



**ANTÔNIO MARCOS SILVA
BRENNO COSTA CLEMENTE**

**AVALIAÇÃO DE DESEMPENHO DO PROTOCOLO
DE GATEWAY REDUNDANTE VRRP: UMA OPÇÃO
AO HSRP EM ROTEADORES CISCO**

**INCONFIDENTES-MG
2015**

**ANTONIO MARCOS SILVA
BRENNO COSTA CLEMENTE**

**AVALIAÇÃO DE DESEMPENHO DO PROTOCOLO DE
GATEWAY REDUNDANTE VRRP: UMA OPÇÃO AO HSRP
EM ROTEADORES CISCO**

Trabalho de Conclusão de Curso apresentado como pré-requisito de conclusão do curso de Graduação Tecnológica em Redes de Computadores no Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais – Câmpus Inconfidentes, para obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Vinícius Ferreira de Souza

**INCONFIDENTES-MG
2015**

**ANTONIO MARCOS SILVA
BRENNO COSTA CLEMENTE**

**AVALIAÇÃO DE DESEMPENHO DO PROTOCOLO DE
GATEWAY REDUNDANTE VRRP: UMA OPÇÃO AO
HSRP EM ROTEADORES CISCO**

Data de aprovação:

Me. André Luigi Di Salvo – IFULDEMINAS – Inconfidentes

Ivan Paulino Pereira – IFULDEMINAS – Inconfidentes

Kleber Marcelo da Silva Rezende – IFULDEMINAS – Inconfidentes

Avaliação de Desempenho do Protocolo de Gateway Redundante VRRP: uma opção ao HSRP em roteadores Cisco

Brenno C. Clemente¹, Antônio M. Silva², Orientador Vinícius F. De Souza³

Setor de Informática e Redes
IFSULDEMINAS – Campus Inconfidentes – Inconfidentes, MG – Brasil

¹brennoclemente@hotmail.com, ²ant.marcos.silv@gmail.com,
³vinicius.souza@ifsulde Minas.edu.br

Abstract. *This paper presents a performance evaluation of the redundant gateway protocol Virtual Router Redundancy Protocol (VRRP), implemented in a setting that uses equipment from Cisco Systems manufacturer. By comparing held with Cisco proprietary protocol, the same function, Hot Standby Router Protocol (HSRP), it was found in the analysis of monitored parameters that VRRP protocol is a viable alternative for gateway redundancy configuration in Cisco equipment.*

Resumo. *Este trabalho apresenta uma avaliação de desempenho do protocolo de gateway redundante Virtual Router Redundancy Protocol (VRRP), implementado em um cenário que utiliza equipamentos da fabricante Cisco Systems. Através da comparação realizada com o protocolo proprietário Cisco, de mesma função, Hot Standby Router Protocol (HSRP), verificou-se na análise dos parâmetros monitorados que o protocolo VRRP é uma alternativa viável para a configuração de redundância de gateway em equipamentos Cisco.*

1. Introdução

Em redes de computadores, o termo disponibilidade torna-se essencial quando o assunto é a oferta de serviços baseados na arquitetura cliente/servidor e a troca de dados críticos em um enlace WAN (*Wide Area Network*). O parâmetro disponibilidade indica o tempo que a rede permanece em funcionamento de forma ininterrupta, incluindo possíveis falhas de hardware ou software, além de manutenções preventivas e corretivas [PAULINO, 2010;MAIA, 2013].

Para garantir alta disponibilidade é necessário o uso de mecanismos de tolerância a falhas e balanceamento de carga. Essa implementação pode ser realizada no lado do cliente ou no lado da operadora. Nesse contexto, a redundância é uma técnica amplamente utilizada em vários níveis, desde a comunicação envolvendo o cabeamento até a replicação de servidores e ativos de rede. Outro mecanismo de redundância é a duplicação de gateways [PAULINO, 2010;SHINN, 2009].

Na maioria das redes de computadores, um único equipamento é utilizado como *default gateway* e todos os hosts no mesmo segmento encaminham suas mensagens para essa máquina *gateway*, que funciona como uma única saída da rede interna para a rede externa. Mesmo que existam enlaces e equipamentos duplicados, quando ocorre uma falha na máquina *gateway* ou no enlace que dá acesso ao *gateway*, a comunicação com a rede externa é interrompida.

Para manter a disponibilidade da rede nesse cenário, são utilizados os protocolos de *gateway* redundante. Tais protocolos gerenciam os enlaces redundantes e são capazes de, ao detectar uma falha no enlace, habilitar um caminho secundário previamente configurado. Shinn (2009) afirma que a principal característica desses protocolos é permitir que vários *gateways* troquem mensagens, com a finalidade de perceberem se devem ou não assumir o lugar de outro *gateway*, seja por uma falha ou por necessidade de balanceamento de carga.

Quando se discute redundância de *gateways*, dois protocolos têm sido amplamente utilizados: VRRP (*Virtual Router Redundancy Protocol*) e HSRP (*Hot Standby Router Protocol*). O primeiro, definido na RFC 5798, é independente de fabricante e, portanto, pode ser configurado em qualquer equipamento. Já o segundo, formalizado na RFC 2281, é um protocolo proprietário Cisco.

No protocolo VRRP, os endereçamentos reais e virtuais podem participar, efetivamente, do processo de redundância. O roteador principal, chamado de mestre, tem o papel de enviar mensagens para os roteadores de *backup*. Quando o roteador mestre falha, os roteadores de *backup* percebem a ausência de mensagens, e o roteador em espera com a prioridade mais alta assume como roteador mestre [NADAS, 2010].

O protocolo HSRP permite a configuração de um conjunto de roteadores operando em comum acordo, para apresentar a ilusão de um único roteador virtual para os hosts na rede local. Esse conjunto é conhecido como grupo de HSRP ou grupo em espera. Um único roteador eleito no grupo, denominado roteador ativo, é responsável por encaminhar os pacotes que os *hosts* enviam ao roteador virtual. Em caso de falha do roteador ativo, um roteador eleito como *standby* assume as funções do roteador ativo.

Apenas os roteadores nos modos ativo e em *standby* enviam mensagens de HSRP periódicas, depois do protocolo ter concluído o processo de eleição do roteador em *standby* [LI et al., 1998].

Atualmente, as infraestruturas de redes reúnem soluções de diferentes fabricantes em camadas distintas da arquitetura de rede. Apesar de possuírem interoperabilidade com soluções de outros fabricantes, os equipamentos Cisco utilizam algumas tecnologias com direito proprietário, o que faz do protocolo HSRP uma solução exclusiva da Cisco para redundância de *gateways*.

Como a literatura referente ao assunto é escassa, este trabalho apresenta uma topologia de rede com *gateways* redundantes, a fim de analisar o desempenho do protocolo VRRP em equipamentos Cisco, comparado à solução proprietária, mediante a avaliação de alguns parâmetros selecionados, verificou-se o comportamento dos roteadores Cisco, configurados com o protocolo VRRP, no instante de falha do *gateway* padrão. Os resultados obtidos apontam o protocolo VRRP como uma opção viável para a redundância de *gateways* em soluções Cisco.

2. Referencial Teórico

Nesta seção é apresentado os trabalhos os quais foram imprescindíveis para fomentar a ideia de aplicação dos protocolos e tais métodos de aplicação.

Shinn (2009) em seu trabalho relata com ênfase que o futuro da arquitetura de redes de computadores é diretamente ligado a evolução do uso da redundância de link, uma vez que quanto maior for a necessidade do dispositivo estar conectado, maior é a necessidade de se ter uma redundância eficiente.

Conforme Forouzan (2008), os protocolos de *gateway* redundante são parte integrante para uma nova arquitetura de redes de computadores. Com a evolução das características dos protocolos TCP/IP com o advento do IPV6, uma nova leva de equipamentos tornar-se-ão parte integrante da rede, tendo em vista o conceito de IoT (*Internet of Things*). Desta maneira com um maior número de itens conectados a Internet a população necessitará de uma conexão mais veloz e estável a rede mundial de computadores, assim sendo, Frouzan destaca três protocolos de redundância de *gateway* VRRP, HSRP, GLBP os quais são empregados para manter uma conexão redundante a rede.

Junior (2008), em seu trabalho Alta disponibilidade em roteadores: Um ambiente de teste, faz uma comparação técnica e financeira sobre a utilização do HSRP em equipamentos da fabricante Cisco Systems como sendo uma das melhores soluções para o mercado de grande porte levando em consideração algumas questões como suporte técnico a equipamentos e o grande leque de atuação da empresa em equipamentos e soluções de TI, tendo assim uma solução completa para a TI. Em contrapartida ele apresenta os baixos custos do uso do VRRP, uma vez que é livre para implementação em todo tipo de roteador que dê suporte a protocolos de redundância de *gateway* e a roteadores virtuais implementados em equipamentos com sistema operacional Linux, assim garantindo uma solução de redundância de *gateway* de baixo custo financeiro e com desempenho agradável comparado a hardwares dedicados.

No trabalho Tolerância a Falhas utilizando Protocolos de Gateway Redundantes, apresentado nos Anais da I Escola Regional de Alto Desempenho de São Paulo, o autor Kraemer (2010), demonstra uma comparação entre: redes de computadores implementadas com hardware dedicado Cisco x redes de computadores implementadas com hardwares não dedicados dotados do sistema operacional Linux Debian versão 7, já configurado para exercer a função de redundância de *gateway* a partir do protocolo VRRP. Nesta comparação vale destacar que o resultado final mesmo com o protocolo HSRP apresentando melhores resultados, foi satisfatório o uso do VRRP em equipamento não dedicado uma vez que sua implementação foi de baixo custo e a disparidade de resultados não foi algo consideravelmente grande.

Com a atual literatura disponível, não foi encontrado um trabalho que compare a implementação do protocolo VRRP em roteadores Cisco, visando uma interoperabilidade de fabricantes. Desta maneira este trabalho torna-se algo essencialmente importante uma vez que a interoperabilidade é algo pensado em todos projetos de redes de computadores.

3. Protocolos de Gateway Redundante

Protocolos de gateway redundante são responsáveis por garantir uma plena disponibilidade em redes de computadores, tais protocolos garantem que mesmo quando um dos links fique inativo outro assuma em seu lugar, chaveando o tráfego entre links distintos.

Conforme pode-se observar na Figura 1, toda rede a qual faça uso destes protocolos, necessita ter dois ou mais roteadores de saída para a rede externa. Este trabalho contempla os protocolos VRRP e do HSRP conforme já mencionado anteriormente. De acordo com Paulino (2010), a utilização de técnicas para garantir a redundância de gateway, começou a ser empregada em larga escala, a partir da última década onde tivemos a popularização dos microcomputadores e smartphones, de tal maneira que a maioria das empresas se tornaram reféns da tecnologia da informação e seus agregados.

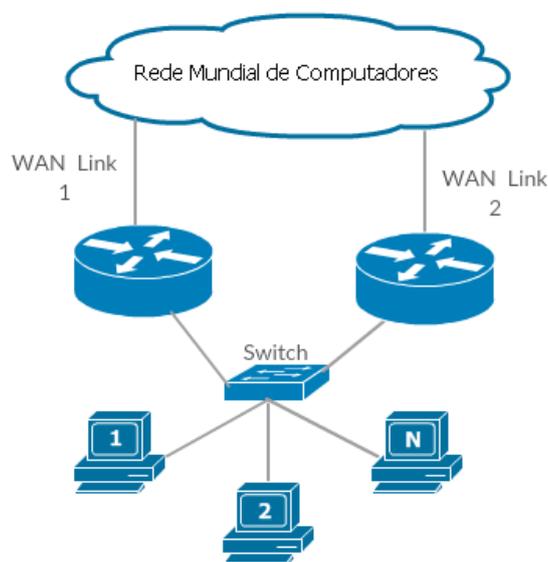


Figura 1 – Exemplo de cenário implementado com protocolo de gateway redundante.

2.1 Virtual Router Redundancy Protocol (VRRP)

De acordo com Kraemer (2010), no protocolo VRRP os endereços reais e virtuais podem participar efetivamente do processo de redundância. Quando o roteador mestre fica inoperante, 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 varia entre 1 até 254, e 100 é considerado como valor padrão.

O VRRP possui as seguintes características com objetivos de otimizar a utilização do protocolo: *tracking* (utilizado para verificar o status da interface a ser monitorada), preempção (determinar a prioridade do roteador na fila) e *timer adjustments* (ajustar o tempo necessário para executar cada tarefa). O tráfego específico de mensagens do protocolo são todos a partir do endereço 224.0.0.18 na porta IP 112 [NADAS, 2010].

Conforme pode-se observar na Figura 2 a configuração do VRRP no roteador não requer configurações avançadas, porém o endereço IP configurado na linha 4 deve ser um endereço diferente da interface a qual será configurado o protocolo, porém dentro da mesma faixa de endereços, sendo então um endereço IP virtual.

```
1. interface F1/0
2. ip address XXX.XXX.XXX.XXX MMM.MMM.MMM.MMM
3. vrrp 1 description GRUPO_VRRP_1
4. vrrp 1 ip YYY.YYY.YYY.YYY !Endereço IP Virtual do MASTER
5. vrrp 1 priority 120 !(default é 100)
6. vrrp 1 preempt
7. no shutdown
8. track 2 interface serial 1/0 line-protocol
```

Figura 2 – Exemplo de configuração do protocolo VRRP Mestre.

2.2 Hot Standby Router Protocol (HSRP)

Este protocolo utiliza das mesmas técnicas de otimização citadas no VRRP, para se obter um melhor resultado, sendo estas as técnicas: *tracking* (utilizado para verificar o status da interface a ser monitorada), preempção (determinar a prioridade do roteador na fila) e *timer adjustments* (ajustar o tempo necessário para executar cada tarefa) [LI et al., 1998].

O tráfego específico de mensagens do protocolo na versão 1 são todos a partir do endereço 224.0.0.2 na porta UDP 1985 e na versão 2 o endereço utilizado é 224.0.0.102 tendo a mesma porta UDP para utilização [LI et al., 1998].

Observamos então que o protocolo HSRP, utiliza da mesma maneira de configuração a qual foi apresentada na Figura 2, esta que por sua vez trata do protocolo VRRP. Observamos abaixo na Figura 3 que a alteração significativa é a mudança no primeiro comando na terceira linha de configuração e que como no VRRP mantém na quarta linha o uso de um endereço IP virtual.

```

1. interface F1/0
2. ip address XXX.XXX.XXX.XXX   MMM.MMM.MMM.MMM
3. standby 1 description GRUPO_HSRP_1
4. standby 1 ip YYY.YYY.YYY.YYY !Endereço IP Virtual do Ativo HSRP
5. standby 1 priority 120 !(default é 100)
6. standby 1 preempt
7. no shutdown
8. track 2 interface serial 1/0 line-protocol

```

Figura 3 – Exemplo de configuração do protocolo HSRP Ativo.

3. Materiais e Métodos

Os dois protocolos de *gateway* redundante referenciados neste trabalho, VRRP e HSRP, possuem modos de funcionamento e configurações semelhantes as apresentadas nos anexos A e B. A ideia por trás de ambos os protocolos é relativamente simples: chavear o tráfego de um roteador para o outro em caso de queda do enlace ou do próprio roteador.

O experimento foi realizado a partir de um teste de bancada no Laboratório de Redes Cisco do IFSULDEMINAS – Campus Inconfidentes, localizado no Setor de Informática e Redes. Para a configuração do cenário proposto conforme a Figura 4, foram utilizados dois roteadores Cisco 2811 (série 2800), um switch Cisco Catalyst (série 2960) e dez hosts com o sistema operacional Windows 8. Para reproduzir a redundância de link, foram usados nos testes um link da rede local de alunos (link principal) e outro da rede local de professores (link secundário), em redes IP distintas, para simular dois provedores de acesso a internet distintos.

Durante os testes, os seguintes parâmetros foram monitorados: consumo total de memória DRAM (*Dynamic Random Access Memory*) pelo roteador, uso da memória DRAM pelo protocolo avaliado, consumo total de CPU (*Central Processing Unit*) pelo roteador, uso de CPU pelo protocolo analisado, NetFlow (fluxo de mensagens específicas) dos protocolos VRRP e HSRP, tráfego de rede, taxa de erro de bits e o tempo de recuperação de cada protocolo a partir da interrupção do *gateway* padrão. Tais parâmetros foram escolhidos para serem analisados uma vez que de acordo com a literatura Cisco disponível, ambos afetam diretamente o desempenho geral da rede, pois todo o tráfego interno e externo a rede necessita ser roteado para se chegar ao destino desta maneira, um mal desempenho do roteador em questão afeta todo o sistema [CISCO SYSTEMS, 2013].

O tráfego de dados, utilizado para o experimento, foi gerado a partir de um servidor de arquivos localizado na rede local de professores, e acessível a partir da rede local de alunos. As dez estações clientes foram programadas para executar uma rotina de download, iniciando ao mesmo tempo, o download contínuo de um arquivo de 6,5 GB no servidor de arquivos.

Neste ponto, cabe destacar que, após a entrada em operação do roteador secundário, o atraso no tráfego gerado é ligeiramente reduzido, pois o servidor de

arquivos está conectado no mesmo segmento de rede. Porém, essa variação foi insignificante e não impactou na análise realizada, pois o período de interesse corresponde ao momento em que ocorre a alternância do *gateway* padrão.

Todos os testes aconteceram no período noturno, durante o mês de julho (férias escolares), de modo que não havia nenhum tráfego interno direcionado ao servidor utilizado no trabalho. Foram realizados, ao todo, 10 testes (um por dia) com duração de 10 minutos cada teste. A interrupção no link principal ocorreu sempre no 4º minuto e o restabelecimento do link aconteceu no 6º minuto. Tais tempos foram utilizados pois foi verificado que o software utilizado para monitorar os roteadores necessita de no mínimo 3 minutos para iniciar o arquivamento das variáveis do roteador e após iniciado o processo já temos os gráficos disponíveis a partir do sexto minuto de operação.

A Figura 4 apresenta a topologia simplificada da rede implementada no laboratório para a avaliação dos protocolos de *gateway* redundante. A nomenclatura de rede (Rede Alunos / Rede Professores) conforme pode-se observar na Figura 4, foi utilizada apenas para localização interna ao laboratório citado no segundo parágrafo da Seção 3 – Materiais e Métodos, levando em consideração que Rede Alunos (ISP1) e Rede Professores (ISP2) ilustram a presença de dois provedores de acesso à Internet distintos.

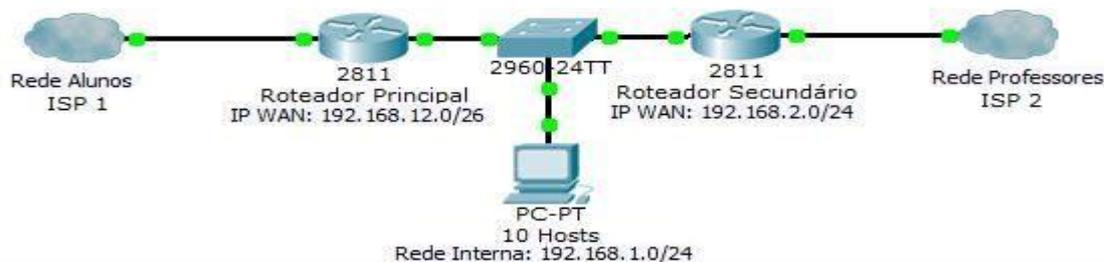


Figura 4 - Representação simplificada da topologia de rede configurada.

3.1 Software *Cisco Configuration Professional* (CCP)

Todos os dados monitorados foram adquiridos por meio do software CCP (*Cisco Configuration Professional*). O CCP é uma ferramenta proprietária utilizada para monitorar equipamentos Cisco e que permite realizar configurações cotidianas de um modo mais simples, via interface gráfica ao invés de usar a CLI (*Command-Line Interface*) [CISCO SYSTEMS, 2013].

O CCP está disponível a partir de um cadastro no site da fabricante Cisco, após seu download, para executar sua instalação é necessário estar com a última versão da ferramenta Java instalada [CISCO SYSTEMS, 2013].

Para utilizar o software CCP é necessário a realização de algumas configurações específicas no roteador o qual se quer monitorar, tais configurações são apresentadas abaixo na Figura 6.

1. (config)# ip http server !Comando usado para permitir o servidor http do roteador.
2. (config)# ip http secure-server !Comando usado para permitir o servidor https do roteador.
3. (config)# ip http authentication local !Comando usado para realizar a autenticação local.
4. !Cria-se então um usuário com nível de privilégio 15
5. (config)# username <usuário> privilege 15 password 0 <senha>

Figura 5 – Configurações do roteador para habilitar o servidor http e acesso remoto.

Após a instalação do CCP ele lhe apresentara uma tela conforme a Figura 6 logo abaixo. Nesta etapa de configuração é necessário que já tenha configurado o usuário e senha conforme dito anteriormente e demonstrado na Figura 5. Desse modo, basta preencher os dados solicitados pelo software, e clicar em OK para adicionar o roteador ao CCP.

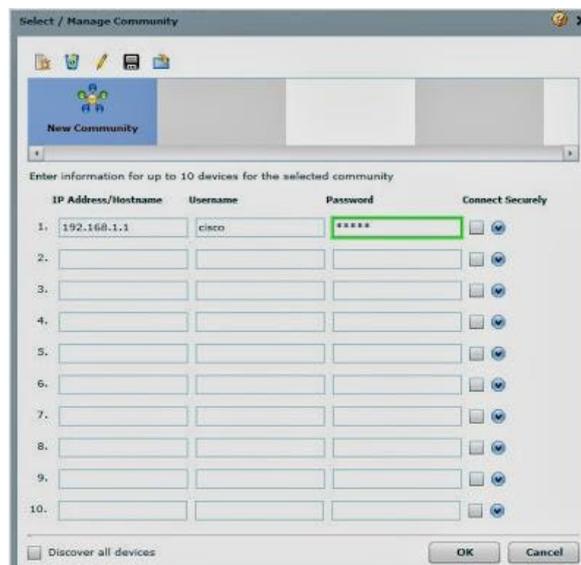


Figura 6 – Cadastro de dispositivos no CCP.

A Figura 7 representa a tela com o roteador já adicionado ao CCP.

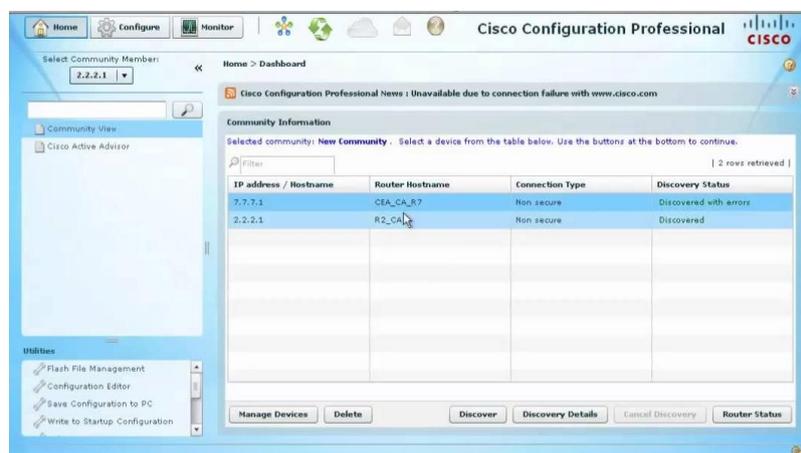


Figura 7 – Apresentação de roteadores adicionados ao CCP.

A Figura 7 apresenta uma tela com todos os roteadores já adicionados ao CCP, desta maneira para selecionar algum dos roteadores para monitorar ou configurar, basta clicar sobre o *hostname* ou endereço IP duas vezes. Assim no ecrã surgiu uma nova tela de acordo com a Figura 8 com um passo-a-passo onde pode selecionar quais as funções a qual deseja configurar ou quais as variáveis de ambiente a serem monitoradas.

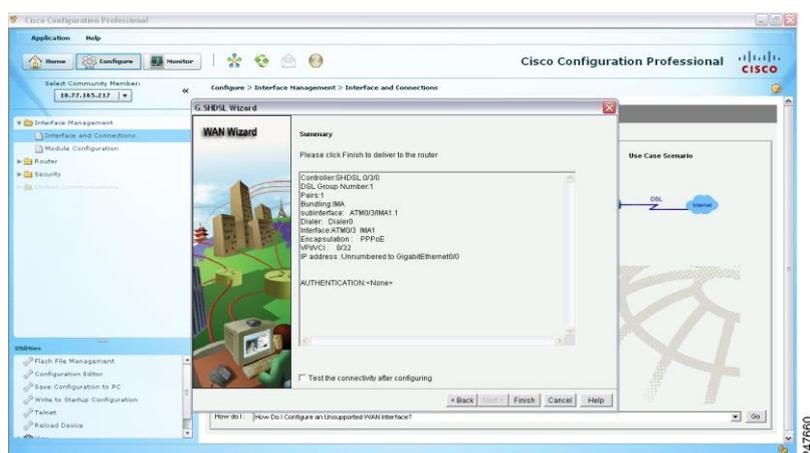


Figura 8 – Passo-a-passo configuração CCP.

Feito isso, a nova janela será apresentada com a *Dashboard* do sistema onde todas as configurações do roteador são apresentadas em seções ao lado esquerdo da tela e suas variáveis monitoradas ao meio da tela, conforme a Figura 9 apresenta.

Como o foco deste trabalho não é a plena utilização do software CCP, caso haja alguma dúvida, basta recorrer a literatura utilizada neste trabalho (*Cisco Configuration Professional User Guide*) como base a utilização de tal software.

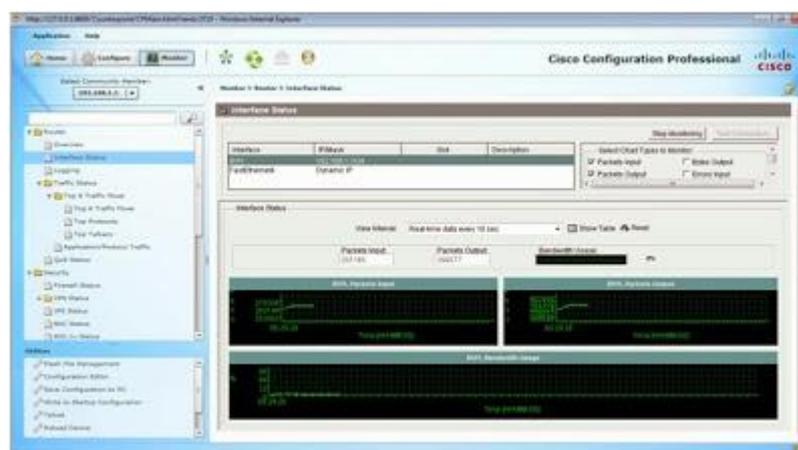


Figura 9 – Dashboard CCP.

3.2 Modelagem dos Dados

Após a realização dos experimentos, os dados coletados foram modelados conforme o teste de *t de Student*, através do software estatístico SAS (*Statistical Analysis System*), o qual podemos ver uma de suas telas na Figura 10. O método *t de Student* foi aplicado pois a quantidade de amostras resultantes após os 10 dias coletando os dados foi inferior a 100 [SCHLOTZHAVER & LITTELL, 1997].

Os dados obtidos a partir do CCP, são apresentados em texto simples separando colunas por vírgula (,) e linhas por ponto e vírgula (;). Assim, utilizamos o Software SAS não apenas para realizar a análise estatística, mas também para que se organize os dados para que fique claro sua visualização, caracterizando a modelagem dos dados. Ressaltando que a metodologia aplicada a análise estatística pelo software SAS não é parte integrante do escopo deste trabalho, onde visamos destacar apenas os resultados.

O SAS não requer configurações específicas a máquina, ressaltando que a versão utilizada foi a “*For Student and Teachers*” a qual disponibiliza todos os recursos disponíveis das outras versões para qualquer cidadão que possua um e-mail institucional acadêmico.

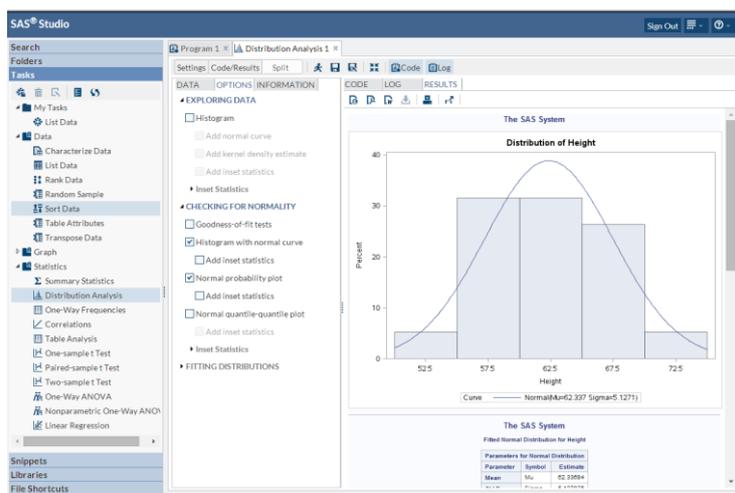


Figura 10 – SAS.

4. Resultados e Discussão

As Tabelas 1 e 2 exibem os resultados, após tratamento do software SAS, de alguns parâmetros selecionados para avaliação, referentes aos 10 testes realizados. Os resultados expressos nestas tabelas estão em porcentagem, com exceção da coluna Convergence Time expressa em hora/minutos/segundos/milissegundos e da coluna LAN Traffic apresentada em bits por segundo (bps), ambas na Tabela 2.

A Tabela 1 indica, para os dois protocolos, os seguintes parâmetros: consumo total de memória (*Memory Usage*), consumo total de CPU (*CPU Usage*), tráfego específico do protocolo (*Prot. Traffic – NetFlow*) e taxa de erro de bits (*Bits Error*).

TABELA 1 - Avaliação do uso total de memória e CPU, NetFlow e taxa de erro de bits.

Protocols	Memory Usage	CPU Usage	Prot. Traffic - NetFlow	Bits Error
VRRP	48,35%	24,77%	0,14%	0,10%
HSRP	45,03%	24,06%	0,13%	0.10%

A Tabela 2 lista, também para ambos os protocolos, os seguintes parâmetros: tempo de recuperação do protocolo (*Convergence Time*), uso de memória pelo protocolo (*Memory Usage Prot.*), uso de CPU pelo protocolo (*CPU Usage Prot.*) e tráfego na porta LAN (*Local Area Network*) (*LAN Traffic*).

TABELA 2 - Avaliação da recuperação, uso de memória e CPU do protocolo e tráfego na LAN.

Protocols	Convergence Time	Memory Usage Prot.	CPU Usage Prot.	LAN Traffic (bps)
VRRP	00:00:05:53	1,92%	0,20%	2,831,047.14
HSRP	00:00:13:00	0,90%	0,12%	2,800,553.09

Com base nos resultados, verifica-se que os dois protocolos tiveram desempenho próximo na maior parte das variáveis analisadas. O protocolo proprietário HSRP, comparado ao VRRP, apresentou menor uso de recursos do roteador (memória e CPU), além de gerar um menor tráfego específico de mensagens do protocolo. A diferença na taxa de erro de bits foi insignificante. O tráfego na rede interna usando o protocolo VRRP foi, aproximadamente, 1,09% superior ao tráfego na LAN com o protocolo HSRP.

As variações observadas nos parâmetros analisados são justificadas por uma diferença no tempo padrão de envio das mensagens dos protocolos. No VRRP, o roteador envia mensagens periódicas (*Link-State Advertisement – LSA*) a cada 1 segundo, e aguarda até 3 segundos (*holdtime*) pela próxima mensagem LSA. Se o *holdtime* exceder e o roteador não receber outra LSA, o enlace é considerado falho e o protocolo inicia o processo de substituição do *gateway*. Já no caso do protocolo HSRP, esses tempos são iguais a 3 segundos para as mensagens periódicas (*hello*) e 10 segundos para o *holdtime*. O ajuste desses parâmetros pode alterar o resultado da comparação. Neste trabalho, os protocolos foram avaliados considerando os valores padrões de tempo para as mensagens.

Com um fluxo de mensagens periódicas três vezes maior que o HSRP, o protocolo VRRP apresentou maiores variações no uso de recursos do roteador, no *NetFlow* e no tráfego da porta LAN. Por outro lado, o fato de possuir um *holdtime* menor, fez com que o VRRP tivesse um tempo de recuperação da falha no *gateway* menor que o HSRP, conforme mostra a coluna *Convergence Time* na Tabela 2.

5. Conclusão

O protocolo VRRP foi mais rápido para detectar a falha no enlace e definir um novo gateway padrão, em função dos tempos menores que utiliza para mensagens periódicas e holdtime. As estações clientes experimentaram um tempo sem conexão, em média, 50% menor com o protocolo VRRP configurado. Apesar do maior uso de recursos do roteador, essa diferença não foi significativa a ponto de comprometer o desempenho da rede. Com a performance apresentada nos testes realizados, e as vantagens de estar disponível em plataformas Linux e possuir balanceamento de carga nativo, ao contrário do HSRP, o protocolo VRRP apresentou-se como uma solução viável e eficiente para infraestruturas de rede que empregam soluções de diferentes fabricantes, incluindo Cisco Systems.

Referências

CISCO SYSTEMS, Inc. (San Jose). **Cisco Configuration Professional User Guide**. 2013. Version 2.7. Disponível em: <http://www.cisco.com/c/dam/en/us/td/docs/net_mgmt/cisco_configuration_professional/v2_7/olh/ccp.pdf>. Acesso em: 24 ago. 2015.

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

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.

LI, Dawn et al. **Cisco Hot Standby Router Protocol (HSRP)**. RFC 2281. 1998.

MAIA, Luiz Paulo. **Arquitetura de Redes de Computadores**. 2 ed. Rio de Janeiro: LTC, 2013.

NADAS, Stephen. **Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6**. RFC 5798. 2010.

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.

SCHLOTZHAVER, S.D.; LITTELL, R.C. **SAS: system for elementary statistical analysis**. 2.ed. Cary, 1997. 905p.

SHINN, Swe Kyawt. Fault Tolerance Virtual Router for Linux Virtual Server. **In: Future Networks, 2009 International Conference on**. IEEE, 2009. p. 273-275.

Anexo A – Configuração dos Roteadores VRRP

Nesta seção apresentamos as configurações específicas dos roteadores implementados com o protocolo HSRP, conforme a realidade deste trabalho.

A.1. Configuração do roteador VRRP denominado “Principal”.

1. ! Last configuration change at
19:41:28 UTC Sun Dez 12 2015
by admin
2. version 15.0
3. service timestamps debug
datetime msec
4. service timestamps log datetime
msec
5. no service password-encryption
6. hostname Master
7. boot-start-marker
8. boot-end-marker
9. no logging buffered
10. no aaa new-model
11. ip source-route
12. ip cef
13. ip dhcp excluded-address
192.168.1.1 192.168.1.3
14. ip dhcp pool fa0
15. import all
16. network 192.168.1.0
255.255.255.0
17. domain-name activedom
18. dns-server 200.131.80.30
200.131.80.29
19. default-router 192.168.1.3
20. multilink bundle-name
authenticated
21. license udi pid CISCO2811 sn
FTX1445A1HE
22. username admin privilege 15
password 0 cisco
23. track 1 interface FastEthernet0/1
line-protocol
24. track 2 interface FastEthernet0/0
line-protocol
25. interface FastEthernet0/0
26. description \$ETH-LAN\$
27. ip address 192.168.12.64
255.255.255.192
28. ip nat outside
29. ip virtual-reassembly
30. duplex auto
31. speed auto
32. interface FastEthernet0/1
33. description \$ETH-LAN\$
34. ip address 192.168.1.1
255.255.255.0
35. ip nat inside
36. ip virtual-reassembly
37. duplex auto
38. speed auto
39. vrrp 1 description G_VRRP
40. vrrp 1 ip 192.168.1.3
41. vrrp 1 priority 120
42. vrrp 1 preempt
43. vrrp 1 track 1 interface
FastEthernet0/1 decrement 20
44. vrrp 1 track 2 interface
FastEthernet0/0 decrement 20

```

45. interface Serial0/0/0
46. no ip address
47. shutdown
48. clock rate 125000
49. interface Serial0/0/1
50. no ip address
51. shutdown
52. clock rate 125000
53. ip forward-protocol nd
54. ip http server
55. ip http authentication local
56. ip nat inside source list 1 interface
    FastEthernet0/0 overload
57. ip route 0.0.0.0 0.0.0.0
    FastEthernet0/0
58. access-list 1 remark CCP_ACL
    Category=2
59. access-list 1 permit 192.168.1.0
    0.0.0.255
60. access-list 1 permit 192.168.12.0
    0.0.0.63
61. control-plane
62. line con 0
63. line aux 0
64. line vty 0 4
65. login
66. scheduler allocate 20000 1000
67. end

```

A.2. Configuração do roteador HSRP denominado “Secundário”.

```

1. ! Last configuration change at
    21:06:50 UTC Sun Dez 12 2015
    by admin
2. version 15.0
3. service timestamps debug
    datetime msec
4. service timestamps log datetime
    msec
5. no service password-encryption
6. hostname BACKUP
7. boot-start-marker
8. boot-end-marker
9. no aaa new-model
10. ip source-route
11. ip cef
12. ip dhcp excluded-address
    192.168.1.1 192.168.1.3
13. ip dhcp pool pool_stand
14. import all
15. network 192.168.1.0
    255.255.255.0
16. domain-name standdom
17. dns-server 200.131.80.30
    200.131.80.29
18. default-router 192.168.1.3
19. multilink bundle-name
    authenticated
20. license udi pid CISCO2811 sn
    FTX1445A1HF
21. username admin privilege 15
    password 0 cisco
22. interface FastEthernet0/0
23. description $ETH-LAN$
24. ip address 192.168.2.12
    255.255.255.0
25. ip nat outside
26. ip virtual-reassembly

```

```

27. duplex auto
28. speed auto
29. interface FastEthernet0/1
30. description $ETH-LAN$
31. ip address 192.168.1.2
    255.255.255.0
32. ip nat inside
33. ip virtual-reassembly
34. duplex auto
35. speed auto
36. vrrp 1 description G_VRRP
37. vrrp 1 ip 192.168.1.3
38. vrrp 1 priority 120
39. vrrp 1 preempt
40. interface Serial0/0/0
41. no ip address
42. shutdown
43. clock rate 125000
44. interface Serial0/0/1
45. no ip address
46. shutdown
47. clock rate 125000
48. ip forward-protocol nd
49. ip http server
50. ip http authentication local
51. ip nat inside source list 1 interface
    FastEthernet0/0 overload
52. ip route 0.0.0.0 0.0.0.0
    FastEthernet0/0
53. access-list 1 remark CCP_ACL
    Category=2
54. access-list 1 permit 192.168.2.0
    0.0.0.255
55. access-list 1 permit 192.168.1.0
    0.0.0.255
56. control-plane
57. line con 0
58. line aux 0
59. line vty 0 4
60. login
61. scheduler allocate 20000 1000
62. end

```

Anexo B – Configuração dos Roteadores HSRP

Nesta seção apresentamos as configurações específicas dos roteadores implementados com o protocolo HSRP, conforme a realidade deste trabalho.

B.1. Configuração do roteador HSRP denominado “Principal”.

```

1. ! Last configuration change at
    20:41:28 UTC Sun Dez 12 2015
    by admin
2. version 15.0
3. service timestamps debug
    datetime msec
4. service timestamps log datetime
    msec
5. no service password-encryption
6. hostname ACTIVE
7. boot-start-marker
8. boot-end-marker
9. no logging buffered
10. no aaa new-model
11. ip source-route
12. ip cef

```

```

13. ip dhcp excluded-address
    192.168.1.1 192.168.1.3
14. ip dhcp pool fa0
15. import all
16. network 192.168.1.0
    255.255.255.0
17. domain-name activedom
18. dns-server 200.131.80.30
    200.131.80.29
19. default-router 192.168.1.3
20. multilink bundle-name
    authenticated
21. license udi pid CISCO2811 sn
    FTX1445A1HE
22. username admin privilege 15
    password 0 cisco
23. track 1 interface FastEthernet0/1
    line-protocol
24. track 2 interface FastEthernet0/0
    line-protocol
25. interface FastEthernet0/0
26. description $ETH-LAN$
27. ip address 192.168.12.64
    255.255.255.192
28. ip nat outside
29. ip virtual-reassembly
30. duplex auto
31. speed auto
32. interface FastEthernet0/1
33. description $ETH-LAN$
34. ip address 192.168.1.1
    255.255.255.0
35. ip nat inside
36. ip virtual-reassembly
37. duplex auto
38. speed auto
39. standby 1 ip 192.168.1.3
40. standby 1 priority 120
41. standby 1 preempt
42. standby 1 name tcc_hsrp
43. standby 1 track 1 decrement 20
44. standby 1 track 2 decrement 20
45. interface Serial0/0/0
46. no ip address
47. shutdown
48. clock rate 125000
49. interface Serial0/0/1
50. no ip address
51. shutdown
52. clock rate 125000
53. ip forward-protocol nd
54. ip http server
55. ip http authentication local
56. ip nat inside source list 1 interface
    FastEthernet0/0 overload
57. ip route 0.0.0.0 0.0.0.0
    FastEthernet0/0
58. access-list 1 remark CCP_ACL
    Category=2
59. access-list 1 permit 192.168.1.0
    0.0.0.255
60. access-list 1 permit 192.168.12.0
    0.0.0.63
61. control-plane
62. line con 0
63. line aux 0
64. line vty 0 4
65. login
66. scheduler allocate 20000 1000
67. end

```

B.2 Configuração do roteador HSRP denominado “Secundário”.

```
1. ! Last configuration change at 21:06:50 UTC Sun Dez 12 2015
   by admin
2. version 15.0
3. service timestamps debug
   datetime msec
4. service timestamps log datetime
   msec
5. no service password-encryption
6. hostname STANDBY
7. boot-start-marker
8. boot-end-marker
9. no aaa new-model
10. ip source-route
11. ip cef
12. ip dhcp excluded-address
    192.168.1.1 192.168.1.3
13. ip dhcp pool pool_stand
14. import all
15. network 192.168.1.0
    255.255.255.0
16. domain-name standdom
17. dns-server 200.131.80.30
    200.131.80.29
18. default-router 192.168.1.3
19. multilink bundle-name
    authenticated
20. license udi pid CISCO2811 sn
    FTX1445A1HF
21. username admin privilege 15
    password 0 cisco
22. interface FastEthernet0/0
23. description $ETH-LAN$
24. ip address 192.168.2.12
    255.255.255.0
25. ip nat outside
26. ip virtual-reassembly
27. duplex auto
28. speed auto
29. interface FastEthernet0/1
30. description $ETH-LAN$
31. ip address 192.168.1.2
    255.255.255.0
32. ip nat inside
33. ip virtual-reassembly
34. duplex auto
35. speed auto
36. standby 1 ip 192.168.1.3
37. standby 1 priority 110
38. standby 1 preempt
39. standby 1 name tcc_hsrp
40. interface Serial0/0/0
41. no ip address
42. shutdown
43. clock rate 125000
44. interface Serial0/0/1
45. no ip address
46. shutdown
47. clock rate 125000
48. ip forward-protocol nd
49. ip http server
50. ip http authentication local
51. ip nat inside source list 1 interface
    FastEthernet0/0 overload
```

```
52. ip route 0.0.0.0 0.0.0.0
    FastEthernet0/0
53. access-list 1 remark CCP_ACL
    Category=2
54. access-list 1 permit 192.168.2.0
    0.0.0.255
55. access-list 1 permit 192.168.1.0
    0.0.0.255
56. control-plane
57. line con 0
58. line aux 0
59. line vty 0 4
60. login
61. scheduler allocate 20000 1000
62. end
```

