UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTOS ACADÊMICOS DE ELETRÔNICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

BENETH SANTANA TORQUATO
JEFFERSON DA CRUZ

SIMULAÇÃO E ANÁLISE DE REDUNDÂNCIA EM LANS

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2015

BENETH SANTANA TORQUATO
JEFFERSON DA CRUZ

SIMULAÇÃO E ANÁLISE DE REDUNDÂNCIA EM LANS

Trabalho de Conclusão de Curso de Graduação, apresentado ao Curso Superior de Tecnologia em Sistemas de Telecomunicações, do Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Prof. Dr. Augusto Foronda

CURITIBA
2015

TERMO DE APROVAÇÃO

BENETH SANTANA TORQUATO
JEFFERSON DA CRUZ

SIMULAÇÃO E ANÁLISE DE REDUNDÂNCIA EM LANS

Este trabalho de conclusão de curso foi apresentado no dia 3 de dezembro de 2015, como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Telecomunicações, outorgado pela Universidade Tecnológica Federal do Paraná. Os alunos foram arguidos pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Coordenador de Curso
Departamento Acadêmico de Eletrônica

_____
Prof. Esp. Sérgio Moribe
Responsável pela Atividade de Trabalho de Conclusão de Curso
Departamento Acadêmico de Eletrônica

BANCA EXAMINADORA

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
UTFPR

_____
Prof. Mestre Lincoln Herbert Teixeira
UTFPR

_____
Prof. Dr. Augusto Foronda
Orientador - UTFPR

“A Folha de Aprovação assinada encontra-se na Coordenação do Curso”

A nossos pais, pelo exemplo de vida e apoio.

AGRADECIMENTO(S)

À família, que nos deram suporte e apoio para não desistirmos do sonho de graduação.

Aos professores os quais nos ensinaram os caminhos para desenvolvermos a disciplina aplicada e também incentivando o estudo, para que possamos nos tornar profissionais ainda mais qualificados.

À nossos colegas de classe eu muito nos ajudaram a vencer as barreiras do conhecimento, do cansaço, do desânimo, trazendo um pouco de descontração em momentos em que estávamos nos sentindo derrotados, mas também seriedade no momento de cumprirmos as obrigações perante os professores.

RESUMO

TORQUATO, Beneth S.; DA CRUZ, Jefferson. **Simulação e Análise de Redundância em LANs**. 2015. NÚMERO_DE_FOLHAS (SEM CONTAR A CAPA) f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

Com o avanço da tecnologia e o grande crescimento das redes de telecomunicações, é fundamental que as redes sejam estáveis e confiáveis. O bom planejamento e configuração são elementos indispensáveis para que uma rede funcione de forma ininterrupta, evitando paralisação dos serviços utilizados e fornecidos através da mesma. Para que isto seja possível é dada a utilização de equipamentos redundantes configurados com protocolos específicos para este fim.

Palavras chave: Tecnologia. Redundância. Redes.

ABSTRACT

TORQUATO, Beneth S.; DA CRUZ, Jefferson. **Simulação e Análise de Redundância em LANs**. 2015. NÚMERO_DE_FOLHAS (SEM CONTAR A CAPA) f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

With the advancement of technology and the growth of telecommunications networks, its fundamental that the networks be stable and reliable. The planning and configuration are essential for a non-stopping network, avoiding it of stop working. The use of extra equipment's and protocols is necessary for a good network.

Keywords: Technology. Extra. Network.

LISTA DE ILUSTRAÇÔES

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

ARP	Adress Resolution Adress
BPDU	Bridge Protocol Data Unit
CDP	Cisco Discovery Protocol
EIGRP	Enhanced Internet Gateway Routing Protocol
FHRP	First Hop Redundandy Protocol
GLBP	Gateway Load Balancing Protocol
HSRP	Hot-Standby Routing Protocol
IGRP	Internet Gateway Routing Protocol
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
RSTP	Rapid Spanning Tree
STP	Spanning Tree
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VIP	Virtual Internet Protocol
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundandy Protocol
WAN	Wide Area Network

SUMÁRIO

1 INTRODUÇÃO

Em ambientes de rede há diversos aspectos que podem ser considerados pontos de possíveis falhas para o sistema, sendo estas falhas eventos danosos para empresas, é de suma importância que estas redes possuam redundâncias.

O projeto bem-sucedido de uma rede de computadores pode ser representado pela capacidade desta em oferecer os serviços essenciais requeridos por seus usuários e por preservar os seus principais componentes na eventual ocorrência de falhas (PROJETODEREDES, 2015).

Atualmente nenhuma empresa consegue manter-se em operação sem uma conexão estável com a internet, e devido à isso um projeto bem desenvolvido e implantado é prioridade quando fala-se em rede.

Para criar uma redundância, é necessária a utilização de mais equipamentos, formando-se anéis de rede e assim, criando vários caminhos para que a comunicação seja ininterrupta. Além da utilização de equipamentos adicionais, é necessária a configuração correta dos mesmos, caso contrário, pode ocorrer um *loop* de roteamento.

Alguns protocolos foram criados justamente para resolução desse problema, o "*Spanning Tree Protocol"* para camada 2 e os "*First Hop Redundancy Protocol"* para camada 3.

1.2 PROBLEMA

O grande tráfego de dados presente em empresas de quaisquer tamanhos, seja interno ou externo, tem aumentado muito e a tendência é que continuem a aumentar.

Diante disso, é comum que as empresas necessitem de ambientes de comunicação que lhes permitam seguir com o fluxo de dados contínuo, mesmo que hajam falhas no ambiente de redes, mas como é possível obter uma rede redundante?

Através da simulação de um ambiente de rede devidamente configurado com os protocolos corretos, será mostrado como deixar um ambiente de rede local funcionando de maneira contínua, fazendo uso do software Packet Tracer da Cisco.

1.3 OBJETIVOS

Analisar redes de telecomunicações e problemas de redundância, a fim de entender o funcionamento das mesmas e obter a capacidade de planejar uma rede sólida e confiável.

1.3.1 Geral

Desenvolver, configurar e simular uma rede corporativa redundante, aplicando falhas e testando a confiabilidade da mesma.

1.3.2 OBJETIVOS ESPECÍFICOS

- Montar uma LAN;
- Estudar o funcionamento dos equipamentos de rede;
- Implantar a rede desenvolvida no simulador Packet Tracer;
- Configurar os equipamentos da rede;
- Analisar o comportamento dos dados nessa rede;
- Aplicar falhas com o intuito de simular ocorrências reais;
- Testar o funcionamento e confiabilidade da rede principal e redundância;
- Demonstrar a operação de redes redundantes.

1.4 Justificativa

Com base no que foi introduzido, será mostrada através de simulação a solução para a redundância em ambientes LAN, extremamente apropriada para o ambiente de qualquer empresa que dependa de um fluxo de dados contínuo e que não esteja disposta a pagar o preço pelo mal funcionamento do mesmo.

Como a simulação será efetuada utilizando o software Packet Tracer, mostrará como executar a configuração de equipamentos da mesma marca, que é líder no mercado de *Routing and Switching*.

1.5 PROCEDIMENTOS METODOLÓGICOS

A implementação do projeto será através de simulação em software, visto que uma simulação física se torna inviável devido ao custo e tamanho da rede simulada.

O software utilizado será o Packet Tracer, e o projeto será realizado em etapas. Desenho da rede, configuração dos equipamento, teste da rede sem falhas, inserção de falhas, teste de confiabilidade.

A etapa de desenho da rede consiste em projetar e montar a rede no simulador, de forma que seja possível simular uma grande rede e inserir falhas comuns em ambientes reais.

Na segunda etapa será feita a configuração dos equipamentos utilizados, com o objetivo de criar uma redundância eficiente.

O teste inicial da rede tem o objetivo de verificar se a rede está devidamente configurada e funcional.

A quarta etapa é a inserção de falhas na rede, com o intuito de simular ocorrências comuns em redes reais, tais como rompimentos e mal funcionamento dos equipamentos.

A quinta e ultima etapa é o teste de funcionamento da rede com falhas, sendo esta a fase do projeto em que será verificado a confiabilidade do mesmo, que deverá manter a conexão total da rede.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 A HISTÓRIA DAS REDES

As redes foram criadas na década de 60, utilizando-se cartões perfurados para armazenamento de dados. Essa era uma prática lenta e trabalhosa de se trabalhar, e cada cartão armazenava cerca poucas dezenas de caracteres.

Em 1969, nos Estados Unidos, foi criada a Arpanet, que é considerada o embrião da internet atual. Inicialmente criada com 4 nós, era usada para interligar quatro universidades. A Arpanet cresceu rapidamente, e em 1973 já fazia conexão entre 30 instituições, sendo elas universidades, instituições militares e empresas. Cada ponto era ligado à outros dois pontos, assegurando assim a total funcionalidade da rede. Em 1974 surgiu o protocolo TCP/IP, que acabou se tornando o protocolo padrão na Arpanet e na Internet atual. O TCP/IP permitiu a criação de recursos muito utilizados atualmente, como o e-mail, o Telnet e o FTP.

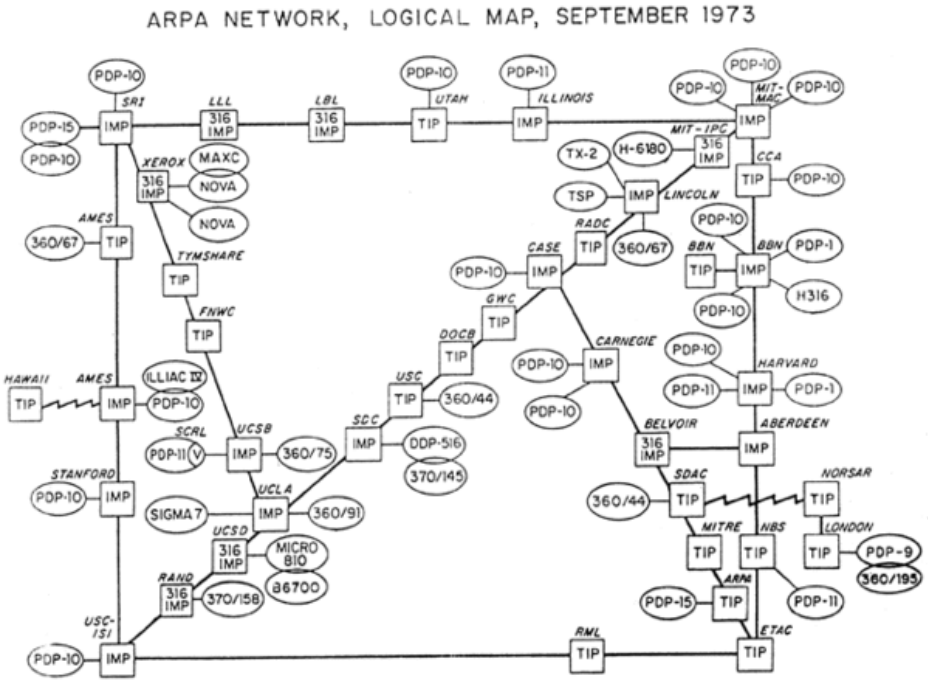

Figura 1 (HARDWARE. 2015)

Antes do TCP/IP, em 1973, foi criado o padrão Ethernet, que era capaz de transmitir 2.94 megabits utilizando cabos coaxiais e interligar até 256 estações de trabalho. Porém, o meio de transmissão não era necessariamente o cabo coaxial, podendo-se utilizar, posteriormente, cabos de fibra óptica ou até mesmo o ar, no caso da internet wireless. Com o crescimento da rede aumentou a dificuldade de manter e distribuir uma lista com todos os hosts conectados, e com isso surgiu o DNS em 1980.

Na década de 1990, com a abertura ao acesso à internet, as redes cresceram de forma assustadora, fazendo com que a um computador só fosse realmente útil se estivesse conectado à internet.

2.2 CONCEITOS DE REDE

Nos primórdios das redes de computadores, não existia um padrão de comunicação, sendo assim, não era possível interligar equipamentos de diferentes fabricantes. Para resolver este problema, foi criado em 1970 o modelo OSI de referência, o qual permitia a interoperabilidade entre fabricantes.

Esse modelo é dividido em 7 camadas, Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace e Física. Cada camada representa a maneira como os dados são tratados.

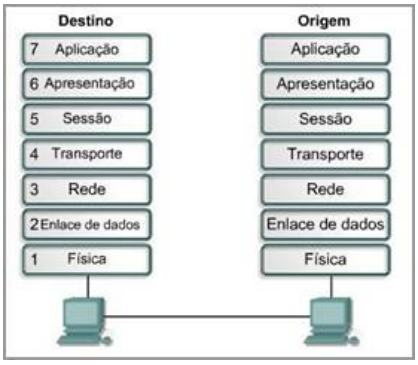

Figura 2 (TELECO. 2015)

Nesse modelo, os dados que são gerados em cada camada pelo transmissor, somente são lidos pela mesma camada no receptor, ou seja, a camada de Rede não tem a capacidade de ler os dados gerados na camada de Transporte, e assim ocorre com todas as outras camadas.

Funcionalidade de cada camada:

Aplicação: Esta é a ligação direta entre o usuário e a rede, composta por softwares como e-mails e navegadores.

Apresentação: Camada responsável pela codificação e decodificação dos dados, tornando-os apresentáveis à camada de aplicação.

Sessão: É nessa camada que é estabelecida a comunicação entre dois computadores. Existem três tipos de comunicação: *Simplex,* onde somente uma estação transmite e a outra somente recebe. *Half duplex,* onde ambas estações transmitem e recebem dados, porém um de cada vez. E *Full Duplex,* que permite a transmissão e recepção simultânea de dados nas duas estações.

Transporte: Essa camada é responsável por garantir a comunicação ponto-a-ponto. Tem como característica adequar o formato dos dados de acordo com a tecnologia utilizada na comunicação, assim como também garante a recepção dos dados na sequência correta, e caso haja algum erro de transmissão, faça a retransmissão dos dados perdidos.

Rede: Responsável por encaminhar os dados na rede, verificando o melhor caminho a ser seguido. É nesta camada que o endereçamento IP é atribuído.

Enlace de dados: Tem o objetivo de converter os dados gerados na camada de rede em bits e prover a transferência desses bits no meio.

Física: É o meio em si, envolvendo todos os equipamentos utilizados para criação da rede, como cabeamento, roteadores, etc.

Rede LAN / WAN

LAN, ou *Local Area Network* (Área de rede local), é uma rede de dados pequena com alta velocidade e baixo nível de erros. Essas redes locais podem conectar diversos dispotivos diferente, sendo computadores, impressoras e outros dispositivos. Isso permite por exemplo, que empresas compartilhem impressoras entre departamentos diferentes, evitando a compra de mais equipamentos. Principais características de um a LAN:

- Opera dentro de uma área geográfica limitada;
- Permite o multi-acesso o meio físico com muita largura de banda;
- Controla de forma privada, redes sob administração local;
- Fornece conectividade em tempo integral com os serviços locais;
- Conecta fisicamente dispositivos adjacentes;

Com o grande crescimento das redes, percebeu-se que as LANs já não eram suficientes para atender à demanda, pois as empresas tornavam-se pequenas ilhas, redes isoladas do mundo exterior. A solução foi criar redes de longa distância, fazendo assim com que as empresas possam comunicar-se entre si.

Essas redes são chamadas de WAN (*Wide Area Network*), e podem estar em diferentes cidades ou até países. Normalmente as WANs são propriedade de grandes empresas, e são contituidas por satélites e fibras opticas. Como fornecem conexões entre cidades e países, empresas menores, com necessidade de comunicação com o mundo, alugam essas redes. Principais características de uma rede WAN:

- Opera em grandes áreas geográficas;
- Permite acesso a interfaces seriais operando a baixas velocidades;
- Fornece conectividade em tempo integral e parcial;
- Conecta dispositivos separados por áreas amplas, até mesmo globais;

Comutação

É chamada de comutação a maneira como os dados são trocados em uma rede, ou seja, a utilização dos recursos da rede para troca de dados entre dois computadores. Existem duas principais formas de comutação: a comutação de circuito e a comutação de pacotes. Na comutação por circuitos, existe um caminho pré-definido para a entrega dos dados. Na comutação por pacotes, cada pacote é endereçado e enviado sem ter a certeza de que haverá um caminho para se comunicar com o receptor.

Principais características da comutação por circuitos:

- Uma conexão ponto-a-ponto é estabelecida entre transmissor e receptor antes do inicio da transmissão, e caso não exista um caminho disponível, a conexão não é estabelecida;
- Total disponibilidade e conexão para transmissão de dados;

- Suporte a aplicações sensíveis a atrasos;

Principais características da comutação por pacotes:

- Circuitos virtuais são estabelecidos ao longo da rede;
- Diversas conexões logicas podem ser estabelecidas em uma única conexão física;
- Meio de transmissão é compartilhado;
- Atua na camada 3 do modelo OSI (Rede);

Roteamento

Roteamento é a definição do caminho que os dados a serem transmitidos vão percorrer do transmissor até o receptor. Esse caminho pode ser definido do inicio ao fim antes do inicio da transmissão (roteamento estático) ou pode ser passo a passo, de acordo com o andamento dos dados pela rede (roteamento dinâmico).

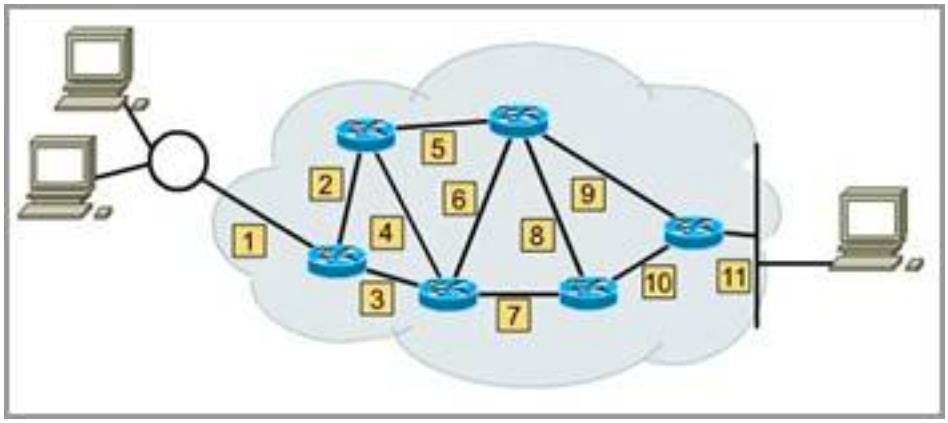

Figura 3 (TELECO. 2015)

No roteamento estático o caminho a ser percorrido pelos dados é pré-definido, normalmente pelo administrador da rede. Uma vez definido esse caminho, o mesmo não é alterado durante a transmissão, independente de falhas na rede.

Já no roteamento dinâmico, os roteadores definem o caminho automaticamente, de acordo com as condições da rede, levando em considerações equipamentos com falhas, adição de novos equipamentos, etc. Para isso, cada roteador utiliza protocolos de roteamento para estabelecer uma comunicação com os demais roteadores, e assim definir a rota mais rápida a ser seguida. Os principais protocolos de roteamento são: RIP (*Routing Information Protocol*), IGRP (*Internet Gateway Routing Protocol*), EIGRP (*Enhanced Internet Gateway Routing Protocol*) e OSPF (*Open Shortest Path First*).

Sem os protocolos de roteamento, seria impossível manter uma rede grande como a internet, pois as mudanças nessa rede são constantes.

2.3 PROTOCOLOS

Protocolo é definido como um conjunto de regras, nas quais será estabelecida uma comunicação entre dispositivos. Ou seja, cada protocolo é o idioma em que as estações irão de comunicar. Os protocolos foram criados com a necessidade de padronizar os métodos de conexão entre computadores, sem a necessidade de um software específico para cada conexão. Existem diversos protocolos atualmente, sendo alguns abertos e outros proprietários. Os abertos são padrões da internet, e os proprietários são utilizados em ambientes específicos.

TCP/IP

Desenvolvido pelo Departamento de Defesa Americano na década de 1960, tem como objetivo principal proteger os dados transmitidos, sem que os mesmos sejam interceptados. É um conjunto do protocolo IP (*Internet Protocol*) e TCP (*Transmission Control Protocol*).

Funcionalidades do TCP/IP:

- Obter um protocolo padrão para diferentes tipos de redes
- Interoperabilidade entre fabricantes
- Constituir uma comunicação confiável e escalonável
- Dinâmico e de fácil configuração.

O TCP é um protocolo de controle de transmissão, e tem a função de prover uma conexão segura entre os hosts. Com ele, todos os pacotes transmitidos são identificados e enviados em sequência. O TCP também possui a função de multiplex, que permite transmitir em série informações que chegam em paralelo.

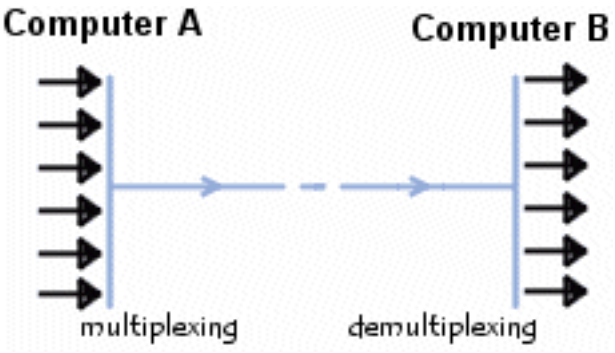

Figura 4 (CCM. 2015)

O IP é um protocolo de conectividade, responsável por endereçar, fragmentar e reunir os pacotes transmitidos, porém, não assegura a entrega desses pacotes.

Os protocolos TCP/IP podem ser aplicados em qualquer rede, sendo básica como um ponto-a-ponto ou até uma rede muito complexa.

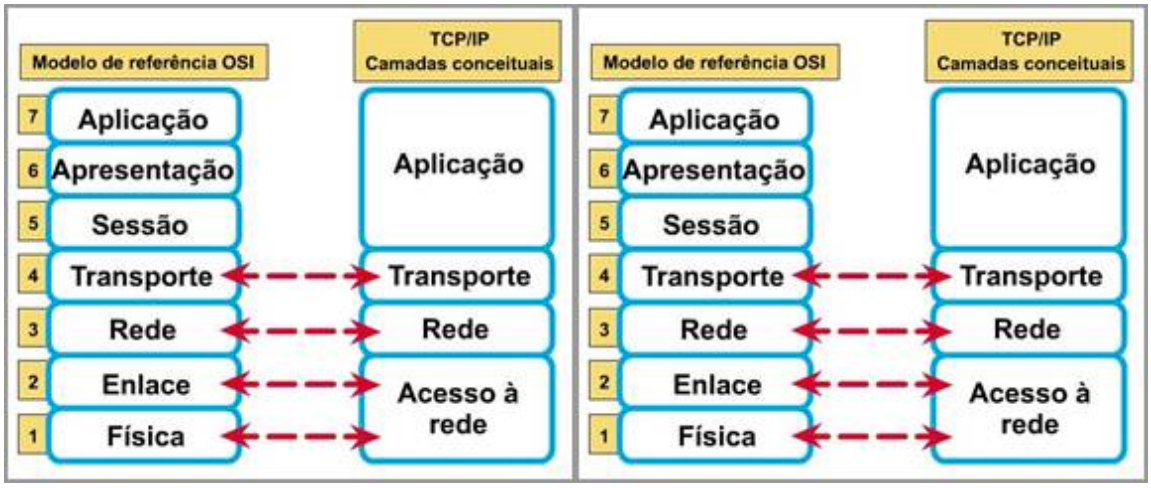

Figura 5 (TELECO. 2015)

Os protocolos TCP/IP formam camadas conceituais, que são comparados ao modelo OSI, conforme Figura.

A camada e Acesso à rede provê meios para que os dados sejam transmitidosà outros computadores da mesma rede.

A camada de Rede (também conhecida como camada Internet), realiza a comunicação entre as máquinas, onde cada uma recebe um endereço IP. Todas as camadas de níveis superiores utilizam esse endereço IP atribuído para identificar a máquina em questão.

A camada de transporte é responsável pelo transporte dos dados fim-a-fim, sem se preocupar com elementos intermediários. Nesta camada existem dois protocolos, UDP (*User Datagram Protocol*) e TCP. A diferença entre esses protocolos é que o UDP simplesmente manda os dados ao destino, sem se preocupar com a entrega dos mesmos.

O protocolo UDP, além de não ser orientado a conexão, também não é confiável, pois não oferece verificação para entrega de dados. Protocolos não orientados a conexão, são protocolos que não avisam o receptor que os dados foram enviados, diferentemente dos protocolos orientados a conexão, os quais

mandam um aviso para o receptor, preparando o mesmo para receber os dados enviados.

O TCP, ao contrário do UDP, é orientado à conexão, o que o torna muito mais seguro nas comunicações, pois garante a entrega dos dados enviados.

A camada de aplicação é a camada responsável pela conexão entre os dados e protocolos com o usuário, utilizando para isso serviços de comunicação.

HSRP e VRRP

Esses dois protocolos são praticamente iguais em termos de configuração e funcionalidades, porem, o HSRP é proprietário da cisco, ou seja, funciona somente em equipamentos da cisco. Já o VRRP é um protocolo aberto e roda em qualquer equipamento que suporte a RFC 3768.

A função básica de ambas é chavear de um equipamento para outro, em caso de falha no equipamento principal, mantando assim o bom e continuo funcionamento da rede.

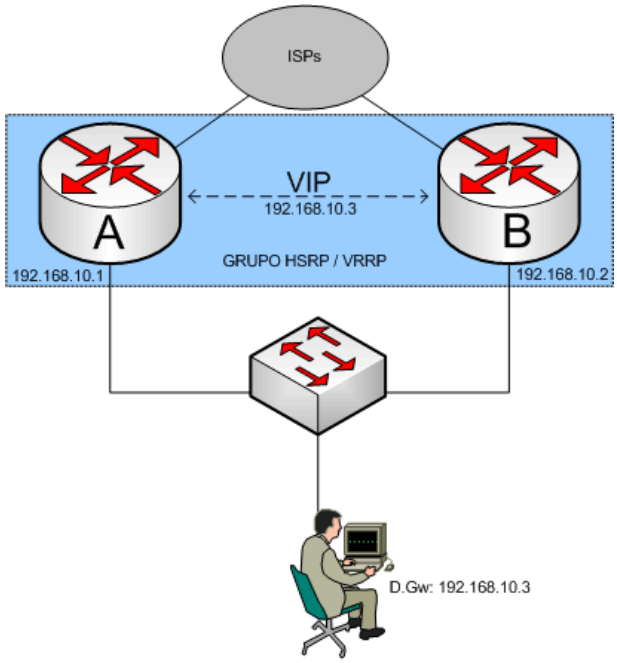

Figura 6 (CCNA. 2015)

A imagem exemplifica uma rede com HSRP ou VRRP implantados, de forma que a rede local LAN veja ambos os roteadores como um IP só, chamado de VIP (virtual IP). Apesar de utilizar dois roteadores, esses protocolos não fazem o balanceamento de dados entre eles, mas deixam um roteador em funcionamento como padrão, e o segundo roteador fica em modo de *backup*, ou *stand-by* no caso do HSRP. Assim, o segundo roteador só entra em operação caso o roteador principal pare de funcionar.

Ambos os protocolos permitem o monitoramento das interfaces e até da tabela de roteamento, havendo assim a possibilidade que se configure qual será o parametro para que seja feito o chaveamento dos roteadores. Esse parâmetro pode ser desde a queda de uma interface ou até uma entrada falha na tabela de roteamento. Esse controle, quando bem configurado, permite que a rede seja bem estável e sólida, mantando-se sempre em funcionamento.

Existe também a opção de retornar o tráfego de dados automaticamente para o roteador principal, assim que a falha do mesmo seja solucionada. No VRRP essa opção é ativa por *default*, e no HSRP deve ser ativada manuamente.

GLBP

O GLBP, assim como o HSRP, é um protocolo proprietario da cisco. Relativamente novo, criado em 2005, tem como objetivo fazer algo que nem o VRRP nem o HSRP fazem, que é balancear os dados entre os roteadores utilizados. O modo com que o GLBP faz isso é implementando diferentes MACs para cada roteador, ou seja, o gateway padrão é o mesmo para todos os usuarios, porem o gateway MAC é diferente.

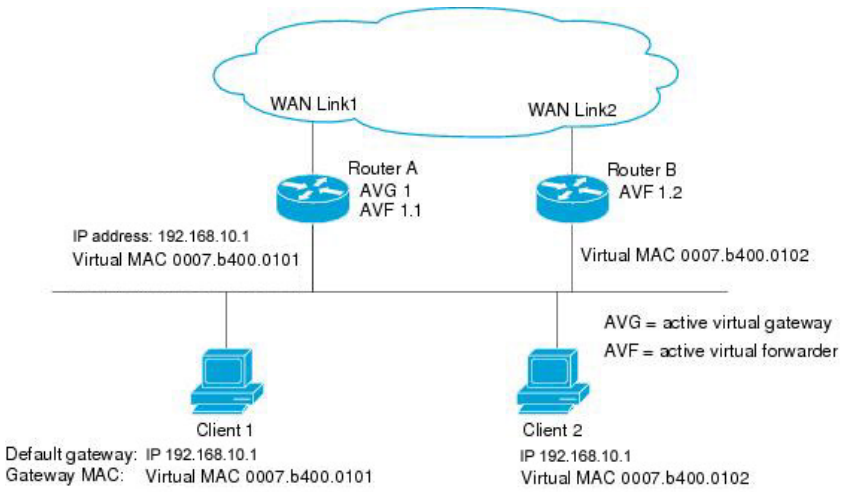

Figura 7 (CCNA. 2015)

Apesar de fazer esse balanceamento, ele não é homogêneo, pois não é feito pacote por pacote.

OSPF

O OSPF (*Open Shortest Path First*) é um protocolo de roteamento que permite a criação de areas de roteamento, ou seja, cada rede é uma area, facilitando assim a

organização e comunicação entre redes. Também é possível criar redes hierárquicas de grande porte sem que seja necessario que cada roteador tenha uma tabela de roteamente para todas as redes.

A grande vantagem do OSPF é o baixo consumo de rede, pois os roteadores trocam informaçoes somente sobre as rotas que sofreram alteraçoes. Porém, para que uma rede de grande porte funcione perfeitamente utilizando o protocolo OSPF, é necessaria a configuração e montagem corretas da rede, que pode ser um tanto complexa.

Para conseguir calcular a melhor rota de transmissão, os roteadores criam e mantém um mapa com todas as rotas da rede, e esse mapa é compartilhado entre todos os equipamentos, sendo alterado sempre que houver uma mudança na rede. Cada roteador mantem em seu banco de dados o mapa de roteamento das redes em que esta ligado, assim tornado a rede mais eficiente e exigindo menos esforço.

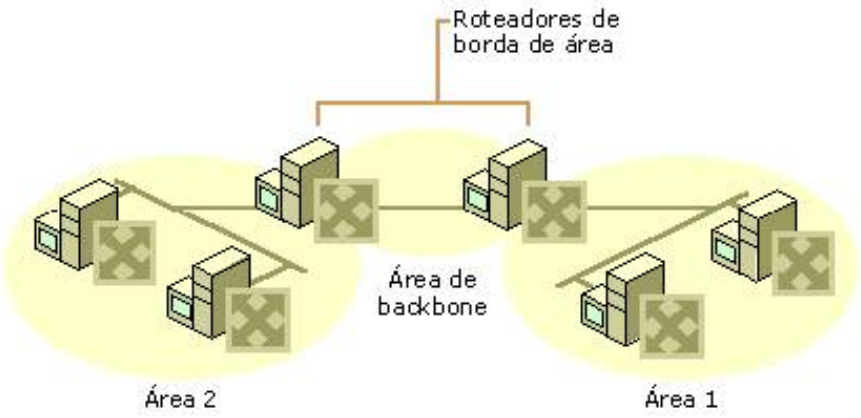

Figura 8 (JULIOBATTISTI. 2015)

Spanning Tree

O Spanning Tree Protocol (STP), é um protocolo desenvolvido para resolver problemas de *loop* em redes configuradas com topolgia de anéis, auxiliando na melhoria da performance da rede.

Com a configuração correta do STP é possível criar redes redundantes sem se preocurar com a geração de *loops*, assim sendo possível formar redes mais estáveis e confiáveis. É possivel também definir as melhores rotas para a transmissão de dados, ou seja, mais eficiente (de menor custo). Caso ocorra alguma falha nesse caminho, o próprio Spanning Tree recalcula a próxima rota mais eficiente. Para que o calculo dessa rota seja feito, é necessário que cada comutador tenha conhecimento total da rede, que é adquirido com mensagens trocadas entre os mesmo, essas mensagens são os BPDUs.

O STP funciona de maneira que fica uma porta em *fowarding*, que é a porta em que os dados serão transmitidos, e a outra em *blocking*, que ficará em *stand-by* para o caso de alguma falha.

Rapid Spanning Tree

Com o grande crescimento das redes, o protocolo STP tornou-se lento, surgindo assim a necessidade de criação de um protocolo mais rápido e eficiente, nesse caso o RSTP (*Rapid Spanning Tree*). O RSTP tem a mesma função do STP, porém com mais agilidade e eficiência.

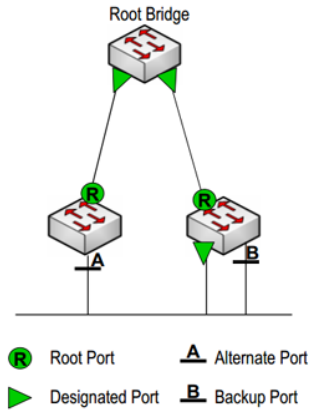

Figura 9 (GTA, UFRJ. 2015)

2.4 CONCEITOS

Desde a criação das redes de computadores até os dias atuais, o crescimento foi inimaginável. De acordo com um estudo realizado pela agência de marketing *We Are Social*, publicado em janeiro de 2015, o Brasil possui 110 milhões de usuários ativos na internet, o que representa 54% da população, sendo assim o terceiro colocado no índice de uso de internet no mundo, ficando atrás das Filipinas e da Tailândia.

Com tamanho crescimento, as redes foram reinventando-se e adaptando-se à constante demanda, e com isso foram criados diversos protocolos e padrões de acesso.

O termo redundância descreve a capacidade de um sistema em superar a falha de um de seus componentes através do uso de recursos redundantes, ou seja, um sistema redundante possui um segundo dispositivo que está imediatamente disponível para o uso quando da falha do sistema primário do sistema. (PROJETODEREDES. 2015)

A redundância de ambientes de comunicação tem recebido uma grande atenção por parte das empresas que necessitam manter o tráfego da rede, independente de seu porte.

Pode-se dizer que um projeto de rede é bem sucedido quando o mesmo tem a capacidade de manter os serviços essenciais funcionando mesmo com eventuais falhas, sendo elas de qualquer natureza.

As falhas podem ser originadas em diversos aspectos, como cabeamento, servidores, sistemas, energia, falhas de projeto, erro humano, dados corrompidos,

degradação dos equipamentos, entre outros. Esses são considerados eventos danosos e prejudicam o funcionamento da rede, afetando assim o desempenho da empresa.

A paralisação temporária dos serviços de rede pode ser definida de duas maneiras:

Indisponibilidade: É um tempo em que a rede fica indisponível ao usuário, ou seja, fora de serviço.

Instabilidade: Nesse caso a rede continua funcionando, mas apresentando variações de desempenho e afetando a experiência dos usuários. Um monitoramento eficiente é imprescindível para que este tipo de falha seja identificada com a maior rapidez possível, para que assim ações de correção possam ser tomadas.

Uma rede bem planejada e desenvolvida deve possuir características que minimizem a ocorrência dessas falhas e trate as mesmas com agilidade e rapidez, diminuindo o tempo de indisponibilidade para o usuário.

Para que não ocorra instabilidade ou até indisponibilidade dos serviços, são utilizadas redundâncias, planejadas e preparadas para que, quando o sistema primário falhar, um sistema secundário seja automaticamente acionado e assuma o controle.

A redundância pode ser feita de varias maneiras, com o objetivo de prevenir diversos tipos de falha, por exemplo, sistemas de ventilação, sistemas operacionais, unidades de disco rígido, servidores, links, dentre outros.

O sistema de backup pode ser planejado de diversas maneiras, não somente com roteadores, mas também com rotas, servidores, software, estações de trabalho, entre outros. Quandofse trata de uma rede de telecomunicações, diversos protocolos devem ser configurados na mesma para que, em caso de falhas, o serviço continue funcionando corretamente.

Surgiu FHRP, que significa *First Hop Redundancy Protocol*, protocolos que oferecem redundância no primeiro salto na rede, na camada 3 (Rede), e para compreender o quão importante são esses protocolos convém um pouco de história. Anos atrás a conexão WAN tinha um valor de Megabyte muito alto, com velocidades muito baixas. Devido a esse motivo era frequentemente adotado um sistema 80/20, 80% do tráfego era para a conexão local e 20% para longas distâncias. Isso fazia

com que o *Default Gateway* fosse pouco relevante, já que a maior parte da conexão ficava confinada localmente.

Com as novas tecnologias para transmissão o valor do megabyte caiu, foi mudada a filosofia de tráfego, e as empresas passaram a mover seus serviços e suas aplicações para fora da rede, utilizando pontos remotos melhor servidos e seguros tratando- se de infraestrutura, por exemplo os datacenters. Hoje o quadro se inverte para um cenário 20/80, ou seja, tem- se 20% como o tráfego local e 80% destinado a WANs. Com uma mudança dessa no comportamento os *Default Gateway* passaram a ser elementos críticos e não podem falhar de maneira alguma.

De acordo com Filippetti (2014) “Hoje, a indisponibilidade de um *gateway* em uma empresa resulta na quase completa ociosidade de seus funcionários, [...]”

O FHRP permite que se configure mais de um *Default Gateway* na rede, mas os *hosts* enxergam apenas um. Existem três protocolos desse tipo:

HSRP (*Hot Standby Routing Protocol*);

VRRP (*Virtual Router Redundancy Protocol*);

GLBP (*Gateway Load Balance Protocol*).

O HSRP é propriedade da Cisco, por isso não roda em produtos de outros fabricantes, e permite que vários roteadores atuem como um roteador virtual, sendo assim, compartilham de um único IP e MAC, chamados de vIP e vMAC. Esse protocolo usa os status *standby* e *active*, aquele marcado como *active* fará o encaminhamento dos pacotes e os outros ficam escutando a rede, ou seja, ficam em estado *listen*. Nesse caso os *standby* não encaminham nada, a não ser pacotes com origem em redes remotas, desde que configurados. Os hosts da rede são configurados com o vIP como *default gateway*, e o processo ARP fará o roteador ativo envie o vMAC ao host. Caso venha a ocorrer indisponibilidade um roteador que estava em modo de espera assume o papel ativo, tornando desnecessário uma eventual manutenção manual e com pouquíssimo impacto nos *hosts*.

Para o caso de ocorrer instabilidade existe a possibilidade de se configurar situações em que o roteador deixe de ser ativo, que não apenas indisponibilidade.

“Desde que a Cisco teve essa grande idéia do HSRP, logo a indústria quis ter tal funcionalidade também para produtos de diferentes fornecedores, por conseguinte, o IETF começou a trabalhar em um FHRP baseado em padrões e o resultado foi o VRRP.”(ROUTERFREAK. 2014).

O VRRP é muito parecido ao HSRP, mas ao invés de *active* e *standby*, os estados são *master* e *backup*. Além disso durante a configuração o VRRP exige a definição do objeto que será monitorado antes, para que posteriormente possa ser incluído no processo VRRP.

O GLBP é de propriedade da Cisco assim como o HSRP, e data de 2005, por isso é relativamente novo. A ideia tratava- se de prover aquilo que o HSRP e o VRRP não conseguiam fazer de maneira descomplicada: Balancear a carga entre os *gateways.*

Os outros dois protocolos apresentados trabalhavam na forma *active* e *standby*, ou seja, havia um ativo e outro(s) em espera. O ideal seria que a carga fosse compartilhada entre todos, melhorando o desempenho da rede. O GLBP permite que o balanceamento de carga entre os roteadores do grupo de forma simples: associando vMACs a um mesmo vIP. Segundo Filippetti (2014, p.347), “O que o GLBP faz é atuar como um *proxy-ARP*, mas enviando, a cada solicitação ARP, o endereço do MAC virtual associado a um router distinto”. Como resultado tem-se um únivo vIP para vários MACs diferentes, os balanceando.

Assim como os outros protocolos, o GLBP precisa deixar em evidência o roteador que será responsável pela coordenação do processo, chamado de *Active Virtual Gateway* (AVG), que será determinado pelo valor maior de prioridade ou endereço IP, caso empate. Os outros roteadores são então chamados de *Active Virtual Forwarders* (AVF), e também cuidarão do processo de encaminhamento de pacotes. Percebe- se que não há o conceito de *standby*, já que de certa forma todos os roteadores da rede em questão estarão agindo ativamente.

O GLBP também conta com a opção de se escolher a forma como o balanceamento será efetivado: por AVF, por host, ou de maneira proporcional ao valor anteriormente definido a um parâmetro *weighting*.

Assim como o GLBP os outros protocolos também permitem balanceamento de carga, porém é necessário que haja mais de um *default gateway* na rede.

Além dos protocolos de redundância para roteadores que foram apresentados anteriormente, também conhecidos como protocolos de alta disponibilidade da camada 3, existe também um protocolo de redundância utilizado na camada 2 (Enlace de dados), onde se encontram os switches, conhecido como *Spanning Tree Protocol* (STP).

O STP tem como objetivo evitar loops em caminhos redundantes, deixando os loops desativados, até que haja necessidade de que sejam ativados.

Com o STP, a chave é para todos os switches na rede elegerem uma ponte raiz que se tornará o ponto principal da rede. Todas as demais decisões da rede, como que porta bloquear e que porta colocar no modo de encaminhamento, são feitas da perspectiva dessa ponte-raiz. Um ambiente comutado, que é diferente de um ambiente de ponte, muito provavelmente lida com múltiplos VLANs. Quando implementada em uma rede de switching, a ponte-raiz normalmente é chamada de switch-raiz. Cada VLAN deve ter a própria ponte-raiz, pois cada uma é domínio de broadcast separado. As raízes das diferentes VLANs podem residir em um único switch ou em vários switches. (Cisco, 2015).

Os switches configurados com o STP trocam informações entre si, chamadas de BPDUs, determinando quem virá a ser o switch- raiz, de acordo com o Bridge ID (BID). O BID é determinado com a junção do MAC do equipamento com o valor de prioridade, que é configurável, e possui 8 bytes de extensão. À partir disso serão determinado os caminhos redundantes e colocados em modo standby.

Deve existir apenas um switch- raiz em um domínio de Broadcast, que terá suas portas designadas em modo forwarding, enviando e recebendo frames normalmente. Os outros switches recebem apenas BPDUs, para o caso de precisarem ser reativadas.

3 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Foi feita uma simulação com foco em HSRP e Spanning Tree. Nesta simulação é possível verificar os diferentes pacotes de comunicação entre os equipamentos, que permitem a redundância quando há algum problema.

3.1 7.1 TOPOLOGIA

A rede em questão possui uma VLAN com seis switches, onde estão configurados o protocolo RSTP, que é uma versão mais rápida do STP, e oito notebooks, representando fisicamente duas salas de um mesmo setor. Dois dos switches estão conectados com roteadores que funcionam como gateways, que apesar de possuírem endereços diferentes estão configurados com o protocolo HSRP, ou seja, um mesmo endereço de *gateway* virtual. Acima há um outro roteador conectado há uma rede diferente, onde se encontra o servidor.

O ambiente é parecido com o da rede de uma pequena empresa, onde funcionários se conectam com um servidor que se encontra em um outro local e não podem ficar muito tempo sem acesso ao mesmo, fazendo- se necessária a redundância.

Durante a simulação, o gateway com prioridade será desligado como se houvesse uma falha, e o HSRP deve entrar em ação, tornando o outro roteador o novo gateway. Será também retirado o caminho nas portas dos switches, para que o protocolo RSTP abra outra porta de acesso, impedindo que a conexão pare por muito tempo.

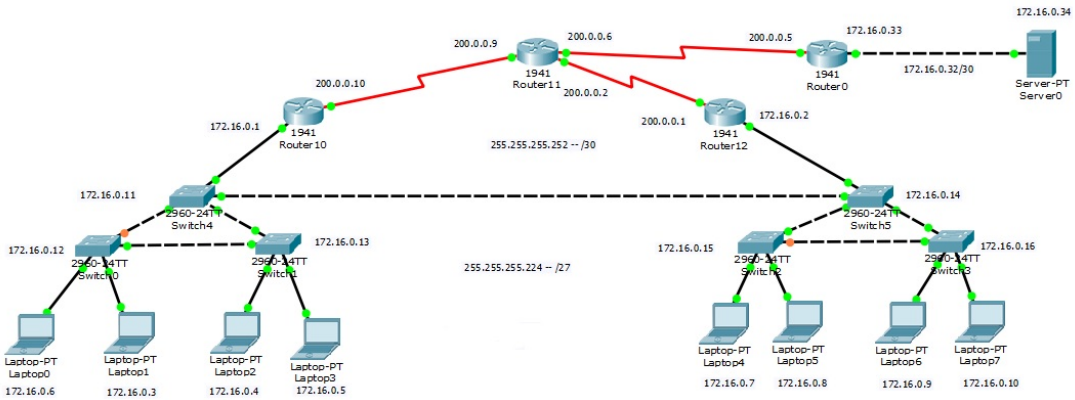

Figura 10 (Autoria própria)

3.2 7.2 TABELA DA REDE

Equipamento	IP	Máscara
Laptop0	172.16.0.6	255.255.255.224
Laptop1	172.16.0.3	255.255.255.224
Laptop2	172.16.0.4	255.255.255.224
Laptop3	172.16.0.5	255.255.255.224
Laptop4	172.16.0.7	255.255.255.224
Laptop5	172.16.0.8	255.255.255.224
Laptop6	172.16.0.9	255.255.255.224
Laptop7	172.16.0.10	255.255.255.224
Switch0	172.16.0.12	255.255.255.224
Switch1	172.16.0.13	255.255.255.224
Switch2	172.16.0.15	255.255.255.224
Switch3	172.16.0.16	255.255.255.224
Switch4	172.16.0.11	255.255.255.224
Switch5	172.16.0.14	255.255.255.224
Router10		
GigabitEthernet0/0	172.16.0.1	255.255.255.224
Serial0/1/0	200.0.0.10	255.255.255.252
Router11		
Serial0/0/0	200.0.0.6	255.255.255.252
Serial0/1/0	200.0.0.9	255.255.255.252
Serial0/1/1	200.0.0.2	255.255.255.252
Router12		
GigabitEthernet0/0	172.16.0.2	255.255.255.240

Serial0/1/0	200.0.0.1	255.255.255.252
Router0		
GigabitEthernet0/0	172.16.0.33	255.255.255.224
Serial0/1/0	200.0.0.5	255.255.255.252
Servidor	172.16.0.34	255.255.255.252
Gateway Virtual	172.16.0.254	255.255.255.224

3.3 7.3 SIMULAÇÃO HSRP (HOT STANDBY ROUTER PROTOCOL)

Como explicado no capítulo anterior, nesse protocolo é feito o uso de um *Gateway* Virtual, ou seja, o *gateway* não é um roteador físico. Nesse caso os roteadores Router10 e Router12 estão recebendo esse protocolo, com o endereço 172.16.0.254.

O roteador com prioridade maior será desligado, simulando um estado de incapacidade e será observada a maneira como o HSRP age, para ativar o próximo roteador.

3.4 7.4 ANÁLISE HSRP

Os comandos utilizados para configuração do HSRP foram:

No Router10 – Modo Terminal de Configuração

```
interface GigabitEthernet0/0
standby 10 ip 172.16.0.254
standby 10 priority 150
standby 10 preempt
```

No Router12 – Modo Terminal de Configuração

```
interface GigabitEthernet0/0
standby 10 ip 172.16.0.254
standby 10 priority 110
```

Usando de uma visão geral, pode- se dizer que o Router10 tem uma prioridade maior, ele assumiu o papel de *gateway* no primeiro momento, e quando desligado, os pacotes passaram a ser roteados pelo Router12, que é o roteador com menor prioridade para ser o g*ateway* virtual.

O protocolo demora de 0.2 a 0.4 segundos para entrar em ação, enquanto isso é impossível que o cliente acesse outras redes, já que o *gateway* configurado nos notebooks é o do *gateway* virtual. Após isso, pacotes HSRP circulam na rede a cada 1 segundo, aproximadamente, sendo que isso serve para verificar se o Router10 ainda está ativo.

Quando o Router10 é desligado espera- se até que o Router12 envie pacotes de verificação para então passar a funcionar como *gateway* virtual, e assim continua até que o Router10 seja ligado novamente. Quando o Router10 é ligado ocorre o envio de pacotes ARP, OSPF e CDP para verificação da rede, e apenas quando há verificação do protocolo por ambos os roteadores é que o Router10 volta a ser o ativo.

3.5 7.5 SIMULAÇÃO STP (SPANNING TREE PROTOCOL)

STP permite a configuração de redundância na camada de enlace (*layer* 2) e não na camada de rede (*layer* 3), como os outros três protocolos mostrados nesse trabalho. Na simulação foi utilizado o RSTP (*Rapid Spanning Tree Protocol*), que deixa o processo bem mais rápido através do uso de apenas três estados distintos de portas, *Discarding, Learning* e *Forwarding.* Ressaltando, que apenas uma VLAN foi utilizada, a VLAN10.

Como foram simulados os switches 2960 da Cisco, o STP vem configurado, sendo que foi utilizado o comando ‘stp mode rstp’ para que ele funcione como RSTP.

No primeiro instante, o protocolo irá prevenir que aconteça uma “tempestade de *broadcast*”, fechando portas de comunicação que possam gerar *loops.*

Será retirado uma das conexões feita por portas de switches que não estão bloqueadas, gerando uma falha de comunicação entre elas, afim de mostrar como o protocolo abrirá o caminho que estava fechado e recuperando a comunicação.

3.6 7.6 ANÁLISE STP

Em um primeiro momento todos os switches funcionam como Raiz, mas após algumas BPDUs serem enviadas e recebidas apenas um roteador permance dessa forma, aquele com o menor BID, e como o mesmo é calculado com a concatenação do MAC e o número de prioridade é impossível que haja empate, uma vez que o MAC é único.

Percebe- se também, que a porta de um switch em cada lado da topologia é fechada. O protocolo STP faz isso, para impedir que haja um *looping* infinito de *broadcast*, calculando qual a menor rota até o switch denominado como raiz, nesse caso, o Switch1.

Quando é retirado um dos caminhos de portas de acesso abertas o RSTP muda quase que instantaneamente a porta, muito mais rápido que o protocolo STP, que demorava entre 30 e 50 segundos. Ocorre o mesmo quando uma porta é desligada, em menos de 3 segundos é recuperada a conexão.

> A cada 2 segundos são enviados pacotes STP, que são na verdade BPDUs que verificam o estado da rede. Teoricamente,

há um tempo de 6 segundos (3 BPDUs perdidas) para que os switches percebam a falta de uma porta, mas na simulação ocorre demasiadamente rápido.

4 CONSIDERAÇÔES FINAIS

Neste trabalho foi estudado a importância das redundâncias em redes, visto que o bom funcionamento é fundamental para seus usuários. Apresentou-se como problema a indisponibilidade, deixando seus utilizadores sem comunicação.

Como solução foi desenvolvido um projeto de rede com redundância de *gateways*, tornando a saída do ambiente local mais seguro e confiável. Para que a simulação ocorresse de forma positiva, foi feito estudo dos equipamentos, topologias, protocolos e configurações necessárias. Para efeitos de teste, foi utilizado um *software* de simulação, o qual permitiu todo este processo.

Com a topologia montada e configurada, inseriu-se falhas em pontos específicos, com a finalidade de garantir a confiabilidade e estabilidade da comunicação, a qual manteve-se intacta.

Durante todo o processo de testes foram coletados dados, os quais permitiram a análise de cada protocolo configurado, visando o entendimento detalhado de cada um. Com essas análises foi possível concluir que com um bom planejamento as redes podem funcionar de maneira confiável e ininterrupta, trazendo benefícios à seus usuários.

REFERÊNCIAS

AMPLAINFO. **Redundância de Caminhos de Rede (Ethernet, STP e RSTP).** Disponível em:

<http://www.amplainfo.com.br/index.php?option=com_content&view=article&id=81%3Aredundancia-de-caminhos-de-rede-ethernet-stp-e-rstp&catid=28%3Atecnologias&Itemid=27>. Acesso em: 21 Mai. 2015.

ANATEL. **Banda Larga – Acessos.** Disponível em:

<http://www.anatel.gov.br/dados/index.php?option=com_content&view=article&id=269>. Acesso em: 10 Nov. 2015.

CCM. **O protocolo TCP.** Disponível em: <http://br.ccm.net/contents/284-o-protocolo-tcp>. Acesso em: 13 Nov. 2015.

CCNA. **VRRP x HSRP x GLBP.** Disponível em:

<http://blog.ccna.com.br/2008/12/16/pr-vrrp-x-hsrp-x-glbp/>. Acesso em: 13 Nov. 2015.

CISCO. **Configuring HSRP**. Disponível em:

<http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1_8_ea1/configuration/guide/3550scg/Swhsrp.html>. Acesso em: 23 mai. 2015

CISCO. **Entendendo e configurando o Spanning Tree Protocol (STP) em Switches Catalyst**. Disponivel em:
< http://www.cisco.com/cisco/web/support/BR/8/82/82594_5.html>. Acesso em: 21 Mai. 2015

CISCO. **Entendendo o Spanning Tree Protocol (802.1w).** Disponível em:

<http://www.cisco.com/cisco/web/support/BR/8/85/85548_146.html>. Acesso em: 17 Nov. 2015.

Filippetti, Marco Aurélio. **CCNA 5.0 Guia Completo para Estudos**. 1ª ed. Florianópolis: Visual Books, 2014.

GTA.UFRJ. **Protocolos: RSTP.** Disponível em:

<http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2012_2/st/index.php?file=protocolos/rstp>. Acesso em 30 Nov. 2015.

HARDWARE. **História das redes.** Disponível em:

<http://www.hardware.com.br/tutoriais/historia-redes/>. Acesso em: 13 Nov. 2015.

JULIOBATTISTI. **Tutorial de TCP/IP – Júlio Battisti – Parte 15 Protocolos de roteamento dinâmico**. Disponível em:

<http://juliobattisti.com.br/artigos/windows/tcpip_p15.asp>. Acesso em: 17 Nov. 2015.

MOBIFEED. **Digital, Social & Mobile in 2015': Detalhes sobre o universo digital no Brasil e no mundo.** Disponível em: <http://www.mobifeed.com.br/digital-social-mobile-in-2015-detalhes-sobre-o-universo-digital-no-brasil-e-no-mundo/>. Acesso em: 10 Nov. 2015.

PROJETODEREDES. **Conceitos de redundância e contingencia.** Disponível em:

<http://www.projetoderedes.com.br/artigos/artigo_conceitos_de_redundancia.php>. Acesso em: 21 Mai. 2015.

ROUTERFREAK. **CCNA study: FHRP or "First Hop Redundancy Protocols".** Disponível em: <http://www.routerfreak.com/ccna-fhrp-hop-redundancy-protocols/>. Acesso em: 23 Jun. 2015.

SLIDESHARE. **Digital, Social & Mobile in 2015.** Disponível em:

<http://pt.slideshare.net/wearesocialsg/digital-social-mobile-in-2015>. Acesso em: 10 Nov. 2015.

TELECO. **MPLS I: Conceitos de Redes.** Disponível em:

<http://www.teleco.com.br/tutoriais/tutorialmplseb1/pagina_2.asp>. Acesso em: 13 Nov. 2015.

ANEXO(S)

Estado do Protocolo para a VLAN10

Switch4

VLAN0010

Spanning tree enabled protocol rstp

Root ID Priority 32778

Address 0001.C99D.B1EE

Cost 19

Port 2(FastEthernet0/2)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)

Address 000B.BE28.C187

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

Fa0/4 Desg FWD 19 128.4 P2p

Fa0/3 Desg FWD 19 128.3 P2p

Fa0/1 Desg FWD 19 128.1 P2p

Fa0/2 Root FWD 19 128.2 P2p

Switch0

VLAN0010

Spanning tree enabled protocol rstp

Root ID Priority 32778

Address 0001.C99D.B1EE

Cost 19

Port 3(FastEthernet0/3)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)

Address 0030.F2B7.0D1A

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

Fa0/1 Desg FWD 19 128.1 P2p

Fa0/2 Desg FWD 19 128.2 P2p

Fa0/3 Root FWD 19 128.3 P2p

Fa0/4 Altn BLK 19 128.4 P2p

Switch1

VLAN0010

Spanning tree enabled protocol rstp

Root ID Priority 32778

Address 0001.C99D.B1EE

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)

Address 0001.C99D.B1EE

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

Fa0/3 Desg FWD 19 128.3 P2p

Fa0/1 Desg FWD 19 128.1 P2p

Fa0/2 Desg FWD 19 128.2 P2p

Fa0/4 Desg FWD 19 128.4 P2p

Switch5

VLAN0010

Spanning tree enabled protocol rstp

Root ID Priority 32778

Address 0001.C99D.B1EE

Cost 38

Port 4(FastEthernet0/4)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)

Address 0060.3E12.DB56

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

Fa0/2 Desg FWD 19 128.2 P2p

Fa0/3 Desg FWD 19 128.3 P2p

Fa0/4 Root FWD 19 128.4 P2p

Fa0/1 Desg FWD 19 128.1 P2p

Switch2

VLAN0010

Spanning tree enabled protocol rstp

Root ID Priority 32778

Address 0001.C99D.B1EE

Cost 57

Port 4(FastEthernet0/4)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)

Address 00D0.BA22.5D9C

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

Fa0/2 Desg FWD 19 128.2 P2p

Fa0/3 Altn BLK 19 128.3 P2p

Fa0/4 Root FWD 19 128.4 P2p

Fa0/1 Desg FWD 19 128.1 P2p

Switch3

VLAN0010

Spanning tree enabled protocol rstp

Root ID Priority 32778

Address 0001.C99D.B1EE

Cost 57

Port 4(FastEthernet0/4)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)

Address 0030.A365.030E

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

Fa0/4 Root FWD 19 128.4 P2p

Fa0/1 Desg FWD 19 128.1 P2p

Fa0/3 Desg FWD 19 128.3 P2p

Fa0/2 Desg FWD 19 128.2 P2p

Estado dos Roteadores na Simulação de HSRP

Router10

interface GigabitEthernet0/0

ip address 172.16.0.1 255.255.255.224

duplex auto

speed auto

standby version 2

standby 10 ip 172.16.0.254

standby 10 priority 150

standby 10 preempt

!

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/1/0

ip address 200.0.0.10 255.255.255.252

clock rate 2000000

!

interface Serial0/1/1

no ip address

clock rate 2000000

shutdown

!

interface Vlan1

no ip address

shutdown

!

router ospf 1

log-adjacency-changes

network 200.0.0.8 0.0.0.3 area 0

network 172.16.0.0 0.0.0.31 area 0

Router11

interface GigabitEthernet0/0

no ip address

duplex auto

speed auto

shutdown

!

interface GigabitEthernet0/1

```
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 200.0.0.6 255.255.255.252
clock rate 2000000
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Serial0/1/0
ip address 200.0.0.9 255.255.255.252
!
interface Serial0/1/1
ip address 200.0.0.2 255.255.255.252
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
```

network 200.0.0.0 0.0.0.3 area 0

network 200.0.0.4 0.0.0.3 area 0

network 200.0.0.8 0.0.0.3 area 0

Router12

interface GigabitEthernet0/0

ip address 172.16.0.2 255.255.255.240

duplex auto

speed auto

standby version 2

standby 10 ip 172.16.0.254

standby 10 priority 110

!

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/1/0

ip address 200.0.0.1 255.255.255.252

!

interface Serial0/1/1

no ip address

clock rate 2000000

shutdown

```
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 200.0.0.0 0.0.0.3 area 0
network 172.16.0.0 0.0.0.31 area 0

Router0

interface GigabitEthernet0/0
ip address 172.16.0.33 255.255.255.224
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
ip address 200.0.0.5 255.255.255.252
!
interface Serial0/1/1
```

```
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 200.0.0.4 0.0.0.3 area 0
network 172.16.0.32 0.0.0.31 area 0
```