UNIVERSIDADE FEEVALE

ALEXANDRE GARCIA

ESTUDO DE PROTOCOLOS DE REDUNDANCIA VRRP, HSRP E GLBP UTILIZANDO IPV6

Novo Hamburgo
2015

ALEXANDRE GARCIA

ESTUDO DE PROTOCOLOS DE REDUNDANCIA VRRP, HSRP E GLBP UTILIZANDO IPV6

Trabalho de Conclusão de Curso
apresentado como requisito parcial
à obtenção do grau de Bacharel em
Ciência da Computação pela
Universidade Feevale

Orientador: Vandersilvio da Silva

Novo Hamburgo
2015

AGRADECIMENTOS

Gostaria de agradecer a todos os que, de alguma maneira, contribuíram para a realização desse trabalho de conclusão, em especial:

Aos meus pais, que sempre forneceram todo o apoio financeiro para meus estudos,

Minha esposa, Cintia, que fez vários esforços para encarar sozinha as responsabilidades de nossa família, para que eu conseguisse fazer este trabalho.

Aos amigos e às pessoas que convivem comigo diariamente, por serem compreensivos em momentos de indisponibilidade minha, durante esse projeto.

RESUMO

Com o esgotamento dos endereços do protocolo IP versão 4, surge a necessidade de utilizar a versão 6 do protocolo. Esta nova versão tem muito mais endereços disponíveis, porem ~~ela~~ não é uma extensão da versão anterior, e deverá ser configurada a parte. Para acessar o conteúdo de um servidor que utilize IPv6, o computador cliente também deve estar configurado com IPv6. Desta maneira tornasse necessário que as redes corporativas tenham implementado o novo protocolo para acompanhar a evolução da rede, porem muitas destas empresas tem recursos para redundância de conexão à internet, devido a dependência de serviços on-line, e esta redundância está configurada sobre endereçamentos IPv4. Torna-se então necessário que estas soluções de redundância sejam testadas com o protocolo IPv6, para verificar se são compatíveis e se não causam nenhum impacto negativo em seu funcionamento. Uma das primeiras formas de prover redundância a uma rede local é utilizar mais de um gateway para o primeiro salto. Para isto existem protocolos padronizados tanto de propriedade de fabricantes quanto de domínio público. Este projeto tem o objetivo fazer a validação do funcionamento de três protocolos de redundância de primeiro salto, VRRP, HSRP e GLBP, em redes IPv4 e IPv6, através de uma rede virtualizada na ferramenta GNS3, e comparar os resultados de desempenho entre as duas versões do protocolo de rede. Ainda apresenta uma pesquisa sobre os protocolos de redundância e uma pesquisa sobre o protocolo IPv6.

Palavras-chave: IPv6. VRRP. HSRP. GLBP. Redundância.

ABSTRACT

With the depletion of IP version 4 protocol addresses, the need arises to use version 6 of the protocol. This new version will have much more available addresses, however it is not an extension of the previous version, and must be configured separately. To access content from a server using IPv6, the client computer must also be configured with IPv6. Thus become necessary for corporate networks have implemented the new protocol to follow the evolution of the network, however many of these companies afford Internet connection redundancy, due to dependence on online services, and this redundancy is configured for IPv4 addresses . It then becomes necessary that these redundancy solutions are tested using the IPv6 protocol, to verify that are compatible and do not cause any adverse effect on its operation. One of the first ways to provide redundancy to a LAN is to use more than one gateway for the first jump. For this there are standardized protocols both manufacturers of property as public domain. This project aims to validate the operation of three first-hop redundancy protocols, VRRP, HSRP and GLBP in IPv4 and IPv6 networks through a virtualized network in GNS3 tool, and compare the performance results between the two versions Network protocol. Also presents a survey of redundancy protocols and research on IPv6.

Key words: IPv6. VRRP. HSRP. GLBP. Redundancy.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

FHRP	First Hop Redundancy Protocol
VRRP	Virtual Router Redundancy Protocol
HSRP	Hot Standby Router Protocol
GLBP	Gateway Load Balancing Protocol
SPOF	Single Point Of Failure
WAN	Wide Area Network
LSA	Link-State Advertisement
AVG	Active Virtual Gateway
AVF	Active Virtual Forwarders
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
CIDR	Classless InterDomain Routing
IOS	Internet Operating System

SUMÁRIO

INTRODUÇÃO

Com a grande difusão de serviços pela internet para as empresas poderem trabalhar, como por exemplo a NFe (Nota Fiscal Eletrônica), a necessidade de estabilidade na conexão com a internet se faz cada vez mais necessária. Porém um link de internet não está livre de sofrer um problema, ocasionando uma perda de conexão com a internet. Se uma empresa tiver um serviço de vendas on-line dependendo deste canal de comunicação, isto pode gerar atrasos ou até uma perda de faturamento.

Para contornar esta situação, estas entidades vêm buscando métodos para que sua conexão com a rede pública fique o máximo possível disponível. Uma destas maneiras é tendo mais de um provedor de internet disponível, provendo redundância do sistema. A redundância é definida como a "capacidade de um sistema em superar a falha de um de seus componentes através do uso de recursos redundantes" (PINHEIRO, 2004). Desta maneira quando um está indisponível, o outro passa a ser o canal de comunicação principal.

Esta troca acaba se tornando trabalhosa quando precisa ser feita manualmente devido às configurações que precisam ser feitas e o tempo de reação da pessoa que está monitorando. Para solucionar esta questão muitas empresas especializadas em redes criaram protocolos específicos para gerenciar estes canais de comunicação com a internet, criando ferramentas para prover alta disponibilidade. Desta maneira na ocorrência de uma falha no equipamento principal (mestre), outro componente do grupo de alta disponibilidade (escravo) assume a tarefa de roteamento, deixando a falha ficar imperceptível aos usuários. (SONDEREGGER et al. 2009).

Esta crescente demanda de serviços associados à internet, assim como o grande número de usuários conectados a dispositivos móveis, como *smartphones* e *tablets*, vem acelerando o esgotamento dos endereços IP versão 4. O Brasil foi o segundo país do mundo com maior alocação de IPv4 ficando apenas atrás dos Estados Unidos, principalmente devido ao crescimento da internet móvel no país, e a tendência para 2014 seria semelhante (NIC.br, 2014a). O estoque de IPv4 da região entrou em fase de “terminação Gradual”, limitando a compra de IPs em 1024 endereços a cada 6 meses, mesmo justificando a necessidade de mais endereços (NIC.br 2014b).

Para superar esta situação a NIC.br vem incentivando os provedores de serviços de internet a se prepararem e implementarem a próxima versão do protocolo, o IP versão 6, ou

simplesmente IPv6. Este protocolo estende a quantidade de IPs disponíveis de 2^{32}, número máximo de endereços IPv4, para 2^{128}, número máximo de endereços do IPv6.

O número de internautas que utilizam o IPv6 no brasil chegou a 1%, que é um percentual baixo, mas é 10 vezes maior que o registado em janeiro de 2015. Este rápido crescimento tende a continuar (IPv6.br, 2015).

O protocolo IPv6 não foi projetado para ser um complemento do IPv4, tão pouco uma extensão. Portanto o IPv6 e o IPv4 não são compatíveis entre si. Mas os dois protocolos podem trabalhar simultaneamente, fazendo com que um host tenha tanto um endereço IPv4 quanto um endereço IPv6. Este método foi batizado de pilha dupla, ou *dual stack*. Desta forma é possível implementar o IPv6 na internet gradualmente, e assim que todos o utilizassem não seria mais necessária a versão 4.

Apesar de muitos provedores de internet estarem se preparando para este cenário, muitas empresas não estão se preparando. Muitas destas empresas já possuem equipamentos que suportam roteamento e outras funcionalidades utilizando IPv6.

Atualmente 99% dos usuários brasileiros estão utilizando a rede exclusivamente por IPv4, incluindo as empresas que utilizam os sistemas de redundância citados anteriormente. Estes serviços utilizam exatamente esta camada de rede, camada 3, para seu funcionamento. Estes têm a necessidade de serem configurados com a versão 6 do protocolo para conseguir acompanhar a migração.

Uma das grandes empresas especializadas na área de rede é a Cisco Systems, que em seus roteadores equipados com o sistema operacional IOS (*Internet Operating System*) utilizam 3 protocolos para fazer redundância: VRRP (*Virtual Router Redundancy Protocol*), HSRP (*Hot Standby Router Protocol*) e GLBP (*Gateway Load Balance Protocol*), que estes permitem compartilhar o mesmo endereço IP entre vários hosts, além de possibilitar a balanceamento de carga (JUNIOR, 2008, p. 2). Este endereço IP é um IP virtualizado, que é configurado nos computadores dos usuários como *gateway default* (CISCO, 2015). Os equipamentos produzidos pela empresa também oferecem suporte ao IPv6.

Motivado pela dificuldade de encontrar informações e documentos sobre a utilização de técnicas de roteamento utilizando a versão 6 do protocolo de internet, este projeto visa um estudo sobre o funcionamento dos protocolos de redundância utilizados pela Cisco a fim de validar a funcionalidade dos mesmos utilizando a próxima geração do protocolo IP, a fim de determinar quais os impactos deste nas estruturas atuais das empresas, bem como verificar se

o nível de disponibilidade dos serviços se mantém conforme o funcionamento com a versão anterior.

O projeto tem como contribuição formar conhecimento sobre a implementação dos serviços de redundância sobre o protocolo IPv6 a fim de, posteriormente, poder ser utilizado em ambientes de produção.

Este trabalho está disposto em quatro capítulos numerados. O primeiro apresenta a fundamentação teórica, abordando os conceitos básicos sobre o funcionamento dos protocolos de rede IPv4 e IPv6 e dos protocolos de redundância de primeiro salto. O capitulo 2 relata as características da ferramenta utilizada para os testes e os métodos utilizados para realizar os testes. O capítulo seguinte demonstra a aplicação dos testes, onde é montado o ambiente padrão para os testes e apresentado o procedimento realizado em cada teste. Por fim o quarto capitulo numerado expõe os resultados obtidos nos testes e as análises realizadas sobre estes resultados.

1 ALTA DISPONIBILIDADE EM IPV4 E IPV6

Neste capítulo serão apresentados os conceitos básicos para o desenvolvimento do trabalho e descrição dos protocolos de redundância.

1.1 IPv4

O protocolo IP, em sua versão quatro, referido neste trabalho como IPv4, tem sua especificação inicial em setembro de 1981 com a RFC 791, que foi posteriormente atualizada em diversas outras RFCs, como a 1349, 2474 e 6864. (USC, 1981, p1).

O endereço deste protocolo é formado por 32 bits, e é expresso em uma notação decimal, onde é dividido em 4 grupos, com 8 bits cada um, chamados de octetos, onde cada um pode ser um valor entre 0 (00000000 em binário e 00 em hexadecimal) e 255 (11111111 em binário e FF em hexadecimal). Formando assim um endereço no formado como o exemplo 192.160.100.123. Este formato possibilita o endereçamento de 2^{32} hosts, que correspondem a mais 4,2 milhões de endereços, que era praticamente a população mundial da época que o protocolo foi especificado. (Coulouris et al. 2013, p108).

Os endereços IP de origem e de destino das mensagens são colocados nos cabeçalhos dos pacotes IP. O cabeçalho do pacote IP é dividido em 14 tipos de campos. Dois destes campos correspondem aos endereços IP de origem e destino, como mostra a figura abaixo:

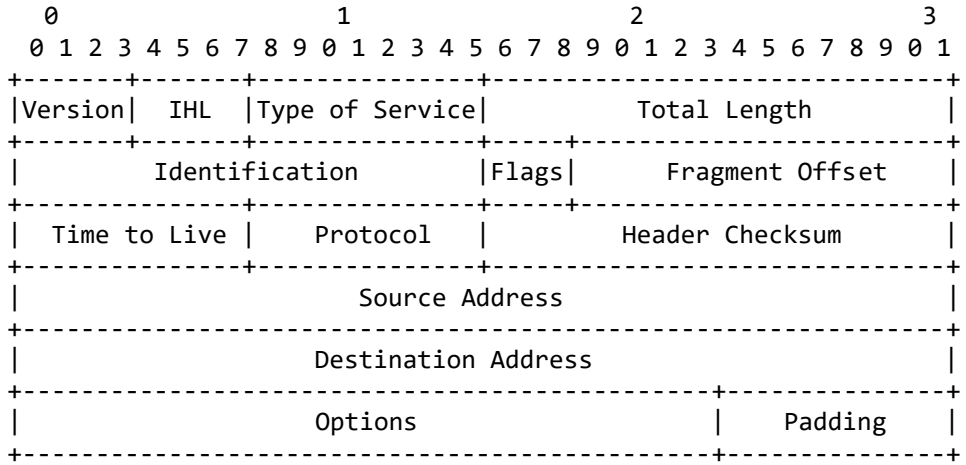


Figura 1.1 – Cabeçalho IPv4
Fonte: USC, 1981

Quando foi concebido o IPv4, foram definidas classes diferentes para satisfazer os requisitos dos tamanhos de redes de organizações. A classe A compreendia a capacidade de 2^{24} hosts em cada rede, a classe B compreendia 2^{16}, aproximadamente 65 mil hosts na mesma rede, e a classe C compreendia 256 hosts em cada rede. Muitas empresas e instituições solicitavam endereços Classe B, superestimando o crescimento de suas redes, e fazendo com que a taxa de alocação de endereços fosse muito rápida.

Atualmente é utilizado juntamente com o endereço uma máscara de sub-rede, que foi introduzida em 1993, especificada na RFC 1519, com o intuito de reduzir a utilização de classes B, e também adiar o esgotamento do IPv4. Isto permitiu que fosse feito o roteamento entre domínios sem classes, e recebeu por isto o nome de CIDR (*Classless InterDomain Routing*). (FULLER et al, 1993, p1-2)

Além do CIDR, foram tomadas também mais duas providências para a prevenir a extinção rápida dos endereços IPv4. A técnica de NAT (*Network Address Translation*), descrito na RFC 1631, foi uma delas, onde não se permitia que computadores e dispositivos acessassem a internet diretamente, mas sim por meio de um dispositivo que fazia a comunicação entre as redes, traduzindo endereços locais (não válidos na internet) em endereços válidos na Internet. A outra providência foi a criação de um protocolo de rede que compreendesse mais endereços, o IPv6. (Coulouris et al. 2013, p110-111).

1.2 IPv6

O IPv6 foi especificado pela primeira vez em dezembro de 1995, na RFC 1883, porém esta especificação foi atualizada e substituída na RFC 2460, de dezembro de 1998, e ainda teve atualizações seguintes em diversas outras RFCs, como a 5095, 6564 e 7045. (DEERING, HIDEN, 1998, p1-3)

Este protocolo tem como principais modificações em relação ao seu antecessor, o IPv4, as seguintes características:

- Expansão do endereçamento de 2^{32} endereços para 2^{128} endereços.

- Simplificação do cabeçalho do protocolo.

- Melhoramento do suporte a extensões e opções.

- Rotulação do pacote para estabelecer fluxo e sequência de pacotes.

- Capacidade de autenticação, privacidade e confidencialidade.

Alguns campos foram removidos do cabeçalho original do IPv4 para IPv6, como por exemplo o “Header Checksum”, deixando o cabeçalho mais simples, mas disponibilizando uma possibilidade para uma extensão deste cabeçalho, através do campo “ Next Header”, possibilitando inclusão de diversas opções. A figura 1.2 mostra o cabeçalho IPv6.

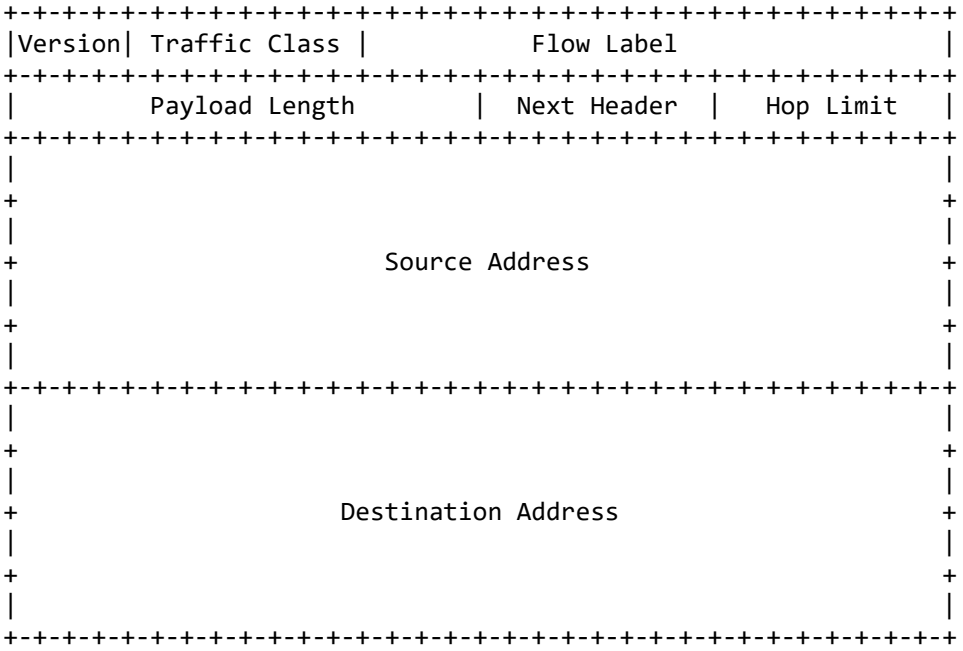


Figura 1.2 – Cabeçalho Básico IPv6
Fonte: DEERING, HIDEN, 1998

O endereço do IPv6 não é expressado através de notações decimais divididas por pontos (.) assim como o IPv4, devido ao seu grande número de bits, e sim através de notações hexadecimais divididas por dois pontos (:). Desta maneira tem-se um endereço composto por 8 grupos com quatro dígitos cada um, como mostra a figura 1.3. (ILUSTRE, 2012, p17)

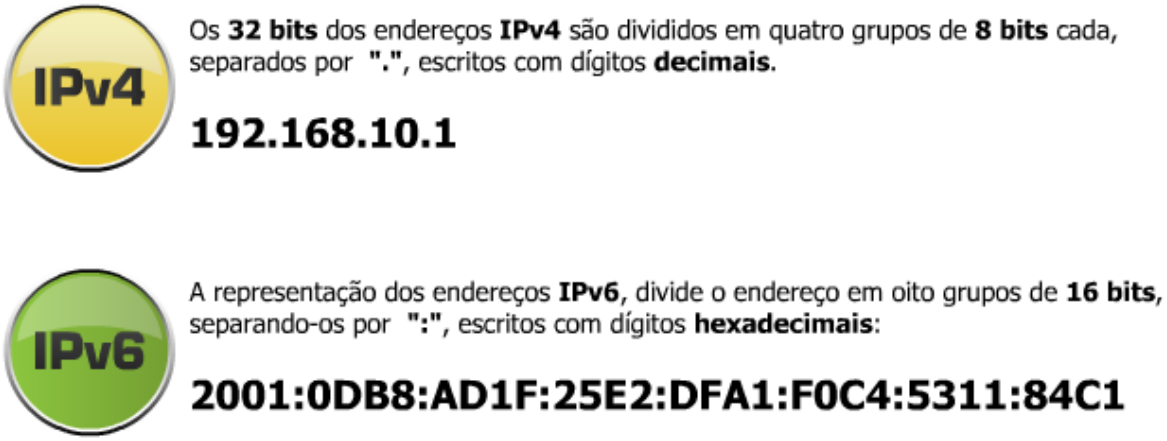


Figura 1.3 – Endereçamento IPv4 e IPv6
Fonte: ILUSTRE, 2012

Endereços IPv6 podem ter uma cadeia de zeros abreviados ou suprimidos, reduzindo a necessidade de digitação destes. Para suprimir uma cadeia de zeros, correspondente a grupos completos, se utiliza duas vezes o dois pontos (::). Esta representação pode ser feita apenas uma vez por endereço. Os zeros à esquerda de cada grupo podem ser eliminados também. (ILUSTRE, 2012, p19). A tabela 1.1 traz exemplos sobre isso.

Expressão do endereço	Ação
FEC0:0000:0000:1234:0000:0000:018C:0045	Endereço completo
FEC0:0000:0000:1234::018C:0045	Simplificação da cadeia de zeros entre os grupos 1234 e 018C
FEC0:0:0:1234::018C:0045	Redução dos demais grupos com cadeias de zeros
FEC0:0:0:1234::18C:45	Redução dos zeros a esquerda dos grupos 018C e 0045

Tabela 1.1 – Redução do endereço IPv6.

Fonte: Autor.

1.3 Alta Disponibilidade

Alta disponibilidade em um sistema significa que este é projetado para permanecer disponível e acessível durante a grande maioria do tempo. Considera-se que para obtenção da alta disponibilidade os recursos sejam no mínimo duplicados, considerando que no caso de uma falha em um deles, o outro assume a demanda, fornecendo redundância. Mesmo nesta situação ainda ocorrerá um pequeno período de indisponibilidade. (SCHENEIDER, 2003 p14).

1.3.1 Disponibilidade

Conforme documentação do ITIL, versão 3, a disponibilidade é a razão de tempo em que um sistema deve estar operante para seus usuários ou dispositivos. Ela é calculada entre a razão do tempo que o serviço fica disponível, que pode ser expressado pelo tempo onde o sistema deveria estar disponível subtraído do tempo em que o sistema ficou inoperante, sobre o tempo total onde o serviço deveria estar operante.

Para a Microsoft, a disponibilidade é classificada pela "regra dos noves", onde quanto maior a quantidade de noves, menor o *downtime*, tempo onde o sistema não está disponível. A tabela abaixo expressa o significado da regra.

%	Downtime (por ano)
100	Nenhum downtime
99,999 (5 noves)	Menos de 5,26 min.
99,99 (4 noves)	De 5,26 a 52 min.
99,9 (3 noves)	De 52 min. a 8 horas e 45 min.
99 (2 noves)	De 8 horas e 45 min. a 87 horas e 56 min
90,0 - 98,9 (1 nove)	87 horas e 56 min a 875 horas 54 min

Tabela 1.2 – O significado dos noves.

Fonte: MICROSOFT, 2015.

1.3.1 Redundância de primeiro salto

O primeiro salto, do inglês *first hop*, é a conexão de um dispositivo de rede, sendo computador ou outro equipamento, com o seu *gateway*, que faz a ligação da rede onde se encontra com outras redes. Para que este *gateway* tenha um backup, de forma a garantir a continuidade da comunicação com outras redes, existem protocolos de redundância do primeiro salto (*First Hop Redundancy Protocol* – FHRP). Estes visam a troca do roteador que faz a comunicação por outro de forma transparente para o usuário. (NASCIMENTO 2014,)

Atualmente encontramos entre os protocolos de redundância de primeiro salto utilizados em equipamentos da CISCO o *Virtual Router Redundancy Protocol* (VRRP), o *Hot Standby Router Protocol* (HSRP), e o *Gateway Load Balancing Protocol* (GLBP). (NASCIMENTO, 2014)

1.3.1.1 Virtual Router Redundancy Protocol (VRRP)

O protocolo de redundância VRRP é um protocolo aberto, onde a versão 2 foi apresentada na RFC 3768, e consiste em prover maior confiança e resolver o problema de ponto de falha único (SPOF – *Single Point of Failure*) de uma rede ao ter apenas um roteador, introduzindo a definição de um roteador virtual (HASHIMOTO, 2009, p30).

Posteriormente a RFC 3768 se tornou obsoleta com a criação da versão 3 do protocolo, que foi apresentada da RFC 5798. (NADAS, ERICSSON, 2010).

O roteador virtual consiste na criação de um grupo de roteadores, incluindo um roteador mestre e um ou mais backups, com um IP virtual e um MAC Virtual. O MAC Virtual recebe uma variação do valor 0000.5e00.01xx, onde os dois últimos caracteres é um valor hexadecimal. Cada *host* da rede comunica com redes externas através deste roteador virtual (H3C, 2015).

Dentro do grupo de roteadores são enviadas mensagens denominadas *Link-State Advertisement* (LSA), que são encaminhadas do roteador mestre para os demais a cada 1 segundo por padrão, e os roteadores *backup* podem opcionalmente aprender este intervalo. Dentro da rede cada roteador tem uma prioridade definida, que varia entre 1 e 254, sendo 100 o padrão, e quando os roteadores *backup* param de receber o LSA, elegem o backup com maior prioridade como mestre. (MORESHI, 2011, p7). Estas mensagens são enviadas para o endereço IP multicast 224.0.0.18 nas redes IPv4, e endereço IP multicast FF02::12 em redes IPv6. (NADAS, ERICSSON, 2010).

O VRRP tem o benefício da redundância, pois implementa múltiplos roteadores como um único gateway para a rede, assim como balanceamento de carga, de maneira manual, pois suporta até 255 roteadores virtuais, contemplando grupos com prioridades e mestres diferentes, distribuindo gateways diferentes para os clientes da rede. (HASHIMOTO 2009, p31).

A figura 1.4 ilustra a topologia básica do VRRP.

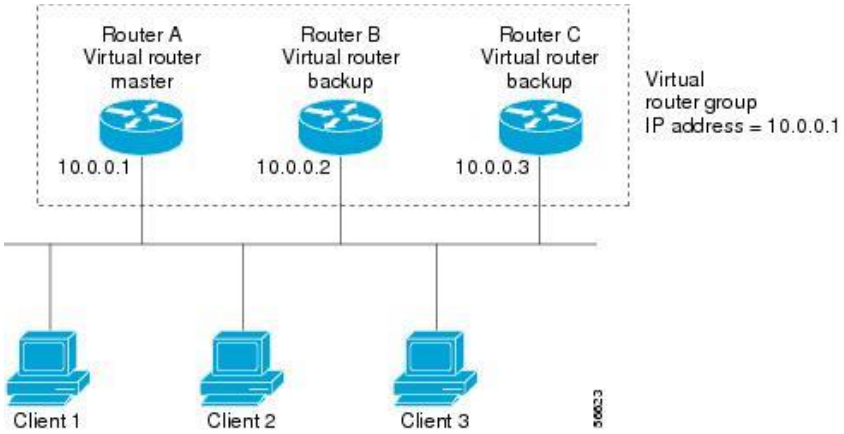


Figura 1.4 – Topologia básica VRRP
Fonte: CISCO, 2011

1.3.1.2 Hot Standby Router Protocol (HSRP)

O protocolo HSRP é um protocolo proprietário desenvolvido pela Cisco Systems, e apresentado pela RFC 2281. Se aplica a rede com dois ou mais roteadores, onde cada um será configurado com um ip fixo da rede e um ip virtual, que será atribuído como gateway dos dispositivos da rede. (PORTO, 2014, p18).

Este protocolo tem duas versões implementadas. Na versão 1 estes roteadores trocam mensagens com pacotes denominados de "*Hello*" através do endereço multicast 224.0.0.2 através da porta UDP 1985 em redes IPv4, e não tem suporte a IPv6. Na versão 2 os roteadores trocam mensagens através do endereço multicast 224.0.0.102 através da porta UDP 1985 em redes IPv4, e do endereço multicast FF02::66 através da porta UDP 2029 em redes IPv6. Estas versões não podem ser misturadas no mesmo grupo, visto que os pacotes de mensagens são diferentes, e pacotes HSRP versão 2 quando recebidos em roteador configurado com HSRP versão 1 são ignorados. (CISCO 2011)

De maneira similar ao VRRP, é definido um roteador ativo, no lugar do mestre do VRRP, e roteadores *stand-by*, no lugar dos *backups* do VRRP. O roteador ativo é aquele que tem maior prioridade entre eles, que por padrão é 100, e geralmente é atribuído manualmente um valor maior para o preferido, pois caso todos estejam com a mesma prioridade, o com endereço IP mais alto é definido como ativo. (PORTO, 2014, p18).

No grupo HSRP é implementado um roteador virtual, com um ip virtual e um endereço MAC virtual. Para o HSRP versão 1 o endereço MAC é uma variação de 0000.0C07.ACxx, onde xx é um número hexadecimal que expressa o número do grupo

HSRP, possibilitando 255 grupos. Para o HSRP versão 2, quando utilizando IPv4, o endereço MAC é uma variação de 0000.0C9F.Fxxx, possibilitando 4095 grupos diferentes, e utilizando IPv6, o endereço MAC é uma variação de 0005.73A0.0xxx, também possibilitando 4095 grupos diferentes. Da mesma maneira que na primeira versão, a variação dos últimos três dígitos expressa o número do grupo HSRP. (CISCO, 2011)

Quando houver uma falha em um roteador do grupo HSRP, sendo uma queda na interface ou uma falha no próximo salto de um roteador (WAN), é decrementado o valor da prioridade deste, para que um outro roteador fique com a prioridade acima do que contem a falha, se tornando o roteador ativo. Assim que o roteador com problema restaurar seu padrão de atividade, ele volta para a prioridade inicial, fazendo com que passe a ser o roteador ativo novamente. (PORTO, 2014, p18).

A figura 1.5 mostra um exemplo de grupo HSRP.

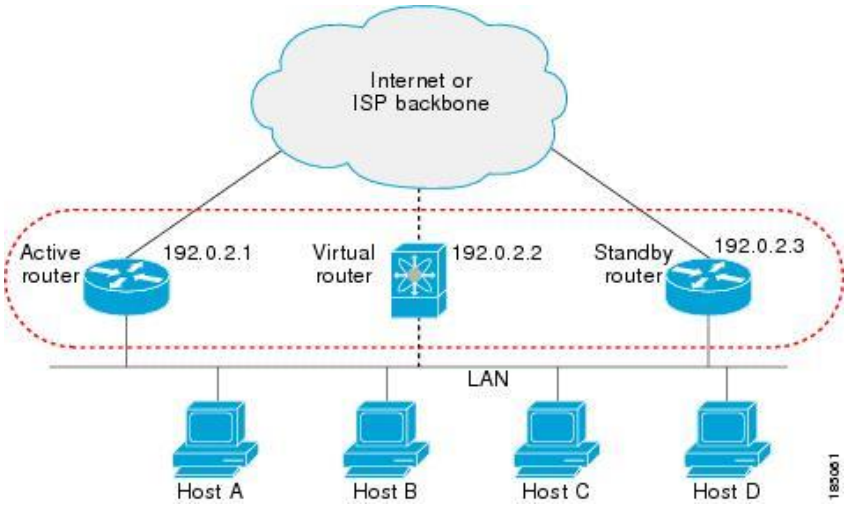


Figura 1.5 – Exemplo de grupo HSRP
Fonte: CISCO, 2011

1.3.1.3 Gateway Load Balancing Protocol (GLBP)

O *Gateway Load Balancing Protocol* (GLBP) também é um protocolo proprietário da Cisco, e apresenta funcionamento semelhante ao VRRP e HSRP, porém com um recurso adicional que permite balanceamento de carga através de saída diferentes no mesmo grupo de roteadores. Isto se deve ao fato de criar um roteador virtual, com um IP virtual, porém com mais de um endereço MAC virtual. Cada roteador que faz parte do grupo recebe o mesmo IP virtual, mas um endereço MAC virtual diferente. Assim para cada requisição ARP para o IP

virtual é respondido um MAC virtual diferente para o dispositivo que requisitou, fazendo com que o pacote seja encaminhado para um roteador diferente. (MORESCHI, 2009, p9)

No GLBP todos os gateways são considerados ativos, e entre os roteadores do grupo são classificados como Active Virtual Gateway (AGV) e Active Virtual Forwarders (AGF). É o AGV que é responsável por responder as requisições ARP, com um endereço MAC virtual utilizado em um roteador do grupo, armazenando na tabela ARP do cliente um MAC diferente para o mesmo IP de gateway, possibilitando assim o balanceamento de carga. (PORTO, 2014, p20).

Assim como nos protocolos anteriores, cada roteador do grupo tem uma prioridade definida, e o roteador com maior prioridade recebe a classificação de AGV, e os demais como AGF. Ao ocorrer falha no AGV, o roteador com maior prioridade entre os AGFs passa a ser o AGV. Porém, no GLBP, quando o roteador com problema retorna a seu estado normal, ele não volta a ser o AGV, tornando isto possível apenas na falha do novo AGV, permitindo uma nova eleição, ou alterando manualmente. (MORESCHI, 2009, p10)

No GLBP existe três métodos para o balanceamento de carga, apresentados a seguir:

- Round-Robin: Distribui os endereços MAC virtuais em ciclo, buscando distribuir igualmente o número de clientes direcionados para cada AVF. (CISCO, 2011)

- Weighted: o AVG usa a atribuição de peso de cada AVF para balancear a carga. Quanto maior for o peso do AVF, mais carga ele receberá. (CISCO, 2011)

- Host dependente: Uma um algoritmo para atribuir o AVF para cada cliente, utilizando o endereço MAC do cliente. Este garante que o cliente receberá sempre o mesmo endereço MAC virtual para o gateway enquanto o grupo do GLBP não for alterado. (CISCO, 2011)

A figura 1.6 mostra um exemplo de grupo GLBP.

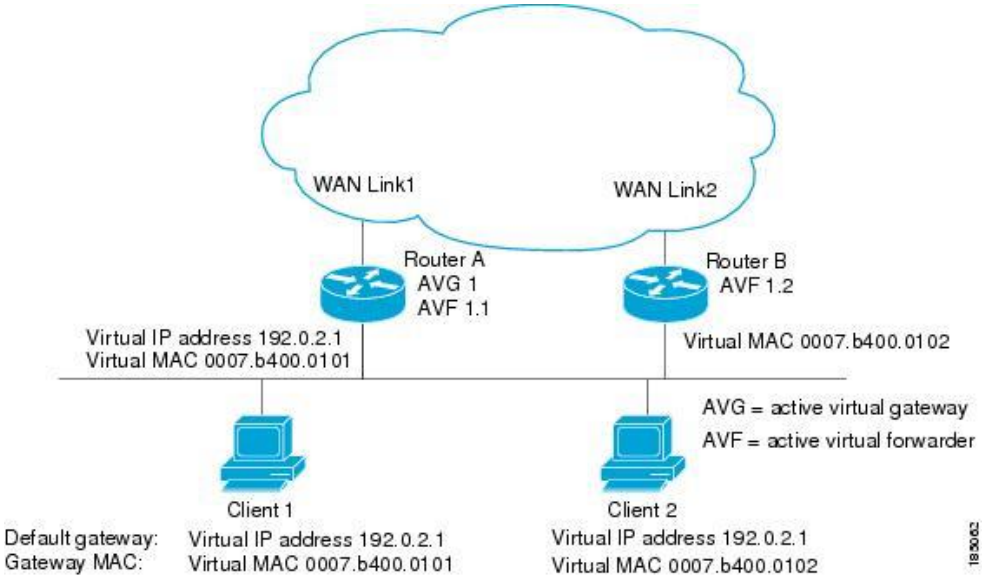


Figura 1.6 – Topologia básica GLBP
Fonte: CISCO, 2015

1.3.2 Trabalhos correlatos

Silva (2013) presenta um trabalho de conclusão de curso de Sistemas de Informação da Universidade Feevale, com um comparativo entre os protocolos de redundância de primeiro salto VRRP e HSRP, utilizando IPv4. Neste trabalho ele realizou testes utilizando a ferramenta GNS3, formando um ambiente virtual com os roteadores Cisco 3725, e computadores com um sistema reduzido Linux. Neste ambiente ele analisou o tempo de indisponibilidade de comunicação em um computador virtual ao ocorrer uma falha no roteador mestre da arquitetura.

Morechi (2011) também apresenta um trabalho para conclusão do curso superior em Tecnologia em Sistemas para Internet, da Universidade tecnológica federal do Paraná, sobre redundância de primeiro salto, utilizando os protocolos GLBP e VRRP, utilizando IPv4. No trabalho ela também utiliza o GNS3 como ferramenta para a montagem do ambiente de simulação.

Ilustre (2012) apresentou no seu trabalho de conclusão para obtenção do grau de bacharel em Sistemas de Informação pela Universidade Feevale, em 2012, um trabalho sobre IPv6, visando um estudo teórico das mudanças e dos cenários de integração com o IPv4, experimentando algumas técnicas de integração utilizando o GNS3, sem apresentar nenhum tipo de redundância de gateway.

2 METODOLOGIA

Este capítulo apresenta as ferramentas utilizadas para desenvolver o trabalho, o ambiente que será montado para as tarefas e uma explicação dos procedimentos que serão adotados para realizar os testes.

2.1 GNS3

O GNS3 é uma ferramenta gratuita, distribuída sobre licença GLP, para simular redes de maneira bem semelhante a uma rede real. Ele permite a utilização de dispositivos de rede, como switches e roteadores, e a inclusão de computadores, como uma imagem com sistema bem simples até a adição de máquinas virtuais.

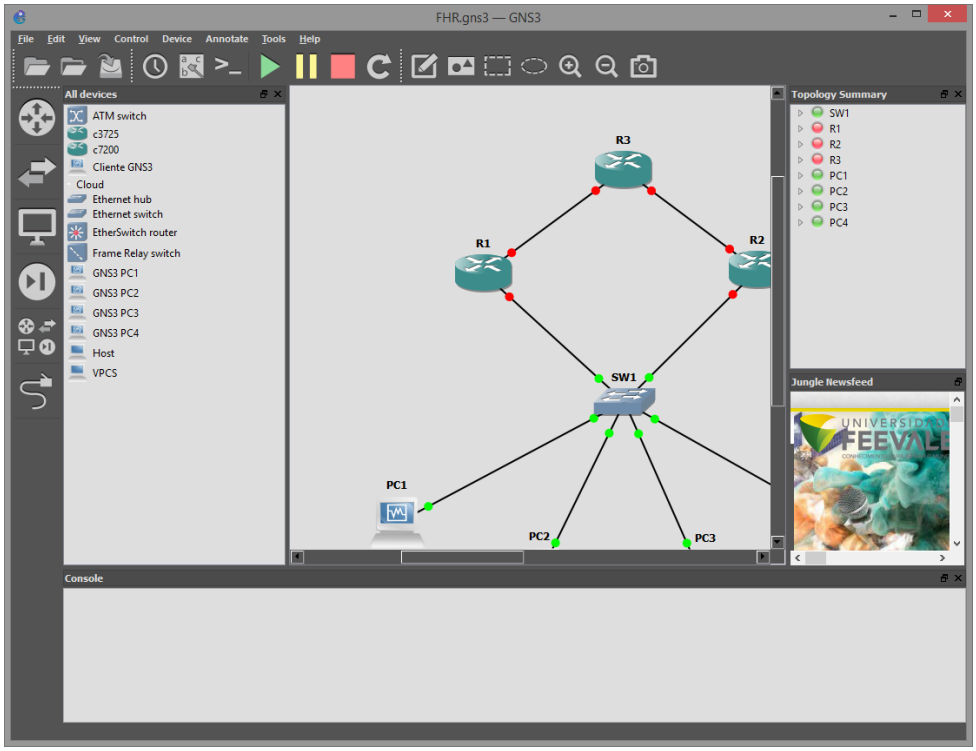


Figura 2.1 – Imagem do software GNS3
Fonte: Autor

O pacote padrão da ferramenta inclui, além do próprio GNS3, os softwares Dynamips, QEMU e Wireshark. O Dynamips tem o propósito de emular o sistema da Cisco IOS (Internetwork Operating System), possibilitando que este seja usado dentro do software de simulação. O IOS deve ser baixado em formato de imagem para que seja utilizado. O

QEMU é um sistema de emulação de maquinas virtuais onde podem ser criados diversos computadores e instalados diversos sistemas operacionais, como Windows e Linux. O Wireshark é um software que faz análise de pacotes de rede.

O GNS3 também suporta a utilização de maquinas virtuais da ferramenta Oracle VirtualBox, similar ao QEMU que vem em seu pacote de instalação.

2.2 Topologia do Ambiente

Para realizar os testes foi criado um ambiente na ferramenta GNS, compondo 3 roteadores, um switch e quatro PCs, estes equivalentes a máquinas virtuais criadas no VirtualBox.

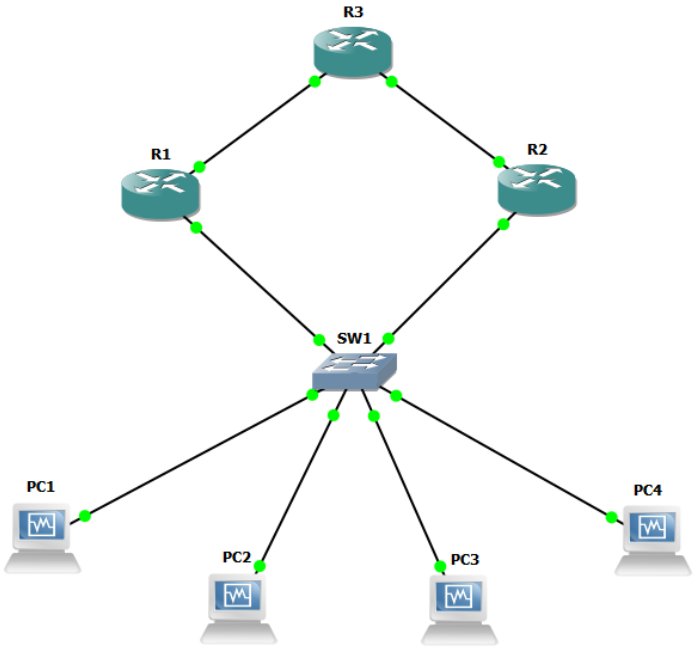


Figura 2.2 – Modelo de ambiente de teste.
Fonte: AUTOR

Os três roteadores do ambiente serão emulações de roteadores da Cisco, configurados a partir do Dynamips com uma imagem deste contendo o sistema operacional IOS. Estes receberão os nomes de R1, R2 e R3.Cada um deles será configurado com duas interfaces de rede. R1 e R2 serão os roteadores que farão composição do grupo dos protocolos de redundância de primeiro salto. R3 será configurado como uma representação de uma rede externa, simulando a internet.

Os quatros PCs serão cada um uma máquina virtual hospedada no VirtualBox, onde será instalado em cada um o sistema operacional Debian 7.8, em sua forma de instalação mínima sem interface gráfica. Estes receberão os nomes de PC1, PC2, PC3 e PC4. Estes computadores têm seus recursos limitados a um processador lógico, utilizando apenas um núcleo do hospedeiro, e 256 MB de memória RAM, para que não sejam consumidos recursos do hospedeiro que podem estar concorrendo com a virtualização dos roteadores virtuais.

O Switch, denominado de SW1, estará configurado para ter 8 portas, estando os PCs conectados nas primeiras 4 portas e os roteadores R1 e R2 nas duas últimas.

2.3 Testes

Os testes irão consistir em configurar os roteadores R1 e R2 com os protocolos de redundância VRRP, HSRP e GLBP, cada um deles utilizando IPv4 e IPv6, totalizando seis configurações diferentes para fazer testes. Para cada uma destas configurações será configurado manualmente o IP virtual resultante como gateway dos PCs do simulador.

De um dos PCs será disparado diversos pacotes ping para um ip do roteador R3, manipulado para ser repetido a cada 150 milissegundos. Durante o processo irá se derrubar a conexão entre o R1 e SW1, simulando assim uma queda do serviço de internet sobre o roteador. A partir deste momento será monitorado quantos pacotes ping não serão respondidos, medindo assim o tempo de indisponibilidade.

Para cada configuração de ambiente serão repetidos 10 testes, a fim de atingir uma média do tempo de indisponibilidade. Todos os resultados serão tabelados e analisados, comparando o desempenho de um protocolo de redundância utilizando IPv4 e IPv6, e comparando o desempenho dos protocolos de redundância entre eles em cada protocolo de rede.

3 APLICAÇÃO

3.1 Configuração Padrão do Ambiente

Para a aplicação dos testes será montado um ambiente padrão sobre a topologia apresentada para os testes.

Para os testes do protocolo de redundância HSRP foi adotado o modelo 7200 de roteador da Cisco, com a versão do IOS Advanced Enterprise Service 15.2(4)S3, visto que este já oferece suporte ao IPv6 sobre este protocolo.

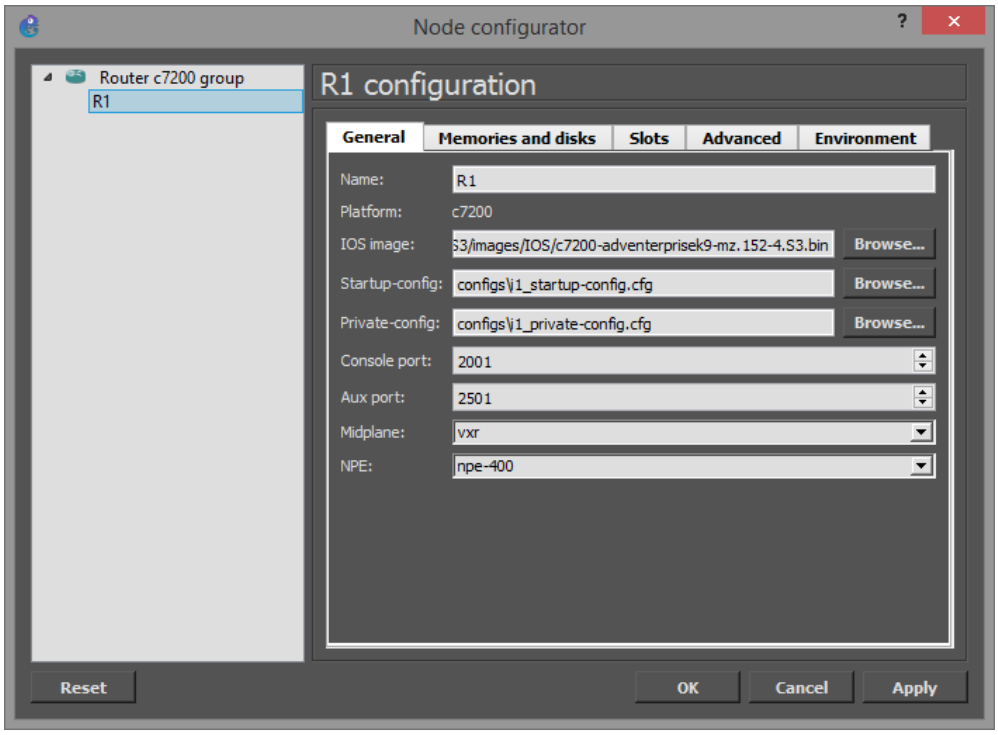


Figura 3.2 – Configuração de R1 com Imagem do IOS 15.2 do roteador Cisco 7200.
Fonte: AUTOR

Para os testes do protocolo de redundância e balanceamento GLBP foi adotado o modelo 3745 de roteador da Cisco, com a versão do IOS Advanced IP Services 12.4(15)T14, visto que esta oferece suporte ao IPv6 sobre este protocolo, pois testes preliminares realizados com o roteador 7200 com a versão 15.2(4)S3 mostraram que o IPv6 neste serviço não é suportado.

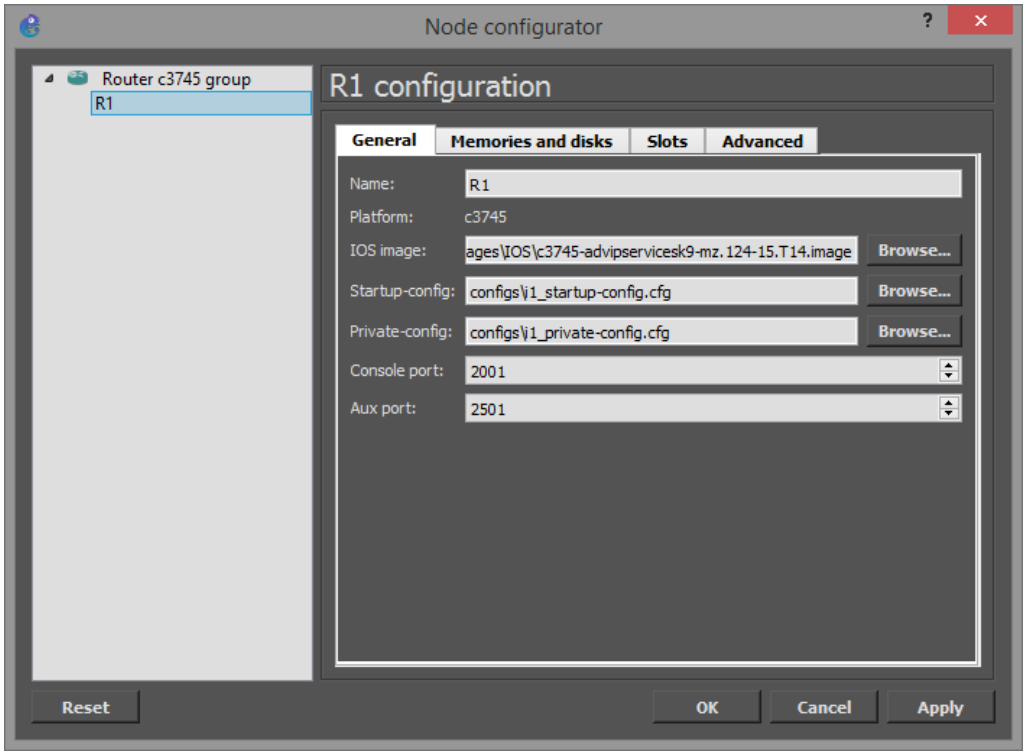


Figura 3.2 – Configuração de R1 com Imagem do IOS 12.4 do roteador Cisco 3745.
Fonte: AUTOR

Para os testes do protocolo de redundância VRRP foram realizados vários testes preliminares com diversas versões do IOS de diversos roteadores, porém nenhuma imagem de sistema compatível com o GNS3 foi encontrada que oferecesse suporte ao IPv6 com este serviço.

Na busca de uma solução da questão buscou-se a ajuda do profissional Vagner Luis de Aguiar, que possui as certificações da Cisco CCNA, CCNA Voice e CCENT. Em ambiente particular do especialista foi simulada a situação com diversas versões do IOS com o GNS3, tentando avaliar se a mesma teria suporta a estas versões. Neste momento verificou-se que as versões mais prováveis de ter a funcionalidade não eram suportadas pelo Dynamips, ferramenta que virtualiza os roteadores no GNS3, e entre diversas versões que eram suportadas pelo virtualizador e foram testadas não havia o suporte para o IPv6 no protocolo de roteamento VRRP.

Apenas para demonstração do resultado do protocolo utilizando IPv4 foram realizados testes utilizando o modelo 7200 de roteador da Cisco, com a versão do IOS Advanced Enterprise Service 15.2(4)S3.

Os endereços das interfaces dos roteadores nos testes IPv4 são atribuídos da seguinte forma: em R1 a interface que faz ligação com o SW1 recebe o endereço 192.168.0.254/24 e a interface que faz ligação com R3 recebe o endereço 10.0.1.1/24, em R2 a interface que faz ligação com o SW1 recebe o endereço 192.168.0.253/24 e a interface que faz ligação com R3 recebe o endereço 10.0.2.1/24, em R3 a interface que faz ligação com o R1 recebe o endereço 10.0.2.2/24, a interface que faz ligação com R2 recebe o endereço 10.0.1.2/24, e é criada uma interface de loopback com o endereço 10.0.9.1/24.

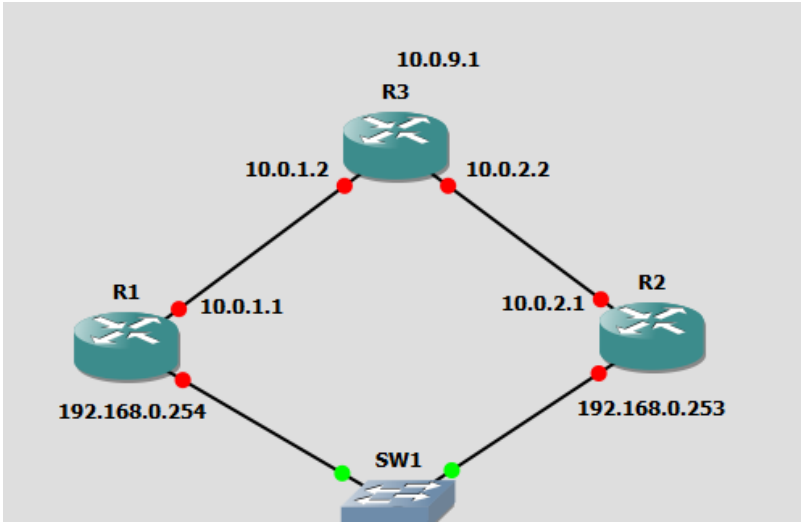


Figura 3.3 – Endereçamento IPv4 das interfaces dos roteadores.
Fonte: AUTOR

De forma semelhante os endereços das interfaces dos roteadores nos testes IPv4 são atribuídos da seguinte forma: em R1 a interface que faz ligação com o SW1 recebe o endereço FC00::FE/64 e a interface que faz ligação com R3 recebe o endereço 4000:1::1/64, em R2 a interface que faz ligação com o SW1 recebe o endereço FC00::FD/64 e a interface que faz ligação com R3 recebe o endereço 4000:2::1/64, em R3 a interface que faz ligação com o R1 recebe o endereço 4000:1::2/64, a interface que faz ligação com R2 recebe o endereço 4000:2::2/64, e é criada uma interface de loopback com o endereço 4000:9::1/64.

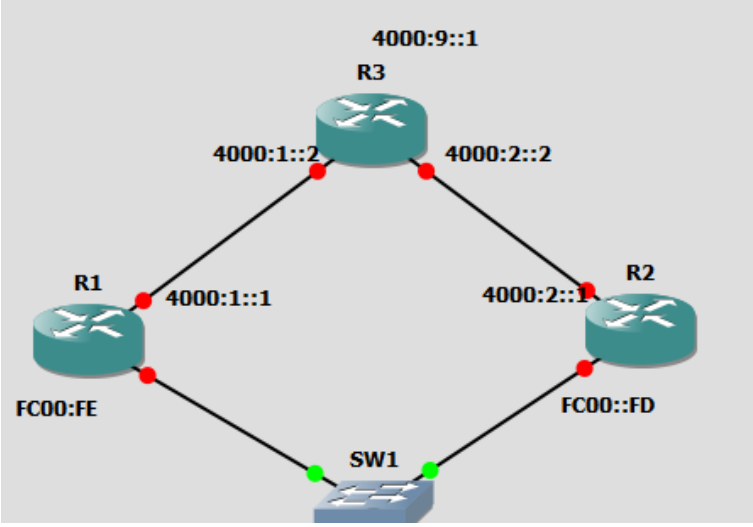


Figura 3.4 – Endereçamento IPv6 das interfaces dos roteadores.
Fonte: AUTOR

Nos 3 roteadores é habilitado um protocolo dinâmico de roteamento, tornando desnecessária a configuração de rotas estáticas entre estes. O protocolo escolhido para isto foi o Open Short Path First (OSPF) na versão 3, encontrado na maioria dos roteadores da Cisco.

Nos computadores virtuais para o Protocolo IPv4 serão atribuídos endereços fixos conforme sua ordem. Para o PC1 será atribuído 192.168.0.1/24, para o PC2 será atribuído 192.168.0.2/24, para o PC3 será atribuído 192.168.0.3/24 e para o PC4 será atribuído 192.168.0.4/24. Nos testes com protocolo IPv6 não serão atribuídos endereços fixos, visto que o próprio protocolo utiliza o *Stateless Address Autoconfigure* (SLAAC), juntamente com o *Neighborhood Discovery* para atribuir o endereço a interface, utilizando o endereço MAC como referência, além do indereço de *link-local* que é atribuído automaticamente na interface, também utilizando o endereço MAC como referência.

```
root@PC1:~# ifconfig eth0
eth0      Link encap:Ethernet  Endereço de HW 08:00:27:05:c5:87
          endereço inet6: fc00::a00:27ff:fe05:c587/64 Escopo:Global
          endereço inet6: fe80::a00:27ff:fe05:c587/64 Escopo:Link
          UP BROADCASTRUNNING MULTICAST  MTU:1500  Métrica:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:1000
          RX bytes:354 (354.0 B)  TX bytes:406 (406.0 B)

root@PC1:~# _
```

Figura 3.5 – Retorno do comando ifconfig para o ambiente com IPv6.
Fonte: AUTOR

O SLAAC é um mecanismo que permite ao computador ou dispositivo gerar seu próprio endereço IP versão 6, com base no reconhecimento da rede local, utilizando os métodos de comunicações ente os dispositivos introduzidos no *Neighborhood Discovery*, necessitando o uso de *Router Advertisement*. (THOMSON et al. 2007, p3). Este recurso dispensa o uso de um servidor DHCP na rede ou configuração manual do endereço nas interfaces de rede.

O *Neighborhood Discovery* é um protocolo utilizado dentro do protocolo de rede IPv6 destinado a determinar os endereços dos computadores e dispositivos vizinhos dentro da mesma camada de rede. (NARTEN et al. 2007, p3). Dentro deste protocolo está definida a comunicação de roteadores disponíveis na rede, chamado de *Router Advertisement*. (NARTEN et al. 2007, p11-16).

A fim de ter mais precisão nos tempos registrados nos testes, nestes computadores também foi instalado uma ferramenta para poder manipular o tempo aguardado pelo ping, chamada FPING. A partir disto desenvolveu-se na linguagem *shell script* dois pequenos programas, um para o protocolo IPv4 e outro para o protocolo IPv6, denominados respectivamente pp e pp6, que executam o comando do programa FPING em sequência, aguardando 95 milissegundos pela resposta do pacote ping quando o roteador está disponível e aguardando 100 milissegundos para o envio de um novo pacote ping caso o roteador não esteja disponível.

```
#!/bin/bash

host=$1

if [ -z $host ]; then
    echo "Usage: `basename $0` [HOST]"
    exit 1
fi

while :; do
    result=`fping -c 1 -t 95 $host | grep '96 bytes'`
    if [ $? -gt 0 ]; then
        echo -e "`date +'%H:%M:%S:%3N'` - host $host is down"
    else
        echo -e "`date +'%H:%M:%S:%3N'` - host $host is up - `echo $result | cut -d ' ' -f 6` ms"
        sleep 0.1
    fi
done
```

Figura 3.6 – Código do programa pp.
Fonte: AUTOR

```
#!/bin/bash

host=$1

if [ -z $host ]; then
    echo "Usage: `basename $0` [HOST]"
    exit 1
fi

while :; do
    result=`fping6 -c 1 -t 95 $host | grep '76 bytes'`
    if [ $? -gt 0 ]; then
        echo -e "`date +'%H:%M:%S:%3N'` - host $host is down"
    else
        echo -e "`date +'%H:%M:%S:%3N'` - host $host is up - `echo $result | cut -d ' ' -f 6` ms"
        sleep 0.1
    fi
done
```

Figura 3.7 – Código do programa pp6.
Fonte: AUTOR

3.2 Procedimentos Realizados

Para habilitar o protocolo de redundância HSRP sobre o protocolo de rede IPv4 precisasse estar em modo privilegiado, entrar no modo de configuração global, e definir a interface de rede na qual se quer habilitar o recurso. Como ao abrir o console do roteador no GNS3 o terminal já entra em modo privilegiado, precisasse apenas entrar com os dois outros comandos.

R1#configure terminal

R1(config)#interface fastEthernet 0/1

Este procedimento será repetido no início da configuração de cada um dos protocolos de redundância para cada protocolo de rede.

3.2.1 Testes com IPv4

A partir do modo de configuração da interface do roteador precisou-se habilitar a redundância de primeiro salto, HSRP, GLBP ou VRRP, definir a prioridade do roteador no grupo, quando habilitado os protocolos HSRP ou VRRP, pois o GLBP fará balanceamento de carga, e habilitar a preempção do protocolo HSRP, pois o VRRP tem esta configuração ativa

por padrão. No teste numerou-se o grupo de roteadores como 1, estabelecendo o endereço IPv4 virtual 192.168.0.200, as prioridades de R1 e R2, que serão 120 e 110 respectivamente.

HSRP	GLBP	VRRP
standby 1 ip 192.168.0.200 standby 1 priority 120 standby 1 preempt	glbp 1 ip 192.168.0.200	vrrp 1 ip 192.168.0.200 vrrp 1 priority 120

Tabela 3.1 – Comandos para habilitar protocolos de redundância em ambiente IPv4.

Fonte: AUTOR.

Neste momento o sistema de redundância já está funcionando, e pode-se verificar seu estado a partir do comando “show standby ” para o protocolo HSRP, “show glbp” para o protocolo GLBP, e “show vrrp ” para o protocolo VRRP, fora do modo de configuração.

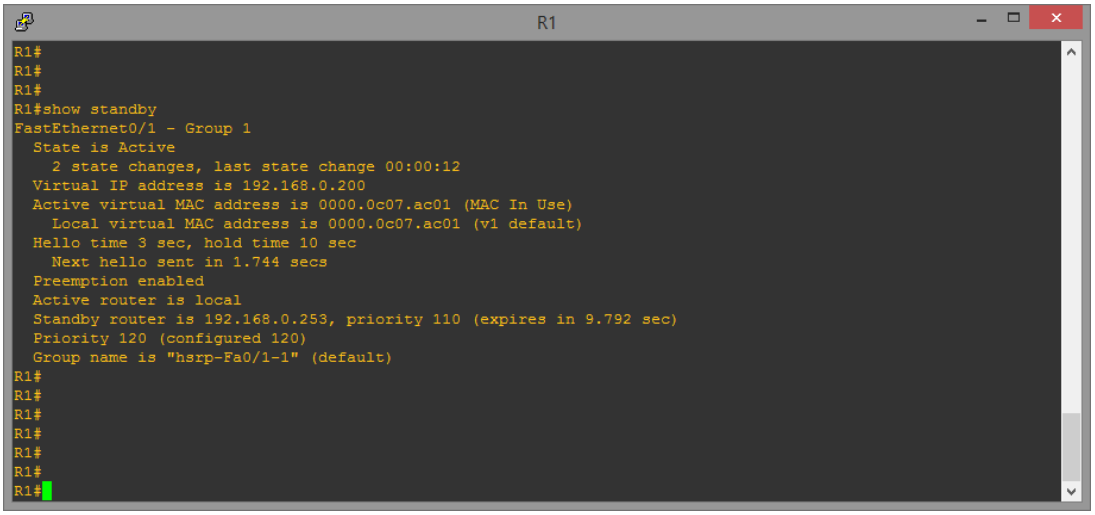


Figura 3.8 – Retorno do comando “show standby” em R1 para ambiente IPv4.

Fonte: AUTOR

Consecutivamente iniciasse um computador virtual do ambiente, inicializando o sistema operacional Linux instalado previamente neste. Neste sistema operacional a interface de rede vem desativada por padrão, e precisasse ativar através de comando, assim como

definir um gateway padrão para o computador, que será o endereço colocado na configuração do protocolo de redundância de primeiro salto.

root@PC1:~#ifconfig eth0 192.168.0.1 netmask 255.255.255.0

root@PC1:~#route add default gw 192.168.0.200 eth0

Utilizou-se agora o PC virtual para realizar os testes de conexão com o endereço configurado na interface de loopback do R3. Utilizando o programa pp executamos o teste de conectividade contra o endereço 10.0.9.1, armazenando o resultado em um arquivo de texto, nomeado com a formação das siglas do protocolo de redundância, sigla do protocolo de rede e número do teste, concatenados.

root@PC1:~#./pp 10.0.9.1 > hsrp_ipv4_1.txt

Mesmo colocando o retorno dentro de um arquivo, o programa FPING, que é chamado dentro do programa pp, exibe na console do computador um retorno do envio do pacote ping, tornando fácil acompanhar quando o destino ficou inacessível e quando ele volta a ficar acessível.

```
10.0.9.1 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 78.5/78.5/78.5
10.0.9.1 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 57.4/57.4/57.4
10.0.9.1 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 98.6/98.6/98.6
10.0.9.1 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 79.9/79.9/79.9
10.0.9.1 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 79.8/79.8/79.8
```

Figura 3.9 – Retorno do comando “pp” na console de um PC virtual quando o destino está acessível.
Fonte: AUTOR

```
10.0.9.1 : xmt/rcv/%loss = 1/0/100%
10.0.9.1 : xmt/rcv/%loss = 1/0/100%
10.0.9.1 : xmt/rcv/%loss = 1/0/100%
10.0.9.1 : xmt/rcv/%loss = 1/0/100%
10.0.9.1 : xmt/rcv/%loss = 1/0/100%
```

Figura 3.10 – Retorno do comando “pp” na console de um PC virtual quando o destino não está acessível.
Fonte: AUTOR

Para simular uma falha no roteador, suspendeu-se a execução de R1, clicando nele com o botão direito e selecionando a opção “*suspend*”. Isto fez com que qualquer rede externa não seja mais acessível através de R1, forçando o roteador R2 a assumir esta função.

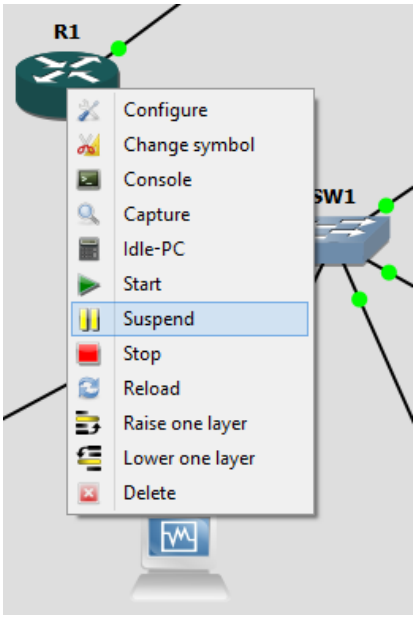


Figura 3.11 – Suspenção do R1, simulando falha no roteador.
Fonte: AUTOR

Acompanhou-se na tela de console do computador virtual até que o retorno passe a indicar que o computador de destino está acessível novamente, e então cancelou-se a execução do programa pp através das teclas “Ctrl” e “C”, pressionadas simultaneamente.

No arquivo gerado pelo teste ficará a hora, minuto, segundo e milissegundo em que o cada pacote ping foi respondido ou em que o tempo de retorno do mesmo foi expirado. Com isto pôde-se verificar o momento onde o destino ficou inacessível e quando voltou a ficar acessível.

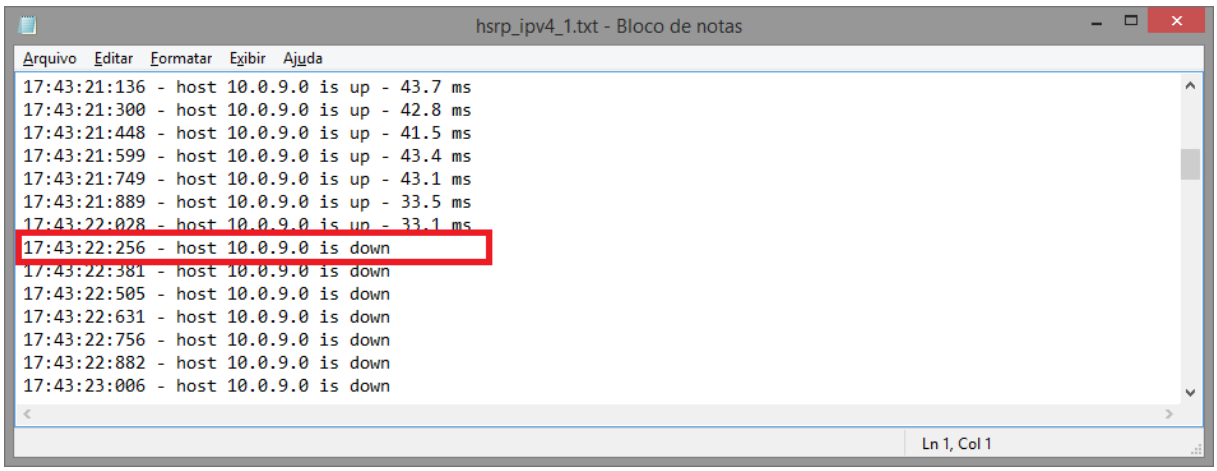


Figura 3.12 – Momento do primeiro pacote ping sem resposta.
Fonte: AUTOR

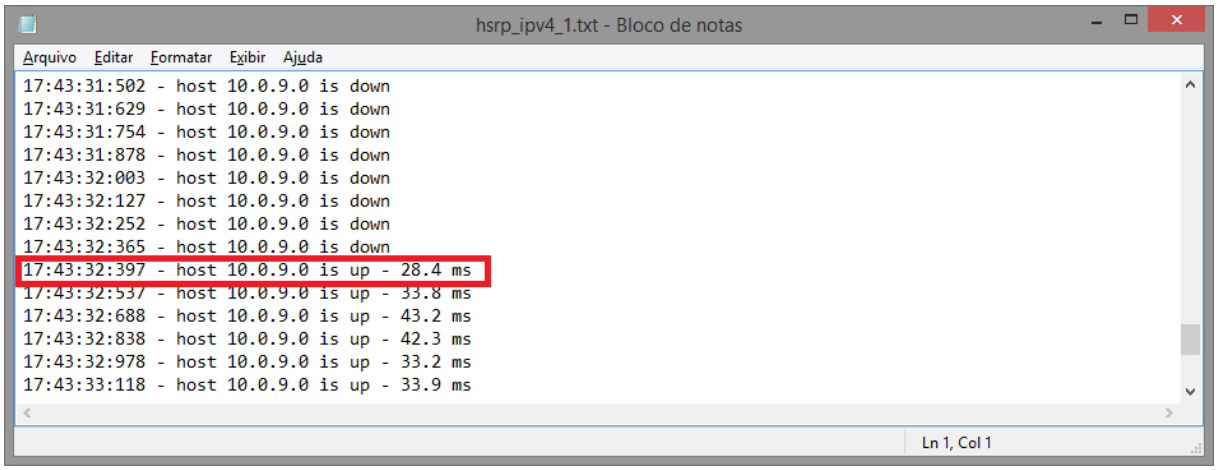


Figura 3.13 – Momento do primeiro pacote ping com resposta.
Fonte: AUTOR

A seguir tirou-se o roteador R1 da suspensão e aguardou-se alguns segundos até que os roteadores voltem a condição normal do HSRP, conforme a prioridade definida. Com os roteadores neste estado pôde-se executar o próximo teste, a partir a execução do programa pp, alterando a nomenclatura do arquivo de saída conforme o número do teste.

3.2.2 Teste com IPV6

Estando no modo de configuração da interface do roteador precisou-se habilitar a redundância de primeiro salto HSRP, definir a prioridade do roteador no grupo do HSRP e habilitar a preempção do protocolo. No teste numerou-se o grupo do HSRP como 1, as prioridades de R1 e R2, que serão 120 e 110 respectivamente, a preempção do protocolo, porém, diferente do HSRP para o IPv4, não definimos o endereço IPv6 virtual do, colocando no ligar deste o parâmetro "autoconfig", que irá gerar um endereço, do tipo *link-local*, conforme a configuração da rede local da interface e o endereço MAC virtual se será atribuído ao HSRP.

HSRP	GLBP
standby 1 ipv6 autoconfig standby 1 priority 120 standby 1 preempt	glbp 1 ipv6 autoconfig

Tabela 3.1 – Comandos para habilitar protocolos de redundância em ambiente IPv6.

Fonte: AUTOR.

Neste momento o sistema de redundância já estava funcionando, e pôde-se verificar seu estado e qual foi o endereço ipv6 atribuído ao HSRP a partir do comando "show standby" para o protocolo HSRP e "show glbp" para o protocolo GLBP, executando fora do modo de configuração.

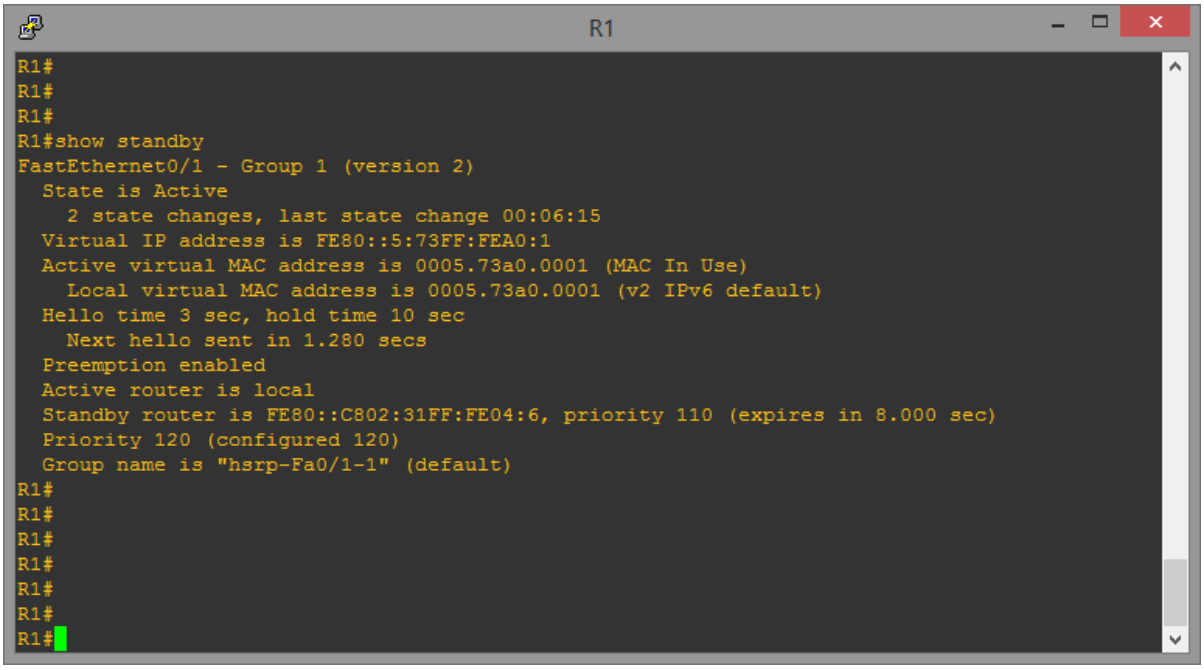


Figura 3.14 – Retorno do comando “show standby” em R1 para ambiente IPv4.
Fonte: AUTOR

Consecutivamente iniciou-se um computador virtual do ambiente, inicializando o sistema operacional Linux instalado previamente neste. Neste sistema operacional a interface de rede vem desativada por padrão, e precisou-se ativar através de comando, porém não precisou-se configurar um IP local, pois o PC reconhece a rede configurada no roteador através da *neighbourhood discovery* do protocolo IPv6 e vem habilitado por padrão ao habilitar um endereço deste protocolo de rede na interface do roteador, e não precisou-se configurar um *gateway* padrão, pois o computador recebe esta informação através do *router advertisement*, que também está habilitado por padrão neste caso.

root@PC1:~#ifconfig eth0 up

Pôde-se verificar qual foi o endereço atribuído a interface do computador através do comando “ifconfig”, e o endereço para gateway através do comando “route –A inet6”.

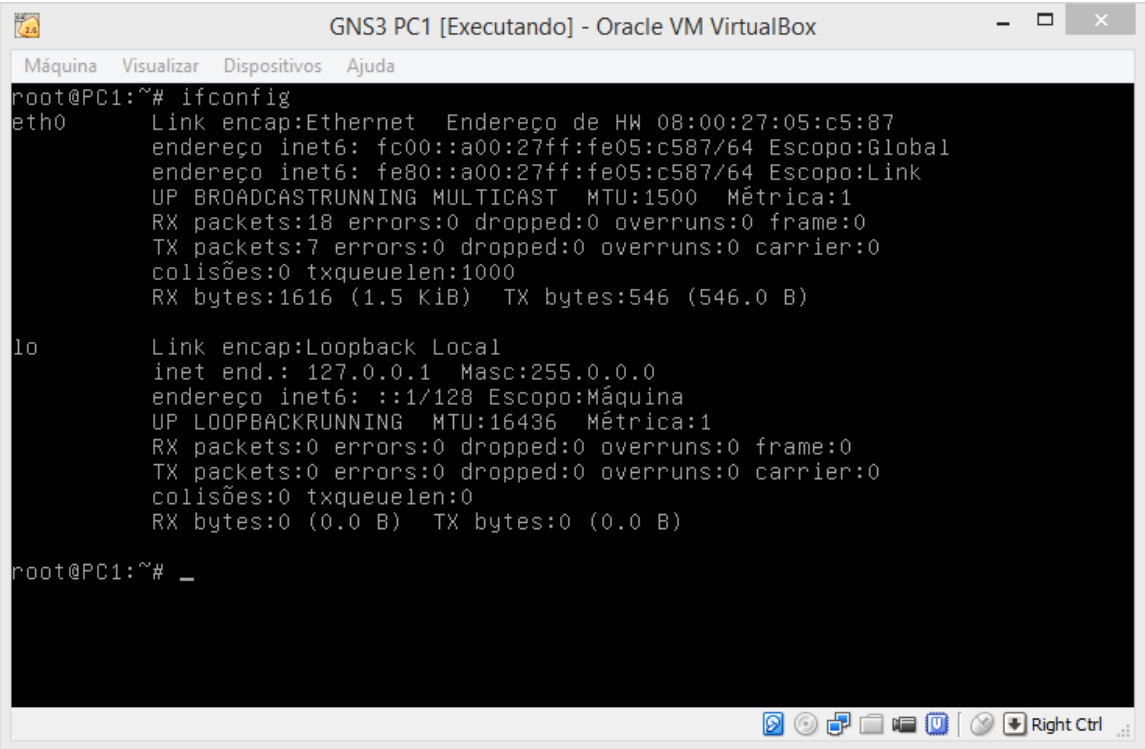


Figura 3.14 – Retorno do comando “ifconfig” em PC1 para ambiente IPv6.
Fonte: AUTOR

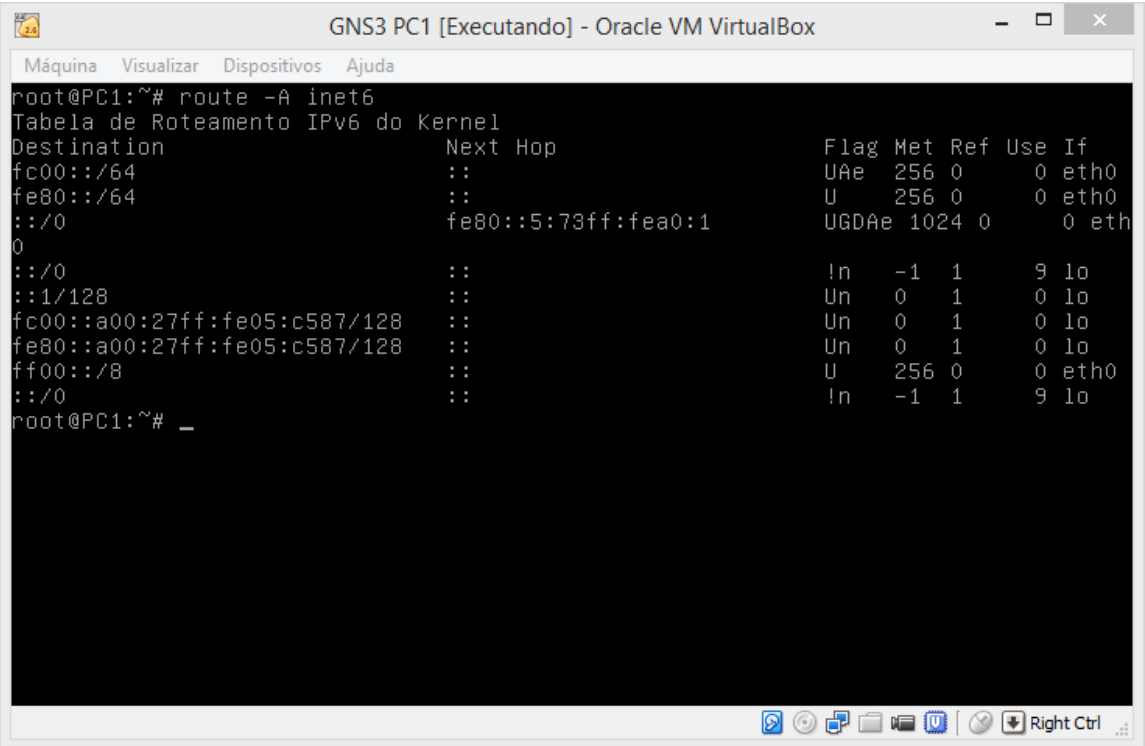


Figura 3.15 – Retorno do comando “rooute –A inet6” em PC1 para ambiente IPv6.
Fonte: AUTOR

De Igual forma ao teste com IPv4, utilizou-se o PC virtual para realizar os testes de conexão com o endereço configurado na interface de loopback do R3. Agora fazendo uso do programa pp6 executamos o teste de conectividade contra o endereço 4000:9::1, também o resultado em um arquivo de texto, nomeado com a formação das siglas do protocolo de redundância, sigla do protocolo de rede e número do teste, concatenados.

root@PC1:~#./pp6 4000:9::1 > hsrp_ipv6_1.txt

Assim como o programa pp, o pp6 exibe na console do computador um retorno do envio do pacote ping, pois utiliza a versão para IPv6 do programa FPING, invocado através do comando “fping6”.

Para simular a falha do roteador utilizou-se o mesmo método empregado no teste com o protocolo IPv4, suspendendo a atividade do roteador R1. Acompanhou-se na console do computador virtual o retorno do programa até que se perceba que os pacotes voltaram a ser respondidos, e então interrompeu-se a execução do programa através das teclas “Crtl” e “C”, pressionadas simultaneamente.

Neste ponto foi reparado que para os testes do protocolo GLBP, na versão 12.4 do IOS, embora houve-se a troca do endereço MAC do gateway para a estação de trabalho virtual, estava se passando aproximadamente 30 segundos após a suspensão de R1 para que os pacotes do ping para R3 voltassem a ser respondidos. Em uma análise do ambiente reparou-se que ao suspender R1 o protocolo de roteamento dinâmico OSPF configurado em R3 apagava todas as rotas para a rede FC00::, e não apenas a rota para R1, fazendo com que este roteador não respondesse aos pacotes desta rede até que fosse reconhecida a rede através de R2 novamente, o que levava um tempo de aproximadamente 30 segundos.

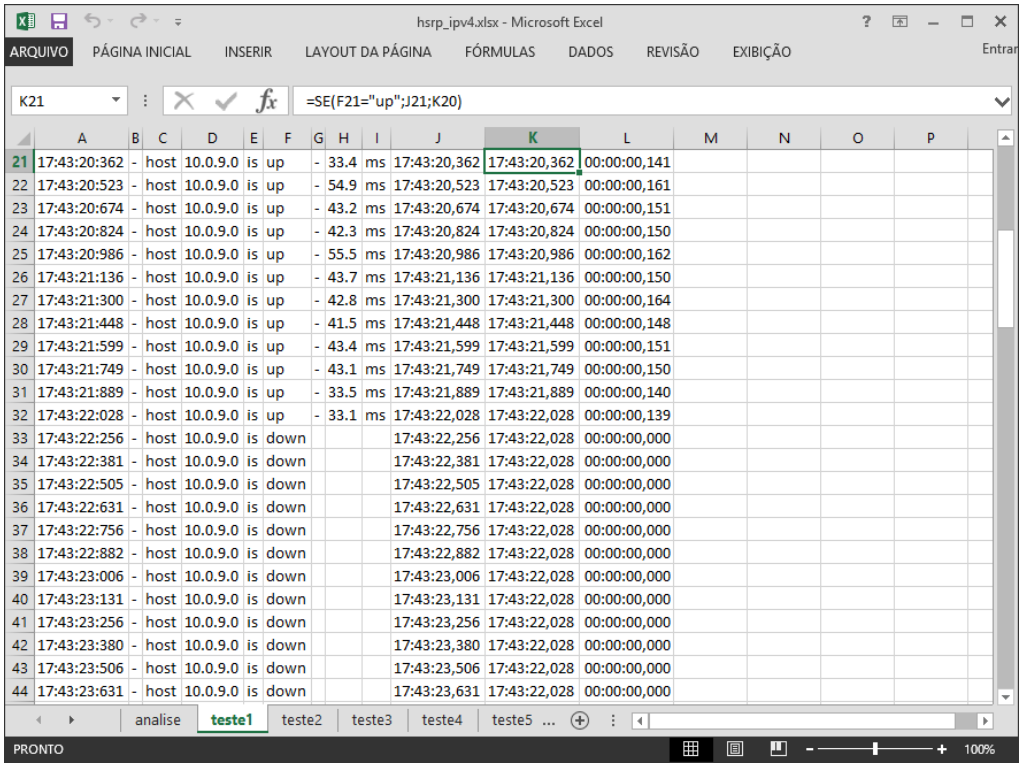
Para contornar a situação foi configurada uma rota estática em R3 para a rede FC00:: através do roteador R2. Desta maneira foi necessário que todos os testes fossem realizados a partir de um computador que recebesse o endereço MAC virtual que fosse correspondente ao R1.

A seguir tirou-se o roteador R1 da suspensão e aguardou-se alguns segundos até que os roteadores voltem a condição normal do HSRP, conforme a prioridade definida. Com os

roteadores neste estado pode-se executar o próximo teste, a partir a execução do programa pp, alterando a nomenclatura do arquivo de saída conforme o teste.

4 ANALISE DOS RESULTADOS

De posse dos arquivos obtidos em cada teste, analisou-se o tempo em que o PC virtual ficou sem comunicação com a rede externa através do software Microsoft Excel, colocando o resultado de cada teste em uma guia. Para verificar este tempo indisponibilidade separamos os dados em colunas e aplicamos formulas para comparar o horário de cada pacote com resposta com o horário do pacote com resposta anterior.



	A	B	C	D	E	F	G	H	I	J	K	L
21	17:43:20:362	-	host	10.0.9.0	is	up	-	33.4	ms	17:43:20,362	17:43:20,362	00:00:00,141
22	17:43:20:523	-	host	10.0.9.0	is	up	-	54.9	ms	17:43:20,523	17:43:20,523	00:00:00,161
23	17:43:20:674	-	host	10.0.9.0	is	up	-	43.2	ms	17:43:20,674	17:43:20,674	00:00:00,151
24	17:43:20:824	-	host	10.0.9.0	is	up	-	42.3	ms	17:43:20,824	17:43:20,824	00:00:00,150
25	17:43:20:986	-	host	10.0.9.0	is	up	-	55.5	ms	17:43:20,986	17:43:20,986	00:00:00,162
26	17:43:21:136	-	host	10.0.9.0	is	up	-	43.7	ms	17:43:21,136	17:43:21,136	00:00:00,150
27	17:43:21:300	-	host	10.0.9.0	is	up	-	42.8	ms	17:43:21,300	17:43:21,300	00:00:00,164
28	17:43:21:448	-	host	10.0.9.0	is	up	-	41.5	ms	17:43:21,448	17:43:21,448	00:00:00,148
29	17:43:21:599	-	host	10.0.9.0	is	up	-	43.4	ms	17:43:21,599	17:43:21,599	00:00:00,151
30	17:43:21:749	-	host	10.0.9.0	is	up	-	43.1	ms	17:43:21,749	17:43:21,749	00:00:00,150
31	17:43:21:889	-	host	10.0.9.0	is	up	-	33.5	ms	17:43:21,889	17:43:21,889	00:00:00,140
32	17:43:22:028	-	host	10.0.9.0	is	up	-	33.1	ms	17:43:22,028	17:43:22,028	00:00:00,139
33	17:43:22:256	-	host	10.0.9.0	is	down				17:43:22,256	17:43:22,028	00:00:00,000
34	17:43:22:381	-	host	10.0.9.0	is	down				17:43:22,381	17:43:22,028	00:00:00,000
35	17:43:22:505	-	host	10.0.9.0	is	down				17:43:22,505	17:43:22,028	00:00:00,000
36	17:43:22:631	-	host	10.0.9.0	is	down				17:43:22,631	17:43:22,028	00:00:00,000
37	17:43:22:756	-	host	10.0.9.0	is	down				17:43:22,756	17:43:22,028	00:00:00,000
38	17:43:22:882	-	host	10.0.9.0	is	down				17:43:22,882	17:43:22,028	00:00:00,000
39	17:43:23:006	-	host	10.0.9.0	is	down				17:43:23,006	17:43:22,028	00:00:00,000
40	17:43:23:131	-	host	10.0.9.0	is	down				17:43:23,131	17:43:22,028	00:00:00,000
41	17:43:23:256	-	host	10.0.9.0	is	down				17:43:23,256	17:43:22,028	00:00:00,000
42	17:43:23:380	-	host	10.0.9.0	is	down				17:43:23,380	17:43:22,028	00:00:00,000
43	17:43:23:506	-	host	10.0.9.0	is	down				17:43:23,506	17:43:22,028	00:00:00,000
44	17:43:23:631	-	host	10.0.9.0	is	down				17:43:23,631	17:43:22,028	00:00:00,000

Figura 4.1 – Procedimento no Excel para análise de tempo de indisponibilidade do teste 1 para HSRP em IPv4.
Fonte: AUTOR

Desta maneira criando um arquivo do Excel para cada protocolo de redundância e rede, com uma guia para cada teste, além de uma guia para um quadro resumo. Neste quando resumo foi coletado, novamente através de formulas, o maior tempo da comparação de horários entre os pacotes com respostas.

4.1 HSRP

A tabela 4.1 expressa os tempos encontrados em cada teste para cada protocolo de rede, com sua média e seu desvio padrão, com o protocolo de redundância HSRP. Como nos testes realizados não foi alterado o *holdtime*, tempo que o roteador aguarda após receber o último pacote de *hello* do outro roteador, que é por padrão 10 segundos, todos os testes ficaram com o tempo próximo ao desta configuração.

HSRP	**IPv4**	**IPv6**
Teste 1	00:00:10,369	00:00:09,592
Teste 2	00:00:09,024	00:00:10,614
Teste 3	00:00:09,658	00:00:10,883
Teste 4	00:00:09,766	00:00:10,136
Teste 5	00:00:10,044	00:00:08,505
Teste 6	00:00:11,024	00:00:09,754
Teste 7	00:00:11,336	00:00:09,904
Teste 8	00:00:08,658	00:00:09,507
Teste 9	00:00:11,595	00:00:09,383
Teste 10	00:00:10,035	00:00:09,383
Média	**00:00:10,151**	**00:00:09,766**
Desvio Padrão	**00:00:00,955**	**00:00:00,675**

Tabela 4.1 – Resultados dos testes do protocolo de redundância HSRP.

Fonte: Autor.

Comparando o tempo médio dos testes de IPv4 e IPv6, o do protocolo mais novo teve um tempo menor, ficando com a média 385 milissegundos a baixo do anterior. Assim como comparando o desvio padrão entre os tempos obtidos nos testes, este valor também se apresentou menor para a versão 6 do protocolo IP, ficando 280 milissegundos menor, demonstrando que neste ambiente a variação entre os tempos de indisponibilidade dos testes é menor que a da versão 4 do mesmo protocolo.

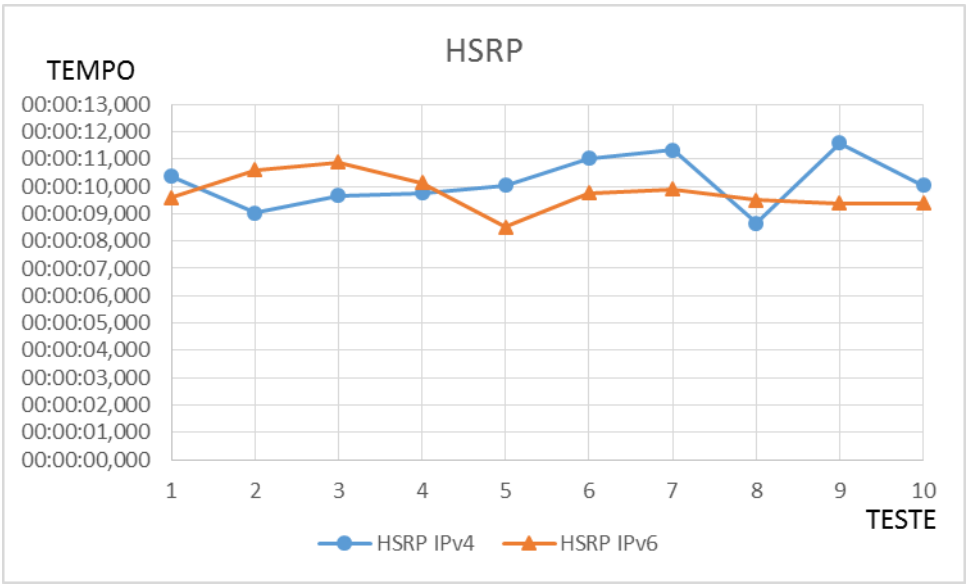


Figura 4.2 – Gráfico comparativo entre os resultados dos testes em HSRP entre IPv4 e IPv6.
Fonte: AUTOR

4.2 GLBP

A tabela 4.2 expressa os tempos encontrados em cada teste para cada protocolo de rede, com sua média e seu desvio padrão, com o protocolo de redundância GLBP. Nestes testes também não foi alterado o *holdtime*, tempo que o roteador aguarda após receber o último pacote de *hello* do outro roteador, que é por padrão 10 segundos, novamente todos os testes ficaram com o tempo próximo ao desta configuração.

GLBP	**IPv4**	**IPv6**
Teste 1	00:00:08,711	00:00:07,944
Teste 2	00:00:09,173	00:00:08,407
Teste 3	00:00:09,056	00:00:10,054
Teste 4	00:00:11,163	00:00:08,798
Teste 5	00:00:08,399	00:00:09,292
Teste 6	00:00:08,915	00:00:08,356
Teste 7	00:00:10,334	00:00:08,548
Teste 8	00:00:09,539	00:00:07,861
Teste 9	00:00:09,840	00:00:08,625
Teste 10	00:00:08,548	00:00:09,775
Média	**00:00:09,368**	**00:00:08,766**
Desvio Padrão	**00:00:00,869**	**00:00:00,731**

Tabela 4.2 – Resultados dos testes do protocolo de redundância GLBP.

Fonte: Autor.

Novamente comparando o tempo médio dos testes de entre os protocolos de rede, o do protocolo IPv6 teve um tempo menor, ficando com a média 602 milissegundos a baixo do protocolo IPv4. Comparando o desvio padrão entre os tempos obtidos nos testes, este valor também se apresentou menor para a versão mais nova do protocolo IP, ficando 138 milissegundos menor, demonstrando que neste ambiente a variação entre os tempos de indisponibilidade dos testes é menor que a da versão mais antiga do protocolo.

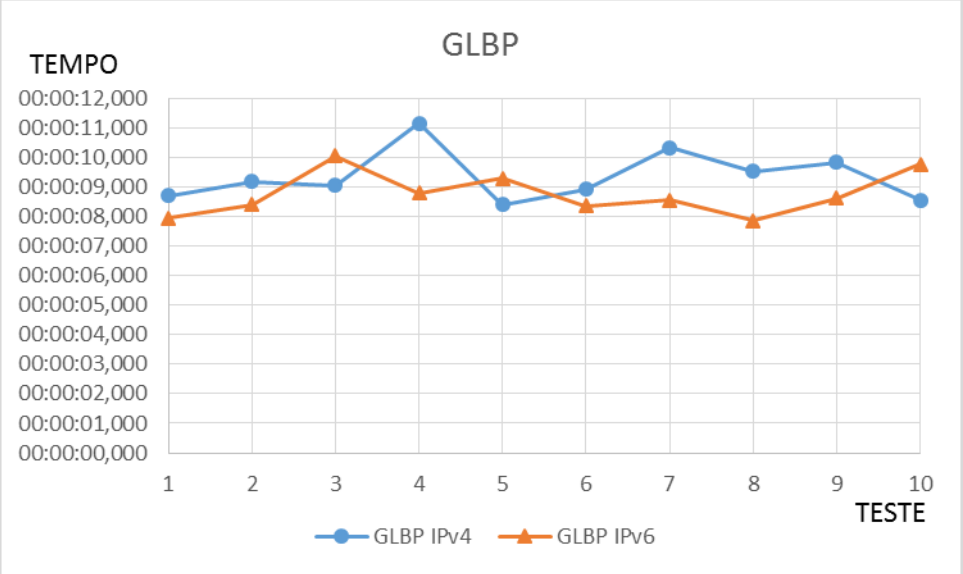


Figura 4.3 – Gráfico comparativo entre os resultados dos testes em GLBP entre IPv4 e IPv6.
Fonte: AUTOR

4.3 VRRP

A tabela 4.3 expressa os tempos encontrados em cada teste para o protocolo de rede IPv4, com sua média e seu desvio padrão, com o protocolo de redundância VRRP, pois conforme explicado anteriormente, no subcapitulo 3.1, não foi encontrada uma imagem do IOS para os roteadores suportados pela ferramenta Dynamips, do software GNS3.

GLBP	IPv4
Teste 1	00:00:03,194
Teste 2	00:00:03,065
Teste 3	00:00:03,603
Teste 4	00:00:03,602
Teste 5	00:00:03,311
Teste 6	00:00:03,449
Teste 7	00:00:03,065
Teste 8	00:00:03,448
Teste 9	00:00:03,818
Teste 10	00:00:03,190
Média	**00:00:03,374**
Desvio Padrão	**00:00:00,253**

Tabela 4.2 – Resultados dos testes do protocolo de redundância VRRP.

Fonte: Autor.

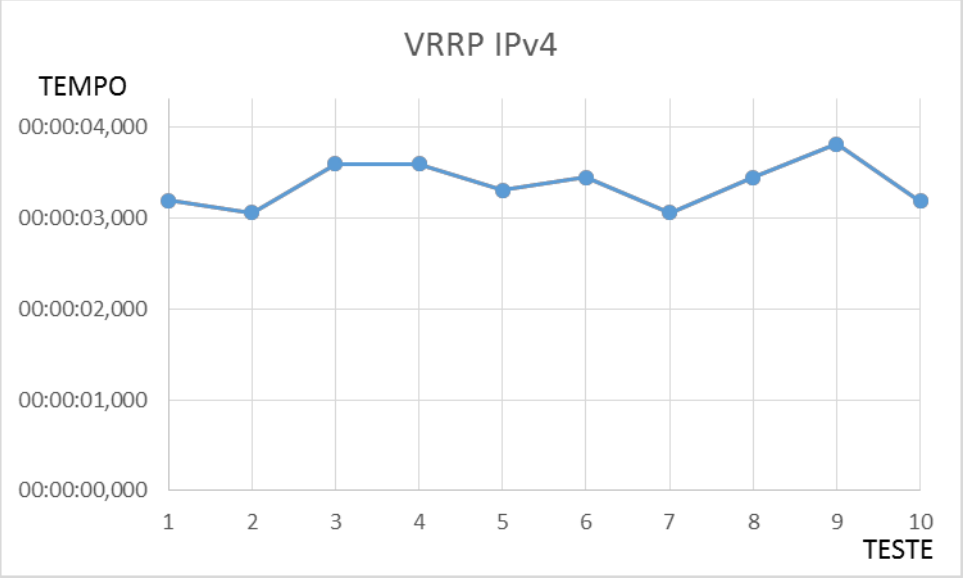


Figura 4.3 – Gráfico demonstrativo dos resultados dos testes em VRRP em IPv4.

Fonte: AUTOR

CONCLUSÃO

Atualmente os serviços de internet são cada vez mais necessários no cotidiano das pessoas, principalmente no ambiente corporativo. Garantir que esta comunicação com a rede mundial permaneça disponível para a boa fluência dos trabalhos produtivos é um desafio constante que profissionais de TI e áreas de comunicações enfrentam. No objetivo de deixar o tempo de disponibilidade destas conexões em 100% do tempo de necessidade, se investe em estruturas e recursos para a prevenção e redundância dos mesmos. Com a chegada da nova versão do protocolo de internet, o IPv6, é preciso verificar muito bem os investimentos em hardwares e softwares para prover estas redundâncias, pois é importante verificar se os mesmos já estão preparados para esta mudança.

Este trabalho analisou o funcionamento e comportamento dos protocolos de redundância HSRP, GLBP e VRRP, disponíveis nos roteadores na empresa Cisco Systems, e tem o objetivo de prover e gerenciar um endereço IP e um ou mais endereços MAC virtuais entre um grupo de roteadores, utilizando estes como *gateway* para os computadores e dispositivos de uma rede, a fim de alternar a rota física de saída desta rede caso houver a falha de um roteador físico deste grupo apresente um problema e se torne indisponível.

O objetivo de realizar a pesquisa bibliográfica sobre os protocolos de redundância de primeiro salto HSRP, GLBP e VRRP, apresentando o funcionamento básico de cada um deles, considera-se plenamente atingido.

O objetivo de apresentar a pesquisa bibliográfica, com a estrutura de endereçamento e funcionamento do protocolo IPv6 considera-se plenamente atingido.

Ao que se refere a apresentação da ferramenta GNS3 e sua aplicação para estudos e simulações, como as aplicações desta utilizadas durante os testes realizados no trabalho, como objetivo considera-se plenamente atingido.

Quanto aos objetivos de realizar os testes dos protocolos de redundância de primeiro salto com os protocolos de rede IPv4 e IPv6, considera-se parcialmente atingido. Isto em função de não ter sido realizados os testes com ambientes mistos conforme planejado. Este processo se tornou muito moroso e de necessidade de mais estudo, extrapolando o tempo disponível para a conclusão do trabalho.

Ao total pode-se afirmar que os objetivos gerais do projeto, verificar impactos durante a transição do IPv4 para o IPv6, assim como verificar se os níveis de disponibilidades

se mantém os mesmo nos dois protocolos, foram parcialmente atingidos. As pesquisas bibliográficas sobre os assuntos pertinentes, o estudo dos protocolos de redundância e a execução dos testes em ambientes com os protocolos de redes isolados foram realizados, embora o teste de um protocolo de redundância em ambiente com o protocolo de rede IPv6 não tenha obtido resultados pela falta de uma versão compatível com a ferramenta utilizada para os testes.

Com base na realização dos testes foi possível verificar que ainda existem dificuldades em fazer a implementação dos serviços de redundâncias para o protocolo IPv6, visto que existem roteadores que utilizam o sistema operacional IOS da Cisco e ainda não receberam atualização para o funcionamento neste novo protocolo, a exemplo do protocolo de redundância VRRP para o roteador c7200 com a versão do IOS Advanced Enterprise Service 15.2(4)S3, com ano de release de 2013, ainda não fornece suporte ao IPv6. Isto pode significar uma mudança significativa para a implementação de um sistema de redundância para IPv6 para uma estrutura que utiliza o VRRP com IPv4 atualmente.

Como sugestão para trabalhos futuros, pode-se realizar os testes em ambientes com os dois protocolos de rede habilitados, e a execução dos testes novamente em versões posteriores as disponíveis durante este trabalho ou outros roteadores de outros fabricantes, a fim de verificar se os novos lançamentos de versões disponibilizam suporte ao IPv6.

REFERÊNCIAS BIBLIOGRÁFICAS

IPv6.br. **1% dos usuários brasileiros com IPv6! 2015**. Disponível em <http://ipv6.br/um-porcento-dos-usuarios-brasileiros-com-ipv6/>. Acessado em 25 de março de 2015.

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

PINHEIRO, José Mauricio dos Santos. **Conceitos de Redundância e Contingência**. Disponível em <http://www.projetoderedes.com.br/artigos/artigo_conceitos_de_redundancia.php#.UTjFnxJYsuJ>. Acessado em 20 de março de 2015

NIC.br. **NIC.br anuncia que o esgotamento de endereços IPv4 acontecerá nos próximos meses**. 2014a. Disponível em <http://nic.br/imprensa/releases/2014/rl-2014-07.htm>. Acessado em 20 de março de 2015.

NIC.br. **Termina o estoque de endereços IPv4 na América Latina**. 2014b. Disponível em <http://www.nic.br/imprensa/releases/2014/rl-2014-19.htm>. Acessado em 20 de março de 2015.

SONDEREGGER, James, BLOMBERG, Orin., MILNE, Kieran., and PALISLAMOVIC, Senad. . **Junos High Availability: Best Practices for High Network Uptime**. O'Reilly Media, Inc. 2009. 656 p.

CISCO. **First Hop Redundancy Protocol (FHRP)**. Disponível em < http://www.cisco.com/c/en/us/products/ios-nx-os-software/first-hop-redundancy-protocol-fhrp/index.html>. Acessado em 25 de março de 2015.

H3C. **VRRP Configuration**. Disponível em <http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/Security_Products/H3C_SecPath_F1000-E/Configuration/Operation_Manual/H3C_SecPath_High-End_OM%28F3169_F3207%29-5PW106/05/201109/725890_1285_0.htm> Acessado em 10 de maio de 2015.

NADAS, S.; ERICSON, Ed. **RFC 5798 Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6**. 2010. Disponível em <https://tools.ietf.org/html/rfc5798#section-1.3>. Acessado em 9 de maio de 2015.

CISCO. **Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x**. 2011. Disponível em <http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/unicast/configuration/guide/l3_cli_nxos.html>. Acessado em 9 de maio de 2015

FILIPPETTI, Marco. **Artigo VRRP x HSRP x GLBP**.2008. Disponível em <http://blog.ccna.com.br/2008/12/16/pr-vrrp-x-hsrp-x-glbp>. Acesso em 16 de maio de 2015

NACIMENTO, Marcelo. **Introdução a Redundância no Primeiro Salto ou FHRP – First Hop Redundancy Protocol**. 2014. Disponível em <http://www.dltec.com.br/blog/cisco/introducao-a-redundancia-no-primeiro-salto-ou-fhrp-first-hop-redundancy-protocols/>. Acessado em 17 de maio de 2015.

MORESCHI, Karen Cristine. **Comparação entre Protocolos de Gateways Redundantes utilizando Roteadores Dedicados**. 2011. 31 p. Trabalho de Conclusão de Curso (Tecnologia em Sistemas para Internet) - Universidade Tecnológica Federal do Paraná, Campo Mourão, 2011.

HASHIMOTO, Gilberto Tadayoshi. **Uma Proposta de Extensão para um Protocolo para Arquitetura de Alta Disponibilidade**. 2009. 79 p. Universidade Federal de Uberlândia, Uberlândia, 2009.

PORTO, Helton Luiz. **Redundância e Balanceamento de Carga em Rede Corporativa**. 2014. 53p. Instituto Federal de Santa Catarina. São José, 2014.

ILUSTRE, Giuli Gilberto. **IPv6 - Estudo Teórico e Análise de Cenários de Integração com IPv4**. 2012. 105 p. Universidade Feevale. Novo Hamburgo, 2012.

SILVA, Vitor Pain da. **Estudo comparativo entre os protocolos de redundância VRRP e HSRP.** 2013. 71 p. Universidade Feevale. Novo Hamburgo, 2013.

COULOURIS, George, DOLLIMORE, Jean, KINDBERG, Tim, BLAIR, Gordon. **Sistemas Distribuídos Conceitos e Projetos**. 5ª Edição. 2013. 1047 p. Bookman Editora Ltda. Porto Alegre, 2013.

MICROSOFT. **Conceitos de alta disponibilidade e recuperação de desastre no SharePoint 2013**. 2015. Disponível em < https://technet.microsoft.com/pt-br/library/jj715263.aspx> . Acessado em 29 de maio de 2015.

USC - University of Southern California. **RFC 791 - INTERNET PROTOCOL**. 1981. 45 p. Disponível em < https://tools.ietf.org/html/rfc791>. Acessado em 02 de junho de 2015.

FULLER, V. LI, T. YU, J. VARADHAN, K. **RFC 1519 - Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy**. 1993. 24 p. Disponível em < https://tools.ietf.org/html/rfc1519>. Acessado em 02 de junho de 2015.

DEERING, S. HINDEN, R. **RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification**. 1998. 39 p. Disponível em < http://tools.ietf.org/html/rfc2460>. Acesado em 04 de junho de 2015.

SCHENEIDER, Márcio Ricardo. **Desmistificando a Alta Disponibilidade**. 2003. 81 p. Universidade Feevale. Novo Hamburgo.

ITIL, https://www.axelos.com/login?ReturnUrl=~%2Fcase-studies-and-white-papers%2Fitil-the-basics-white-paper. 2013. Acessado em 28 de maio de 2015.

NARTEN, T., NORDMARK, E., SIMPSON, W., SOLIMAN, H. **RFC 4861 - Neighbor Discovery in IPv6**. 2007. 97 p. Disponível em < https://tools.ietf.org/html/rfc4861 >. Acessado em 31 de outubro de 2015.

THOMSON, S., NARTEN, T., JINMEI, T. **RFC 4862 - IPv6 Stateless Address Autoconfiguration**. 2007. 30 p. Disponível em < https://tools.ietf.org/html/rfc4862 >. Acessado em 31 de outubro de 2015.

APENDICE A – RESUMO DOS ARQUIVOS TESTES DO HSRP IPV4

Teste 1

17:43:21:889 - host 10.0.9.1 is up - 33.5 ms
17:43:22:028 - host 10.0.9.1 is up - 33.1 ms
17:43:22:256 - host 10.0.9.1 is down
17:43:22:381 - host 10.0.9.1 is down
:
17:43:32:252 - host 10.0.9.1 is down
17:43:32:365 - host 10.0.9.1 is down
17:43:32:397 - host 10.0.9.1 is up - 28.4 ms
17:43:32:537 - host 10.0.9.1 is up - 33.8 ms

Teste 2

17:45:04:626 - host 10.0.9.1 is up - 34.0 ms
17:45:04:776 - host 10.0.9.1 is up - 43.0 ms
17:45:05:004 - host 10.0.9.1 is down
17:45:05:128 - host 10.0.9.1 is down
:
17:45:13:633 - host 10.0.9.1 is down
17:45:13:757 - host 10.0.9.1 is down
17:45:13:800 - host 10.0.9.1 is up - 38.3 ms
17:45:13:940 - host 10.0.9.1 is up - 32.7 ms

Teste 3

17:45:32:461 - host 10.0.9.1 is up - 43.0 ms
17:45:32:613 - host 10.0.9.1 is up - 43.3 ms
17:45:32:840 - host 10.0.9.1 is down
17:45:32:966 - host 10.0.9.1 is down
:
17:45:42:095 - host 10.0.9.1 is down
17:45:42:220 - host 10.0.9.1 is down
17:45:42:271 - host 10.0.9.1 is up - 46.4 ms
17:45:42:432 - host 10.0.9.1 is up - 54.9 ms

Teste 4

17:46:05:758 - host 10.0.9.1 is up - 42.9 ms
17:46:05:909 - host 10.0.9.1 is up - 43.1 ms
17:46:06:137 - host 10.0.9.1 is down
17:46:06:262 - host 10.0.9.1 is down
:
17:46:15:509 - host 10.0.9.1 is down
17:46:15:633 - host 10.0.9.1 is down
17:46:15:675 - host 10.0.9.1 is up - 37.6 ms
17:46:15:825 - host 10.0.9.1 is up - 43.2 ms

Teste 5

17:46:34:079 - host 10.0.9.1 is up - 43.8 ms
17:46:34:240 - host 10.0.9.1 is up - 53.1 ms
17:46:34:467 - host 10.0.9.1 is down
17:46:34:592 - host 10.0.9.1 is down
:
17:46:44:101 - host 10.0.9.1 is down
17:46:44:227 - host 10.0.9.1 is down
17:46:44:284 - host 10.0.9.1 is up - 52.0 ms
17:46:44:425 - host 10.0.9.1 is up - 33.0 ms

Teste 6

```
17:47:12:969 - host 10.0.9.1 is up - 53.2 ms
17:47:13:120 - host 10.0.9.1 is up - 44.3 ms
17:47:13:348 - host 10.0.9.1 is down
17:47:13:474 - host 10.0.9.1 is down
:
17:47:23:978 - host 10.0.9.1 is down
17:47:24:104 - host 10.0.9.1 is down
17:47:24:144 - host 10.0.9.1 is up - 36.2 ms
17:47:24:284 - host 10.0.9.1 is up - 33.1 ms
```

Teste 7

```
17:47:47:398 - host 10.0.9.1 is up - 42.4 ms
17:47:47:549 - host 10.0.9.1 is up - 43.2 ms
17:47:47:776 - host 10.0.9.1 is down
17:47:47:900 - host 10.0.9.1 is down
:
17:47:58:654 - host 10.0.9.1 is down
17:47:58:780 - host 10.0.9.1 is down
17:47:58:885 - host 10.0.9.1 is up - 100 ms
17:47:59:036 - host 10.0.9.1 is up - 43.3 ms
```

Teste 8

```
17:48:46:392 - host 10.0.9.1 is up - 40.9 ms
17:48:46:532 - host 10.0.9.1 is up - 33.6 ms
17:48:46:761 - host 10.0.9.1 is down
17:48:46:887 - host 10.0.9.1 is down
:
17:48:55:018 - host 10.0.9.1 is down
17:48:55:143 - host 10.0.9.1 is down
17:48:55:190 - host 10.0.9.1 is up - 43.1 ms
17:48:55:331 - host 10.0.9.1 is up - 33.6 ms
```

Teste 9

```
17:49:58:215 - host 10.0.9.1 is up - 51.0 ms
17:49:58:365 - host 10.0.9.1 is up - 43.7 ms
17:49:58:594 - host 10.0.9.1 is down
17:49:58:718 - host 10.0.9.1 is down
:
17:50:09:720 - host 10.0.9.1 is down
17:50:09:844 - host 10.0.9.1 is down
17:50:09:960 - host 10.0.9.1 is up - 112 ms
17:50:10:100 - host 10.0.9.1 is up - 34.1 ms
```

Teste 10

```
17:50:31:289 - host 10.0.9.1 is up - 55.0 ms
17:50:31:439 - host 10.0.9.1 is up - 41.6 ms
17:50:31:668 - host 10.0.9.1 is down
17:50:31:793 - host 10.0.9.1 is down
:
17:50:41:300 - host 10.0.9.1 is down
17:50:41:424 - host 10.0.9.1 is down
17:50:41:474 - host 10.0.9.1 is up - 45.2 ms
17:50:41:635 - host 10.0.9.1 is up - 53.8 ms
```

APENDICE B – RESUMO DOS ARQUIVOS TESTES DO HSRP IPV6

Teste 1

12:22:33:811 - host 4000:9::1 is up - 75.0 ms
12:22:34:005 - host 4000:9::1 is up - 86.4 ms
12:22:34:232 - host 4000:9::1 is down
12:22:34:356 - host 4000:9::1 is down
:
12:22:43:443 - host 4000:9::1 is down
12:22:43:554 - host 4000:9::1 is down
12:22:43:597 - host 4000:9::1 is up - 38.9 ms
12:22:43:747 - host 4000:9::1 is up - 44.0 ms

Teste 2

12:28:19:568 - host 4000:9::1 is up - 54.9 ms
12:28:19:740 - host 4000:9::1 is up - 64.9 ms
12:28:19:967 - host 4000:9::1 is down
12:28:20:092 - host 4000:9::1 is down
:
12:28:30:196 - host 4000:9::1 is down
12:28:30:320 - host 4000:9::1 is down
12:28:30:354 - host 4000:9::1 is up - 29.8 ms
12:28:30:493 - host 4000:9::1 is up - 32.5 ms

Teste 3

12:29:06:561 - host 4000:9::1 is up - 53.2 ms
12:29:06:712 - host 4000:9::1 is up - 44.8 ms
12:29:06:940 - host 4000:9::1 is down
12:29:07:065 - host 4000:9::1 is down
:
12:29:17:427 - host 4000:9::1 is down
12:29:17:541 - host 4000:9::1 is down
12:29:17:595 - host 4000:9::1 is up - 49.2 ms
12:29:17:724 - host 4000:9::1 is up - 22.7 ms

Teste 4

12:29:39:049 - host 4000:9::1 is up - 53.3 ms
12:29:39:204 - host 4000:9::1 is up - 44.3 ms
12:29:39:431 - host 4000:9::1 is down
12:29:39:557 - host 4000:9::1 is down
:
12:29:49:163 - host 4000:9::1 is down
12:29:49:287 - host 4000:9::1 is down
12:29:49:340 - host 4000:9::1 is up - 48.8 ms
12:29:49:502 - host 4000:9::1 is up - 54.7 ms

Teste 5

12:30:10:784 - host 4000:9::1 is up - 65.6 ms
12:30:10:946 - host 4000:9::1 is up - 54.1 ms
12:30:11:173 - host 4000:9::1 is down
12:30:11:298 - host 4000:9::1 is down
:
12:30:19:282 - host 4000:9::1 is down
12:30:19:397 - host 4000:9::1 is down
12:30:19:451 - host 4000:9::1 is up - 50.0 ms
12:30:19:580 - host 4000:9::1 is up - 23.0 ms

Teste 6

12:31:31:684 - host 4000:9::1 is up - 43.6 ms
12:31:31:867 - host 4000:9::1 is up - 74.9 ms
12:31:32:094 - host 4000:9::1 is down
12:31:32:218 - host 4000:9::1 is down
:
12:31:41:443 - host 4000:9::1 is down
12:31:41:568 - host 4000:9::1 is down
12:31:41:621 - host 4000:9::1 is up - 48.9 ms
12:31:41:750 - host 4000:9::1 is up - 22.2 ms

Teste 7

12:31:59:192 - host 4000:9::1 is up - 64.9 ms
12:31:59:354 - host 4000:9::1 is up - 55.7 ms
12:31:59:591 - host 4000:9::1 is down
12:31:59:715 - host 4000:9::1 is down
:
12:32:09:077 - host 4000:9::1 is down
12:32:09:201 - host 4000:9::1 is down
12:32:09:258 - host 4000:9::1 is up - 53.0 ms
12:32:09:387 - host 4000:9::1 is up - 23.3 ms

Teste 8

12:33:21:944 - host 4000:9::1 is up - 76.6 ms
12:33:22:104 - host 4000:9::1 is up - 51.7 ms
12:33:22:332 - host 4000:9::1 is down
12:33:22:456 - host 4000:9::1 is down
:
12:33:31:431 - host 4000:9::1 is down
12:33:31:556 - host 4000:9::1 is down
12:33:31:611 - host 4000:9::1 is up - 51.1 ms
12:33:31:740 - host 4000:9::1 is up - 22.7 ms

Teste 9

12:33:54:581 - host 4000:9::1 is up - 55.1 ms
12:33:54:753 - host 4000:9::1 is up - 65.7 ms
12:33:54:979 - host 4000:9::1 is down
12:33:55:103 - host 4000:9::1 is down
:
12:34:03:851 - host 4000:9::1 is down
12:34:03:975 - host 4000:9::1 is down
12:34:04:034 - host 4000:9::1 is up - 54.9 ms
12:34:04:163 - host 4000:9::1 is up - 23.1 ms

Teste 10

12:34:18:605 - host 4000:9::1 is up - 63.3 ms
12:34:18:771 - host 4000:9::1 is up - 56.0 ms
12:34:18:998 - host 4000:9::1 is down
12:34:19:122 - host 4000:9::1 is down
:
12:34:27:973 - host 4000:9::1 is down
12:34:28:097 - host 4000:9::1 is down
12:34:28:154 - host 4000:9::1 is up - 52.7 ms
12:34:28:284 - host 4000:9::1 is up - 22.8 ms

APENDICE C – RESUMO DOS ARQUIVOS TESTES DO GLBP IPV4

Teste 1

13:58:35:225 - host 10.0.9.1 is up - 54.5 ms
13:58:35:386 - host 10.0.9.1 is up - 53.1 ms
13:58:35:614 - host 10.0.9.1 is down
13:58:35:739 - host 10.0.9.1 is down
:
13:58:43:868 - host 10.0.9.1 is down
13:58:43:993 - host 10.0.9.1 is down
13:58:44:097 - host 10.0.9.1 is up - 98.3 ms
13:58:44:258 - host 10.0.9.1 is up - 53.9 ms

Teste 2

13:24:25:968 - host 10.0.9.1 is up - 78.2 ms
13:24:26:152 - host 10.0.9.1 is up - 68.2 ms
13:24:26:386 - host 10.0.9.1 is down
13:24:26:516 - host 10.0.9.1 is down
:
13:24:35:100 - host 10.0.9.1 is down
13:24:35:230 - host 10.0.9.1 is down
13:24:35:325 - host 10.0.9.1 is up - 85.6 ms
13:24:35:509 - host 10.0.9.1 is up - 67.9 ms

Teste 3

13:52:03:870 - host 10.0.9.1 is up - 54.1 ms
13:52:04:030 - host 10.0.9.1 is up - 53.5 ms
13:52:04:258 - host 10.0.9.1 is down
13:52:04:384 - host 10.0.9.1 is down
:
13:52:12:902 - host 10.0.9.1 is down
13:52:13:027 - host 10.0.9.1 is down
13:52:13:086 - host 10.0.9.1 is up - 54.5 ms
13:52:13:247 - host 10.0.9.1 is up - 54.1 ms

Teste 4

13:52:36:482 - host 10.0.9.1 is up - 54.2 ms
13:52:36:643 - host 10.0.9.1 is up - 54.0 ms
13:52:36:871 - host 10.0.9.1 is down
13:52:36:995 - host 10.0.9.1 is down
:
13:52:47:630 - host 10.0.9.1 is down
13:52:47:755 - host 10.0.9.1 is down
13:52:47:806 - host 10.0.9.1 is up - 47.0 ms
13:52:47:956 - host 10.0.9.1 is up - 43.1 ms

Teste 5

13:53:06:335 - host 10.0.9.1 is up - 54.3 ms
13:53:06:495 - host 10.0.9.1 is up - 53.5 ms
13:53:06:723 - host 10.0.9.1 is down
13:53:06:849 - host 10.0.9.1 is down
:
13:53:14:720 - host 10.0.9.1 is down
13:53:14:844 - host 10.0.9.1 is down
13:53:14:894 - host 10.0.9.1 is up - 46.1 ms
13:53:15:056 - host 10.0.9.1 is up - 54.0 ms

Teste 6

13:53:53:727 - host 10.0.9.1 is up - 53.3 ms
13:53:53:888 - host 10.0.9.1 is up - 54.2 ms
13:53:54:115 - host 10.0.9.1 is down
13:53:54:241 - host 10.0.9.1 is down
:
13:54:02:618 - host 10.0.9.1 is down
13:54:02:743 - host 10.0.9.1 is down
13:54:02:803 - host 10.0.9.1 is up - 56.0 ms
13:54:02:964 - host 10.0.9.1 is up - 53.9 ms

Teste 7

13:59:33:909 - host 10.0.9.1 is up - 43.3 ms
13:59:34:070 - host 10.0.9.1 is up - 53.7 ms
13:59:34:298 - host 10.0.9.1 is down
13:59:34:423 - host 10.0.9.1 is down
:
13:59:44:182 - host 10.0.9.1 is down
13:59:44:307 - host 10.0.9.1 is down
13:59:44:404 - host 10.0.9.1 is up - 92.9 ms
13:59:44:554 - host 10.0.9.1 is up - 43.5 ms

Teste 8

14:00:45:021 - host 10.0.9.1 is up - 77.1 ms
14:00:45:181 - host 10.0.9.1 is up - 51.7 ms
14:00:45:409 - host 10.0.9.1 is down
14:00:45:534 - host 10.0.9.1 is down
:
14:00:54:540 - host 10.0.9.1 is down
14:00:54:664 - host 10.0.9.1 is down
14:00:54:720 - host 10.0.9.1 is up - 51.8 ms
14:00:54:859 - host 10.0.9.1 is up - 32.6 ms

Teste 9

14:01:33:444 - host 10.0.9.1 is up - 54.1 ms
14:01:33:606 - host 10.0.9.1 is up - 53.7 ms
14:01:33:832 - host 10.0.9.1 is down
14:01:33:962 - host 10.0.9.1 is down
:
14:01:43:214 - host 10.0.9.1 is down
14:01:43:338 - host 10.0.9.1 is down
14:01:43:446 - host 10.0.9.1 is up - 103 ms
14:01:43:607 - host 10.0.9.1 is up - 54.2 ms

Teste 10

14:03:25:026 - host 10.0.9.1 is up - 54.2 ms
14:03:25:178 - host 10.0.9.1 is up - 44.4 ms
14:03:25:406 - host 10.0.9.1 is down
14:03:25:531 - host 10.0.9.1 is down
:
14:03:33:551 - host 10.0.9.1 is down
14:03:33:675 - host 10.0.9.1 is down
14:03:33:726 - host 10.0.9.1 is up - 46.6 ms
14:03:33:877 - host 10.0.9.1 is up - 43.5 ms

APENDICE D – RESUMO DOS ARQUIVOS TESTES DO GLBP IPV6

Teste 1

20:14:59:649 - host 4000:9::1 is up - 19.8 ms
20:14:59:771 - host 4000:9::1 is up - 15.1 ms
20:14:59:999 - host 4000:9::1 is down
20:15:00:131 - host 4000:9::1 is down
:
20:15:07:496 - host 4000:9::1 is down
20:15:07:620 - host 4000:9::1 is down
20:15:07:715 - host 4000:9::1 is up - 90.5 ms
20:15:07:854 - host 4000:9::1 is up - 34.2 ms

Teste 2

20:16:45:736 - host 4000:9::1 is up - 21.1 ms
20:16:45:867 - host 4000:9::1 is up - 24.4 ms
20:16:46:090 - host 4000:9::1 is down
20:16:46:214 - host 4000:9::1 is down
:
20:16:54:078 - host 4000:9::1 is down
20:16:54:208 - host 4000:9::1 is down
20:16:54:274 - host 4000:9::1 is up - 61.3 ms
20:16:54:403 - host 4000:9::1 is up - 22.9 ms

Teste 3

20:18:21:875 - host 4000:9::1 is up - 15.7 ms
20:18:22:001 - host 4000:9::1 is up - 18.7 ms
20:18:22:226 - host 4000:9::1 is down
20:18:22:351 - host 4000:9::1 is down
:
20:18:31:845 - host 4000:9::1 is down
20:18:31:970 - host 4000:9::1 is down
20:18:32:055 - host 4000:9::1 is up - 81.1 ms
20:18:32:173 - host 4000:9::1 is up - 12.2 ms

Teste 4

20:26:31:991 - host 4000:9::1 is up - 24.5 ms
20:26:32:114 - host 4000:9::1 is up - 17.2 ms
20:26:32:340 - host 4000:9::1 is down
20:26:32:464 - host 4000:9::1 is down
:
20:26:40:704 - host 4000:9::1 is down
20:26:40:829 - host 4000:9::1 is down
20:26:40:912 - host 4000:9::1 is up - 78.9 ms
20:26:41:031 - host 4000:9::1 is up - 12.8 ms

Teste 5

20:28:18:159 - host 4000:9::1 is up - 23.1 ms
20:28:18:277 - host 4000:9::1 is up - 11.8 ms
20:28:18:503 - host 4000:9::1 is down
20:28:18:628 - host 4000:9::1 is down
:
20:28:27:364 - host 4000:9::1 is down
20:28:27:489 - host 4000:9::1 is down
20:28:27:569 - host 4000:9::1 is up - 76.0 ms
20:28:27:698 - host 4000:9::1 is up - 22.0 ms

Teste 6

20:32:41:637 - host 4000:9::1 is up - 35.4 ms
20:32:41:776 - host 4000:9::1 is up - 31.8 ms
20:32:42:001 - host 4000:9::1 is down
20:32:42:126 - host 4000:9::1 is down
:
20:32:49:972 - host 4000:9::1 is down
20:32:50:096 - host 4000:9::1 is down
20:32:50:132 - host 4000:9::1 is up - 31.8 ms
20:32:50:261 - host 4000:9::1 is up - 23.7 ms

Teste 7

20:34:46:767 - host 4000:9::1 is up - 21.2 ms
20:34:46:898 - host 4000:9::1 is up - 23.1 ms
20:34:47:125 - host 4000:9::1 is down
20:34:47:250 - host 4000:9::1 is down
:
20:34:55:239 - host 4000:9::1 is down
20:34:55:364 - host 4000:9::1 is down
20:34:55:446 - host 4000:9::1 is up - 78.1 ms
20:34:55:586 - host 4000:9::1 is up - 33.0 ms

Teste 8

20:38:52:189 - host 4000:9::1 is up - 14.1 ms
20:38:52:326 - host 4000:9::1 is up - 29.7 ms
20:38:52:555 - host 4000:9::1 is down
20:38:52:679 - host 4000:9::1 is down
:
20:39:00:017 - host 4000:9::1 is down
20:39:00:143 - host 4000:9::1 is down
20:39:00:187 - host 4000:9::1 is up - 40.2 ms
20:39:00:327 - host 4000:9::1 is up - 32.3 ms

Teste 9

20:41:17:399 - host 4000:9::1 is up - 26.9 ms
20:41:17:535 - host 4000:9::1 is up - 30.2 ms
20:41:17:762 - host 4000:9::1 is down
20:41:17:887 - host 4000:9::1 is down
:
20:41:25:999 - host 4000:9::1 is down
20:41:26:125 - host 4000:9::1 is down
20:41:26:160 - host 4000:9::1 is up - 31.2 ms
20:41:26:299 - host 4000:9::1 is up - 32.9 ms

Teste 10

20:49:42:332 - host 4000:9::1 is up - 11.7 ms
20:49:42:461 - host 4000:9::1 is up - 21.4 ms
20:49:42:689 - host 4000:9::1 is down
20:49:42:813 - host 4000:9::1 is down
:
20:49:52:082 - host 4000:9::1 is down
20:49:52:206 - host 4000:9::1 is down
20:49:52:236 - host 4000:9::1 is up - 25.7 ms
20:49:52:354 - host 4000:9::1 is up - 12.4 ms

APENDICE E – RESUMO DOS ARQUIVOS TESTES DO VRRP IPV4

Teste 1

12:51:24:246 - host 10.0.9.1 is up - 67.8 ms
12:51:24:440 - host 10.0.9.1 is up - 80.0 ms
12:51:24:677 - host 10.0.9.1 is down
12:51:24:813 - host 10.0.9.1 is down
:
12:51:27:411 - host 10.0.9.1 is down
12:51:27:541 - host 10.0.9.1 is down
12:51:27:634 - host 10.0.9.1 is up - 83.6 ms
12:51:27:829 - host 10.0.9.1 is up - 80.6 ms

Teste 2

12:51:47:949 - host 10.0.9.1 is up - 79.5 ms
12:51:48:142 - host 10.0.9.1 is up - 76.0 ms
12:51:48:376 - host 10.0.9.1 is down
12:51:48:506 - host 10.0.9.1 is down
:
12:51:50:984 - host 10.0.9.1 is down
12:51:51:116 - host 10.0.9.1 is down
12:51:51:207 - host 10.0.9.1 is up - 82.1 ms
12:51:51:402 - host 10.0.9.1 is up - 77.4 ms

Teste 3

12:53:23:236 - host 10.0.9.1 is up - 91.6 ms
12:53:23:450 - host 10.0.9.1 is up - 99.7 ms
12:53:23:684 - host 10.0.9.1 is down
12:53:23:814 - host 10.0.9.1 is down
:
12:53:26:831 - host 10.0.9.1 is down
12:53:26:962 - host 10.0.9.1 is down
12:53:27:053 - host 10.0.9.1 is up - 80.8 ms
12:53:27:236 - host 10.0.9.1 is up - 68.9 ms

Teste 4

12:53:45:282 - host 10.0.9.1 is up - 68.0 ms
12:53:45:497 - host 10.0.9.1 is up - 99.6 ms
12:53:45:730 - host 10.0.9.1 is down
12:53:45:862 - host 10.0.9.1 is down
:
12:53:48:887 - host 10.0.9.1 is down
12:53:49:016 - host 10.0.9.1 is down
12:53:49:099 - host 10.0.9.1 is up - 72.9 ms
12:53:49:271 - host 10.0.9.1 is up - 58.2 ms

Teste 5

12:54:07:284 - host 10.0.9.1 is up - 68.2 ms
12:54:07:478 - host 10.0.9.1 is up - 80.8 ms
12:54:07:717 - host 10.0.9.1 is down
12:54:07:846 - host 10.0.9.1 is down
:
12:54:10:573 - host 10.0.9.1 is down
12:54:10:702 - host 10.0.9.1 is down
12:54:10:789 - host 10.0.9.1 is up - 78.0 ms
12:54:10:983 - host 10.0.9.1 is up - 81.2 ms

Teste 6

12:54:34:212 - host 10.0.9.1 is up - 100 ms
12:54:34:419 - host 10.0.9.1 is up - 90.6 ms
12:54:34:654 - host 10.0.9.1 is down
12:54:34:787 - host 10.0.9.1 is down
:
12:54:37:642 - host 10.0.9.1 is down
12:54:37:778 - host 10.0.9.1 is down
12:54:37:868 - host 10.0.9.1 is up - 81.2 ms
12:54:38:040 - host 10.0.9.1 is up - 58.5 ms

Teste 7

12:54:57:452 - host 10.0.9.1 is up - 89.7 ms
12:54:57:633 - host 10.0.9.1 is up - 68.4 ms
12:54:57:869 - host 10.0.9.1 is down
12:54:57:999 - host 10.0.9.1 is down
:
12:55:00:469 - host 10.0.9.1 is down
12:55:00:599 - host 10.0.9.1 is down
12:55:00:698 - host 10.0.9.1 is up - 89.5 ms
12:55:00:882 - host 10.0.9.1 is up - 69.8 ms

Teste 8

12:55:21:766 - host 10.0.9.1 is up - 99.7 ms
12:55:21:963 - host 10.0.9.1 is up - 78.9 ms
12:55:22:199 - host 10.0.9.1 is down
12:55:22:327 - host 10.0.9.1 is down
:
12:55:25:192 - host 10.0.9.1 is down
12:55:25:322 - host 10.0.9.1 is down
12:55:25:411 - host 10.0.9.1 is up - 79.1 ms
12:55:25:605 - host 10.0.9.1 is up - 80.3 ms

Teste 9

12:55:45:910 - host 10.0.9.1 is up - 58.6 ms
12:55:46:125 - host 10.0.9.1 is up - 101 ms
12:55:46:362 - host 10.0.9.1 is down
12:55:46:492 - host 10.0.9.1 is down
:
12:55:49:729 - host 10.0.9.1 is down
12:55:49:859 - host 10.0.9.1 is down
12:55:49:943 - host 10.0.9.1 is up - 74.4 ms
12:55:50:125 - host 10.0.9.1 is up - 69.3 ms

Teste 10

12:56:10:493 - host 10.0.9.1 is up - 67.9 ms
12:56:10:698 - host 10.0.9.1 is up - 89.3 ms
12:56:10:934 - host 10.0.9.1 is down
12:56:11:064 - host 10.0.9.1 is down
:
12:56:13:670 - host 10.0.9.1 is down
12:56:13:800 - host 10.0.9.1 is down
12:56:13:888 - host 10.0.9.1 is up - 79.6 ms
12:56:14:072 - host 10.0.9.1 is up - 69.3 ms