UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE ESPECIALIZAÇÃO EM REDES E TELEINFORMÁTICA

MATEUS REGAZZO CAMPAGNOLO

ESTUDO E CRIAÇÃO DE MODO DE REDE BALANCEADA E REDUNDANTE UTILIZANDO OS PROTOCOLOS HSRP E BGP

MONOGRAFIA

CURITIBA
2015

MATEUS REGAZZO CAMPAGNOLO

ESTUDO E CRIAÇÃO DE MODO DE REDE BALANCEADA E REDUNDANTE UTILIZANDO OS PROTOCOLOS HSRP E BGP

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Redes e Teleinformática, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR

Orientador: Prof. D.Sc. Kleber Kendy Horikawa Nabas

CURITIBA

2015

RESUMO

CAMPAGNOLO, Mateus R. **Estudo e criação de modelo de rede balanceada e redundante utilizando os protocolos HSRP e BGP.** 2015. **NUMERO DE PAGINAS** 39f. Monografia (Especialização em Redes e Teleinformática). Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

A presente monografia aborda o estudo para a criação de um modelo de rede redundante, com balanceamento de carga, que possa vir a ser seguido em implementações onde faz-se necessário uma rede robusta, tolerante a falhas e que traga confiabilidade ao serviço. Em geral, não é possível atingir estes dois atributos com a utilização de apenas um protocolo de rede, portanto serão combinados neste experimento os protocolos BGP(Border Gateway Protocol), e HSRP(Hot Standby Router Protocol), para atingir o resultado desejado. O projeto inicializa-se com pesquisas sobre os recursos escolhidos, seguido de simulação utilizando o software GNS3, configuração dos equipamentos e analise dos resultados.

Palavras-chave: Redes. Redundância . Balanceamento de Carga. BGP. HSRP.

ABSTRACT

CAMPAGNOLO, Mateus R. **Study and creation of balanced and redundant network model using the HSRP and BGP protocols**. 2015. 39f. Monograph (Specialization in Networks and Teleinformática). Federal Technological University of Paraná. Curitiba, 2015.

This monograph deals with the study for the creation of a redundant network model, with load balancing, which may be followed in implementations where it is necessary a robust network, fault-tolerant and bring reliability to the service. In general, you can not achieve these two attributes with the use of only one network protocol, so will be combined in this experiment protocols BGP (Border Gateway Protocol), and HSRP (Hot Standby Router Protocol) to achieve the desired result. The project starts with research on the chosen features, followed by simulation using GNS3 software, equipment configuration and analysis of results.

Keywords: Networks. Redundancy. Load Balancing. BGP. HSRP

LISTA DE SIGLAS

ARP – Adress Resolution Protocol

AS – Autonomous System

BGP - Border Gateway Protocol

DHCP - Dynamic Host Configuration Protocol

EBGP – External Border Gateway Protocol

GHz – Giga Hertz

HSRP – Hot Satanby Router Protocol

IBGP – Internal Border Gateway Protocol

ICMP - Internet Control Message Protocol

IEEE - Institute of Electrical and Eletronics Engineers

IP – Internet Protocol

ISP - Internet Service Provider

LAN – Local Area Network

MAC - Media Access Control

Mbps - Megabits por Segundo

MHz – Mega Hertz

VLAN – Virtual Local Area Network

QoS – Quality of Service

RFC - Request for Comments

SNMP - Simple Network Management Protocol

TCP - Transmission Control Protocol

TCP/IP - Transmission Control Protocol over Internet Protocol

UDP – User Datagram Protocol

WAN - Wide Area Network

WLAN – Wireless Local Area Network

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Neste capítulo serão tratados os elementos introdutórios relacionados ao estudo e criação de um modelo de rede redundante e rebalanceada utilizando os protocolos BGP e HSRP .

1.1 TEMA

Com o avanço da tecnologia o mercado vem se tornando mais exigente quanto ao quesito disponibilidade, uma vez que muitas das empresas dependem em grande parte do acesso a suas aplicações e de serviços externos, prestados por terceiros, sendo a maior parte deles utilizados através da Internet. Com isso passam a surgir novas necessidade que garantam o total funcionamento da empresa e que tragam confiabilidade ao negocio, evitando transtornos e prejuízos, resultantes da perda de comunicação com as aplicações e demais serviços. Para atender tal demanda o ambiente de redes de computadores deve ser tolerante a falhas de conexão, lógicas e físicas, aos Provedores de Serviços (ISP) ou operadoras que fornecem o acesso de conexão à Internet, e para isso é preciso implementar redundância de enlaces físicos, de forma a possuir mais de um meio acesso com a Internet.

Com a redundância de enlace físico, pode-se aplicar técnicas de duplicação de gateway, através de protocolos como o HSRP (Hot Standby Router Protocol), garantindo redundância no primeiro salto, dentro de sua rede interna . Aplicando esta técnica abre se a possibilidade de utilizar dois ou mais links com um ou mais provedores, dependendo do numero de enlaces criados e do numero de provedores, sendo possível por meio de protocolos como BGP e OSPF, criar um ambiente com balanceamento de carga e redundância na cama de rede.

1.2 OBJETIVOS

Nesta sessão serão trabalhados objetivo geral e objetivos específicos.

1.2.1 Objetivo Geral

Criar um modelo de redes onde são aplicadas técnicas de balanceamento de carga e redundância, utilizando os protocolos HSRP e BGP.

1.2.2 Objetivos Específicos

- Mostrar um modelo de rede que atenda as necessidades de alta disponibilidade em redes;
- Aplicar as uma das técnicas em um ambiente de redes simulado*;*
- Comparar o modelo apresentado de redes com um modelo comumente visto onde não são aplicadas técnicas de redundância e balanceamento;

1.3 JUSTIFICATIVA

Muitas empresas de pequeno e médio porte dependem de um ou vários serviços, muitas vezes cruciais, utilizados por meio do acesso a Internet, disponibilizada por um provedor. Estas empresas normalmente possuem apenas um link com a Internet e por esta razão estão sempre a merce dos problemas de rede variados, que vão desde um rompimento de fibra até uma falha no roteamento do provedor, impossibilitando assim o acesso a Internet e consequentemente aos serviços e aplicações. Neste casos as

empresas necessitam recorrer ao provedor para resolução dos prolemas, porém sabemos que estes problemas muitas vezes demoram a ser resolvidos, podendo trazer prejuízo e outros tipos de complicações. Estes problemas podem ser evitados ou contornados através da implementação de um ambiente de rede que utiliza técnicas de redundância e de balanceamento, que suporte um determinado numero de falhas internas e externas e permita a tomada de ações para contornar problemas de rota entre provedores.

1.4 PROCEDIMENTOS METODOLÓGICOS

Tomando como base a linha de raciocínio de Gil (2002) sobre a classificação das pesquisas, levando em consideração os objetivos de cada uma, esta monografia seguirá os procedimentos técnicos de pesquisa bibliográfica e estudo de campo em ambiente simulado. Pesquisa bibliográfica, pois é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos. A principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de um gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente (GIL, Antônio Carlos, 2002, p. 44-45). Já o estudo de campo é definido, pois procura muito mais o aprofundamento das questões propostas do que a distribuição das características da população segundo determinadas variáveis. Como consequência, o planejamento do estudo de campo apresenta muito maior flexibilidade, podendo ocorrer mesmo que seus objetivos sejam reformulados ao longo da pesquisa. Outra distinção é que no levantamento das informações procura-se identificar as características dos componentes do universo pesquisado, possibilitando a caracterização precisa de seus segmentos (GIL, Antônio Carlos, 2002, p. 53).

2 REFERENCIAIS TEÓRICOS

No presente capitulo serão apresentados conceitos básicos associados a tolerância a falhas e balanceamento de cargas em redes de computadores. Na sequência será apresentada uma solução tecnológica para a implementação de redundâncias e do balanceamento de cargas em nível de camada física/enlace e de camada de rede, com a utilização dos protocolos BGP e HSRP.

2.1 CONCEITOS ASSOCIADOS À TOLERÂNCIA A FALHAS E BALANCEAMENTO DE CARGA.

No ambiente de redes de computadores, sempre há a possibilidade de falhas no sistema estará, causando indisponibilidade dos recursos oferecidos que muitas vezes são de extrema importância para seus usuários. Neste sentido, a concepção de um sistema de alta disponibilidade envolve o uso de técnicas onde se aplicam a prevenção de falhas, a tolerância a falhas, a remoção de falhas e a predição de faltas (AVIZIENIS, 2004).

A tolerância a falhas diz respeito à propriedade de um sistema continuar operando, mesmo quando submetido à falhas de hardware e software. Esta propriedade pode ser obtida através de técnicas de redundância específicas.

2.1.1 Redundância

Define-se redundância como "capacidade de um sistema em superar a falha de um de seus componentes através do uso de recursos redundantes" (PINHEIRO, 2004). Para isso, um sistema depende de recursos alternativos, além do principal, e que estejam disponíveis para assumir o sistema assim que uma falha ocorrera.

Redundância é um termo comum e que pode-se aplicar em diversas áreas alem de redes de computadores, áreas estas que também possuem serviços que não podem

deixar de funcionar, como redes de fornecimento de energia.

2.1.2 Contingência

PINHEIRO (2004) define contingência como “possibilidade de um acontecimento futuro de uma condição existente, incerteza sobre as condições operacionais envolvidas e a resolução destas condições dependerem de eventos futuros”. Ou seja, a possibilidade de um fato ocorrer ou não, com uma situação de risco existente, com certo grau de probabilidade de acontecer.

Sendo assim, quando se projeta um sistema, deve-se definir em conjunto ações para contornar rapidamente o evitar o evento de falha, visando manter o sistema funcionando. Para isso, faz-se necessário um estudo de cada um dos processos em particular, quais os riscos envolvidos em cada um deles, de como afetariam o sistema, quais seriam os mais impactantes, quais as áreas mais críticas, o que poderia paralisar o sistema, e o tempo de recuperação para cada fase, pois são questões que norteiam o plano de contingência. Medidas preventivas e planejadas que suportem, por exemplo, falhas de software, hardware, base de dados, energia, temperatura, perda do link de comunicação e de causas naturais, devem estar incluídas no plano de contingenciamento, ou seja, ações imediatas, para serem executadas, visando o restabelecimento dos serviços, mesmo que parcialmente, diminuindo o tempo de paralisação caso ocorra uma falha.

O plano de contingência deve ter alta disponibilidade de informações de monitoramento. Ser implantado de um modo seguro e eficiente, que possa gerenciar/solucionar os problemas ocorridos, e se possível, ser pró-ativo e disponibilizem a solução da falha independentemente de ações externas, minimizando os impactos, e apenas mantendo relatório dos fatos ocorridos (PORTO 2015).

2.1.3 Disponibilidade

Disponibilidade é definida pelo tempo em que um sistema de rede deve estar disponível para seus usuários (PINHEIRO, 2004). Ela pode ser mensurada em relação ao tempo em que o sistema está em falha (downtime), com o tempo que deve estar disponível. Dependendo do plano de contingência criado para suprir falhas que possam inviabilizar o acesso ao sistema, o tempo disponível pode variar em horas, dias, meses ou até anos.

A figura 1 representa uma tabela do tempo de falha de um sistema, em relação a um ano de operação da uma rede. Uma pequena variação na porcentagem pode considerar uma

grande diferença de tempo. Por isso, é importante estimar a disponibilidade mínima da rede, a fim de montar seu plano de contingência (PORTO 2015).

Segundo PINHEIRO (2004), a disponibilidade pode ser enquadrada em três classes, Disponibilidade Básica, Alta Disponibilidade e Disponibilidade Contínua.

Availability	Downtime per Year (24x7x365)		
99.000%	3 Days	15 Hours	36 Minutes
99.500%	1 Day	19 Hours	48 Minutes
99.900%		8 Hours	46 Minutes
99.950%		4 Hours	23 Minutes
99.990%			53 Minutes
99.999%			5 Minutes
99.9999%			30 Seconds

Figura 1: Exemplo de Disponibilidade

Fonte: PORTO, HELTON LUIZ. Redundância e Balanceamento de Carga em Rede Corporativa.

2.1.4 Balanceamento de Carga

Por ser um dos pontos mais críticos e vulneráveis a falha, a multiplicação de links wan é muito comum em planos de contingência. Dependendo do projeto e a disponibilidade dos recursos dos equipamentos utilizados, o balanceamento de carga entre os links pode ser implementado. Com o balanceamento de carga, pode-se aproveitar os recursos do sistema redundante, ao invés de ficarem ociosos até que ocorra uma falha.

A função de balanceamento entre os links wan é distribuir o tráfego de dados entre eles. Dependendo de sua aplicação, o balanceamento aumenta o desempenho da rede somando a banda dos links, aumentando a capacidade do sistema podendo inclusive prover redundância entre os links. O balanceamento pode ser relativo ao tráfego que entra na rede e ao tráfego que sai, ela pode ser em nível de pacotes, fluxos, destinos, e entre outras possibilidades (PORTO 2015).

2.2 PROTOCOLO HSRP (*Hot Standby Router Protocol*)

HSRP (Hot Standby Router Protocol) é um protocolo de rede proprietário definido pela RFC 2281 desenvolvido pela Cisco. Aplicado em um domínio de rede, em dois ou mais roteadores, cada roteador terá seu ip fixo da rede e também o ip gateway padrão do domínio, comum em todos os roteadores, e chamado de ip virtual. Desta forma, o gateway dos dispositivos finais da rede não precisa ser alterado. Os roteadores trocam mensagens hello a cada 3 segundos através do endereço multicast 224.0.0.2, usando a porta UDP 1985. Para definir o gateway ativo (link principal) ou stand-by (link back-up) no domínio, são definidos prioridades nos roteadores. O roteador que tiver maior prioridade é eleito como ativo. O valor padrão da prioridade é 100, e se não definido, o roteador que

tiver o maior valor ip é eleito ativo, mas geralmente se define a prioridade estaticamente por escolha do administrador da rede.

O HSRP é configurado nos roteadores para que se houver uma falha em alguma regra estabelecida no roteador, como queda de interface ou falta de conectividade no próximo hop (WAN), decrementa-se o valor de sua prioridade, a fim do roteador vizinho se tornar ativo. Caso normalize as regras, o roteador dado como link principal, volta a sua prioridade inicial e seu estado como ativo (PORTO 2015).

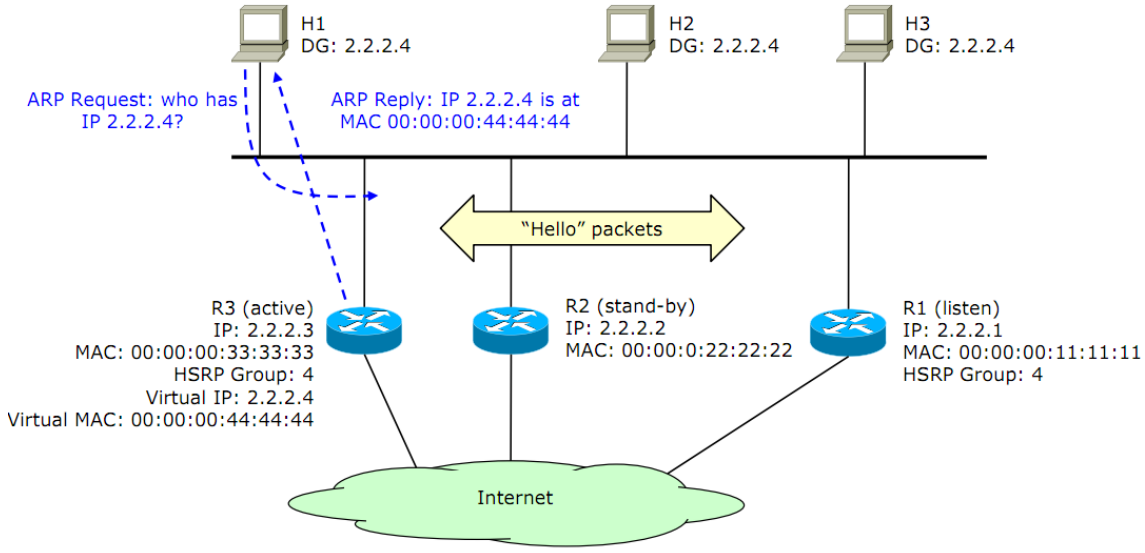

Figura 2: Exemplo de Funcionamento do HSRP

Fonte: RISSO, FULVIO. Redundancy and load balancing at L3 in Local Area Networks Politecnico di Torino

A Figura 2 ilustra o funcionamento do HSRP. Note-se que os hospedeiros estão configurados para um gateway default 2.2.2.4. Este endereço é virtual. O roteador R3, integrante de um grupo de roteadores HSRP e na condição de roteador ativo, responde por requisições ARP. O endereço de MAC fornecido é virtual (00:00:00:44:44:44). Em caso de falha de R3, o roteador R2, até então em stand-by , assume a condição de ativo e o roteador R1 passa a ser stand-by. R2 passa então a responder pelo IP virtual e pelo

MAC virtual.

As seguintes considerações ainda podem ser realizadas sobre o HSRP:

- Cada VLAN é uma LAN separada e portanto utiliza-se cada uma de um gateway default. Neste caso são requeridos múltiplos grupos HSRP;
- Apenas o roteador ativo se utiliza do MAC virtual nos pacotes de HELLO. Desta forma, quando muda de roteador ativo, se existirem switches no caminho, eles aprenderão onde está o novo roteador. Neste sentido, o novo roteador ativo também emite um ARP reply em broadcast;

- Apenas o enlace ligado de saída do roteador ativo é usado. Os enlaces dos demais roteadores ficam desperdiçados. Para tráfego que entra, todos os links podem ser utilizados, permitindo desta forma assimetria no tráfego. Note-se que o HSRP não influencia neste processo, cabendo se for o caso, a um protocolo de roteamento tal como o BGP.

Finalmente, é importante ressaltar que o HSRP não possui mecanismos para balanceamento de tráfego que sai. É possível, no entanto, criar grupos HSRP diferentes, cada um com um gateway ativo definido, de forma que hospedeiros com IP virtual de um grupo encaminham por um gateway enquanto outros hospedeiros encaminham por outro gateway default (PORTO 2015).

2.3 PROTOCOLO BGP (*Border Gateway Protocol*)

O BGP (Border Gateway Protocol) é um protocolo de roteamento dinâmico utilizado por operadoras para interconexão entre sistemas autônomos (Autonomous Systems - AS). Porém, ele é comumente utilizado em redes privadas para transportes de tabela de

roteamento e por seus vários recursos. Em cada enlace há uma sessão bgp ativa com o roteador vizinho (next-hop), enviando e recebendo as tabelas de roteamento dinamicamente.

O BGP é um protocolo utilizado para a troca de informações de roteamento entre sistemas autônomos da Internet. Atualmente é o único protocolo utilizado para este fim. A última versão do BGP é conhecida como BGP4 (RFC4271).

A troca de informações é realizada pelos roteadores de borda dos sistemas autônomos através de sessões TCP (porta 179). Uma nuvem BGP pode ser vista como um conjunto de super nós interligados por links virtuais. O protocolo BGP se aproxima da abordagem por vetor de distâncias. No entanto, ele fornece um caminho completo de sistemas autônomos (AS's) que compõe o caminho para uma determinada rede de destino informada. A métrica usada é o hop em nível de AS.

Roteadores que falam BGP (BGP speakers) podem estar conectados entre dois AS's diferentes (EBGP ou external BGP) ou podem conversar internamente a um AS (IBGP ou Internal BGP).

2.3.1 Atributos do BGP

O uso de alguns atributos das mensagens do BGP, combinados com o seu algoritmo de seleção de rotas, é um instrumento valioso de controle no uso de enlaces e na aplicação de políticas de uso da rede. Pode-se destacar os seguintes atributos:

Atributo AS-PATH: Quando o anúncio de uma rota é publicado por um sistema autônomo, o número de AS deste sistema é adicionado à lista de números AS que o anúncio possui. O AS-PATH será utilizado para escolha dos caminhos, isto é, se um AS recebe anúncios da mesma rede através de diferentes AS vizinhos, então ele pode escolher (dentre outros critérios) o anúncio com menor AS-PATH. É um comportamento

similar ao algoritmo de vetor de distância.

Um AS-PATH também pode ser usado para dar preferência a entrada de tráfego por um determinado caminho do AS. O AS insere múltiplas cópias de seu AS-ID no ASPATH para “enganar” o AS a ele conectado. Abaixo, a figura 4 ilustra o uso de pre-pending no AS-PATH.

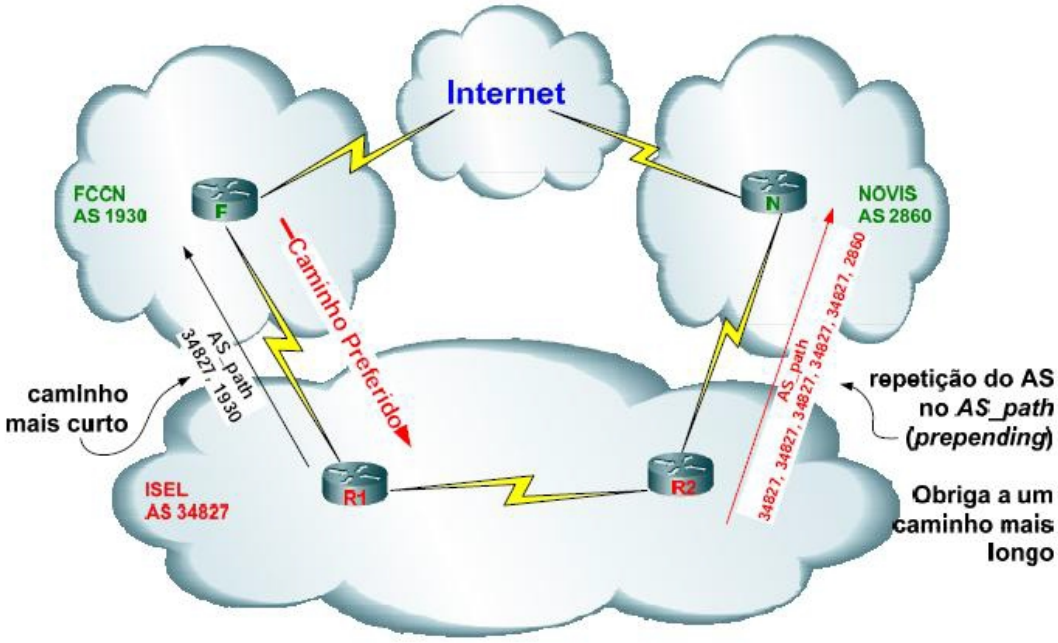

Figura 3: Uso de Pre-Pending no AS-PATH

Fonte:PORTO, HELTON LUIZ. Redundância e Balanceamento de Carga em Rede Corporativa.

Atributo Local Preference: Este atributo é utilizado para dar preferência a um caminho de saída do sistema autônomo. Ele é propagado dentro do mesmo AS ilustrado na figura 4.

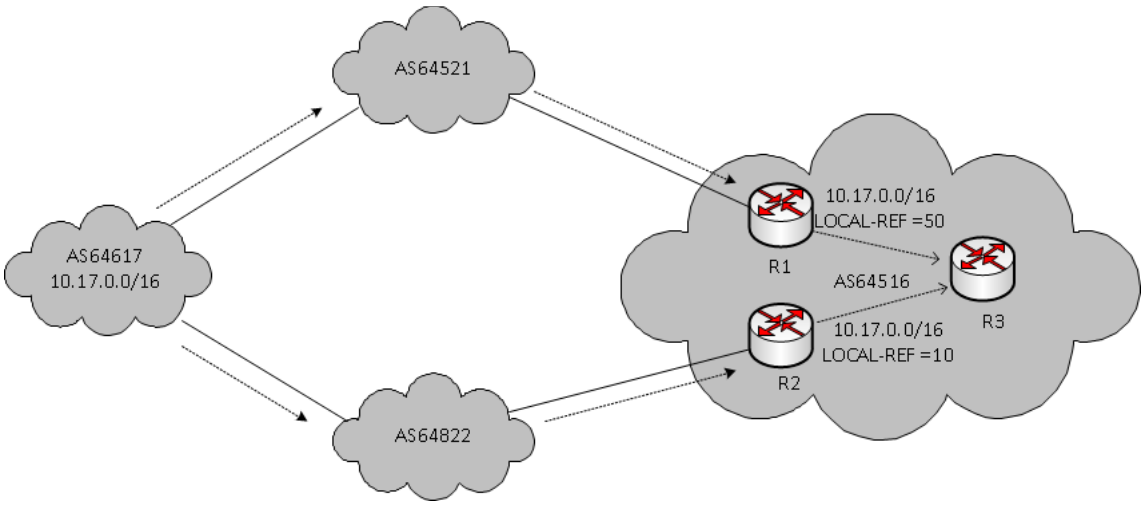

Figura 4: Uso do Atributo Local-Preference

Fonte:PORTO, HELTON LUIZ. Redundância e Balanceamento de Carga em Rede Corporativa.

Atributo MED: este atributo é enviado como sugestão a um AS externo para dar preferência a um dos caminhos entre dois sistemas autônomos. Trata-se somente de uma sugestão porque é o AS externo que decide levando em consideração outros atributos. A figura 5 ilustra o uso do parâmetro MED.

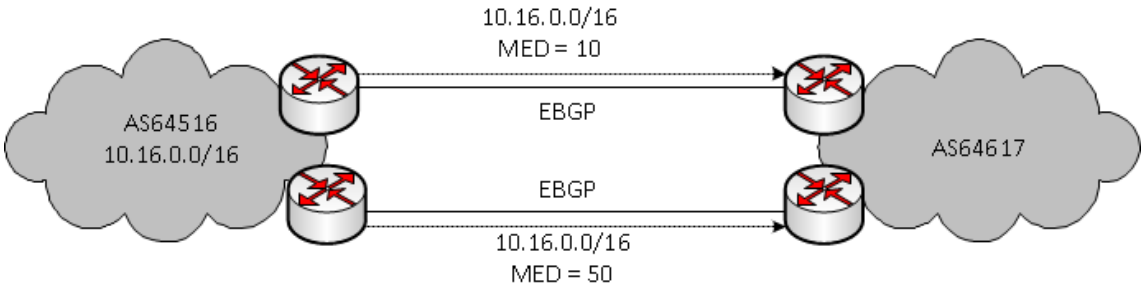

Figura 5: Uso do Parâmetro MED

Fonte:PORTO, HELTON LUIZ. Redundância e Balanceamento de Carga em Rede Corporativa.

Atributo peso: Se um router aprende mais do que uma rota para o mesmo destino, a rota com o maior peso é utilizada como mostra a figura 6. É um atributo proprietário da Cisco. Este atributo não é anunciado a outros roteadores.

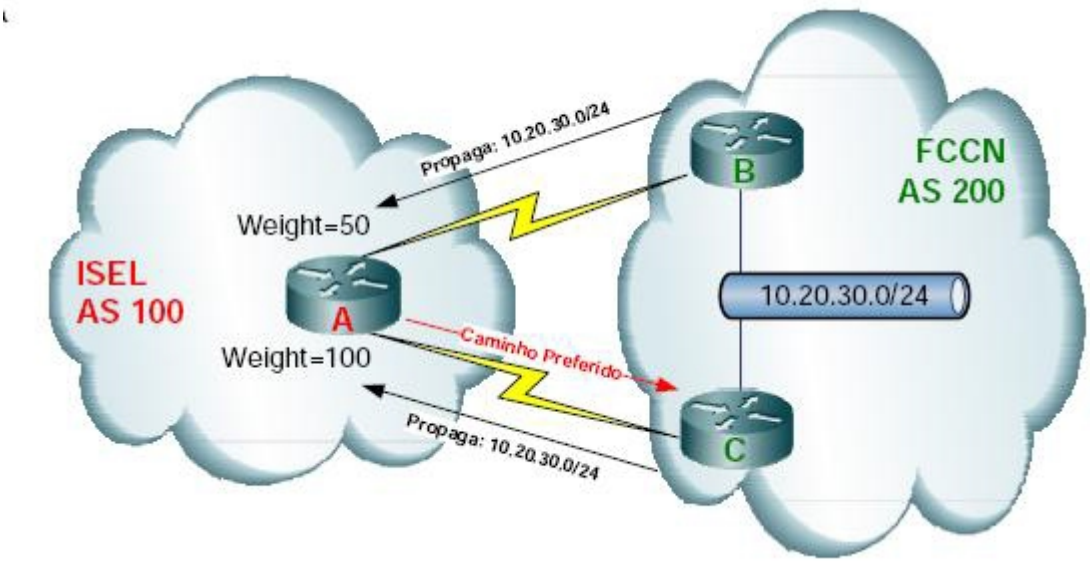

Figura 6: Uso do Parâmetro Peso

Fonte:PORTO, HELTON LUIZ. Redundância e Balanceamento de Carga em Rede Corporativa.

2.3.2 Políticas de Uso

No BGP são criadas regras para que as tabelas de roteamento fiquem duplicadas para cada enlace ou sessão BGP. Se não for aplicada nenhuma métrica ou custo na tabela, o tráfego pode ser balanceado entre os links, tanto por destino, quanto por pacotes. Além do balanceamento, o BGP permite administrar o tráfego de entrada e saída, possibilitando o tráfego sair por um link e entrar por outro, aplicando regras com custos, métricas, AS path prepending, local-prefence, mapeamento de rotas, tal como colocado anteriormente.

O BGP fornece também uma série de filtros que podem ser aplicados às redes para um determinado AS. Por exemplo, existem filtros por prefixo que permitem determinar que um grupo de prefixos de rede somente podem ser recebidos por determinados AS's. Existem também filtros aplicáveis conforme o atributo AS-PATH, permitindo selecionar caminhos que priorizem a passagem por determinados ASs.

São estas características que fazem do BGP um protocolo universalmente aceito

para troca de informações de roteamento entre sistemas e que possibilitam até mesmo a sua aplicação em redes nas bordas do sistema(PORTO 2015).

2.4 Integração de Balanceamento de Carga nas estruturas de acesso

A integração de balanceamento entre links alternativos de acesso é muito explorado por operadoras e clientes, pois se permite um melhor aproveitamento dos recursos oferecidos. Um link ocioso, apenas aguardando um evento de falha ocorrer para enfim ser utilizado, pode ser considerado um desperdício de utilização de banda. O balanceamento entre os links pode melhorar muito o desempenho de um sistema, já que nesta estrutura se soma a banda dos circuitos(PORTO 2015).

2.4.1 Utilização integrada de protocolos de multiplicação de gateway com BGP

Geralmente, os protocolos de multiplicação de gateway são configurados para que se utilize o estado das interfaces wan de camada 2 para leitura do evento da falha, decrementando sua prioridade, e enfim enviar as mensagens de status para os roteadores vizinhos assumirem o sistema. Um grande problema, pois nem sempre a falha pode estar ligada ao um problema de físico no acesso ou na camada 2, pois a conectividade pode ser perdida sem que o protocolo caia, por exemplo. A utilização do BGP pode ser aplicada na leitura da falha pelos protocolos através do status da sessão BGP, pois se não há conectividade com o próximo hop, a sessão BGP cai (down), ou seja, a parametrização da falha estará sendo feita acima na camada 3 de rede, utilizando os recursos de “trackinkg”. O track é um recurso dos roteadores para rastreamento de um objeto ou evento, que permite o acompanhamento de determinados objetos específicos, tomando medidas quando o estado do objeto rastreado sofrer alteração, tais como queda da interface wan, perda de comunicação em um determinado destino, entre outros.

Operadoras utilizam deste sistema para uma melhor performance nos serviços de redundância(PORTO 2015).

3 ESTUDO DE CASO E CRIAÇÃO DO MODELO EM AMBIENTE SIMULADO

Este capítulo apresentará a integração dos protocolos HSRP e BGP visando a criação de um modelo de redes que garanta a mais alta disponibilidade pra o ambiente de redes.

Será demostrado o ambiente que é comumente encontrado e largamente utilizado pelas empresas, para posteriormente demostrar o ambiente pretendido e sua configuração.

O experimento e a criação do modelo serão feitos através do software GNS3, onde serão utilizados roteadores Cisco c3725 emulados, o qual foi escolhido por suportar ambos o protocolos utilizados.

3.1 CENÁRIO COMUM

O cenário comumente utilizado é um modelo rede onde há apenas um CPE na rede local, que possui um link wan ponto-a-ponto, fornecido por uma operadora para acessar uma rede remota externa e com acesso a internet, como demostrado na figura 7.

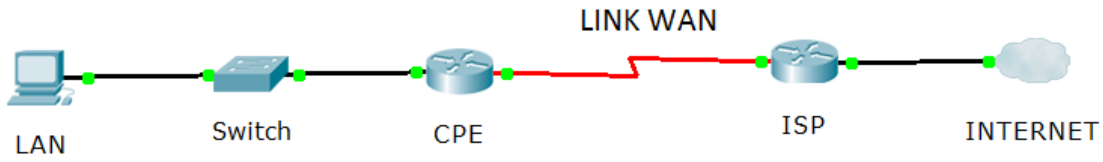

Figura 7: Cenário de rede comum

Fonte: Autoria Propriá

Como pode ser observado acima, o cenário não possui nenhum mecanismo de redundância, ficando todo o sistema depende da disponibilidade do único link, sendo este utilizado para acesso a aplicações externas, entre outras funções, dependendo do foco da empresa.

Este cenário não suporta nenhum tipo de falha física ou logica. Mesmo o link contratado funcionando, a empresa fica a merce de problemas de rota entre os ISPs, oque pode gerar muito transtorno e que há certa dificuldade na resolução destas questões.

3.2 CENÁRIO PRETENDIDO

O cenário pretendido visa garantir a maior disponibilidade possível, suportando até três diferentes falhas simultaneamente, garantindo que a rede continue funcionando mesmo com falhas em vários pontos. Para isso, foi implementado um segundo CPE na estrutura e mais três links WAN, sendo estes de duas operadoras diferentes com estruturas totalmente distintas, estando conectados um link de cada ISP a um roteador. Desta forma, cada roteador terá uma saída por cada operadora.

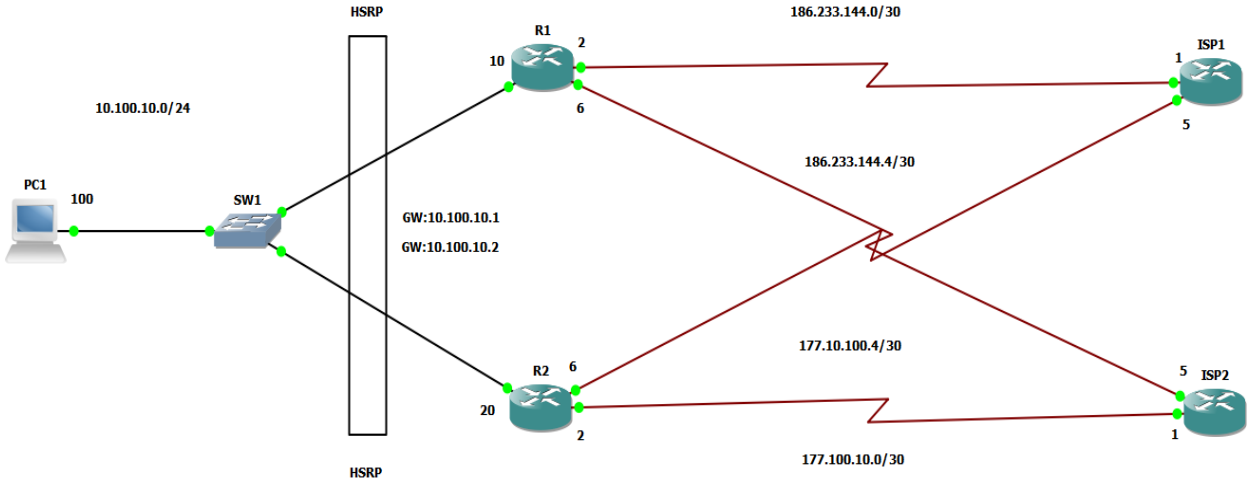

Figura 8: Topologia pretendida

Fonte: Autoria Própria.

Este cenário permitiu a utilização do protocolo HSRP como protocolo de redundância e divisão de carga entre os roteadores, sendo necessária a utilização de dois gateways para isso de forma a evitar que o balanceamento de garga fique inteiramente

por conta do GBP, estando listada a configuração do protocolo HSRP, utilizadas nos roteadores, na tabela 1.

Tabela 1: Configuração HSRP

R1	R2
interface FastEthernet0/0 ip address 10.100.10.10 255.255.255.0 no ip route-cache cef speed 100 full-duplex standby 10 ip 10.100.10.1 standby 10 preempt standby 20 preempt standby 20 ip 10.100.10.2 standby 20 priority 90	interface FastEthernet0/0 description LAN_R2 ip address 10.100.10.20 255.255.255.0 speed auto full-duplex standby 10 preempt standby 10 ip 10.100.10.1 standby 10 priority 90 standby 20 preempt standby 20 ip 10.100.10.2

O BGP foi o protocolo de camada 3 explorado no projeto para configuração do balanceamento, pois possui vários atributos para seleção de rotas (AS path prepending, local-prefence, route-map, rotas estáticas, etc), que ainda permitem a tomada de ações em casos de problemas de rota entre as operadoras.

Nas tabelas 2 , 3 ,4 e 5 estão as configurações aplicadas nos roteadores na rede da empresa e nos roteadores dos ISPs.

Tabela 2: Configuração BGP R1

R1
router bgp 100 bgp log-neighbor-changes neighbor 10.100.10.20 remote-as 100 neighbor 177.100.10.5 remote-as 300 neighbor 186.233.144.1 remote-as 200 maximum-paths 3 maximum-paths ibgp 3 address-family ipv4 redistribute connected redistribute static neighbor 10.100.10.20 activate neighbor 177.100.10.5 activate neighbor 186.233.144.1 activate maximum-paths 3 maximum-paths ibgp 3 no auto-summary no synchronization exit-address-family

Tabela 3: Configuração BGP R2

R2
router bgp 100 bgp log-neighbor-changes neighbor 10.100.10.10 remote-as 100 neighbor 177.100.10.1 remote-as 300 neighbor 186.233.144.5 remote-as 200 maximum-paths 3 address-family ipv4 redistribute connected redistribute static neighbor 10.100.10.10 activate neighbor 177.100.10.1 activate neighbor 177.100.10.1 route-map CORP in neighbor 186.233.144.5 activate neighbor 186.233.144.5 route-map CORP in maximum-paths 3 default-information originate no auto-summary no synchronization network 10.100.10.0 mask 255.255.255.0 exit-address-family

Tabela 4: Configuração BGP ISP1

ISP1
router bgp 200 bgp log-neighbor-changes neighbor 186.233.144.2 remote-as 100 neighbor 186.233.144.6 remote-as 100 maximum-paths 2 maximum-paths ibgp 2 address-family ipv4 redistribute connected redistribute static neighbor 186.233.144.2 activate neighbor 186.233.144.6 activate maximum-paths 2 maximum-paths ibgp 2 default-information originate no auto-summary no synchronization exit-address-family

Tabela 5: Configuração BGP ISP2

ISP2
router bgp 300 bgp log-neighbor-changes neighbor 177.100.10.2 remote-as 100 neighbor 177.100.10.6 remote-as 100 maximum-paths 2 maximum-paths ibgp 2 address-family ipv4 redistribute connected redistribute static neighbor 177.100.10.2 activate neighbor 177.100.10.6 activate maximum-paths 2 maximum-paths ibgp 2 default-information originate no auto-summary no synchronization exit-address-family

3.3 Simulação de falhas.

Após a configuração do ambiente, foram introduzidas falhas em pontos diferentes da rede, de forma a testar a eficacia do modelo no quesito disponibilidade, seguindo abaixo as representações ilustrativas dos testes realizados e do fluxo de dados após a inserção das falhas. Para realização dos teste, foi inserido mais um roteador após os ISPs, conectando ao mesmo um switch genérico e um terminal para onde foram destinados os pacotes ICMP, conforme a figura 9.

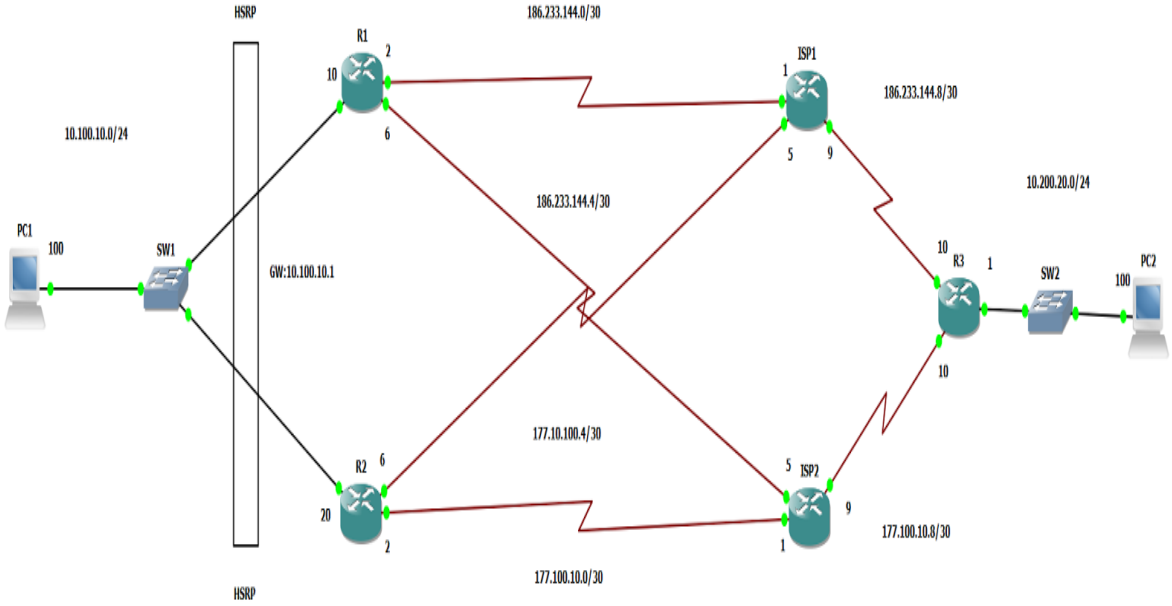

Figura 9: Topologia de teste

Fonte: autoria própria.

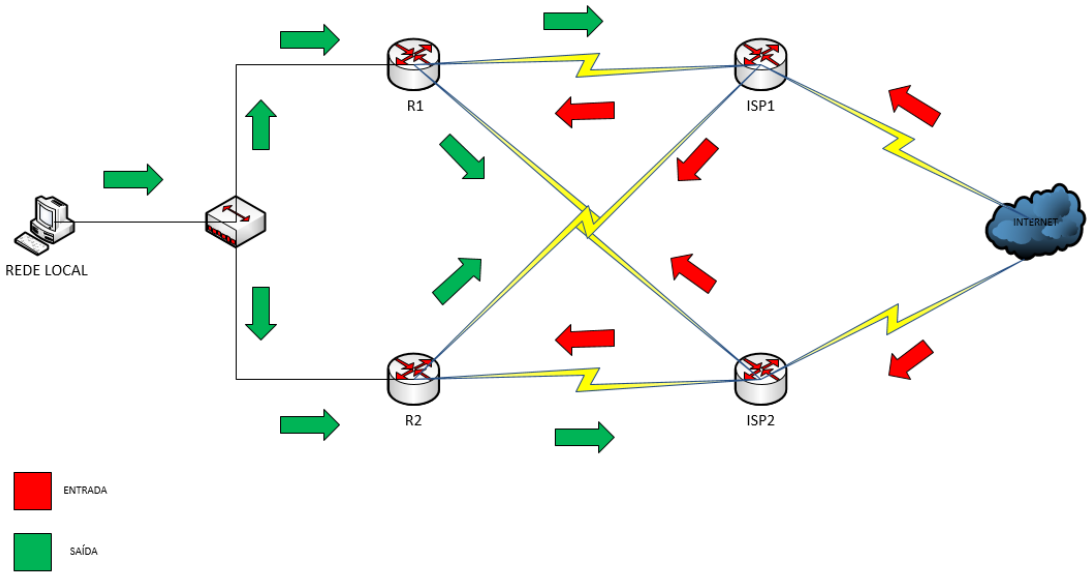

Figura10: Fluxo de dados

Fonte: autoria própria

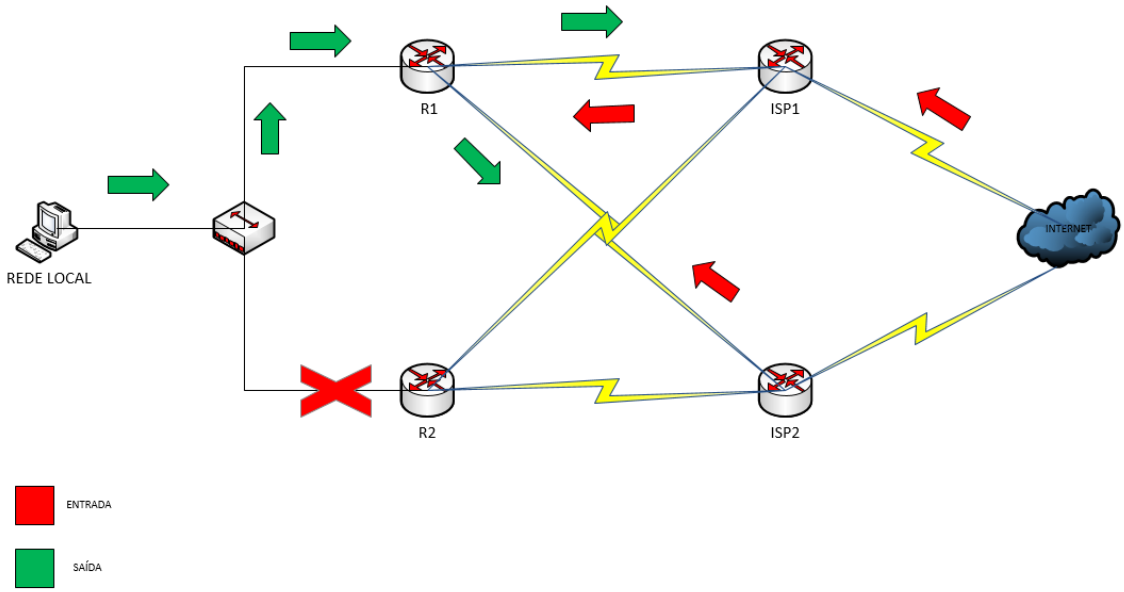

Figura 11: Falha em rede local

Fonte: autoria própria.

Tabela 6: Trace com falha local

TRACE COM FALHA LOCAL
traceroute to 10.200.20.100 (10.200.20.100), 30 hops max, 40 byte packets
1 10.100.10.10 (10.100.10.10) 10.315 ms 10.339 ms 10.351 ms
2 186.233.144.1 (186.233.144.1) 20.312 ms 21.204 ms 20.364 ms
3 186.233.144.10 (186.233.144.10) 22.556 ms 21.613 ms 22.618 ms
4 10.200.20.100 (10.200.20.100) 10.539 ms 11.498 ms 10.575 ms

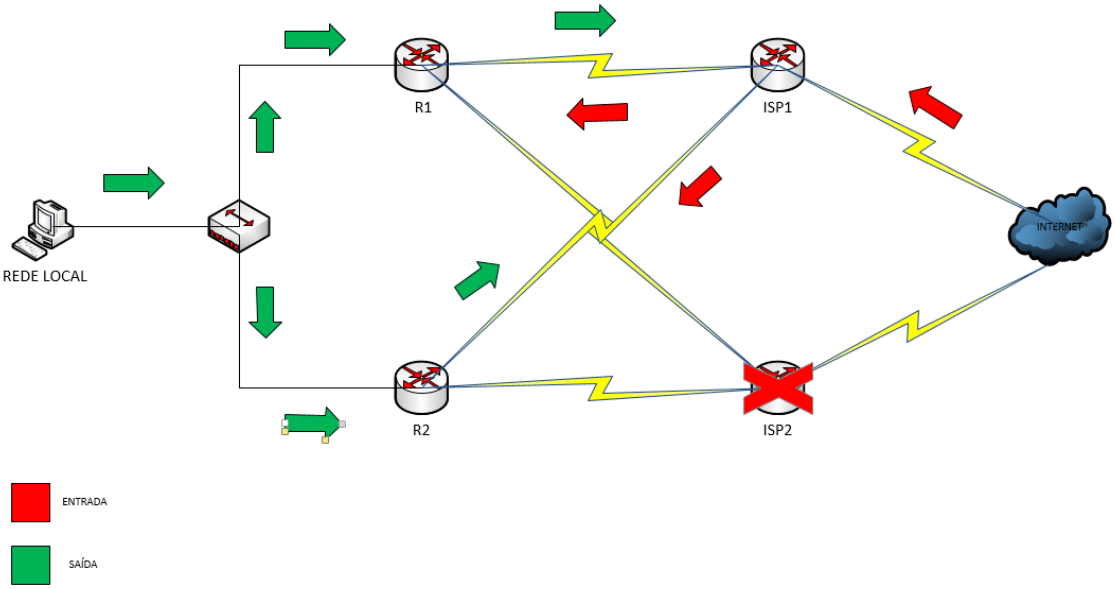

Figura 12: Falha ISP

Fonte: autoria própria.

Tabela 7: Trace com falha no ISP2

TRACE COM FALHA NO ISP2
traceroute to 10.200.20.100 (10.200.20.100), 30 hops max, 40 byte packets
1 10.100.10.20 (10.100.10.10) 10.127 ms 10.203 ms 10.224 ms
2 186.233.144.5 (186.233.144.1) 15.510 ms 16.504 ms 20.512 ms
3 186.233.144.10 (186.233.144.10) 25.261 ms 20.310 ms 23.287 ms
4 10.200.20.100 (10.200.20.100) 10.493 ms 10.492 ms 10.556 ms

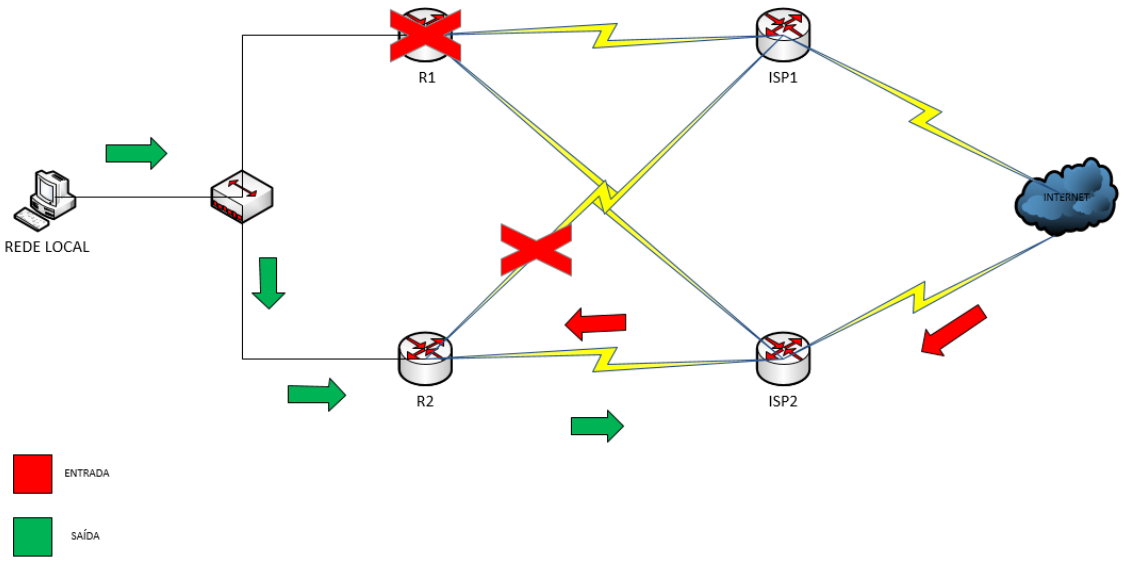

Figura 13: Falhas múltiplas

Fonte: autoria própria

Tabela 8: Trace com falhas múltiplas

TRACE COM FALHAS múltiplas
traceroute to 10.200.20.100 (10.200.20.100), 30 hops max, 40 byte packets
1 10.100.10.20 (10.100.10.10) 10.221 ms 11.542 ms 11.846 ms
2 177.100.10.1 (177.100.10.1) 30.051 ms 28.783 ms 30.106 ms
3 177.100.10.10 (186.233.144.10) 21.620 ms 21.470 ms 22.278 ms
4 10.200.20.100 (10.200.20.100) 11.003 ms 10.927 ms 10.428 ms

4 CONSIDERAÇÕES FINAIS

Com a crescente necessidade por manter o acesso as aplicações funcionando, as empresas passam a ter de investir mais em seu ambiente de redes visando o funcionamento de suas operações.

Atualmente, em sua grande maioria, as empresas possuem diversos recursos que dependem da disponibilidade de sua rede, como telefonia, aplicações remotas, transações bancarias, entre outras, oque torna primordial o funcionamento da rede em período integral e por esse motivo a implementação de um ambiente que atenda esta demanda é de suma importância.

A partir das referencias utilizadas para pesquisa vemos que há diversas soluções possíveis, podendo implementar diversos recursos diferente de maneiras diferentes.

O modelo criado garante o funcionamento do serviço uma vez que o mesmo suporta varias falhas simultâneas e proporciona certo gral de controle para falhas fora da estrutura da empresa, já que o mesmo utiliza-se de 4 links com duas operadoras distintas. A implementação deste modelo pode não ser viável para toda empresa, uma vez que manter 4 links dedicados pode ser dispendioso financeiramente e dependendo do foco e porte da empresa acaba não sendo interessante. Neste caso é necessário um estudo do caso especifico da situação para criação de um modelo que atenda as necessidades da empresa.

REFERÊNCIAS

Configuring HSRP . Disponivel em <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1_8_ea1/configuration/guide/3550scg/Swhsrp.html> Acessado em 26/03/2015

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa.** 4ª. ed. São Paulo: Atlas, 2002.

KRAEMER, VILAR, GOLDMAN. Tolerância a Falhas utilizando protocolos de Gateway Redundantes. Disponível em: <http://www.ime.usp.br/~gold/publications/pdf/erad2010.pdf>Acesso em 25/03/2015

PINHEIRO, JOSÉ MAURÍCIO DOS SANTOS. Conceitos de Redudância e Contingência.http://www.projetoderedes.com.br/artigos/artigo_conceitos_de_redundancia.php#.UTjFnxJYsuJ. Acessado em 25/03/2015.

PORTO, HELTON LUIZ. Redundância e Balanceamento de Carga em Rede Corporativa. Disponivel em: <http://wiki.sj.ifsc.edu.br/wiki/images/3/36/TCC_HeltonLuizPorto.pdf > Acessado em 25/03/2015.

RISSO, FULVIO. Redundancy and load balancing at L3 in Local Area Networks Politecnico di Torino .http://netgroup.polito.it/teaching/prlc/LAN%20-%20L3%20redundancy.pdf Acessado em 27/03/2015.