UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COORDENAÇÃO DE INFORMÁTICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS PARA INTERNET

KAREN CRISTINE MORESCHI

COMPARAÇÃO ENTRE PROTOCOLOS DE GATEWAYS REDUNDANTES UTILIZANDO ROTEADORES DEDICADOS

TRABALHO DE CONCLUSÃO DE CURSO

CAMPO MOURÃO
2011

KAREN CRISTINE MORESCHI

COMPARAÇÃO ENTRE PROTOCOLOS DE GATEWAYS REDUNDANTES UTILIZANDO ROTEADORES DEDICADOS

Trabalho de Conclusão de Curso de graduação do Curso Superior de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador:Prof.MSc. Alessandro Kraemer

CAMPO MOURÃO
2011

ATA DA DEFESA DO TRABALHO DE CONCLUSÃO DE CURSO

As **vinte horas** do dia **vinte e cinco de novembro de dois mil e onze** foi realizada na sala F102 da UTFPR-CM a sessão pública da defesa do Trabalho de Conclusão do Curso Superior de Tecnologia em Sistemas para Internet do acadêmico **Karen Cristine Moreschi** com o título **COMPARAÇÃO ENTRE PROTOCOLOS DE GATEWAY REDUNDANTES UTILIZANDO ROTEADORES DEDICADOS**. Estavam presentes, além do acadêmico, os membros da banca examinadora composta pelo professor **Me. Alessandro Kraemer** (Orientador-Presidente), pelo professor **Me. Luiz Arthur Feitosa dos Santos** e pelo professor **Me. Frank Helbert**. Inicialmente, o aluno fez a apresentação do seu trabalho, sendo, em seguida, arguido pela banca examinadora. Após as arguições, sem a presença do acadêmico, a banca examinadora o considerou **Aprovado** na disciplina de Trabalho de Conclusão de Curso e atribuiu, em consenso, a nota _____. Este resultado foi comunicado ao acadêmico e aos presentes na sessão pública. A banca examinadora também comunicou ao acadêmico que este resultado fica condicionado à entrega da versão final dentro dos padrões e da documentação exigida pela UTFPR ao professor Responsável do TCC no prazo de **quinze dias**. Em seguida foi encerrada a sessão e, para constar, foi lavrada a presente Ata que segue assinada pelos membros da banca examinadora, após lida e considerada conforme.

Observações:

_____

_____

Campo Mourão, 25 de novembro de 2011.

Prof. Me. Luiz Arthur Feitosa dos Santos Membro	Prof. Me. Frank Helbert Membro	Prof. Me. Alessandro Kraemer Orientador

A folha de aprovação assinada encontra-se na coordenação do curso.

RESUMO

MORESCHI, Karen Cristine. **Comparação entre protocolos de gateway redundantes utilizando roteadores dedicados**. 2011. 32 f. Trabalho de Conclusão de Curso (Graduação) – Curso Superior de Tecnologia em Sistemas para Internet. Universidade Tecnológica Federal do Paraná. Campo Mourão, 2011.

Com a crescente demanda em manter dados estratégicos altamente disponíveis, se faz necessário impulsionar cada vez mais a criação de novas tecnologias que sejam tolerantes a falhas. Neste cenário, surgem os protocolos de *gateways* redundantes, onde por meio de equipamentos duplicados fazem com que a comunicação não seja interrompida, mesmo mediante a falhas. Os protocolos de *gateways* redundantes referenciados neste trabalho são o VRRP e GLBP, protocolos que possuem caraterísticas e configurações distintas. Tais protocolos foram submetidos a testes, e por meio de análise dos resultados, foi identificado que o protocolo VRRP se recupera mais rápido mediante a falhas no ambiente.

Palavras-chave: Protocolo de *gateway* redundante. VRRP. GLBP. Tolerância a falhas. Alta disponibilidade.

ABSTRACT

MORESCHI, Karen Cristine. **Comparison between redundant gateway protocols using dedicated routers**. 2011. 32 f. Trabalho de Conclusão de Curso (Graduação) – Curso Superior de Tecnologia em Sistemas para Internet. Universidade Tecnológica Federal do Paraná. Campo Mourão, 2011.

With the increasing demands to maintain strategic data highly available, it becomes enhancing the creation of new technologies that are fault tolerant. In this scenario, there are redundant gateway protocols, where many ways of duplicate equipment make the communication is not interrupted, even that one link is down The redundant gateway protocols referenced in this work are VRRP and GLBP, protocols that have different features and settings. These protocols were tested, and through analysis of the results, it was identified that the VRRP protocol will recover more fast in the environment.

Keywords: Redundant gateway protocol. VRRP. GLBP. Fault tolerance. High Availability.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

O crescente avanço da Internet vem demandando o surgimento de tecnologias que consigam ampliar o desempenho de rede. Muitas empresas utilizam redes Intranet para troca de dados estratégicos, e na maior parte esses dados são críticos e devem estar altamente disponíveis. Para garantir a alta disponibilidade no contexto WAN (*Wide Area Network*) é necessário o uso de enlaces redundantes. A alta disponibilidade é implementada com mecanismos de tolerância a falhas e balanceamento de carga. Essa implantação pode acontecer no lado do cliente como dentro da operadora de telecomunicação (PAULINO, 2010).

Na maioria das redes de computadores apenas um equipamento é utilizado como *gateway* padrão e todos os *hosts* deste segmento encaminham solicitações para este *gateway* padrão. Mesmo com enlaces e equipamentos duplicados, quando há uma falha no dispositivo comutador ou no enlace principal, ocorre interrupção das comunicações. Os protocolos que gerenciam os enlaces redundantes percebem a falha do enlace e habilitam um caminho secundário, previamente configurado. É desta maneira que se tem a alta disponibilidade. O principal exemplo desta tecnologia é a redundância de *gateways.*

O objetivo deste trabalho é elaborar um cenário de rede de computadores com enlaces redundantes para que sejam executados e comparados os protocolos de alta disponibilidade VRRP (*Virtual Router Redundancy Protocol*) e GLBP (*Gateway Load Balancing Protocol*).

Para verificar qual protocolo se destacará em determinadas situações propostas no cenário de rede será utilizado o critério de tempo de recuperação em caso de falha. Ou seja, qual protocolo consegue se adequar mais rapidamente quando há uma interrupção no enlace físico. O ambiente de rede utilizado para coleta de dados conterá roteadores dedicados. Os testes de desempenho serão feitos por meio de solicitações *echo* ICMP (*Internet Control Message Protocol*).

A partir deste contexto será possível:

- Explorar cada um dos protocolos de *gateway* redundantes (VRRP e GLBP) definindo como se dá o funcionamento e quais são os

parâmetros de configuração de cada um;

- Elaborar um cenário de rede de computadores e executá-lo para cada protocolo explorado;
- Encaminhar solicitações ICMP;
- Analisar os dados coletados para identificar características de desempenho dos protocolos.

Embora existam diversas tecnologias de *gateway* redundantes, é importante que elas sejam comparadas para indicar em que contexto cada uma pode ser considerada melhor. Um exemplo de contexto é o de disponibilidade 99,999%, onde o tempo de recuperação em caso de falha deve ser satisfatoriamente baixo. De certa maneira, este trabalho contribuirá também com os projetistas de redes de computadores apresentado-lhes características de cada protocolo. Portanto, os resultados e as características podem ser utilizados para tomada de decisões.

2 METODOLOGIA

Os protocolos de *gateway* redundantes referenciados neste trabalho (GLBP e VRRP) possuem características e configurações distintas e devem ser explorados afim de adquirir conhecimento para realizar a configuração de cada um no ambiente de teste. Esta é a primeira etapa.

Na etapa seguinte será elaborado o cenário de testes através do simulador GNS3 contemplando 4 roteadores dedicados, sendo que um dos roteadores contem uma interface *Loopback* que representa o cliente. Foi utilizado está abordagem pelo fato de que esse cliente processa apenas mensagens ICMP e utilizar um sistema operacional completo demandaria muito recurso desnecessário. Além disto, o cenário irá conter 1 *switch* e um computador com VMware.

Para coleta de dados será utilizado o comando ping. Este comando realiza requisições ICMP que informam sobre o tempo gasto para contatar um *host* com IP na rede. O ICMP é um protocolo de mensagens de controle da Internet e serve para relatar erros e fazer trocas de informações entre equipamentos da rede, como computadores e roteadores. Com este protocolo é possível diagnosticar problemas e falhas encontradas na comunicação de um determinado segmento.

Depois da coleta dos dados será realizada a análise dos mesmos. O critério de comparação é o tempo que o algoritmo do protocolo de *gateway* redundante leva para se recuperar de uma interrupção brusca, onde o acesso do enlace principal é interrompido. Quanto menor for esse tempo, mais eficiente é o processo de recuperação.

3 REFERÊNCIAL TEÓRICO

Neste capítulo serão apresentadas as características dos protocolos de *gateway* redundantes VRRP e GLBP.

A comunicação entre diferentes redes só é possível por meio do uso de equipamentos chamados de roteadores. O roteador encaminha as solicitações que recebe para o *gateway* de destino e devolve a resposta ao solicitante. Um exemplo simples de comunicação entre redes diferentes é um computador fazendo acesso a Internet. A Figura 1 a seguir exemplifica tal situação.

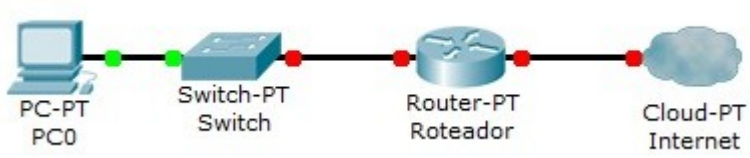

Figura 1 – Cenário de acesso a Internet.
Fonte: Autoria própria.

O roteador verifica o cabeçalho IP e utiliza as tabelas de encaminhamento para encaminhar o pacote até o destino, fazendo o processo que é conhecido como encaminhamento (Ferreira, 2005). O *gateway* pode ser compreendido como o nó que distribui o tráfego de uma estação de trabalho a outro segmento de rede.

Os protocolos de *gateway* redundante surgiram da necessidade de manter uma rede sempre operante, utilizando equipamentos replicados para que no momento que ocorre uma falha na comunicação do enlace principal, o substituto assume o seu lugar, não deixando a rede indisponível, trazendo para esta, a alta disponibilidade.

Além dos protocolos de *gateway* redundantes selecionados para este trabalho (VRRP e GLBP) também há outros protocolos conhecidos, chamado de CARP (*Common Address Redundancy Protocol*) e o HSRP (*Hot Standby Router Protocol*) que permitem compartilhar o mesmo endereço IP entre vários *hosts*, além de possibilitar a configuração do balanceamento de carga (JUNIOR, 2008, p. 2).

O critério de seleção dos protocolos deste trabalho foi baseado na capacidade que o protocolo possui de ser configurado em equipamentos dedicados atuais. Assim, somente os protocolos VRRP e GLBP possuem essa capacidade. O protocolo CARP foi descartado porque só pode ser configurado em ambiente OpenBSD, e o ambiente de testes representa um cenário dentro da operadora de telecomunicação, onde são exigidos equipamentos e sistemas mais robustos. O HSRP foi descartado porque é depreciado no ambiente de telecomunicação.

A seguir são apresentados os detalhes de cada um dos protocolos de *gateway* redundantes abordados nesta pequisa.

3.1 VRRP

O protocolo conhecido como VRRP *(Virtual Router Redundancy Protocol)* é um protocolo não-proprietário, detalhado pela RFC 3768. “Neste protocolo os endereçamentos reais e virtuais podem participar efetivamente do mecanismo de redundância” (KRAEMER, et al., 2010, p.10).

As trocas de mensagens entre os roteadores da rede são chamadas de *Link-State Advertisement* (LSA). O roteador principal, chamado de mestre, tem o papel de enviar essas mensagens para os roteadores de *backup*. Os LSA são encaminhados a cada 1 segundo por padrão. Os roteadores em estado de *backup* podem ser configurados para reconhecer o intervalo de tempo em que o roteador mestre encaminha os LSA. Essas mensagens são enviadas através do endereço *multicast* 224.0.0.18.

Quando o roteador mestre fica inoperacional, ocorre o processo de eleição, e um roteador *backup* torna-se mestre. Os roteadores em estado *backup* percebem a ausência de LSA e então o roteador que possui a prioridade mais alta assume como roteador mestre, sendo que a prioridade vária entre 1 até 254, e 100 é considerado como valor padrão.

No VRRP ocorre também o balanceamento de carga. O tráfego é balanceado porque diferentes endereços de *gateway* são distribuídos entre as

estações cliente. “Assim, os roteadores não ficam em estado de *backup* dedicado” (KRAEMER, et al., 2010, p. 9).

Há também o termo chamado *Preempt*, que faz com que a “rede volte à situação considerada mais desejável, ou seja, logo que a rede volte a situação inicial os equipamentos principais e secundário deverão ser os mesmos que eram anteriormente à anomalia que levou à comutação. Caso não seja definido, tal reposição não acontece” (PAULINO, 2010, p. 42).

Na figura 2, há um cenário demonstrativo do protocolo VRRP. As solicitações ARP (*Address Resolution Protocol*) enviadas pelo Cliente ao seu *gateway*, que no caso, é o IP Virtual, são respondidas pelo roteador mestre. O roteador *backup* fica ocioso até que ocorra uma falha com o roteador mestre.

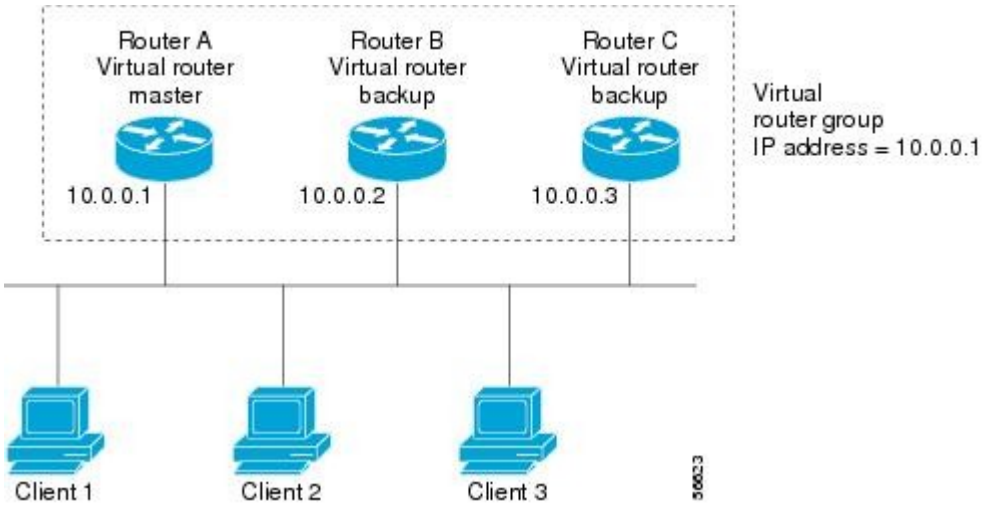

Figura 2 – Cenário demonstrativo do protocolo VRRP.
Fonte: CISCO SYSTEM. Disponível via http como <http://bit.ly/v7ArpN>.
Acesso em 05 dez. 2011, 18:00.

3.1.1 Parâmetros de configuração do VRRP

O quadro 1 apresenta alguns dos comandos utilizados para configurar o VRRP. A configuração do protocolo ocorre na interface console dos roteadores que farão parte do esquema de redundância.

Descrição	Sintaxe do comando
Atribuir uma prioridade ao roteador VRRP (valor padrão é 100)	**vrrp** *group* **priority** *level*
Alterar o tempo das mensagens LSA (valor padrão é 1 segundo)	**vrrp** *group* **timers advertise** [**msec**] *interval*
Aprender o intervalo dos LSA enviador pelo roteador mestre	**vrrp** *group* **timers learn**
Desativar a preempção (o padrão é de antecipar)	**no vrrp** *group* **preempt**
Alterar o delay da preempção (por padrão é 0 segundos)	**vrrp** *group* **preempt** [**delay** *seconds*]
Usar autenticação para as mensagens LSA	**vrrp** *group* **authentication** *string*
Atribuir um endereço de IP Virtual	**vrrp** *group* **ip** *ip-address* [**secondary**]

Quadro 1 – Comandos para configuração do VRRP.
Fonte: Hucaby (2006).

3.2 GLBP

O GLBP (*Gateway Load Balancing Protocol*) é um protocolo proprietário Cisco. Similar ao VRRP, este protocolo também faz a redundância de *gateway e* realiza o balanceamento de carga.

No GLBP também existe um IP virtual entre os roteadores, além disso, é possível atribuir vários endereços MAC (*Media Access Control*) para este endereço de IP Virtual. Assim como os demais protocolos, cada computador conhece um único *gateway,* que é o virtual.

Ainda no GLBP, os *gateways* reais são classificados em AVG *(Active Virtual Gateway)* e AVF *(Active Virtual Forwarders).* Os roteadores em estado AVF, também são conhecidos como escravos. O roteador AVG, conhecido como mestre, atribui um endereço MAC distinto a cada um dos demais roteadores do grupo. Segundo MACEDO (2008, p. 32) “para cada requisição ARP recebida para o endereço virtual, o *gateway* virtual ativo responde com um dos endereços MAC virtual, transferindo a responsabilidade do encaminhamento dos pacotes ao dono daquele MAC e

conseguindo desta forma o balanceamento”.

Os métodos de balanceamento de carga fornecidos pelo GLBP são:

- *Round robin*: a responsabilidade em transmitir o tráfego é feita de maneira uniforme entre todos os roteadores AVF, sendo este o método padrão utilizado pelo GLBP (Hucaby, 2006);
- *Weighted*: a escolha do roteador que irá transmitir o tráfego ocorre através da interface de ponderação, sendo os roteadores AVF com peso acima do limite estipulado os responsáveis por esta função (Hucaby, 2006);
- *Host-dependent*: as solicitações ARP realizadas por um cliente são atendidas sempre pelo mesmo endereço MAC (Hucaby, 2006).

A eleição do roteador AVG é feita através de uma eleição, onde o roteador escolhido é aquele que possui o maior valor de prioridade do grupo ou então, possui o endereço IP maior entre todos os demais roteadores, sendo que este ultimo caso só é possível caso todos os roteadores estejam configurados com o valor de prioridade padrão, sendo este o valor de 100. O valor de prioridade pode variar entre 1 a 255.

Caso ocorra a falha do roteador AVG, ocorre uma nova eleição onde o roteador que possuir a maior prioridade assume o estado de roteador AVG. A preempção não é ativa como padrão, desta maneira, o roteador que ocorreu a falha só irá retornar ao estado de AVG no momento que o atual roteador neste estado falhe, permitindo assim uma nova eleição.

Segundo Hucaby (2006), a escolha do roteador AVF que irá ser atribuído com o MAC Virtual ocorre através de uma função de ponderação, sendo que todos os roteadores são configurados com um peso máximo de 100, que pode variar entre 1 e 254. O peso irá ser decrementado, onde existe um valor limite que estipula quando o roteador está apto para receber o MAC Virtual, caso o peso do roteador esteja inferior ao limite, este deixará de ser AVF, repassando o papel a outro roteador do grupo.

A figura 3 apresenta a topologia do protocolo GLBP. Neste cenário, o método de balanceamento de carga utilizado é o *Host-dependent*, pois o Client 1 encaminha suas solicitações ARP sempre para o mesmo MAC Virtual, assim como ocorre com o Cliente 2.

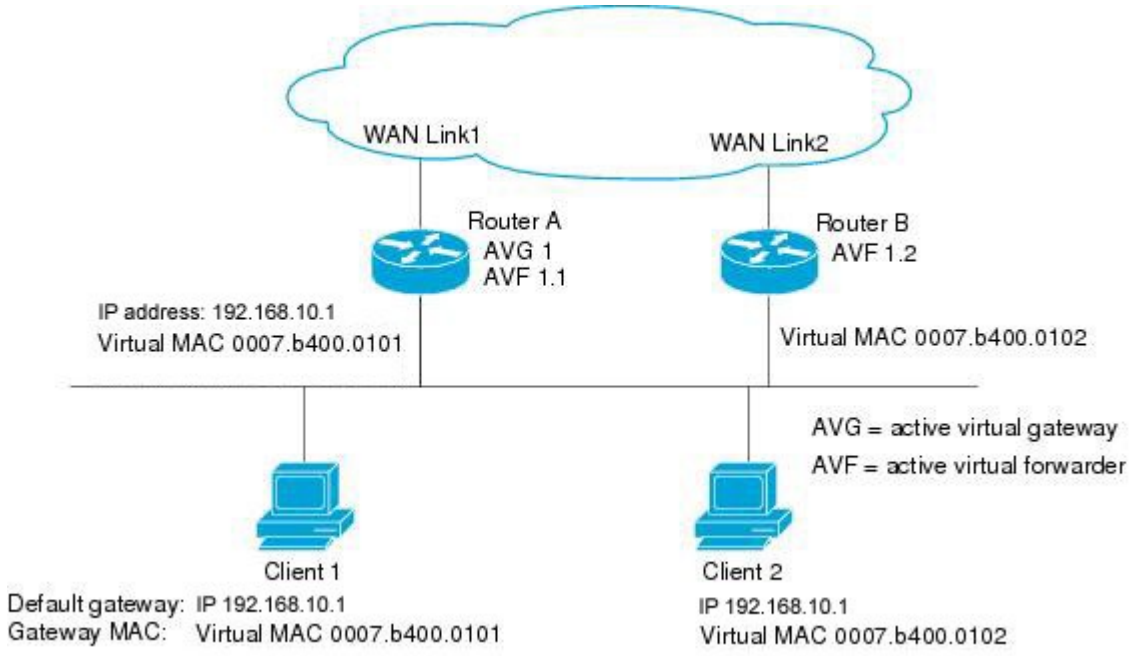

Figura 3 – Exemplo de cenário com o protocolo GLBP.
Fonte: CISCO. Disponível via http como <http://bit.ly/tFML9U> Acesso em 23 nov. 2010, 20:00.

3.2.1 Parâmetros de configuração do GLBP

O quadro 2 apresenta alguns comandos utilizados para configurar o GLBP. Tal configuração ocorre na interface console do roteador.

Descrição	**Sintaxe do comando**
Atribui uma prioridade	**glbp** *group* **priority** *level*
Habilitar a preempção	**glbp** *group* **preempt** [**delay minimum** *seconds*]
Definir um objeto a ser rastreado	**track** *object-number* **interface** *type mod/num* {**line-protocol** | **ip routing**}
Definir os limitadores da ponderação	**glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]
Rastrear um objeto	**glbp** *group* **weighting track** *object-number* [**decrement** *value*]
Definir o método de balanceamento de carga	**glbp** *group* **load-balancing** [**round-robin** | **weighted** | **host-dependent**]
Atribuir o endereço do roteador virtual	**glbp** *group* **ip** [*ip-address* **[secondary]]**

Quadro 2 – Comandos para configuração do GLBP.
Fonte: Hucaby (2006).

3.3 BREVE COMPARAÇÃO DOS PROTOCOLOS

O quadro 3 apresenta as principais características dos protocolos de *gateway* redundantes VRRP e GLBP.

Protocolo	**Equipamentos necessários**	**Forma de endereçamento**	**Balanceamento de carga**	**Tempo padrão**
VRRP (solução aberta)	Roteadores dedicados ou Plataformas Linux	Um ou mais IP e MAC Virtuais. Os IP e MAC reais também podem ser utilizados.	Cada estação cliente recebe um endereço de *gateway* diferente	1 seg. (LSA) 3 seg. (*Holdtime*)
GLBP (proprietário)	Roteadores CISCO	Um IP Virtual e vários MAC virtuais que identificam os roteadores do grupo	Cada estação cliente pode receber MAC distinto a cada solicitação ARP	3 seg. (*Hello*) 10 seg. (*Holdtime*)

Quadro 3 – Comparação entre os protocolos de *gateway* redundantes.
Fonte: Kraemer (2010).

3.4 CONTEXTO DE REDE WAN

Redes WAN são gerenciadas por ISPs (*Internet Service Provider*), classificados em três níveis (Forouzan e Sophia, 2008). No nível 1 estão os ISPs responsáveis pelas conexões nacionais e internacionais, dando forma a Internet. No nível 2 estão os ISPs de serviços regionais que conectam-se ao nível 1. Neste nível são vendidos serviços de rede WAN e é onde atuam as principais operadores de telecomunicação. Por fim, no nível 3 estão os provedores locais, normalmente para usuários domésticos.

Este trabalho explora os recursos e termos abordados no contexto dos ISPs de nível 2, que estão mais ligados a oferta de redes WAN. Embora os *gateways* redundantes possam ser implantados em qualquer contexto.

4 CONSTRUÇÃO DO CENÁRIO E AVALIAÇÃO DO EXPERIMENTO

O cenário utilizado para a execução dos testes está representado pela Figura 4.

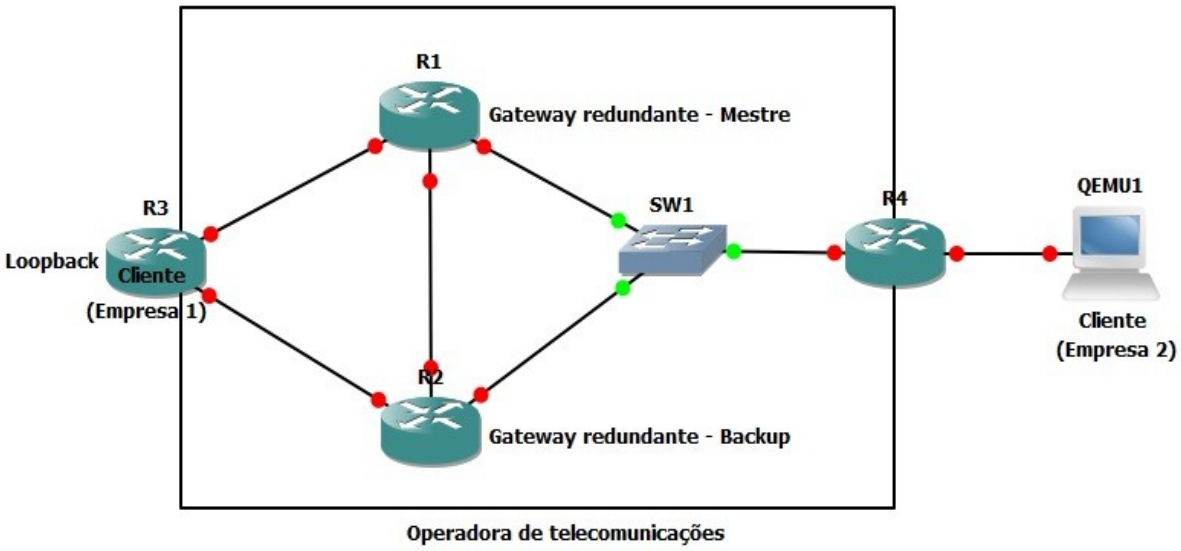

Figura 4 – Cenário de testes utilizado pelos protocolos de *gateway* redundante.
Fonte: Autoria própria.

Para implantação do cenário da Figura 4 foi utilizado o software de simulação GNS3 (GNS3, 2011). Os equipamentos dentro do retângulo representam uma operadora de telecomunicações, e é neste ambiente que irá ocorrer a configuração dos protocolos de *gateway* redundante.

Os roteadores nomeados de R1 e R2 foram configurados com os protocolos de *gateway* redundante. O R1 foi delegado como roteador Mestre. Enquanto isso, o R2 foi configurado para sempre atuar como roteador de *backup*.

Além disto, todos os roteadores do cenários foram configurados com rota estática e com o protocolo EIGRP (protocolo dinâmico), que identifica para o roteador as rotas alternativas que poderão ser utilizadas caso o enlace com a rota estática esteja indisponível.

No roteador que representa o Cliente Empresa 1 foi adicionado uma interface virtual (*Loopback*). Esta interface é responsável por encaminhar e receber as solicitações feitas pelo comando ping, presente no outro extremo da rede, representado pelo Cliente Empresa 2. No Cliente Empresa 2 foi implantada uma máquina virtual com VMware, onde foi instalado o sistema operacional Windows XP.

Os testes são feitos através de solicitações Ping encaminhadas pela VMware até a interface virtual *Loopback* configurada no roteador Cliente Empresa 1.

Foram efetuados dois tipos de teste para ambos os protocolos de *gateway* redundante. O primeiro teste consiste no encaminhamento de solicitações Ping pela VMware até o Cliente Empresa 1 por um tempo de 10 minutos. O outro teste efetuado ocorreu da mesma forma, porém o enlace do roteador Mestre era interrompido, ou seja, a interface onde estava configurado os protocolos era desativada a cada intervalo de 1 minuto, e 1 minuto depois era ativado novamente para que o impacto dessa interrupção pudesse ser avaliado.

Os arquivos de configurações dos roteadores mestre e backup de ambos protocolos estão nos anexos A e B.

4.1 ANÁLISE DOS RESULTADOS

Como foi abordado anteriormente, a avaliação dos resultados tem como base o tempo de resposta das solicitações ICMP (comando Ping). No primeiro momento os protocolos são comparados em relação ao balanceamento de carga. Assim, quanto menor for o tempo de resposta do Roteador Cliente, mais eficiente é o protocolo, já que o cenário é dedicado, inexistindo qualquer outra espécie de congestionamento que pudesse impactar no experimento. Outro fator de análise é o tempo que os *gateways* redundantes levam para se recuperar da interrupção brusca.

A Figura 5 apresenta a dispersão de tempo dos protocolos VRRP e GLBP, e a Figura 6 apresenta a média e o desvio padrão dessa dispersão.

Os resultados demonstram que o GLBP consegue balancear a carga ICMP de maneira mais veloz (11%). Por outro lado, os dois protocolos demonstram ser

bastante estáveis, variam pouco.

A Figura 7 apresenta os resultados nos casos em que houve a interrupção do enlace. No contexto onde há queda de enlace o VRRP se apresenta como uma tecnologia mais eficiente. Isto se deve porque o seu algoritmo consegue perceber e reagir mais rapidamente a falta de sinalização no enlace de rede. Uma razão para isto é que os *gateways* redundantes envolvidos confiam no estado de seus vizinhos tolerando tempos mais curtos (o padrão é 3 segundos no VRRP). Em contrapartida, o GLBP tolera 10 segundos.

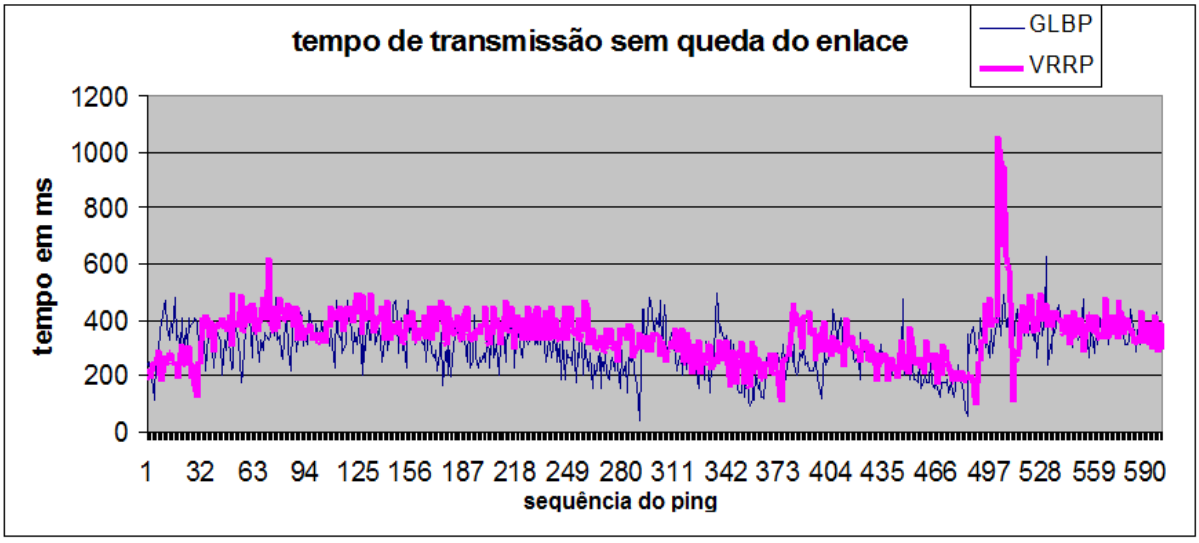

Figura 5 – Dispersão de tempo de transmissão em condições normais.
Fonte: Autoria própria.

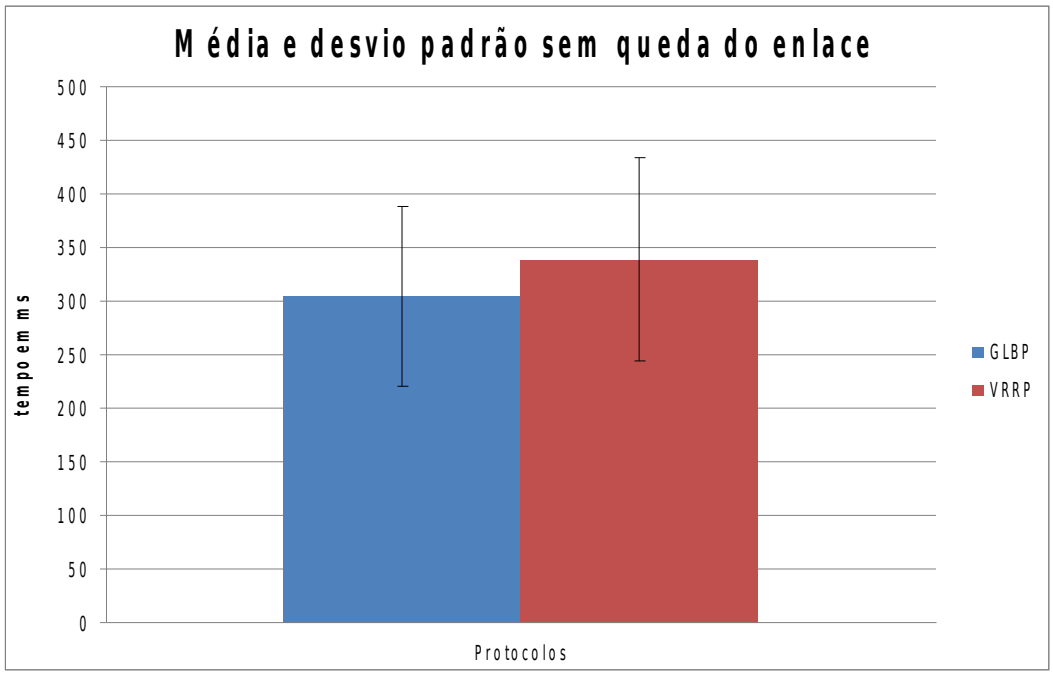

Figura 6 – Média e desvio padrão do tempo de transmissão em condições normais.
Fonte: Autoria própria.

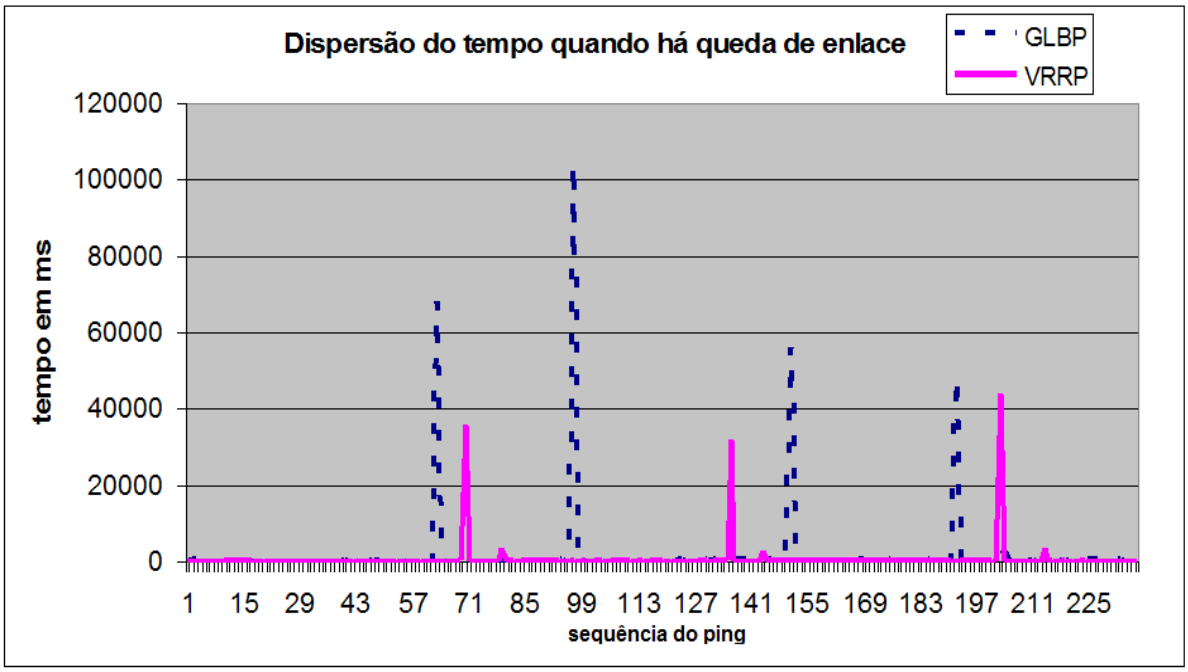

Figura 7 – Dispersão de tempo de transmissão quando há queda de enlace.
Fonte: Autoria própria.

5 CONSIDERAÇÕES FINAIS

A principal característica dos protocolos VRRP e GLBP é que eles gerenciam um mesmo IP virtual, distribuído entre um grupo de roteadores com endereços IP reais diferentes. O administrador de rede pode ajustar os padrões de tempo das mensagens de estado (*holdtime e hello/lsa*), tentando melhorar o desempenho do protocolo. Para os clientes da rede WAN, todo esse processo é transparente, pois eles conhecem apenas o IP do *gateway* Virtual, que continua o mesmo, independentemente do *gateway* que foi interrompido.

Entre os protocolos explorados, o VRRP demonstrou ser o que se recupera/elege
mais rapidamente o novo *gateway* Mestre. O papel do Mestre é importante porque é ele quem determina o balanceamento de carga. Uma razão para a eficiência do VRRP frente ao GLBP é que seus padrões de tempo de percepção de vizinhos são menores. Um potencial trabalho futuro é equalizar os tempos de percepção de vizinhos desses protocolos. Nestas condições, talvez o VRRP não iria continuar ganhando em eficiência.

Em condições de tráfego onde não há interrupção de enlace, o VRRP também se destacou. Neste contexto não há configuração de tempo. Contudo, o algoritmo do VRRP é certamente mais eficiente no processo de balanceamento de carga.

Outra condição de experimento futuro é ampliar a quantidade de computadores e de tráfego de rede para observar se o desempenho desses protocolos permanece linear.

REFERÊNCIAS

FERREIRA, Filipa Silva. SANTOS, Nélia Catarina Gaspar Gil dos Santos. **Clusters de Alta Disponibilidade. Abordagem OpenSource.** 2005. 108 f. Instituto Politécnico de Leiria, Escola Superior de Tecnologia e Gestão, 2005. Disponível em: < http://mosel.estg.ipleiria.pt/files/Artigo.pdf >. Acesso 28 abr. 2011, 19:30.

FOROUZAN, B. A.; SOPHIA C. F. **Protocolo TCP/IP**. 3. ed. Brasil: McGraw Hill, 2008.

GNS3. Disponível em: < http://www.gns3.net >. Acesso em: 28 nov. 2011, 15:30.

HUCABY, David. **CCNP BCMSN Official Exam Certification Guide**. 4. ed. USA: Cisco Press, 2006.

JUNIOR, João Eurípedes Pereira. **Alta disponibilidade em roteadores: Um ambiente de teste.** 2008. 7f.

KRAEMER, Alessandro; GOLDMAN, Alfredo; VILAR, Kaio. **Tolerância a Falhas utilizando Protocolos de Gateway Redundantes.** Anais da I Escola Regional de Alto Desempenho, São Paulo, n.1, p. 9-12, 2010.

MACEDO, Luís Gustavo Junqueira de. **Soluções de Balanceamento e Contigência em Circuitos WAN.** 2008. 48 f. Monografia (Especialização em Tecnologias, Gerência e Segurança de Redes de Computadores) – Instituto de Informática, Universidade Federal do Rio Grande do Sul, 2008. Disponível em: < http://www.lume.ufrgs.br/handle/10183/15976 >. Acesso em: 15 set. 2010, 20:00.

PAULINO, Ricardo Júlio Matos. **Redes de Computadores de Alta Disponibilidade.** 2010. 243 f. Dissertação (Mestrado) – Escola Superior de Tecnologia de Setúbal, Instituto Politécnico de Setúbal, 2010. Disponível em: < http://www.ltodi.est.ips.pt/jomm/mestrados/Ricardo Paulino.pdf >. Acesso em: 19 maio 2010, 14:20.

ANEXO A – CONFIGURAÇÃO DOS ROTEADORES VRRP

Configuração do roteador R1

```
Current configuration : 1084 bytes
! Last configuration change at 20:19:10 UTC Thu Oct 27 2011
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
hostname R1
boot-start-marker
boot-end-marker
no aaa new-model
ip source-route
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
interface FastEthernet0/0
 ip address 192.17.0.2 255.255.255.0
 shutdown
 speed auto
 duplex auto
interface FastEthernet0/1
 ip address 192.16.0.2 255.255.255.0
 speed auto
 duplex auto
 vrrp 10 ip 192.16.0.1
 vrrp 10 priority 200
interface FastEthernet1/0
 ip address 172.17.0.5 255.255.255.252
```

```
 speed auto
 duplex auto
interface FastEthernet1/1
 no ip address
 shutdown
 speed auto
 duplex auto
router eigrp 100
 network 10.0.0.0
 network 172.17.0.0
 network 192.17.0.0
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.16.0.4
control-plane
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Configuração do roteador R2

```
Current configuration : 1016 bytes
! Last configuration change at 20:25:25 UTC Thu Oct 27 2011
version 12.2
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
hostname R2
boot-start-marker
boot-end-marker
no aaa new-model
ip source-route
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
interface FastEthernet0/0
 ip address 192.18.0.2 255.255.255.0
 speed auto
 duplex auto
interface FastEthernet0/1
 ip address 192.16.0.3 255.255.255.0
 speed auto
 duplex auto
 vrrp 10 ip 192.16.0.1
interface FastEthernet1/0
 ip address 172.17.0.6 255.255.255.252
 speed auto
 duplex auto
interface FastEthernet1/1
 no ip address
 shutdown
 speed auto
 duplex auto
router eigrp 100
 network 10.0.0.0
 network 11.0.0.0
 network 172.17.0.0
```

```
 network 192.18.0.0
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.16.0.4
control-plane
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

ANEXO B – CONFIGURAÇÃO DOS ROTEADORES GLBP

Configuração do roteador R1

```
Current configuration : 1084 bytes
! Last configuration change at 20:19:10 UTC Thu Oct 27 2011
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
hostname R1
boot-start-marker
boot-end-marker
no aaa new-model
ip source-route
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
interface FastEthernet0/0
 ip address 192.17.0.2 255.255.255.0
 shutdown
 speed auto
 duplex auto
interface FastEthernet0/1
 ip address 192.16.0.2 255.255.255.0
 speed auto
 duplex auto
 glbp 10 ip 192.16.0.1
 glbp 10 priority 200
interface FastEthernet1/0
 ip address 172.17.0.5 255.255.255.252
```

```
 speed auto
 duplex auto
interface FastEthernet1/1
 no ip address
 shutdown
 speed auto
 duplex auto
router eigrp 100
 network 10.0.0.0
 network 172.17.0.0
 network 192.17.0.0
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.16.0.4
control-plane
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```

Configuração do roteador R2

```
Current configuration : 1016 bytes
! Last configuration change at 20:25:25 UTC Thu Oct 27 2011
version 12.2
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
hostname R2
boot-start-marker
boot-end-marker
no aaa new-model
ip source-route
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
interface FastEthernet0/0
 ip address 192.18.0.2 255.255.255.0
 speed auto
 duplex auto
interface FastEthernet0/1
 ip address 192.16.0.3 255.255.255.0
 speed auto
 duplex auto
interface FastEthernet1/0
 ip address 172.17.0.6 255.255.255.252
 speed auto
 duplex auto
 glbp 10 ip 192.16.0.1
interface FastEthernet1/1
 no ip address
 shutdown
 speed auto
 duplex auto
router eigrp 100
 network 10.0.0.0
 network 11.0.0.0
 network 172.17.0.0
```

```
 network 192.18.0.0
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.16.0.4
control-plane
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
end
```