Alta disponibilidade em redes IPv6 críticas utilizando o protocolo CARP

Carlos Kenji Kitahara, Lennon Soeiro
IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo
cakenji@gmail.com e lennonjs@gmail.com

Dr. Alexandre José Barbieri de Souza
IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo
abarbieris@hotmail.com

***Resumo*—A crescente dependência dos negócios com a TI aumenta a necessidade das organizações de adotarem soluções de alta disponibilidade em sua infraestrutura de rede. O protocolo Common Address Redundancy Protocol (CARP) é uma solução livre desenvolvida pelo grupo OpenBSD que fornece redundância em nível de gateway. O objetivo deste artigo é avaliar a utilização do protocolo CARP em redes IPv6 e realizar uma análise comparativa com outros protocolos específicos de redundância de gateway como o HSRP, VRRP e GLBP, além do protocolo NDP utilizado em redes IPv6. Na avaliação foi realizado um experimento com o objetivo de medir o tempo de recuperação do protocolo CARP após a interrupção do gateway padrão em uma rede com roteamento OSPFv3 configurado.**

I. INTRODUÇÃO

Para muitas empresas, a informação e a tecnologia que a suporta representa o seu bem mais valioso [6], tornando a área da Tecnologia da Informação (TI) fundamental para a execução dos seus acordos e transações comerciais (negócio) [1]. Consequentemente é essencial que sejam implementadas soluções garantam a disponibilidade das redes de computadores, que são os elementos principais da infraestrutura de TI.

A disponibilidade é a garantia de que um sistema computacional possa ser acessado por seus usuários quando estes necessitarem acessá-lo. O mecanismo de disponibilidade envolve a redundância de hardware, inteligência de software e protocolos para identificar a existência de falha do sistema principal para iniciar e concluir um processo de transferência dos serviços para sistemas alternativos [4].

Uma das técnicas adotadas para se evitar as indisponibilidades nas redes de computadores, prover tolerância a falhas e garantir a continuidade dos serviços críticos de TI é a utilização de gateways redundantes. A figura 1 mostra uma estrutura básica de redundância de rede com dois roteadores.

Este artigo foi desenvolvido com intuito de avaliar o protocolo de redundância de gateways CARP (Common Address Redundany Protocol) em redes IPv6 e realizar uma análise comparativa com os protocolos HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol) e GLBP (Gateway Load Balance Protocol) além do protocolo NDP (Neighbor Discovery Protocol) utilizado em redes IPv6. No processo de avaliação foi realizado um experimento visando medir o tempo de recuperação gasto pelo protocolo após a interrupção do gateway principal em uma rede IPv6.

O artigo está organizado da seguinte forma, a seção 2 descreve os protocolos HSRP, VRRP, GLBP, o protocolo NDP para redes IPv6 e o protocolo CARP. A seção 3 apresenta a análise comparativa dos protocolos. A seção 4 apresenta o experimento com o protocolo CARP e seu resultado e a seção 5 a conclusão do artigo. Finalmente na seção 6 apresentam-se sugestões de trabalhos futuros.

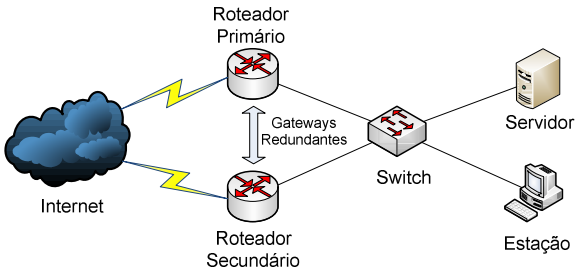

Figura 1. Estrutura Básica de Redundância.

II. PROTOCOLOS DE REDUNDÂNCIA RELACIONADOS

Além do protocolo CARP existem outras soluções que podem ser utilizadas para prover redundância de gateways. Dentre as soluções destacam-se os protocolos HSRP e GLBP da empresa Cisco Systems e o VRRP criado pela IETF e disponível nos produtos de muitas empresas tais como Juniper Networks, 3Com Corporation e a própria Cisco Systems. O VRRP é implementado também em plataformas livres como Linux e BSD [5].

Outro protocolo que pode fornecer redundância é o *Neighbor Discovery Protocol* (NDP) em redes IPv6. Utilizando este protocolo, os equipamentos recebem informações sobre os roteadores da rede através da mensagem enviada periodicamente chamada *Router Advertisement* e podem detectar uma falha através do mecanismo *Neighbor Unreachability Detection* [13].

A seguir apresentam-se resumidamente os protocolos HSRP, VRRP, GLBP e o protocolo NDP para redes IPv6.

A. *HSRP (Hot Standby Router Protocol)*

O HSRP é um protocolo de redundância desenvolvido pela empresa Cisco Systems que fornece tolerância a falhas no contexto de gateway. O protocolo permite que dois ou mais roteadores pertencentes a um grupo chamado *HSRP group* ou *standby group* compartilhem um endereço IP e um endereço MAC denominados endereços virtuais.

Apenas um dos roteadores denominado *active* é responsável pelo encaminhamento dos pacotes. Os demais

roteadores dentro do grupo são chamados *standby* e permanecem em um estado de espera. A definição dos papéis *active* e *standby* é realizada através de um processo de eleição em que o roteador de maior prioridade é designado como ativo. Periodicamente os roteadores trocam mensagens chamadas *Hello* com o objetivo de identificar possíveis falhas.

No caso de uma falha no roteador designado como ativo, o roteador *standby* assume o endereço IP e o endereço MAC virtuais. Se o roteador designado como *standby* falha ou ele torna-se o roteador ativo, uma nova eleição é realizada para designação de um novo roteador *standby*. A identificação de uma falha é realizada através do parâmetro *Hold Time* que é o intervalo de tempo na qual os roteadores aguardam as mensagens do tipo *Hello*. Caso um roteador não receba mensagens *Hello* no período informado pelo parâmetro *Hold Time* considera-se que o outro roteador está indisponível [12].

B. VRRP (Virtual Router Redundancy Protocol)

Assim como o HSRP o VRRP é um protocolo que fornece redundância de gateway e permite o compartilhamento de um endereço IP e endereço MAC por vários roteadores. Um dos roteadores denominado de *Master* é o responsável pelo encaminhamento dos pacotes. Os outros roteadores pertencentes ao grupo de redundância são denominados *Backup*.

A definição do papel de *Master* também é definido por um processo de eleição em que o roteador com maior prioridade é eleito o roteador principal.

O intervalo de tempo da troca de mensagens entre os roteadores é configurado pelo parâmetro *Advertisement_Interval* que por padrão é igual a 1s. Já a identificação da falha é realizada através do parâmetro *Master_Down_Interval* calculado pela fórmula [11]:

$$(3 * \text{Master\_Adver\_Interval}) + \frac{((256 - \text{priority}) * \text{Master\_Adver\_Interval})}{256}$$

O parâmetro *Master_Adver_Interval* possui valor inicial igual ao *Advertisement_Interval.* Decorrido o tempo configurado no parâmetro *Master_Down_Interval*, após a falha do roteador *Master,* inicia-se automaticamente um novo processo de eleição do roteador responsável pelo encaminhamento de pacotes.

C. GLBP (Gateway Load Balance Protocol)

Protocolo de redundância desenvolvido pela empresa Cisco Systems que além de fornecer tolerância a falhas oferece também balanceamento de carga no contexto de gateway. O balanceamento de carga é realizado através do compartilhamento pelos roteadores de um único IP virtual e múltiplos endereços MAC.

Tecnicamente, o funcionamento do protocolo GLBP é muito similar ao HSRP, porém o gateway que antes estava em modo *standby* passa a ser utilizado em paralelo como um gateway ativo.

Membros de um grupo do GLBP elegem o roteador de maior prioridade como o *Active Virtual Gateway* (AVG). Este roteador determina um endereço MAC para cada um dos roteadores do grupo que são denominados *Active Virtual Forwarder* (AVF). Para cada requisição ARP recebida para o endereço virtual, o AVG responde com um dos endereços MAC virtual, transferindo a responsabilidade do encaminhamento dos pacotes ao dono daquele MAC, possibilitando assim o balanceamento [3].

Os roteadores de um grupo GLBP comunicam-se através de mensagens *Hello* enviadas a cada 3 segundos e assim como o HSRP após 10 segundos sem o recebimento da mensagem *Hello* o equipamento é considerado como indisponível e um processo de eleição é iniciado.

D. NDP (Neighbor Discovery Protocol)

Uma das funcionalidades nas redes IPv6 é o protocolo NDP que habilita a detecção de roteadores (*Router Discovery*). Apesar de não ser um protocolo específico para redundância de gateways ele pode fornecer alta disponibilidade em uma rede IPv6.

Os processos do NDP utilizam 5 tipos diferentes de pacotes ICMPv6 [13], um par de mensagens *Router Solicitation* e *Router Advertisement*, um par de mensagens *Neighbor Solicitation* e *Neighbor Advertisement* e uma mensagem *Redirect*.

No processo de identificação de um roteador em seu enlace, um nó envia uma mensagem *Router Solicitation* utilizando *multicast*. Roteadores no mesmo enlace respondem com a mensagem *Router Advertisement* ao nó solicitante que configura o endereço do roteador. Periodicamente roteadores enviam mensagens *Router Advertisement* utilizando *multicast* em seu enlace.

A falha de um roteador pode ser detectada por um host através do mecanismo *Neighbor Unreachability Detection*. Para confirmação de que um roteador está ativo nós enviam mensagens *unicast Neighbor Solicitation* e aguardam mensagens *Neighbor Advertisement*. Visando evitar tráfego excessivo essas mensagens são enviadas apenas para nós que estão trafegando dados ativamente e após a indicação de que um roteador não está comunicando. Utilizando os parâmetros padrão do protocolo NDP, leva-se aproximadamente 38 segundos para que o nó perceba que um roteador está indisponível e altere o roteador padrão para outro roteador [13].

E. CARP (Common Address Redundany Protocol)

O protocolo CARP, Common Address Redundancy Protocol, desenvolvido pelo projeto OpenBSD também tem por objetivo garantir a redundância através do compartilhamento de um endereço IP virtual por múltiplos computadores. Sua criação pela comunidade O*pen Source* serve como alternativa livre e segura ao protocolo VRRP que possui sua especificação reivindicada pela empresa Cisco Systems [2].

O computador principal denominado *Master* responde a qualquer tráfego ou requisições ARP direcionadas para o IP compartilhado. Os outros membros do grupo são denominados *Backup* assim como no VRRP. Cada computador pode pertencer a mais de um grupo de redundância por vez [9].

O computador *Master* envia anúncios CARP com maior freqüência e é influenciado pelos parâmetros *advbase* e *advskew* pela fórmula ***advbase + (advskew/255))***. O primeiro parâmetro é a base do intervalo de anúncios já o segundo influencia o intervalo de anúncios CARP. Quanto menor o valor maior a probabilidade de o computador ser considerado *Master* [8]. O valor padrão para *advbase* é 1 segundo e para *advskew* é 0.

Cada membro do grupo verifica se a periodicidade de seu anúncio é menor que os anúncios do nó *Master*. Se por alguma razão o nó *Master* falhar após o valor correspondente a ***3*(advbase + (advskew/255)))*** segundos [7] todos os computadores *Backup* enviam seus anúncios baseados em seus próprios parâmetros. Aquele de maior freqüência é eleito o novo mestre.

No quesito segurança o protocolo CARP utiliza o algoritmo de assinatura HMAC SHA-1 para a checagem de integridade e autenticidade dos anúncios [8].

III. COMPARAÇÃO ENTRE OS PROTOCOLOS

Após a apresentação dos protocolos é possível a realização de uma análise comparativa levando em consideração características como tempo total gasto para a recuperação, ou seja, quando o outro roteador (backup) assume o IP do gateway no caso de uma falha no roteador principal, balanceamento de carga e suporte a IPv6. As tabelas I e II apresentam as principais características dos protocolos HSRP, VRRP, GLBP e CARP. Apesar de o NDP fornecer alta disponibilidade ele não é um protocolo específico de redundância de gateways desse modo sua comparação ficou restrita apenas ao tempo de recuperação.

Podem-se visualizar características comuns entre o protocolo CARP e os outros protocolos específicos de redundância de gateways como a possibilidade de configuração de *preempt*, ou seja, tornar o roteador com maior prioridade sempre o mestre, suporte a IPv6 e a utilização do protocolo de transporte UDP para troca de mensagens entre os roteadores. No caso do balanceamento de carga apenas os protocolos CARP e GLBP podem realizar o balanceamento utilizando um único IP virtual. Para os protocolos HSRP e VRRP o balanceamento de carga é realizado utilizando-se vários IPs virtuais.

Conforme tabelas I e II tanto o protocolo CARP quanto os outros protocolos possibilitam a configuração do intervalo de tempo dos anúncios do roteador mestre e do tempo para que os roteadores backup elejam um novo roteador principal após a falha do roteador mestre. O protocolo CARP assim como o VRRP nos padrões de configuração possui tempo de recuperação menor que o dos protocolos proprietários.

Em relação ao protocolo NDP utilizado em redes IPv6 constata-se que dentro ainda das configurações padrões, todos os protocolos de redundância gateways apresentados possuem tempo de recuperação menor que o NDP que é de aproximadamente 38 segundos. Vale destacar que no protocolo NDP é possível reduzir os parâmetros de tempo porém essa configuração causa um aumento significativo no tráfego principalmente em enlaces com muitos nós.

Tabela I
CARACTERÍSTICAS DOS PROTOCOLOS HSRP E VRRP

Protocolos	HSRP	VRRP
Criado por	Cisco	IETF
Intervalo de anúncios do roteador mestre	Padrão 3 seg	Padrão 1 seg
Tempo de recuperação	Padrão 10 seg	Padrão 3 seg
Ajuste de tempo	Sim	Sim
Preemption	Sim	Sim
Protocolo de Transporte	UDP/1985	UDP/112
Balanceamento de Carga	Cada estação cliente recebe um endereço de gateway diferente	Cada estação cliente recebe um endereço de gateway diferente
Suporte a IPV6	Sim	Sim
Endereço Virtual	00:00:0C:07:AC:{group}	00:00:5E:00:01:{VRID}

Tabela II
CARACTERÍSTICAS DOS PROTOCOLOS GLBP E CARP

Protocolos	GLBP	CARP
Criado por	Cisco	OpenBSD
Intervalo de anúncios do roteador mestre	Padrão 3 seg	Padrão 1 seg
Tempo de recuperação	Padrão 10 seg	Padrão 3 seg
Ajuste de tempo	Sim	Sim
Preemption	Sim	Sim
Protocolo de Transporte	UDP/3222	UDP/112
Balanceamento de Carga	Sim	Sim
Suporte a IPV6	Sim	Sim
Endereço Virtual	00:07:b4{group, AVF}	00:00:5E:00:01:{VHID}

IV. EXPERIMENTO

O experimento com o protocolo CARP visa medir o tempo de recuperação após a queda do roteador principal. No experimento também foi configurado roteamento com o protocolo OSPFv3 [10] com o propósito de identificar o impacto do tempo de recuperação do protocolo CARP em uma rede com roteamento configurado. A topologia do experimento encontra-se na figura 2.

Através da estação foram gerados pacotes ICMPv6 para o IP configurado nos gateways redundantes e para o servidor. Durante o envio dos pacotes o roteador mestre foi interrompido e realizada a medição do tempo total para que a comunicação fosse restabelecida. Para o experimento foram definidas 10 amostras.

Na montagem do ambiente da figura 2 foram utilizados os sistemas operacionais Windows XP e Debian 6.0.3 respectivamente para a estação e o servidor. Nos roteadores foi utilizado o sistema operacional FreeBSD 8.2. O software utilizado para roteamento foi o Quagga e o tempo de indisponibilidade foi calculado através da captura de pacotes ICMPv6 utilizando-se o software Wireshark. As figuras 3 e 4 contêm o resultado das informações coletadas.

O protocolo CARP teve como tempo médio de recuperação 2,93 segundos e desvio padrão 0,06. Já o protocolo OSPFv3, conforme figura 3, teve como tempo médio de convergência 37,44 segundos e desvio padrão 0,79.

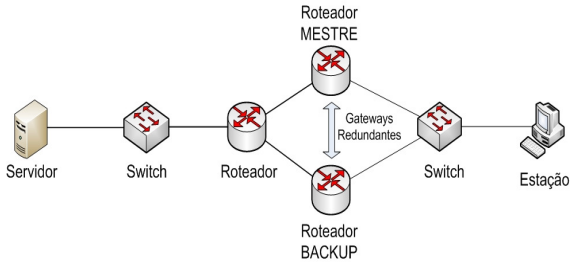

Figura 2**:** Topologia para avaliação dos protocolos

O resultado mostra que nas configurações padrões, o tempo de recuperação do protocolo CARP é significativamente menor que o tempo de convergência do protocolo OSPFv3 indicando desse modo que em uma rede com roteamento OSPFv3 configurado e que utiliza o protocolo CARP para redundância de gateway a disponibilidade será impactada principalmente pelo tempo de convergência do protocolo de roteamento.

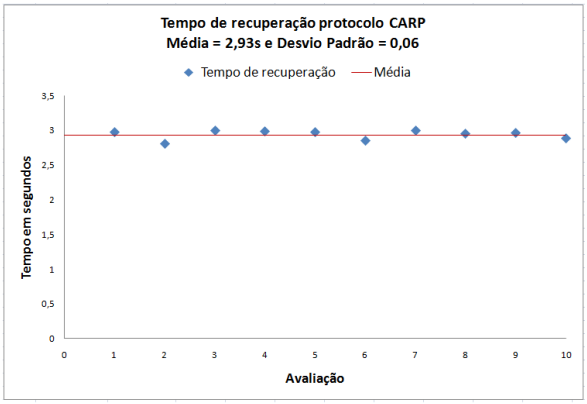

Figura 3: Tempo de recuperação CARP

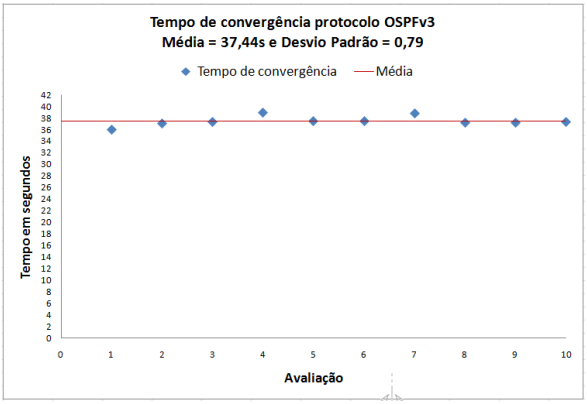

Figura 4: Tempo de convergência OSPFv3

V. CONCLUSÃO

A disponibilidade da infraestrutura de TI, em especial da rede de computadores, é fundamental para muitas organizações já que o negócio das empresas está cada vez mais dependente da tecnologia. Para garantir a disponibilidade da rede em ambientes críticos é essencial que soluções como a utilização de gateways redundantes sejam adotadas pelas organizações.

Visando avaliar o protocolo CARP foi realizada uma análise comparativa com outros protocolos específicos de redundância de gateways dentre eles o HSRP, VRRP e o GLBP além do protocolo NDP utilizado em redes IPv6. Verificou-se que o protocolo CARP suporta várias características presentes em outros protocolos como a configuração de *preempt*, suporte a IPv6 e balanceamento de carga. Além disso, constatou-se que na configuração padrão, o tempo de recuperação do protocolo CARP é menor que o dos protocolos HSRP, GLBP e NDP.

No experimento realizado com o protocolo CARP em uma rede com roteamento OSPFv3 foi possível identificar que a disponibilidade, na configuração padrão dos protocolos, será afetada pelo tempo de convergência do protocolo OSPFv3.

VI. TRABALHOS FUTUROS

O escopo deste trabalho limitou-se ao estudo da alta disponibilidade fornecida pelo protocolo CARP. Como pesquisa futura sugere-se estudar o processo de balanceamento de carga do protocolo CARP. Outra sugestão de trabalho seria analisar experimentalmente o desempenho do protocolo CARP utilizando vários níveis de tráfego.

REFERÊNCIAS

[1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação. Rio de Janeiro: ABNT, 2008.

[2] CARP. "The Common Address Redundancy Protocol", Disponível em http://www.openbsd.org/faq/faq6.html#CARP. Acessado em 08/04/2012.

[3] Cisco, GLBP – Gateway Load Balancing Protocol. Disponível em http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html. Acessado em 12/05/2012.

[4] E. Lopes Filho, "Arquitetura de Alta Disponibilidade para Firewall e IPS baseada em SCTP", Dissertação de Mestrado em Ciência da Computação, Universidade Federal de Uberlândia, Minas Gerais, 2008.

[5] G. Attebury and B. Ramamurthy, "Router and Firewall Redundancy with OpenBSD and CARP", Department of Computer Science and Engineering, University of Nebraska-Lincoln, in IEEE ICC 2006.

[6] IT GOVERNANCE INSTITUTE. "Control Objectives for Information and Related Technology 4.1 (Cobit 4.1)". 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA 2007. Tradução e revisão pelo Projeto COBIT-BR.

[7] OpenBSD Manual Pages, ifconfig (8) Disponível em http://www.openbsd.org/cgi-bin/man.cgi?query=ifconfig#end. Acessado em 08/04/2012.

[8] P. Danhieux, "CARP The Free Fail-over Protocol", Global Information Assurance Certification Paper, SANS Institute, 2004

[9] PF: Firewall Redundancy with CARP and pfsync, Disponível em http://www.openbsd.org/faq/pf/carp.html. Acessado em 08/04/2012.

[10] R. Coltun, D. Ferguson, J. Moy and A. Lindem, Ed., "OSPF for IPv6", RFC 5340, July 2008.

[11] S. Nadas, "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6". IETF, RFC 5798, 2010.

[12] T. Li, B. Cole, P. Morton and D. Li, "Cisco Hot Standby Router Protocol (HSRP)" . IETF, RFC 2281, 1998.

[13] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.