

Tolerância a Falhas utilizando Protocolos de *Gateway* Redundantes

Alessandro Kraemer¹, Kaio Vilar², Alfredo Goldman³

¹Coordenação de Informática – Universidade Tecnológica Federal do Paraná (UTFPR)
Campo Mourão – PR – Brazil

²Centro de Atendimento Técnico ao Cliente – Embratel - Brasília – DF - Brazil

³Departamento de Ciência da Computação – Instituto de Matemática e Estatística –
Universidade de São Paulo (IME-USP)
São Paulo – SP - Brazil

kraemer@utfpr.edu.br, kavilar@embratel.com.br, gold@ime.usp.br

Abstract. *The goal of this paper is to compare fault-tolerant protocols inside of redundancy gateway context. For this purpose, performance tests were conducted with specific protocols, like HSRP, VRRP and GLBP. The results indicate which protocol will recover more quickly from the interruption of the default gateway.*

Resumo. *O objetivo deste artigo é comparar protocolos de tolerância a falhas em contexto de gateway redundante. Para tanto, foram executados testes com protocolos específicos, como HSRP, VRRP e GLBP. Os resultados apontam qual protocolo se recupera mais rapidamente a partir da interrupção do gateway padrão.*

1. Introdução

A tecnologia de tolerância a falhas é considerada um requisito em sistemas de missão crítica [Song e Choi, 2001, p.315]. A redundância é uma técnica importante deste contexto. Ela ocorre em vários níveis, desde a comunicação envolvendo o cabeamento até a replicação de servidores e ativos de rede. A duplicação de *gateways* também é um exemplo de uso de redundância [Lefrève et al., 2006, p.258].

Shinn [2009] descreve mecanismos de *gateways* redundantes. A característica principal desses protocolos é que vários *gateways* trocam mensagens a fim de perceber se podem assumir o lugar de outro, seja por falha ou por necessidade de balanceamento de carga.

Este artigo apresenta os mecanismos de redundância utilizados pelos protocolos HSRP (*Hot Standby Router Protocol*), VRRP (*Virtual Router Redundancy Protocol*) e GLBP (*Gateway Load Balance Protocol*). Por fim, é apresentado um cenário de rede com *gateways* redundantes utilizado para avaliar esses protocolos. O cenário foi implementado em laboratório de redes com roteadores CISCO e computadores com Linux, procurando gerar estresse de acessos HTTP, como comumente ocorre em situações reais de uso da Internet.

2. Protocolos de *Gateway* Redundantes

2.1. Protocolo HSRP

O HSRP é padronizado pela RFC 2281 e consiste em configurar grupos de roteadores com endereçamento IP e MAC distintos. Assim, existirão vários *gateways* para uma mesma rede. Os roteadores possuem um segundo endereço, chamado de IP Virtual e MAC Virtual. Este endereço é idêntico em todos os roteadores do domínio [Shinn, 2009, pp.274]. Contudo, os computadores da rede conhecem apenas um *gateway* virtual.

Os roteadores envolvidos neste processo trocam mensagens conhecidas como *Hello*, a fim de verificar o estado operacional do seu vizinho. Dentro do grupo de roteadores, apenas um roteador fica em estado Ativo e os demais ficam em estado de *backup*. Embora o HSRP não possua balanceamento de carga nativo, é possível implementá-lo criando vários grupos com IP Virtuais distintos [Shinn, 2009, pp.274].

2.2. Protocolo VRRP

O VRRP é uma alternativa ao HSRP, detalhado pela RFC 3768. Neste protocolo, os endereços reais e virtuais podem participar efetivamente do mecanismo de redundância. A comunicação entre os *gateways* ocorre através de mensagens similares ao *Hello*, mas são conhecidas como *Link-State Advertisement (LSA)*. O papel de enviar essas mensagens é do roteador conhecido como Mestre [Shinn 2009, p.274] [Song e Choi, 2001, p.317]. Quando o Mestre falha, outro roteador com prioridade logo abaixo percebe a ausência de LSA e assume seu papel.

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

2.3. Protocolo GLBP

A principal diferença do GLBP em relação aos demais é que ele consegue atribuir diferentes endereços MAC para um mesmo IP Virtual. No HSRP e no VRRP existe um *gateway* principal e os outros são *backup*, enquanto no GLBP, os *gateways* de *backup* são também conhecidos como encaminhadores. Os encaminhadores também são ativos.

No GLBP existem dois tipos de *gateways* ativos: o *Gateway Virtual Ativo (AVG)* e o *Gateway Virtual Encaminhador (AVF)*. O AVG é eleito pelo grupo e os AVF são seus *backups*. A cada solicitação ARP feita ao AVG é devolvido o MAC Virtual de outro roteador AVF. Com este mecanismo, o endereço MAC do *gateway* armazenado na tabela ARP do cliente não é o mesmo em todas as estações, permitindo o balanceamento da carga [Satapati et al., 2004, pp.02].

2.4. Comparação entre os Protocolos

O objetivo da comparação é descobrir quanto tempo é gasto até que os elementos de rede percebam que o *gateway* principal foi interrompido e que um novo caminho deve ser seguido. Embora este critério seja importante, ele não pode ser analisado isoladamente. Também é importante considerar os padrões de tempo de cada protocolo. Quando um roteador recebe uma mensagem *Hello/LSA*, ele a torna válida somente por um período de tempo, isto é conhecido como *holdtime*. Se o *holdtime* exceder e não

chegar outra mensagem, o enlace é considerado falho, dando início a substituição de *gateway*. O ajuste desses parâmetros pode alterar o resultado da comparação. Neste artigo, os protocolos são avaliados considerando seus padrões de tempo (Tabela 1).

Tabela 1. Características dos protocolos de *gateway* redundantes.

Protocolo	Equipamentos necessários	Forma de Endereçamento	Balaceamento de carga	Tempo padrão
HSRP proprietário	Roteadores CISCO	Um IP e um MAC Virtuais idênticos em cada roteador do grupo	Não é nativo	3 seg. (<i>Hello</i>) 10 seg. (<i>Holdtime</i>)
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. (<i>LSA</i>) 3 seg. (<i>Holdtime</i>)
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. (<i>Hello</i>) 10 seg. (<i>Holdtime</i>)

A Figura 1 representa o cenário elaborado para avaliação destes protocolos. Nesse cenário, cada computador tem o papel de executar acessos HTTP por meio de um aplicativo Java elaborado para este fim. O tempo total do acesso considera desde a conexão até o recebimento do conteúdo do site. O teste consiste em interromper o *gateway* padrão enquanto são realizados vários acessos ao servidor. Nesses momentos, os aplicativos mantêm a sessão com o servidor, mas o tempo gasto se diferencia do acesso normal. O mesmo sistema de avaliação se repetiu 10 vezes para cada protocolo.



Figura 1. Cenário para avaliação dos protocolos de *gateway*.

A Figura 2 apresenta o resultado da avaliação, indicando o tempo gasto para que a sessão do momento da interrupção fosse direcionada ao novo *gateway* padrão. Por exemplo, durante a segunda interrupção, tanto para o GLBP quanto para o HSRP, o tempo da sessão HTTP foi o mesmo nas duas estações (aproximadamente 13 segundos). Por outro lado, no VRRP foram gastos apenas 3 segundos.

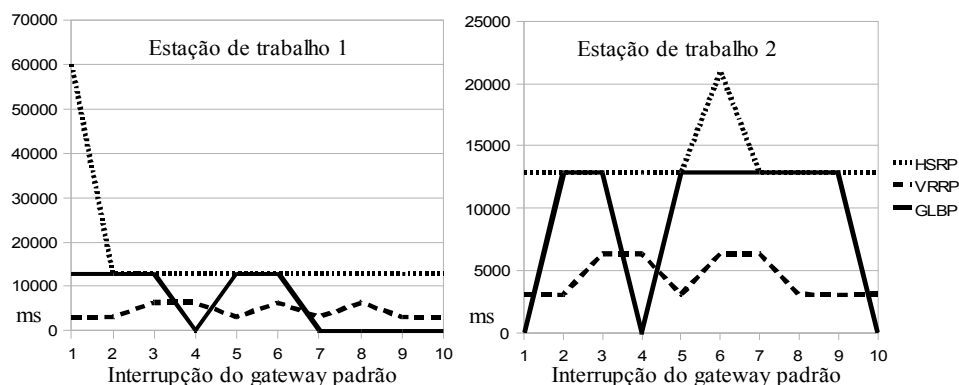


Figura 2. Resultado da avaliação.

Embora os *gateways* tenham sido interrompidos apenas 10 vezes em cada configuração de protocolo, foi possível observar um comportamento padrão. O VRRP consegue ser o mais rápido na definição do novo *gateway* padrão, chegando algumas vezes a consumir apenas $\frac{1}{4}$ do tempo dos demais protocolos, e no pior caso chegando a 50%. O GLBP mantém um tempo linear de recuperação e em alguns casos consegue ser totalmente transparente, com tempos muito próximos ao estado anterior da interrupção do *gateway*, como apresenta a Figura 2 ao declínio linear do 4º processo de interrupção. Por fim, o HSRP possui tempos de recuperação similares ao GLBP, mas sem os casos especiais de acesso com tempos imperceptíveis. A desvantagem do HSRP é que em seu estado de configuração padrão não existe balanceamento de carga, o que pode ter influenciado no resultado final.

3. Considerações Finais

A principal característica dos protocolos HSRP, VRRP e GLBP é que eles gerenciam um mesmo IP de *gateway* 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, tentando melhorar o desempenho do protocolo. Para as estações de trabalho, todo esse processo é transparente, pois elas conhecem apenas o IP 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* padrão. Uma razão para isto é que seus padrões de tempo de mensagens *Hello* e *holdtime* são menores que os demais protocolos. Outra característica importante é o custo da implantação. Os três protocolos explorados podem ser configurados em roteadores CISCO, mas o VRRP também está disponível em plataformas Linux, o que também pode ser considerada uma vantagem em relação aos demais. O protocolo GLBP tem melhor desempenho que o HSRP, já que os padrões de tempo são os mesmos e em alguns acessos o GLBP demonstrou ser totalmente transparente. Demais testes devem ser realizados ajustando os tempos das mensagens de estado dos protocolos GLBP e VRRP.

Referências

- Lefèvre, L., Neira, P. and Gasca, R. M. (2006). High Availability support for the design of stateful networking equipments. In IEEE Computer Society, pages 254-261. Proceedings of the First International Conference on Availability, Reability and Security.
- Shinn, S. K. (2009). Fault Tolerance Virtual Router for Linux Virtual Server. In IEEE Computer Society, pages 273-275. International Conference on Future Networks.
- Satapati, S., Wilson, I. H. and McLaggan, D. Network Address Translation with Gateway Load Distribution. US Patent 2004/0215752, filed Mar, 28, 2003, and issued Oct, 28, 2004.
- Song, S. and Choi, B. (2001). Scalable Fault-Tolerant Network Design for Ethernetbased Wide Area Process Control Network Systems. In IEEE Computer Society, pages 315-323. 8th IEEE International Conference on Emerging Technologies and Factory Automation.