas internas.

Ao lado desta última sede, existe uma residência que foi adaptada como refeitório, onde mais de 40 funcionários possuem acesso à alimentação das 7:00 às 18:00.

2.3 Organograma Administrativo

O organograma administrativo não quer dizer exatamente que haja uma hierarquia forte dentro da empresa. Não há uma política bem definida sobre quais setores são responsáveis pelo o que e a definição que se tem, muda-se constantemente. Esta flexibilidade, comum em *startups*, permitiu o rápido crescimento da empresa, acomodando as diversas mudanças necessárias. A figura Figura 1 representa a atual organização da empresa.

2.4 Plataforma de Produtos

A empresa possui atualmente 3 produtos no mercado:

a) *Gerencianet Pagamentos:* sistema desenvolvido para a gestão de cobranças e pagamentos virtuais, com a possibilidade de envio de cobranças por e-mail, gerar botões de pagamento, cadastrar pagamentos recorrentes e integrar com outros sistemas. O site do sistema é: <gerencianet.com.br>

b) *Fortunus:* sistema para emissão e controle de boletos e carnês. O cliente pode enviá-los por e-mail ou pelos correios. A impressão e postagem é feita pela própria Gerencianet. O site do produto é: <fortunus.com.br>

c) *Kuiper:* sistema de criação de lojas virtuais, com interface de controle e gestão de produtos, de vendas e estoque. Possui integração com o Google Analytics, que

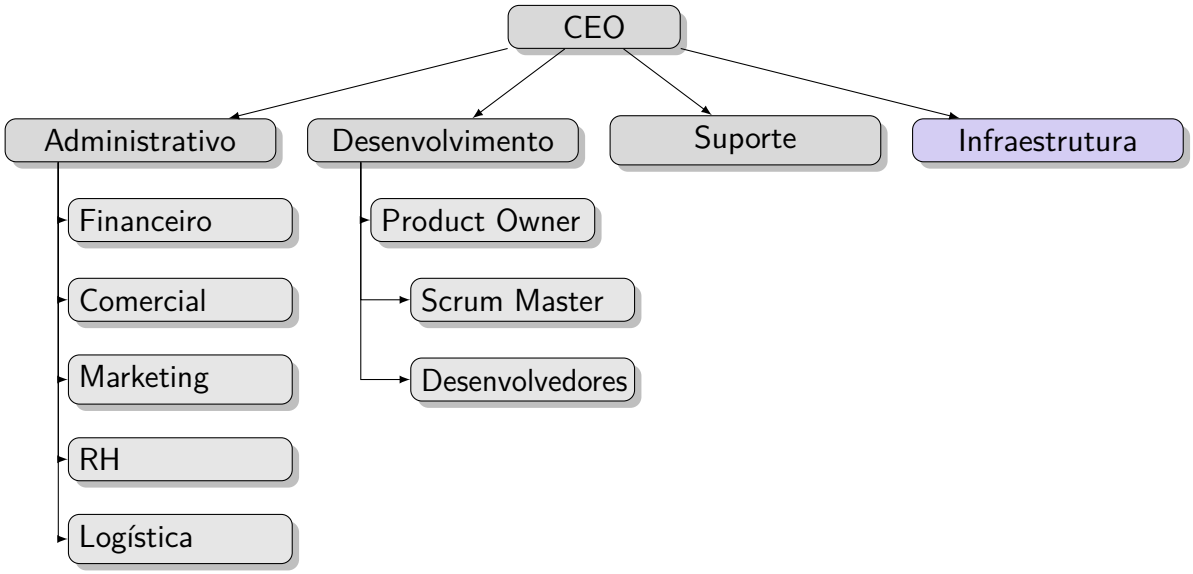

Figura 1 – Organograma Administrativo da Empresa.

fornece um *feedback* para o cliente sobre as visitas à loja virtual, e otimização nos principais sites de busca, auxiliando o usuário a ter o seu site nas primeiras páginas de resposta dos buscadores. O site do produto é: <kuiper.com.br>

3 Revisão da Literatura

Neste capítulo do relatório de estágio, serão descritos os conhecimentos necessários para a função desempenhada no estágio.

A seção 3.1 explica como funciona o roteamento de pacotes através de uma rede. A seção 3.2 explica o que é um Sistema Autônomo e como faz para obtê-lo. A seção 3.3 explica sobre o protocolo de roteamento BGP e qual a sua importância na Internet. A seção 3.4 explica sobre algumas regras que há nas sessões BGP entre os Sistemas Autônomos.

3.1 Roteamento

De uma maneira geral, o *roteamento* envolve duas atividades básicas: compartilhar informações sobre a topologia da rede e calcular o melhor caminho entre um nó de origem e um nó de destino (CâMARA, 2000). O nó, de posse das informações da topologia, calcula os caminhos para alcançar os outros nós. Estes caminhos são chamados de *rotas*.

O papel do nó, quando chega um pacote de dados, é verificar se o destino é ele mesmo e, caso não seja, encaminhá-lo para o destino. Neste momento, acontece um problema: decidir qual é a melhor rota para encaminhar a informação. Para se escolher a melhor rota, é necessário possuir informações atualizadas sobre a rede. Por causa desta constante necessidade de se ter informações da rede, é preciso verificar a topologia dela constantemente. Isso é importante porque um nó que é alcançável através de uma rota, por algum problema técnico, pode não ser mais alcançável ou aquela mesma rota pode não ser mais a melhor.

Durante a comunicação entre os nós é imprescindível que haja roteamento dos pacotes. Para que o encaminhamento ocorra, os algoritmos de roteamento utilizam uma tabela de roteamento. Esta tabela contém remetentes e destinatários, além de indicar para qual vizinho é necessário enviar um pacote para que este alcance o destino pela melhor rota conhecida. As informações que são inseridas nesta tabela são determinadas pelo protocolo de roteamento.

O protocolo de roteamento descreve como o repasse de informações sobre os nós irá acontecer e pode ser estático ou dinâmico(CâMARA, 2000).

Os protocolos estáticos não se adaptam às constantes mudanças nas rotas, a não ser em caso de falhas. Uma rota é definida inicialmente e é modificada somente quando ocorre problemas na transmissão. Os dinâmicos modificam as rotas à medida em que há necessidade, fazendo constantes análises do estado da rede. Essas análises da rede são feitas de acordo com a métrica específica do algoritmo.

Entre os protocolos de roteamento dinâmico, podemos destacar o *Link State* e o *Distance Vector*. Um protocolo *link state* envia periodicamente para todos os nós informações de roteamento sobre seus vizinhos. Esta forma de difundir a informação é chamada de *flooding*. O *distance vector* envia toda a sua tabela de roteamento, mas somente para os nós vizinhos (CLAUSEN; JACQUET, 2003).

Por ter uma visão mais apurada da rede, os algoritmos *link state* tem menos chances de gerarem *loops*, mas precisam usar recursos sofisticados para diminuir a sobrecarga (*overhead*) na rede, devido ao grande volume de mensagens de controle. No caso do *distance vector*, apesar de gerar um fluxo menor de dados na rede, é necessário ter uma preocupação com a possibilidade de se ter *loops*, comparando-o com o *link state*.

Uma forma específica para se definir o custo de uma rota é chamada de métrica de roteamento. A métrica tem como objetivo associar custos aos enlaces. Estes custos dão suporte para a escolha do melhor caminho. Quanto menor for o custo dos enlaces de um caminho, melhor será este caminho.

3.2 Sistemas Autônomos

Assim como temos um endereço IP *(Internet Protocol)* público, individual para cada interface de rede conectada à Internet, um sistema autônomo, conhecido também como AS, é a identificação única de uma entidade. Esta entidade, identificada com um número chamado de ASN (*Autonomous System Number*), possui o direito de uso de blocos de endereço IPv4 e/ou IPv6. Os blocos de endereço IP são atribuídos aos AS e estes blocos são divulgados através das interconexões que um AS faz com outro AS, utilizando o protocolo de roteamento BGP.

Para se obter um AS é preciso entrar em contato com uma entidade regional de registro, conhecida como RIR (*Regional Internet Registries*, que geralmente cobre alguns países em determinada região. Opcionalmente pode-se fazer o pedido de um AS para uma entidade nacional de registro, conhecida como NIR. No Brasil, o NIR é o Registro.br. Através desta entidade é solicitado o ASN e os endereços públicos. O pedido de blocos IPv4 estão cada vez mais burocráticos e com razão. A quantidade de IPv4 disponíveis para alocação está chegando ao fim. De acordo com o site de fomento do IPv6 no Brasil, <http://ipv6.br>, o estoque de IPv4 no LACNIC [1] acabou no dia 10 de junho de 2014.

A IANA, autoridade máxima na atribuição de números na Internet, padronizou através da RFC 1930 Hawkinson e Bates (1996) que os ASs são identificados com números de 16 bits, os ASN, que vão de 0 até 65535. Dentro deste bloco, o intervalo entre 64496 e 64511, incluindo-os, é reservado para documentação e o intervalo entre 64512 e 65534, incluíndo-os, é reservado para uso privado. Os dois conjuntos de números reservados são padronizados

[1] RIR responsável pela América Latina e Caribe

conforme RFC 5398 Huston (2008) e RFC 6996 Mitchell (2013), respectivamente, e não podem ser alocados para nenhum sistema autônomo.

Para que um sistema autônomo seja alcançável na Internet, é necessário que haja uma conexão com outro sistema autônomo. Esta conexão pode ser de 3 tipos: multihomed, stub e trânsito (REKHTER; GROSS, 1991). A Figura 2 ilustra os tipos de ASs.

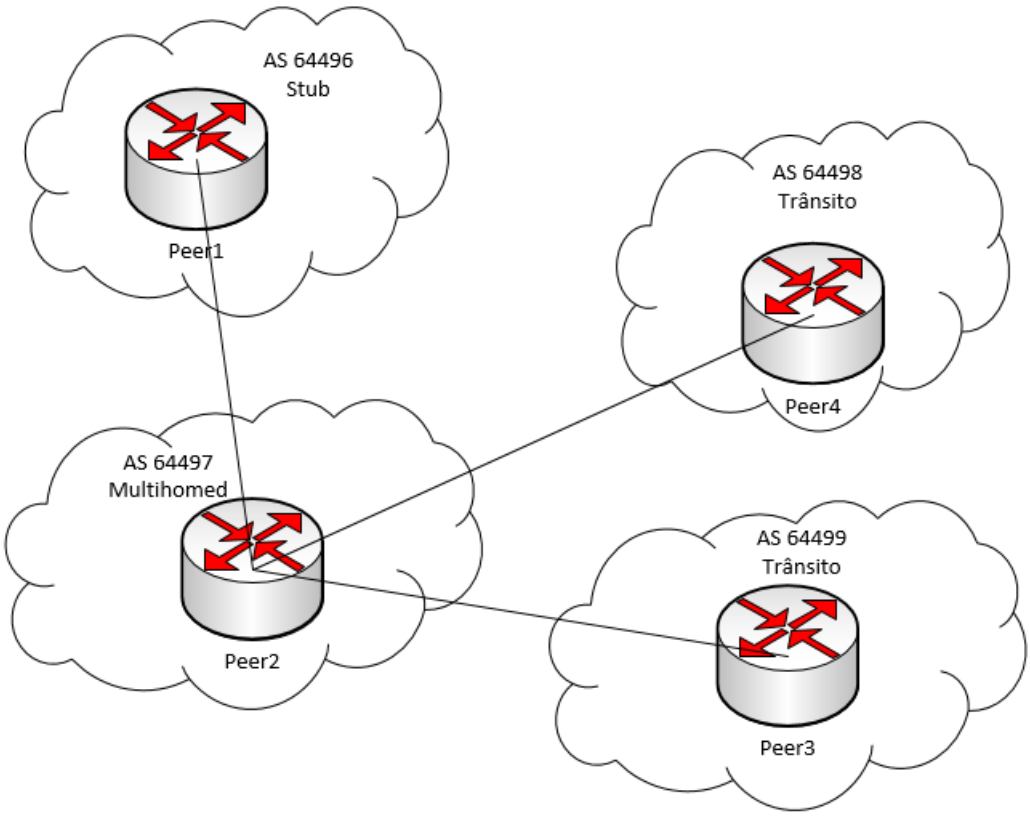

Figura 2 – Exemplo de AS Stub, Multihomed e de Trânsito.

Os AS multihomed, representado na Figura 2 pelo AS 64497 são aqueles que estão conectados à dois ou mais ASs. Desta forma, quando um dos ASs ficar inacessível ou passar por algum tipo de problema que impeça a conectividade, o AS multihomed não fica inacessível.

Um AS Stub, representado na Figura 2 pelo AS 64496 é um AS que possui conexão somente com outro AS. Geralmente, um AS stub possui somente conexão local e um único caminho para alcançar a Internet. Este tipo de interconexão pode ser usado para se construir redes privadas.

Para que os ASs multihomed tenham conectividade, eles precisam de conexões com ASs de trânsito. Este tipo de AS, representado na Figura 2 pelo AS 64498 e 64499 recebe as rotas propagadas e as repassa para os outros ASs conectados.

3.3 O Protocolo BGP

O BGP é um protocolo de roteamento dinâmico usado para fazer interconexão de ASs. Este é o protocolo padrão utilizado nas conexões inter-AS e já está na sua 4º versão.

O protocolo BGP é responsável por escolher o melhor caminho através dos inúmeros ASs interconectados(KUROSE; ROSS, 2010). O algoritmo de seleção do melhor caminho possui muitos atributos que permitem uma personalização mais granular, porém, o padrão do BGP é escolher o caminho mais curto, ou seja, o caminho que possua a menor quantidade de saltos. O seu funcionamento no que tange a propagação de rotas é simples. Entre cada AS vizinho é estabelecida uma sessão BGP, que é utilizada para a troca de tabelas de roteamento, permitindo que todos os ASs consigam comunicar entre si, através de outros ASs intermediários. Esta é a topologia comumente encontrada com ASs multihomed e de trânsito. Cada nó desta rede de ASs divulga blocos de endereço IP para os seus vizinhos. Estes blocos podem ser do próprio AS ou blocos aprendidos com os vizinhos interconectados.

As sessões BGP possuem 2 tipos: iBGP e eBGP. A Figura 3 ilustra os dois tipos de sessão.

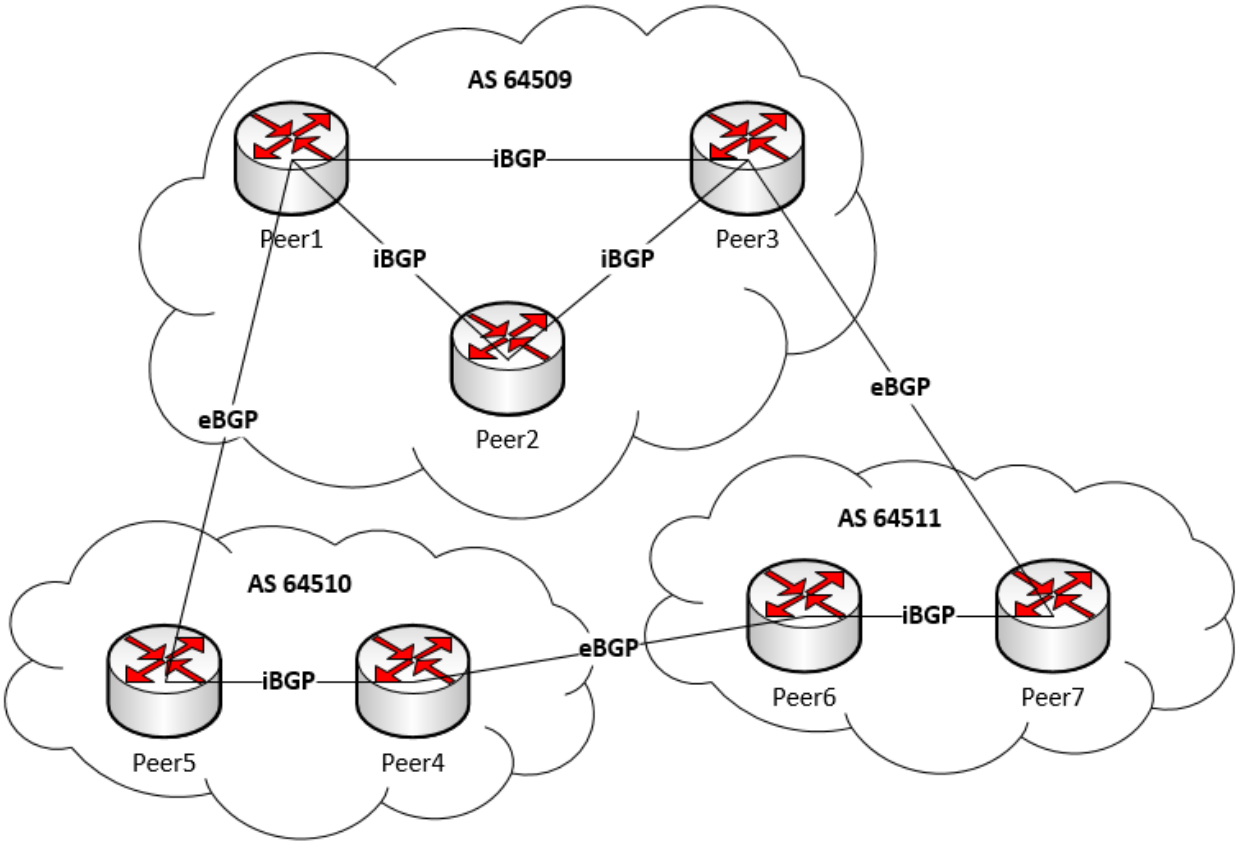

Figura 3 – Exemplo de sessão iBGP e eBGP.

O primeiro tipo é formado por roteadores, também chamados de peers, dentro do

mesmo sistema autônomo. O eBGP é formado por *peers* conectados em ASs diferentes.

Neste cenário, caso não fosse utilizado nenhum protocolo de roteamento dinâmico, quando houvesse uma queda de conexão entre o Peer3 e o Peer7, alguém com conhecimento técnico e da topologia precisaria intervir rapidamente para desviar o fluxo de dados para a conexão entre o Peer1 e o Peer5. No cenário proposto na figura o roteamento estático não seria uma tarefa de grande complexidade. O problema cresce quando consideramos todos os 49 mil ASs[2]. A gerencia, mesmo que individual de todos os ASs nos colocaria em um cenário propício a falhas humanas. Com um protocolo de roteamento dinâmico, não há necessidade de manipular tabelas de roteamento. O protocolo possui inteligência suficiente para escolher outras rotas para chegar no mesmo destino.

É neste ponto que entra a importância da redundância da rede. Se um AS possui sessão BGP com um único provedor, caso o provedor tenha algum problema, o AS cliente deste provedor também terá. Quando um AS possui várias sessões BGP com diferentes provedores, se um deles falhar, os outros ASs "esquecem"a rota através do provedor *off-line*.

Esta última situação pode ser ilustrada com a Figura 3. Caso haja uma desconexão entre o Peer1 e o Peer5, a comunicação entre os 3 ASs continua ocorrendo porque existe uma redundância entre o AS 64509 e o AS 64511, através dos Peer3 e Peer7. Neste caso específico, há uma redundância de rota, ou seja, caso uma rota pare de funcionar, outra rota entra em funcionamento. Poderia existir também uma redundância de *link*, onde entre dois peers tenha mais de um enlace. Neste último exemplo, caso um *link* físico se rompa, existe outro, fazendo a redundância do *link*.

As várias sessões BGP entre diversos provedores, tornam a internet cada vez mais tolerante a falhas.

3.3.1 A escolha da Rota

Considerando cenários onde existam mais de uma rota possível para o mesmo destino, o BGP precisa selecionar uma delas. Para selecionar uma rota, existem uma sequência de regras seguidas(KUROSE; ROSS, 2010).

O primeiro atributo é chamado de *LOCAL PREF*[3]. Este atributo é definido pelo administrador de rede e não é propagado nas sessões eBGP. Com este atributo o administrador de rede consegue priorizar rotas. Quanto maior for o valor do atributo, maior preferência terá em relação às outras.

Quando o atributo *LOCAL PREF* não é definido, todas as rotas possuem o mesmo valor. Neste caso, a rota selecionada será a mais curta, onde o atributo tem o nome de

[2] Informação encontrada em <http://bgp.he.net/report/netstats> no dia 11/10/2014

[3] Alguns fabricantes de equipamento chamam este atributo de *WEIGHT*, mas segue o mesmo raciocínio: quanto maior o valor, maior preferência tem a rota

AS-PATH. A escolha de rotas baseada na quantidade de saltos é uma característica de protocolos *distance vector*, mas não se pode atribuir esta classe ao BGP porque este critério não é o único utilizado.

Pode acontecer o empate entre os atributos anteriores. Quando isso acontece, a rota selecionada é a do roteador mais próximo. Este atributo, chamado de *NEXT-HOP*, determina qual roteador está mais próximo do roteador de borda do destino.

Geralmente não é necessário mais do que estes três atributos para selecionar a melhor rota, mas, caso precise, existem outros atributos. O último deles é a rota com o menor endereço no primeiro salto.

3.3.2 *Full Routing* e *Partial Routing*

Cada roteador que faz a conexão BGP com algum provedor de trânsito recebe deste provedor uma tabela contendo todas as rotas que ele aprendeu. Esta tabela possui atualmente mais de 510 mil prefixos. Com esta tabela é possível alcançar qualquer ponto da Internet. Porém nem todo roteador suporta esta tabela. Quando um equipamento a recebe, é necessário fazer um processamento das informações, o que pode durar alguns minutos, dependendo do hardware do equipamento.

Um AS, ao solicitar uma sessão BGP com um AS de trânsito pode escolher entre receber a tabela integral aprendida, chamada de *Full Routing*, ou pode escolher por receber uma fração destas rotas aprendidas. Esta fração é chamada de *Partial Routing*. Os prefixos aprendidos em uma tabela Partial Routing são escolhidos pelo AS de trânsito e consequentemente reduz a flexibilidade do AS que recebe as rotas. Para o AS cliente alcançar os prefixos que não são passados através da tabela partial routing é necessário configurar uma rota padrão através do AS de trânsito. É esperado que o AS de trânsito saiba o caminho até o destino não aprendido.

3.4 *Bogons*

A IANA determina quais blocos de endereço IPv4 são públicos, ou seja, exclusivos para uso na Internet e quais blocos são exclusivos para uso em redes internas, conhecidos como endereços privados. Os endereços privados podem ser utilizados em qualquer rede interna, sem o risco de haver conflito, porém, não podem ser utilizados na Internet, uma vez que os blocos de endereço IPv4 públicos são reservados para este fim(REKHTER et al., 1996). Conforme a RFC 4193 Hinden e Haberman (2005), os endereços IPv6 reservados para uso em redes locais são chamado de *Unique Local Addresses* (ULAs) e sua restrição ao uso na Internet é a mesma. Os reservados para uso público são chamados de *Global Unicast*.

O fato da IANA reservar blocos de endereços IP para uso exclusivo em redes internas não coíbe os ASs de divulgarem estes blocos através de seus vizinhos ASs, seja por falha de configuração ou não. Estes blocos divulgados erroneamente são chamados de Bogons. Para que não haja roteamento da rede interna para a rede externa, são necessários filtros para descartarem estes endereços quando forem recebidos através dos ASs vizinhos.

Um outro tipo de bogons são os blocos de endereços IP que ainda não foram alocados para nenhum AS mas, assim como os endereços privados, podem ser divulgados através da sessão BGP erroneamente. Estes blocos também devem ser descartados, já que eles ainda não são oficialmente de nenhum AS. A filtragem destes blocos evita ataques anônimos e reduzem o custo computacional, não considerando estes destinos no momento em que o roteador constrói as rotas.

A filtragem destes prefixos ocorre no momento da sessão BGP e durante as atualizações recebidas. O roteador, ao receber um prefixo, compara com os prefixos configurados nos filtros. Um filtro eficaz instrui o roteador a descartar aquele prefixo, deixando de armazenar aquele possível destino.

3.5 Alternativas ao BGP

Antes de considerar o BGP como solução definitiva, outras soluções foram analisadas. Com o uso de mais de um provedor de acesso à Internet, não é necessário se ter um AS para que os usuários da rede interna tenha conectividade no caso da queda de um dos ISPs.

O problema que levou a empresa a adotar o BGP é no caso do acesso ao sistema pelos clientes. Junto de um ISP, também é fornecido endereços IP para uso. Estes endereços são de propriedade do ISP que forneceu e, por causa disso, ficam inacessíveis quando o provedor tem alguma queda. Esta queda deixam servidores inacessíveis também.

Utilizando um bloco próprio e um sistema autônomo, o endereço IP é acessível através de qualquer ISP conectado ao AS da empresa. A queda de um dos ISPs não causa a inacessibilidade, tornando o acesso redundante. Esta característica torna o uso de BGP imprescindível para aumentar a disponibilidade de rede para os clientes.

4 Atividades Desenvolvidas

Neste capítulo são descritas as atividades desenvolvidas, bem como o tempo aproximado gasto em cada tarefa.

4.1 Lista de Atividades

As atividades descritas sofreram pequenos ajustes à medida em que descobertas foram feitas e necessidades foram surgindo.

a) *Estudo do processo de solicitação de ASN e blocos IPv4 e IPv6*: apesar de parecer uma tarefa simples, o Registro.BR exige muita informação e por causa do problema de esgotamento dos IPv4, exigiu-se também projeto e planejamento justificando o uso e a aquisição dos blocos de endereços e do ASN.

b) *Pedido do ASN ao Registro.BR*: conhecendo melhor o procedimento, foi submetido o formulário de solicitação de ASN junto de outros documentos necessários.

c) *Estudos e treinamento em BGP Avançado:* um treinamento foi custeado pela empresa e teve duração de 1 semana. Além do treinamento, estudos paralelos foram feitos afim de obter o máximo de conhecimento no menor tempo possível.

d) *Esclarecimentos e Argumentações ao Registro.BR*: a entidade, após a entrada da documentação de solicitação de ASN, iniciou uma discussão com o objetivo de entender melhor o cenário da empresa e os objetivos do pedido. Caso a entidade julgue que para atender as necessidades justificadas existam outras soluções, ela pode indeferir o pedido.

e) *Solicitação de Trânsito IPv4 aos ISPs*: esta tarefa teve como objetivo negociar sessões BGP com os provedores de Internet que atendem a empresa para anúncio do bloco IP da Gerencianet, fechando novos contratos ou alterando-os quando necessário. Esta tarefa só pôde ser iniciada depois que o Registro.BR liberou o ASN e os blocos de endereço IP.

f) *Estabelecimento da Sessão BGP com os ISPs*: depois da parte burocrática, veio a parte técnica, que foi a configuração do roteador de borda e os testes necessários.

g) *Bogons e a Team-cymru*: a Cymru é uma organização que divulga através de sessões BGP blocos de IP que são considerados bogons, ou seja, endereços não atribuídos à nenhum ASN ou endereços reservados para outros fins que não seja roteamento pela Internet.

h) *Realização de Testes*: esta atividade teve como objetivo fazer testes pontuais, colocando alguns servidores escolhidos para responderem à solicitações feitas para endereços de IP do bloco designado ao ASN da empresa.

i) *Alteração dos endereços IP dos servidores*: depois de todos os testes executados, foi o momento de colocar em produção. A migração dos serviços para serem roteados através das sessões BGP foram feitos em etapas, observando e corrigindo eventuais problemas.

j) *Monitoramento*: foram adicionados aos servidores que monitoram o datacenter, instruções para monitorarem as sessões BGP, avisando aos responsáveis nos casos de interrupção da sessão BGP.

4.2 Cronograma das Atividades

O cronograma das atividades foi se formando à medida em que os primeiros estudos e treinamentos foram feitos. A Tabela 1 mostra as atividades divididas em semanas.

Tabela 1 – Cronograma de Atividades de Estágio.

	15/09 19/09	22/09 26/09	29/09 03/10	06/10 10/10	13/10 17/10	20/10 24/10	27/10 31/10	03/11 07/11	10/11 14/11	17/11 21/11
Atividade a										
Atividade b										
Atividade c										
Atividade d										
Atividade e										
Atividade f										
Atividade g										
Atividade h										
Atividade i										
Atividade j										

4.3 Descrição das Atividades

4.3.1 Atividade a: Estudo do processo de solicitação de ASN e blocos IPv4 e IPv6

Esta etapa foi o primeiro contato com a tecnologia com uma abordagem mais prática. Estudos anteriores foram feitos sobre sessões BGP mas com uma abordagem mais superficial. Foi preciso ler e compreender toda a política do Registro.BR[1]. Foi preciso fazer

[1] Disponível em <http://registro.br/tecnologia/provedor-acesso.html?secao=numeracao>

consultas até mesmo ao setor administrativo para tirar dúvidas quanto ao cadastro da empresa na receita federal.

Uma outra parte deste estudo foi levantar os custos para se obter o ASN e os blocos. Para atender a demanda da empresa, que era de não depender somente de um ISP para o acesso dos clientes, foi pedido um bloco IPv4 /24[2] e um bloco IPv6 /48. Dos dois blocos recebidos pela empresa, somente o IPv4 foi implantado, substituindo os endereços IPv4 disponibilizado pelas operadoras.

4.3.2 Atividade b: Pedido do ASN ao Registro.BR

O pedido ao Registro.BR foi feito através do preenchimento de um formulário[3]. Este formulário possui perguntas sobre a entidade solicitante do ASN, contatos para eventuais comunicados ou incidentes, além de perguntas técnicas como a quantidade de ativos de redes que utilizarão os endereços IP.

No formulário o solicitante se depara com algumas perguntas que acaba forçando-o a ter um mínimo de planejamento. Caso contrário, a chance de não demonstrar organização e real necessidade à entidade é alta. Outra pergunta que pode deixar algumas empresas com receio de responder é com relação à topologia interna da rede. Esta informação, se passada para mãos erradas pode comprometer a segurança. O Registro.BR, através de sua política de privacidade[4] assegura que as informações só são repassadas à terceiros em decorrência de ação judicial.

Nesta atividade a dificuldade apareceu ao fazer o levantamento da rede e fazer um planejamento com relação à distribuição dos endereços de IP dentro da rede. Como não havia documentação da topologia da rede da empresa, esta etapa gastou aproximadamente 2 dias.

4.3.3 Atividade c: Estudos e treinamento em BGP Avançado

Conforme a entidade divulga em seu portal, o tempo para análise do formulário é de até 2 semanas. Para não se perder tempo, foi planejado um treinamento durante este tempo. O curso teve duração de 1 semana e teve conhecimento bem avançado com relação ao protocolo de roteamento BGP. Muito estudo paralelo foi necessário para conseguir acompanhar a turma, já que era formada por alunos com conhecimento bem avançado. Apesar da dificuldade em algumas atividades práticas, foi possível absorver o suficiente para implementar a solução. Outro ponto muito interessante do treinamento foi a rede

[2] O /24, na linguagem técnica, faz referência ao número de bits de valor 1 na máscara de rede. Esta máscara define que a rede possui 256 endereços

[3] Disponível em <http://registro.br/tecnologia/numeracao-pedido-form.txt>

[4] Disponível em <http://cgi.br/politica-de-privacidade>. O Registro.BR é um departamento do Comitê Gestor da Internet (CGI)

de contatos estabelecida. Alguns dos colegas foram fonte de grandes descobertas, quando alguns problemas foram surgindo e na hora da escolha do equipamento.

4.3.4 Atividade d: Esclarecimentos e Argumentações ao Registro.BR

Depois de uma análise feita pelo Registro.BR sobre o formulário de solicitação de ASN, foi iniciado um diálogo via e-mail para uma espécie de convencimento da entidade da necessidade da empresa. Esta parte foi bem interessante porque quando era questionado sobre algumas tecnologias, uma lista de exemplos era enviada. As tecnologias desconhecidas até aquele momento foram anotadas e estudadas posteriormente para conhecimento próprio e possíveis implementações em momentos oportunos.

4.3.5 Atividade e: Solicitação de Trânsito IPv4 aos ISPs

Quando o Registro.BR liberou o sistema autônomo e os blocos de endereço IPv4 e IPv6, foi escolhido o IPv4 para começar. A decisão veio pelo tardio amadurecimento do protocolo IPv6 no Brasil e pelos produtos e mecanismos de segurança da empresa, baseados somente no IPv4. Iniciou-se um constante contato com três provedores de Internet para estabelecimento das sessões. Neste momento foi possivel ver o quanto existem empresas que, apesar de grandes, possuem tanta burocracia interna que engessa os pedidos dos clientes. Em uma delas, a solicitação aberta ainda não foi finalizada.

O processo com os outros dois provedores, desde a abertura da solicitação até o contato técnico confirmando a manobra durou aproximadamente 1 semana. A configuração da rede no lado dos provedores, por causa da grande complexidade da rede de provedores que atendem muitas regiões do país, passavam por etapas. Estas etapas, apesar dos provedores serem diferentes, coincidiam. Começavam com um contato telefônico para entender a solicitação, já que o atendente que abriu a solicitação não tem conhecimento técnico suficiente para descrever com detalhes o pedido. Após este contato, um segundo contato era mais técnico e tinha como objetivo testar se a configuração que o provedor fez na própria rede estava funcionando corretamente. A maior dificuldade foi entender os termos técnicos que eram usados nos contatos telefônicos, mas que foram elucidados durante as conversas.

A necessidade de estabelecer sessão com mais de um provedor teve como objetivo implementar a redundância de rotas, exclusivamente. Quando se estabelece diversas sessões BGP, em caso de queda de uma das sessões, o acesso à Internet dos profissionais não é perdida e, principalmente, o acesso dos clientes ao sistema também não.

4.3.6 Atividade f: Estabelecimento da Sessão BGP com os ISPs

Depois que o pedido foi parcialmente finalizado, chegou a parte do teste de fechamento da sessão. Foi nesta atividade que se mostraram mais úteis os conhecimentos adquiridos no treinamento e na literatura. Apesar do procedimento ser simples, aferir se estava ocorrendo tudo bem não é tão simples assim. Surgiram muitas dúvidas bem específicas que com a experiência de se trabalhar todos os dias foram sendo sanadas.

No momento em que a sessão BGP com as duas operadoras foi estabelecida, a implementação de filtros fez falta. Como estava em testes, o prejuízo foi somente da conexão à Internet ficar temporariamente lenta. Quando o tráfego das interfaces de rede que estavam ligados nos roteadores dos ISPs foram verificados, notou-se que 100% da banda disponível estava sendo usada, situação anormal até momentos antes. O motivo de tamanho tráfego foi que o protocolo BGP calculou que a melhor rota entre os dois provedores seria passando pelo AS recém configurado. Para corrigir a falha, foi aplicado um filtro.

O filtro é uma ou mais instruções que são aplicadas diretamente na comunicação das sessões BGP. Uma característica padrão da sessão BGP é repassar todas as rotas aprendidas em uma sessão para o roteador da outra sessão e vice-versa. Para que isso não aconteça, aplica-se um filtro. Este filtro, aplicado na propagação das rotas configuradas e aprendidas, descarta todos os blocos diferente dos blocos atribuídos ao AS. Por exemplo: o AS 64496 possui o bloco 177.66.12.0/24 e aprendeu, através de BGP, o caminho até o bloco 200.160.0.0/16. O filtro adequado neste caso descartaria qualquer anúncio que não fosse do bloco 177.66.12.0/24.

Além da necessidade do filtro para não tornar o AS da Gerencianet em um AS de trânsito entre as operadoras, outros filtros também foram necessários. De acordo com a RFC 1918 Rekhter et al. (1996) existem alguns endereços IPv4 que não podem ser usados na Internet e, por isso, não podem ser recebidos na sessão. Foram criados filtros para descartar os endereços de IP privados listados na RFC 1918. Filtros com este objetivo também é configurado nos provedores que a Gerencianet possui sessão BGP, de acordo com os seus próprios técnicos. A configuração destes filtros foi uma medida de segurança caso algum dos provedores se descuide.

4.3.7 Atividade h: Bogons e a Team-cymru

Depois da criação dos filtros, surgiu uma dúvida: como descartar blocos de endereços IP que ainda não tinham sido alocados para nenhuma empresa. Foram feitas algumas pesquisas que levaram até o Team-cymru. Esta organização fornece uma lista com todos os blocos de endereços IP privados e todos os blocos que não foram atribuídos para nenhuma empresa. Os blocos não atribuídos podem ser utilizados por *hackers* para diversas

finalidades como ataques *DDoS*. Este ataque tem como mecanismo de funcionamento inundar servidores com requisições de acesso. O alto volume destas requisições pode sobrecarregar servidores, fazendo com que não consigam mais responde-las.

Outro recurso interessante disponibilizado pelo Team-cymru é a distribuição desta lista através de sessões BGP. Desta forma, não é necessária a constante revisão dos filtros no roteador, já que a organização faz este serviço. Foi feito o contato com a equipe do Team-cymru e foi disponibilizado para a empresa uma sessão BGP para esta finalidade.

4.3.8 Atividade i: Realização de Testes

Para efetuar os testes, foi colocado um servidor com uma página de Internet disponível e e atribuído ao mesmo um endereço de IP válido. Depois de testar o acesso através de outras redes (por exemplo: redes 3G), foi constatado o perfeito funcionamento da configuração da sessão.

A segunda etapa do teste foi migrar, gradativamente, os endereços IP dos servidores com acesso externo. O endereço web de alguns sistemas começaram a ter tráfego também através dos IPs divulgados através da sessão BGP. Esta etapa da tarefa envolveu ações de reconfiguração do *firewall* e do servidor DNS da empresa. Depois que a resolução de nomes estava respondendo também o bloco da empresa, foi iniciado um acompanhamento do tráfego através do *firewall*. À medida em que os testes foram tendo sucesso, outros servidores com serviços diferentes foram colocados à prova também. Foram utilizados servidores web, servidores DNS e um servidor com acesso SSH. Este último foi colocado somente para o teste.

Outro teste realizado foi o tempo de convergência, ou seja, quanto tempo é preciso para que toda a rede da empresa se estabilize quando uma das sessões cair. Foram feitos diversos testes de queda e ajustes na frequência em que o protocolo verificava a atividade do vizinho da sessão BGP. A melhor configuração obtida precisa de aproximadamente 10 segundos pra identificar que a sessão caiu e um pouco mais 1 minuto para que toda a tabela de rotas seja atualizada.

4.3.9 Atividade j: Alteração dos endereços IP dos servidores

Depois da segurança que os testes com servidores forneceu, iniciou-se a migração completa de todos os serviços. A primeira medida foi revisar e ajustar todas as regras no *firewall*, de forma que o acesso não fosse perdido quando o usuário fizesse o acesso ao sistema utilizando um endereço de IP da operadora. O próximo passo foi alterar todos os endereços de IP no servidor DNS, reduzindo também a validade daquela informação. Esta medida foi tomada para que eventuais erros de configuraçao não fossem *cacheados* por muito tempo em outros servidores DNS.

Após as mudanças no DNS, iniciou-se uma constante observação nos acessos através do *firewall*, um policiamento das redes sociais e constante contato com a equipe de suporte telefônico, afim de se encontrar algum problema de conectividade que fosse surgindo. Paralelo à isso, observou-se também a quantidade de acesso ao antigo endereço IP, afim de descobrir o porque daquele acesso. Como haviam serviços hospedados em outras empresas, foi necessário alterar no código-fonte das aplicações externas os endereços IP.

Depois que todos os endereços IP foram alterados e o serviço estava estabilizado, foi necessário aumentar o TTL (Time-to-Live) dos registros DNS, ou seja, aumentar a validade da informação novamente. Quando a validade é baixa o consumo de recurso e banda dos servidores DNS da empresa aumenta, já que é necessária mais consultas de outros servidores.

Esta atividade, apesar de extensa e com grandes responsabilidades, não apresentou grandes dificuldades mas sim um extenso serviço de duplicação das regras do firewall para permitir também os novos endereços IP.

4.3.10 Atividade k: Monitoramento

Paralelo ao projeto da redundância da rede, houve um projeto da implementação da aplicação *Zabbix* como alternativa para monitorar todos os ativos da empresa. Foi então adicionada à lista de serviços monitorados o estado das sessões BGP da empresa, emitindo alertas no caso de queda.

O monitoramento é feito verificando se a sessão BGP com os ISPs está ativa. A conexão possui uma propriedade que diz qual o estado da conexão. Se o estado é diferente de *connected*, o *zabbix* emite um alerta através de mensagem de texto informando que a sessão caiu. O mesmo acontece quando a sessão volta ao estado *connected*. Este tipo de monitoramento, além de desencadear uma ação junto ao ISP, auxilia também na obtenção de desconto no serviço. Alguns dos contratos prevê redução no valor da mensalidade à medida em que o serviço fica inoperante.

Esta atividade exigiu a compreensão do protocolo de obtenção de dados *SNMP* por parte do pessoal responsável pelo mecanismo de monitoramento e duas reuniões para explicar a importância do monitoramento e quais são os efeitos da queda de uma sessão BGP.

5 Conclusão

O projeto executado no estágio teve como objetivo garantir, através de múltiplos provedores de Internet, que o acesso à Internet dos funcionários esteja sempre disponível e que o acesso aos sistemas da empresa também estejam sempre on-line para os clientes.

O estágio na Gerencianet atendeu muito bem as expectativas criadas. À medida em que as tarefas foram avançando e erros foram sendo cometidos, o incentivo à descoberta era mantido sempre, criando um ambiente descontraído para a pesquisa e a aplicação de conhecimentos adquiridos na universidade. A liberdade que os administradores da empresa dão aos funcionários permitiu que procedimentos e regras de negócios da aplicação fossem discutidas e mudadas.

O estágio trouxe grandes contribuições. A área que foi apresentada e adequadamente proposta permitiu o contato com tecnologias as quais a universidade não conseguiria fornecer na mesma intensidade e, principalmente, no mesmo teor de exigência.

Este período de estágio permitiu também a aplicação de grande parte do conteúdo aprendido nas disciplinas de *Redes de Computadores* e *Administração de Servidores Linux*. Estas disciplinas forneceram um sólido conhecimento, permitindo a continuidade dos estudos. Sem estas duas disciplinas em especial, não seria possível, por exemplo, acompanhar o treinamento custeado pela empresa.

O estágio também foi uma oportunidade de se trabalhar com novas metodologias de desenvolvimento, em particular, métodos ágeis, na qual as equipes têm a liberdade de moldar o planejamento conforme a demanda.

Como trabalho futuro haverá uma pesquisa sobre alternativas para se balancear a carga entre todos os *links* da empresa.

Este balanceamento tem como objetivo distribuir a carga de *upload* e *download* entre os provedores de acesso à Internet que prestam serviço para a Gerencianet. Este balanceamento reduziria uma possível saturação de algum *link* de dados, uma vez que toda a carga não estaria sobre um único ISP. Além disso, haveria um consumo de todos os *links*, trazendo para a empresa uma relação entre custo e benefício mais atraente quando comparado com o uso de IPSs somente para emergências.

Referências

CLAUSEN, T.; JACQUET, P. *Optimized Link State Routing Protocol (OLSR)*. IETF, 2003. RFC 3626 (Experimental). (Request for Comments, 3626). Disponível em: <http://www.ietf.org/rfc/rfc3626.txt>. Citado na página 20.

CâMARA, D. Estudo de algoritmos de roteamento para redes móveis ad hoc. *Disertação de Mestrado da Universidade Federal de Minas Gerais, Belo Horizonte, Brasil*, 2000. Citado na página 19.

HAWKINSON, J.; BATES, T. *Guidelines for creation, selection, and registration of an Autonomous System (AS)*. IETF, 1996. RFC 1930 (Best Current Practice). (Request for Comments, 1930). Updated by RFCs 6996, 7300. Disponível em: <http://www.ietf.org/rfc/rfc1930.txt>. Citado na página 20.

HINDEN, R.; HABERMAN, B. *Unique Local IPv6 Unicast Addresses*. IETF, 2005. RFC 4193 (Proposed Standard). (Request for Comments, 4193). Disponível em: <http://www.ietf.org/rfc/rfc4193.txt>. Citado na página 24.

HUSTON, G. *Autonomous System (AS) Number Reservation for Documentation Use*. IETF, 2008. RFC 5398 (Informational). (Request for Comments, 5398). Disponível em: <http://www.ietf.org/rfc/rfc5398.txt>. Citado na página 21.

KUROSE, J.; ROSS, K. *Redes de Computadores e a Internet*. 5. ed. [S.l.]: Pearson, 2010. Citado 2 vezes nas páginas 22 e 23.

MITCHELL, J. *Autonomous System (AS) Reservation for Private Use*. IETF, 2013. RFC 6996 (Best Current Practice). (Request for Comments, 6996). Disponível em: <http://www.ietf.org/rfc/rfc6996.txt>. Citado na página 21.

REKHTER, Y.; GROSS, P. *Application of the Border Gateway Protocol in the Internet*. IETF, 1991. RFC 1268 (Historic). (Request for Comments, 1268). Obsoleted by RFC 1655. Disponível em: <http://www.ietf.org/rfc/rfc1268.txt>. Citado na página 21.

REKHTER, Y. et al. *Address Allocation for Private Internets*. IETF, 1996. RFC 1918 (Best Current Practice). (Request for Comments, 1918). Updated by RFC 6761. Disponível em: <http://www.ietf.org/rfc/rfc1918.txt>. Citado 2 vezes nas páginas 24 e 31.