CENTRO PAULA SOUZA

**FACULDADE DE TECNOLOGIA DE AMERICANA**

**Curso de Tecnologia em Segurança da Informação**

Vinicius Luis da Silva

# PROTOCOLOS DE PROTEÇÃO ETHERNET

**Americana, SP**

**2014**

CENTRO PAULA SOUZA

**FACULDADE DE TECNOLOGIA DE AMERICANA**

**Curso de Tecnologia em Segurança da Informação**

Vinicius Luis da Silva

# PROTOCOLOS DE PROTEÇÃO ETHERNET

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Tecnologia em Segurança da Informação, sob a orientação do Prof.º Marcus Vinícius Lahr Giraldi.

Área de concentração: Redes de Computadores

**Americana, S. P.**

**2014**

**FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS**

**Dados Internacionais de Catalogação-na-fonte**

Silva, Vinicius Luis da

S581p Protocolos de proteção Ethernet. / Vinicius Luis da Silva. – Americana: 2014.

52f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Me. Marcus Vinícius Lahr Giraldi

1. Rede de computadores I. Giraldi, Marcus Vinícius Lahr II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.519

Vinicius Luis da Silva

# Protocolos de Proteção Ethernet

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Redes de Computares.

Americana, 06 de Dezembro de 2014.

**Banca Examinadora:**

Marcus Vinicíus Lahr Giraldi (Presidente)
Mestre
Fatec Americana

Maria Cristina Luz Fraga Moreira Aranha (Membro)
Mestre
Fatec Americana

Edson Roberto Gaseta (Membro)
Especialista
Fatec Americana

## AGRADECIMENTOS

Agradeço a primeiramente a minha esposa e a minha filha, que abriram mão da minha companhia em muitos momentos para que esse trabalho fosse realizado.

Agradeço também ao Profº. Marcus Vinícius Lahr Giraldi, pelo apoio na realização desse trabalho.

Aos todos os professores da Fatec Americana, que todos os dias enfrentam o desafio de transmitir conhecimento aos alunos que se propõem a aprender.

E agradeço a Fatec Americana e a todos os funcionários, que me proporcionaram um ensino gratuito e de qualidade.

Obrigado a todos.

## DEDICATÓRIA

Dedico esse trabalho a minha esposa Milena e a minha filha Isabella, pois é por elas que vou à luta todos os dias.

Dedico também a minha mãe Silvia, meu padrasto Claudemir, e meus irmãos Jeferson e Raquel, pois sempre me incentivaram a ir em busca do que eu queria.

Por último ao meu pai Afonso, que sempre foi meu referencial de caráter e inteligência.

"A persistência é o caminho do êxito.”

Charles Chaplin

## RESUMO

Este trabalho tem por objetivo apresentar o conceito e aplicação dos protocolos STP (*Spanning Tree Protocol*) e EAPS (*Ethernet Automatic Protection Switching*), com foco em suas utilizações como protocolos de proteção de tráfego de dados em redes *ethernet*.

Ambos os protocolos são tratados de forma objetiva a abordar o tema de proteção de redes e exemplificados com cenários que auxiliam a compreensão do conteúdo.

Após a apresentação de conceitos dos protocolos, funcionalidades, exemplos de aplicações e configurações de equipamentos, o trabalho apresenta em sua conclusão um estudo de caso onde a utilização dos protocolos é aplicada em um cenário concreto de uma grande empresa do mercado de telecomunicações.

O estudo de caso é baseado na análise da topologia de rede atual utilizada pela empresa no atendimento de seus clientes, onde ocorre a avaliação do atual cenário e o apontamento de um problema encontrado. Fechando o estudo de caso, há a apresentação de uma proposta de correção do problema encontrado e a análise do acarretamento dessa mudança.



**Palavras Chave:** *Spanning Tree*; STP; EAPS; *Ethernet*; 802.1D; G.8031;

**ABSTRACT**

*This work aims to present the concept and the implementation of protocols STP (Spanning Tree Protocol) and EAPS (Ethernet Automatic Protection Switching), focusing on their use as protection protocols of data traffic in ethernet networking.*
*Both protocols are treated with the objective for addressing the issue of protection of networks and exemplified with scenarios that help understanding the contents.*
*After the presentation of concepts of protocols, features, examples of applications and device settings, the work presents in its conclusion a case study where the use of protocols is implemented in a concrete scenario of a large company in the telecommunications market.*
*The case study is based on analysis of current network topology used by the company in servicing its customers, which occurs an assessment of the current situation and the appointment of the problem encountered. Closing the case study, there is the presentation of a proposal to fix the problem found and the analysis of the entailment of this change.*

**Keywords:** *Spanning Tree*; STP; EAPS; *Ethernet*; 802.1D; G.8031;

**SUMÁRIO**

## LISTA DE FIGURAS E DE TABELAS

# 1 INTRODUÇÃO

Os computadores foram criados com o intuito de resolver problemas e tratar informações, porém, a necessidade de compartilhar essas soluções e informações tratadas apareceu quase que juntamente com essas máquinas. Devido a essa necessidade, o conceito de redes de computadores começou a surgir, porém, a evolução significativa dessa comunicação só ocorreu entre o final da década de 70 e inicio da década de 80.

Inicialmente as redes de computadores criadas faziam parte de instituições militares, de ensino e pesquisa, principalmente nos Estados Unidos.

Um dos grandes saltos na evolução das redes foi a criação do modelo de referência TCP/IP, conforme escrito por Marco Filippetti (2008, p. 35)

> [...] em 1974 Bob Kahn e Vinton G. Cerf criaram o modelo de referência TCP/IP, que em principio não era um modelo de referência, e sim um conjunto de protocolos para controle das redes e das informações trafegadas nelas. A pesquisa de Kahn e Cerf, foi motivada pela RFP lançada pelo Departamento de Defesa Americano devido a necessidade de transportar dados de maneira segura e ágil. O DoD recebeu inúmeros modelos de universidades diferentes, mas em 1976 o modelo TCP/IP foi escolhido para criarem a ARPANET. Devido a isso o modelo também é conhecido como modelo DoD.

Após a popularização das redes, as instituições e empresas ficaram dependentes delas e a disponibilidade das redes passou a ser foco entre elas. Para aumentar a disponibilidade dessas redes, foram criados protocolos para controle de conexões redundantes, protocolos esses chamados de protocolos de proteção de tráfego. Nesse estudo iremos tratar dois protocolos que dentre outras funções atuam como gerenciadores de conexões redundantes em redes *ethernet*, o *Spanning Tree Protocol* (IEEE 802.1D) e o *Ethernet Automatic Protection Switching* (ITU G8031).

Este trabalho, portanto, tem como objetivo abordar os protocolos STP e EAPS, bem como meios de configurá-los em *switches* do fabricante Datacom. O funcionamento básico desses protocolos serão apresentados, e posteriormente analisados do ponto de vista de suas utilizações como meio de gerenciar topologias que utilizam *links* redundantes para proteção de tráfego nas redes *ethernet*.

Para que esse objetivo fosse alcançado, pesquisas e análises dos protocolos foram realizadas, e também um estudo de caso foi feito com o intuito de mostrar o funcionamento e a utilização desses importantes protocolos em um ambiente real.

Como dito anteriormente a alta disponibilidade das redes é muito importante atualmente, e está em grande foco principalmente devido ao grande crescimento da utilização das redes *Metro Ethernet*. Os protocolos STP e EAPS, assim como suas variações, são amplamente utilizados nessas redes e estão disponíveis em equipamentos de vários fabricantes. Ambos os protocolos possuem fácil implementação e controle, porém, é necessário conhecê-los muito bem para utilizar-se de todas as suas funções e não os tornarem um ponto de falha nas redes.

# 2 PROTEÇÃO DE REDES ETHERNET

As redes *ethernet* são as redes que mais evoluíram nas ultimas décadas. A tecnologia de pacotes criada por Robert Metcalf em 1972 é hoje o tipo de rede mais utilizada nas grandes empresas, e a que mais cresce em número de adeptos.

Esse crescimento ocorre devido à facilidade de implantação, baixo custo, alta escalabilidade, uso estatístico e compartilhado das bandas, entre outros motivos.

De acordo com a empresa CPqD (2008, p. 1)

> O Ethernet evoluiu consideravelmente ao longo dos seus 35 anos de existência, partindo de uma tecnologia criada para redes locais operando a 10 Mbit/s sobre um cabo metálico compartilhado para uma tecnologia de comutação de múltiplas aplicações operando a 10 Gbit/s sobre fibra óptica.
>
> O potencial de oferta de alta capacidade a baixos custos proporcionado pelo Ethernet tem elevado o interesse no uso dessa tecnologia também em aplicações metropolitanas, corporativas e de longa distância, que hoje utilizam tecnologias mais complexas e custosas como ATM, SDH e Frame Relay.

As redes *ethernet* atuais são compostas basicamente de *switches*, equipamentos de camada 2 – camada de Enlace do modelo de referência OSI – baseados em comunicação através de endereçamento MAC (*Media Access Control*). As velocidades do acesso *ethernet* até o momento variam de 10 Mbit/s até 10 Gbit/s e caminham em conjunto com a combinação de cabeamento, conectores e *hardwares* utilizados. Os tipos de cabeamentos mais utilizados para redes *ethernet* são UTP (*Unshielded Twisted Pair*) e Fibra Óptica, de diversas velocidades e tipos. Podemos ver a relação de cabeamentos na Tabela 1, que compara os tipos de cabeamento, velocidade e distância atingida.

**Tabela 1 – Padrões de Cabeamento**

| PADRÃO | BANDA BASE | DISTÂNCIA ATINGIDA | TIPO DE CABO |
|---|---|---|---|
| 10Base2 | 10 Mbit/s | 185 metros | Thinnet – Cabo Coaxial |
| 10Base5 | 10 Mbit/s | 500 metros | Thicknet – Cabo Coaxial |
| 10BaseT | 10 Mbit/s | 100 metros | CAT3 - Par trançado sem blindagem - UTP |
| 100BaseTX | 100 Mbit/s | 100 metros | CAT5, 6 e 7 - Par trançado sem blindagem - UTP |
| 100BaseFX | 100 Mbit/s | 400 metros | 65.2/125µ Fibra Monomodo |
| 1000BaseCX | 1 Gbit/s | 25 metros | Par trançado blindado - STP |
| 1000BaseT | 1 Gbit/s | 100 metros | CAT5 - 4 pares trançado sem blindagem - UTP |
| 1000BaseSX | 1 Gbit/s | 260 metros | 62.5/50µ Fibra Multimodo |
| 1000BaseLX | 1 Gbit/s | 10 Km | 9µ Fibra Monomodo |

**Fonte: Filippetti, 2008**

Devido ao grande interesse das empresas nas redes *ethernet*, um dos pontos de maior foco é a disponibilidade das redes, ou seja, que ela esteja sempre acessível e com o funcionamento dentro dos padrões idealizados. Para que a rede sempre esteja perto dos 100% de disponibilidade, são usados conexões redundantes, equipamentos redundantes e topologias em anel. Para que essas soluções funcionem corretamente e não criem problemas, são necessários mecanismos que controlem essas topologias e façam com que a rede se comporte da melhor maneira possível em casos de falhas. Esses mecanismos de controle são os chamados protocolos de proteção *ethernet*.

## 2.1 PROTOCOLOS DE PROTEÇÃO *ETHERNET*

Os protocolos de proteção *ethernet* são utilizados para controlar, manter e gerenciar as conexões protegidas (redundantes) das redes *ethernet*. Existem alguns protocolos de proteção e cada um atua a sua maneira, o foco desse trabalho serão os protocolos STP (*Spanning Tree Protocol*) homologado pelo IEEE (*Institute of Electrical and Electronics Engineers*) no padrão 802.1D e o EAPS (*Ethernet*

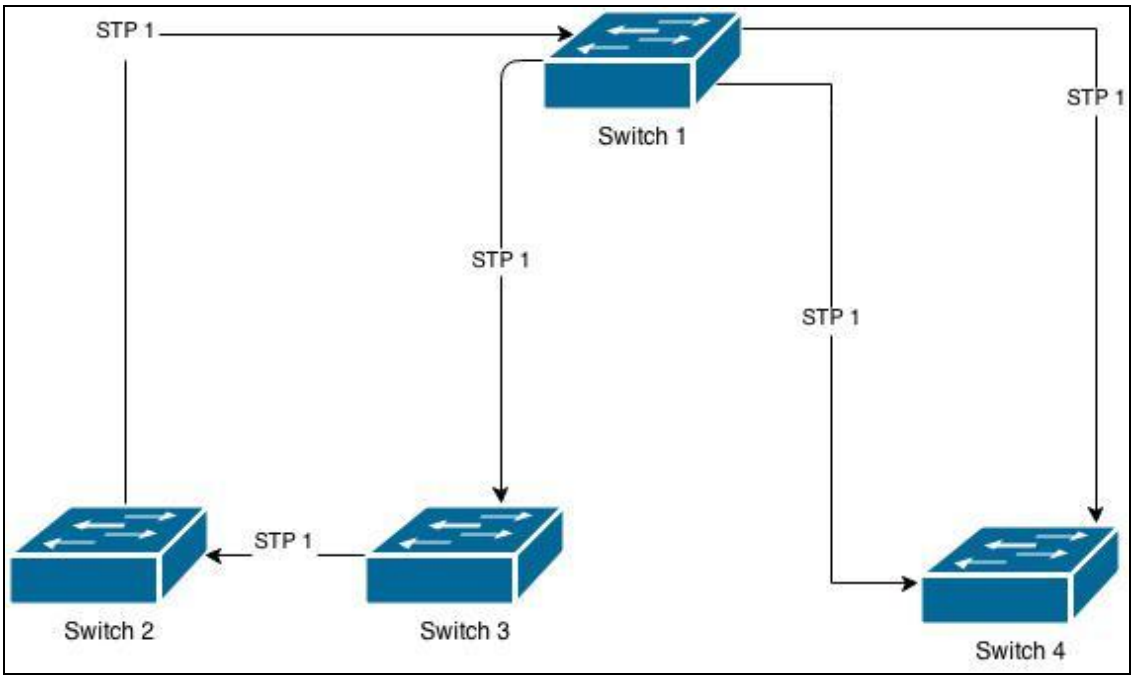
*Automatic Protection Switching*) homologado pelo ITU (*International Telecommunication Union*) no padrão G.8031.

Cada protocolo possui sua gama de topologias onde podem ser implementados, mas cada um possui particularidades que devem ser levadas em conta na hora da sua implementação. Ambos os protocolos podem ser utilizados em conjunto para atender necessidades distintas, de acordo com o objetivo dos implantadores.

Algumas topologias onde os protocolos STP e EAPS podem ser aplicados estão representadas nas Figuras 1, 2 e 3.

Na Figura 1 podemos ver uma topologia de quatro *switches*, onde temos somente uma instância de STP rodando e controlando as conexões redundantes.

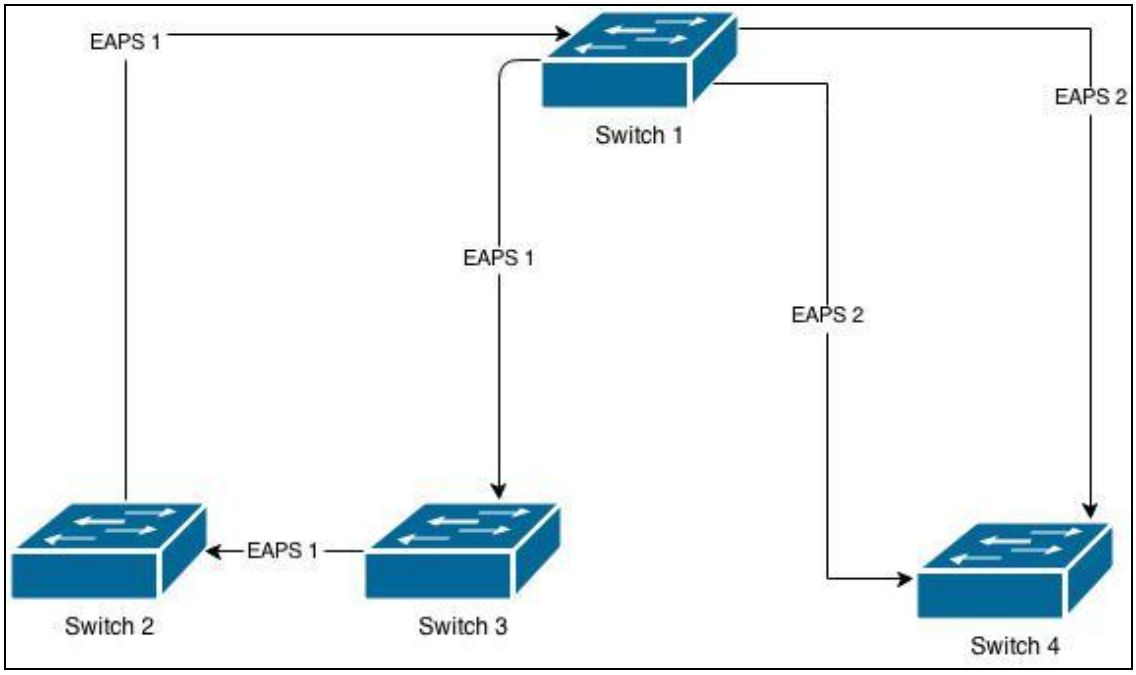
**Figura 1 – Topologia STP**




**Fonte: Autoria Própria**

Na Figura 2 temos a mesma topologia da Figura1, onde duas instâncias de EAPS estão rodando, isso ocorre devido à limitação de topologias em anel do EAPS que veremos no decorrer desse estudo.

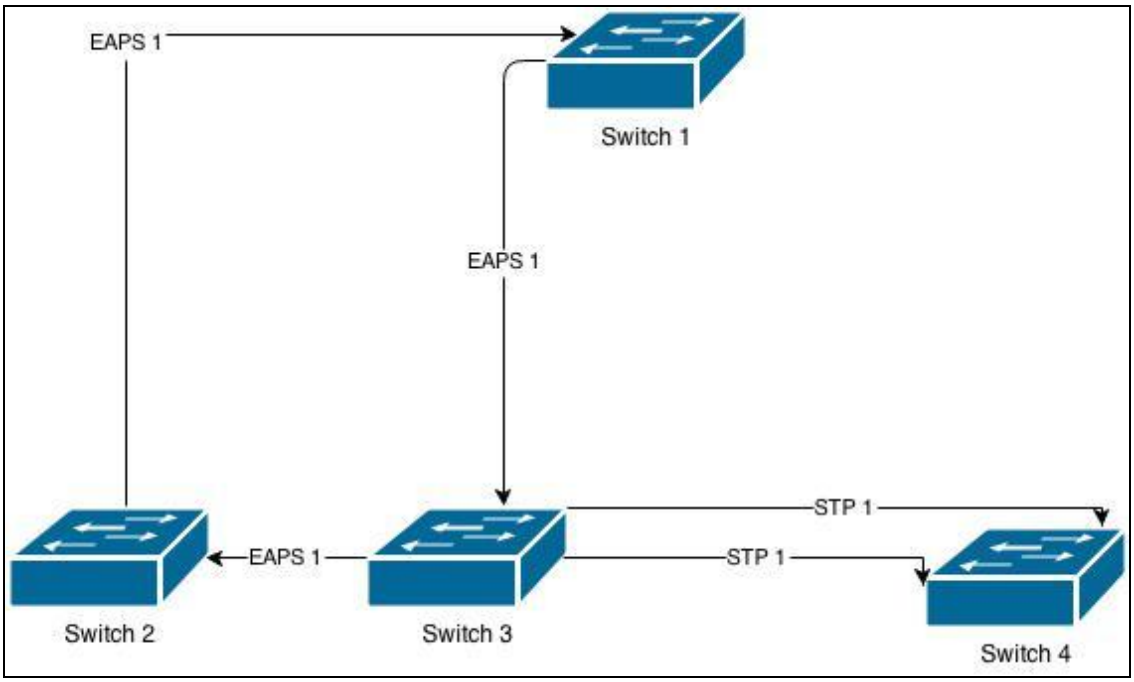
**Figura 2 – Topologia EAPS**




**Fonte: Autoria Própria**

Na Figura 3 temos uma topologia mista com STP e EAPS, ambas atuando em trechos distintos da rede. Isso pode ocorrer sem problemas, contanto que não acha sobreposição de interfaces e protocolos. Também trataremos essa questão mais a frente no decorrer desse estudo.

**Figura 3 – Topologia Mista**




**Fonte: Autoria Própria**

Pode-se notar através das topologias apresentadas, que existem várias situações onde podemos atuar com os dois protocolos em uma mesma topologia ou até mesmo com os dois ao mesmo tempo. Essa necessidade do uso de um ou outro protocolo é identificada através da análise da rede, de acordo com a necessidade dos administradores de redes.

# 3 STP - *SPANNING TREE PROTOCOL*

O protocolo *spanning tree* foi desenvolvido pela DEC (*Digital Equipament Corporation*) e posteriormente ele foi modificado e homologado pelo IEEE no padrão IEEE 802.1d, e é o protocolo de proteção *default* para as redes *ethernet*.

Como escrito por Marco Filippetti (2008, p. 96)

> A extinta DEC (Digital Equipament Corporation) foi a criadora original do protocolo Spanning Tree. O IEEE homologou posteriormente sua própria versão do protocolo, denominada IEEE 802.1d. Os switches Cisco utilizam a versão IEEE do protocolo Spanning Tree, que não é compatível com a versão original da DEC.

A principal função do STP é a inibição de *loops* nas redes *ethernet* decorrentes do uso de *links* redundantes (Marco Filipetti, 2008).

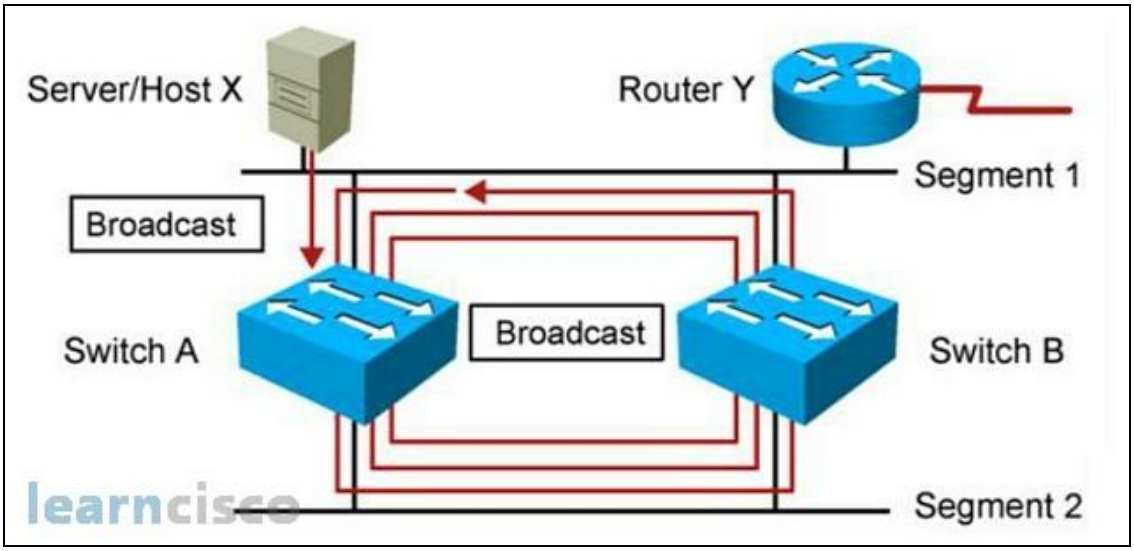
O *loop* de camada 2 nada mais é do que o tráfego entre *switches* de um ou mais *frames* que não conseguem alcançar o seu endereço MAC de destino. Isso faz com que ele vá de um *switch* para o outro e retorne novamente ao anterior, e assim sucessivamente, fazendo um caminho infinito até que alguma falha na rede ocorra e o impeça de continuar circulando entre os *switches*.

Como as redes precisam de conexões redundantes para o aumento da disponibilidade dos serviços conectados a elas, caso não tenhamos um protocolo de proteção atuando, *loops* de camada 2 podem acontecer. Os *loops* acontecem devido à duplicação dos *frames ethernet* quando o *switch* recebe um *frame* com um endereço MAC de destino desconhecido, ou com o destino para o MAC FF:FF:FF:FF:FF:FF que é o endereço de *broadcast* da camada 2.

Como mostra a Figura 4, essa duplicação de *frames* ocorre quando temos dois *switches* interligados por conexões redundantes e o protocolo STP não está habilitado. Neste cenário, o *switch* A ao receber um *frame* de *broadcast* ou com destino desconhecido irá encaminhar esse *frame* para todas as interfaces do *switch* menos a que o originou, e isso inclui as duas interfaces que interconectam com o *switch* B. Após esse envio, o *switch* B receberá esse *frame* duplicado, um por cada

interface conectada ao *switch* A. Ao receber esses dois *frames*, o *switch* B fará igual ao *switch* A e encaminhará para todas as portas do *switch* menos a que o originou, mandando novamente os dois *frames* de volta para o *switch* A. Essa ação resulta em um *loop* infinito, e a cada *loop* os *frames* são duplicados. Diferentemente dos pacotes de camada 3, os *frames* de camada 2 não possuem um TTL (*Time To Live*) e nesse cenário só irão parar de trafegar entre os *switches* na ocorrência de alguma falha nos equipamentos ou queda de alguma interconexão. Essa duplicação constante dos *frames* resulta no consumo da banda disponível e no aumento do processamento nos *switches*, por fim, causando o travamento dos equipamentos e consequentemente a queda da rede. Essa falha é conhecida como *broadcast storm*.

**Figura 4 – *Broadcast Storm***




**Fonte: LearnCisco, 2014**

O protocolo *spanning tree* resolve esse tipo de problema monitorando a rede e desativando os links redundantes, com isso evitando o *loop* de camada 2.

O funcionamento do protocolo *spanning tree* é claramente entendido na afirmação, “o STP monitora constantemente a rede identificando todos os links em atividade e certificando-se que loops de rede não ocorram, através da desativação de links redundantes” (Marco Filippetti, 2008, p. 96).

## 3.1 RECONHECIMENTO DA REDE

Para que o protocolo STP funcione corretamente e a redundância entre em ação sem falhas quando necessário, é extremamente importante que o protocolo reconheça a rede completamente. No STP esse reconhecimento é chamado de convergência. A fase convergência é extremamente importante para que o STP tenha o mapeamento de toda a rede, a fim de que possa controlar o encaminhamento do tráfego, que a redundância funcione corretamente e não ocorram *loops* na rede.

Assim que uma rede é instalada e os equipamentos são ligados, os *switches* que a compõem iniciam o processo de convergência, durante esse processo não há transmissão de dados, somente há a transmissão de BPDUs (*Bridge Protocol Data Units*). BPDUs são *frames* trocados pelos *switches* via *broadcast* com as informações necessárias para o reconhecimento da rede por eles e também para que seja eleito o *switch*-raiz (*root bridge*) que será o responsável por controlar e definir o funcionamento da rede de camada 2.

Esse processo está claramente descrito por Marco Filippetti (2008, p. 96)

> Em uma rede, apenas um switch-raiz pode existir. Todas as interfaces ou portas do switch-raiz são denominadas “portas designadas” (designated ports) e encontram-se sempre no modo de operação denominado “modo de encaminhamento” (forwarding-state). Interfaces operando em modo de encaminhamento podem tanto enviar quanto receber dados.
>
> Os outros switches presentes na rede são denominados não-raiz (non-root bridges). No caso desses switches, a porta com “menor custo” (determinada pela largura de banda do link em questão) ao switch-raiz é chamada de “porta-raiz” (root port) e também se encontrará em modo de encaminhamento, podendo enviar e receber dados. As portas restantes com menor custo ao switch-raiz serão denominadas “portas designadas”. Se em uma rede com diversos switches o custo de duas (ou mais) portas for o mesmo, o ID do switch deverá ser usado e será considerada designada a porta referente ao switch com o menor ID. As portas restantes serão consideradas portas não-designadas. Estas se encontrarão em modo bloqueio (blocking mode), não podendo enviar ou receber dados.

Toda vez que há uma alteração na rede, seja por falha em um dos *links*, falha em equipamentos ou inserção de novos equipamentos, isso acarreta novamente na execução do processo de convergência na rede.

## 3.2 ELEIÇÃO DO *SWITCH*-RAIZ, PORTA-RAIZ E PORTAS DESIGNIDAS

A eleição do *switch*-raiz ocorre através das trocas dos BPDUs entre os *switches*, e é feito com o uso do *Bridge* ID. O *switch* com o menor *Bridge* ID é eleito o *switch*-raiz e irá controlar o STP.

O *Bridge* ID é a combinação do MAC *Address* do *switch* com a prioridade (*priority value*). A prioridade *default* do STP homologado pelo IEEE é 32.768 (IEEE, 2004, p. 153), porém, ela pode ser alterada pelo administrador da rede.

Ao iniciar a convergência os *switches* através dos BPDUs analisam a prioridade de cada um, e o com a menor prioridade será eleito o *switch*-raiz. É muito comum os *switches* terem os valores de prioridade *default* configurados, e caso isso ocorra, o *switch* com o menor MAC *address* será o escolhido.

Já para a eleição das portas que ficaram em atividade ou ficaram bloqueadas, o STP utiliza basicamente o custo do *link*. Como escrito por Marco Filippetti (2008, p. 97), “para se determinar a(s) portas(s) que será(ão) usada(s) para comunicação com o switch-raiz, você precisa definir, antes o “custo” do link conectado à porta em questão. O protocolo STP faz isso se baseando na largura de banda disponível para cada link”.

Caso o custo do *link* seja o mesmo para as conexões, a porta de maior número será a porta bloqueada. Por exemplo, caso o *switch* possua conexões nas portas 1 e 2 e essas portas tenham o mesmo custo, a porta de número 2 será porta bloqueada.

*Switches* que compõem uma rede rodando STP podem ter várias portas designadas, porém, somente uma porta-raiz. A porta-raiz será a porta de menor caminho e custo até o *switch*-raiz.

## 3.3 ESTADOS DAS PORTAS NO STP

Quando um *switch* está rodando o protocolo *spanning tree*, as portas variam entre cinco estados, “[...] *disabled*, *blocking*, *listening*, *learning*, *forwarding*, e *broken* [...]” (IEEE, 2004, p. 153).

Isso é visto claramente no texto de Marco Filippetti (2008, p. 98)

> Blocking: Não encaminhará frames. Pode receber e analisar BPDUs. Todas as portas de um switch encontram-se em modo blocking quando ele é ligado;
>
> Listening: Recebe e analisa BPDUs para certificar-se de que não ocorrerão loops na rede antes de começar o encaminhamento de frames;
>
> Learning: Registra os endereços dos hardwares conectados às interfaces e forma a tabela MAC. Não encaminha frames, ainda;
>
> Forwarding: Envia e recebe frames.

O modo *broken* corresponde ao estado onde a porta está apresentando falha ou está indisponível (IEEE, 2004, p. 35).

## 3.4 FUNCIONAMENTO DO STP

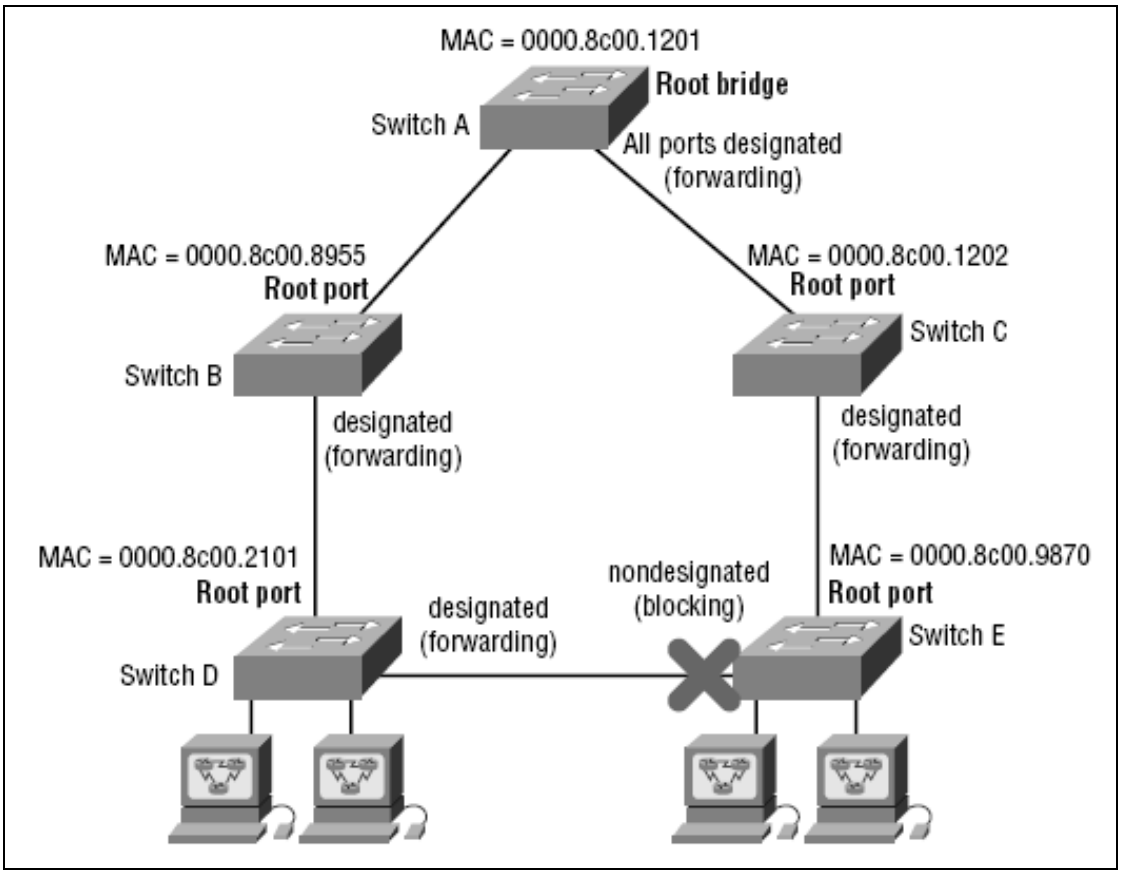
Em uma nova rede, após todo o processo de convergência, onde como explicado será eleito o *switch*-raiz, a porta-raiz de cada *switch*, as portas designadas e por fim a porta que ficará bloqueada, a rede entrará em funcionamento e começará a encaminhar os *frames*. Quando um novo equipamento é conectado a uma porta habilitada de um *switch*, essa porta passará do estado *blocking* para o estado *listening*. No estado *listening* irá verificar se recebe algum BPDU, não recebendo BPDU irá perceber que este equipamento não é um novo *switch* na rede e passará para o estado *learning* onde aprenderá o endereço MAC do novo equipamento e adicionará em sua tabela de endereços. A última ação do *switch* é passar a porta para o estado *forwarding*, onde irá liberar a porta para encaminhar e receber *frames* normalmente, com isso, adicionando um novo equipamento a rede.

No caso de uma porta ter uma nova conexão com um *switch*, ao receber os BPDUs, a rede irá parar de encaminhar *frames* e iniciará novamente o processo de convergência.

Tomando como cenário a topologia da Figura 5, com a rede já convergida, o *switch*-raiz monitora a rede através das BPDUs e procura a todo o momento alguma alteração, como por exemplo, a queda da conexão entre o *Swtich* C e o *Switch* E.

Após essa queda, o STP automaticamente parará o encaminhamento de frames da rede toda e iniciará o novamente o processo de convergência. Após mapear a rede novamente, a conexão entre o *Switch* E e o *Switch* D será liberada para o tráfego e a rede voltará a atividade normal. Quando essa conexão for restabelecida, novamente ocorrerá a convergência.

**Figura 5 – Funcionamento STP**




**Fonte: BrainMatics, 2014**

Todo esse processo se faz necessário, para que a tabela de endereços MAC de cada *switch* seja consistente com as dos demais *switches*, evitando falhas. O tempo desse processo pode variar de acordo com o tamanho da rede e capacidade de processamento dos equipamentos, mas leva em média 50 segundos (Marco Filippetti, 2008, p. 98).

# 4 EAPS - *ETHERNET AUTOMATIC PROTECTION SWITCHING*

O protocolo EAPS foi criado pela Extreme Networks e posteriormente homologado pelo ITU no padrão G.8031 de 2008. O protocolo foi criado com o intuito de trazer o padrão de proteção APS, utilizado em redes SDH/SONET com topologias em anel, para as redes *ethernet*. Com isso, reduzindo o tempo de chaveamento (*failover*) para os padrões das redes PSTN (*Public Switched Telephone Network*) e aumentando a disponibilidade das redes. Essa alta disponibilidade e velocidade do protocolo aumentou o interesse dos fabricantes e hoje ele é um dos protocolos mais usados nas redes *Metro Ethernet* pelo mundo, sendo recomendado pelo MEF (*Metro Ethernet Forum*).

Segundo a empresa Extreme Networks (2012, p. 2), “o EAPS permite que redes IP tenham o nível de resiliência e disponibilidade que os usuários necessitam para suas tradicionais redes de voz”, e também afirma que “além do EAPS permitir *failover transparent* aos usuários, ligações VoIP não caem e transmissões de vídeos não congelam ou travam” (Extreme Networks, 2012, p. 2).

Como foi criado com o intuito de imitar a proteção dos anéis SDH/SONET o EAPS G.8031 possui uma atuação básica e sua topologia é limitada a anéis simples, porém, sem limites de equipamentos. Nas topologias em anel sempre temos uma via principal e uma via de proteção, topologia essa chamada de linear 1+1.

Segundo afirma a empresa Datacom (2013, p. 72)

> [...] EAPS foi desenvolvido para atender somente as topologias em anel, normalmente utilizadas em redes ethernet metropolitanas. Devido a grande capacidade de transmissão das redes Metro Ethernet existe a necessidade de haver redundância/proteção do tráfego em caso de falha.

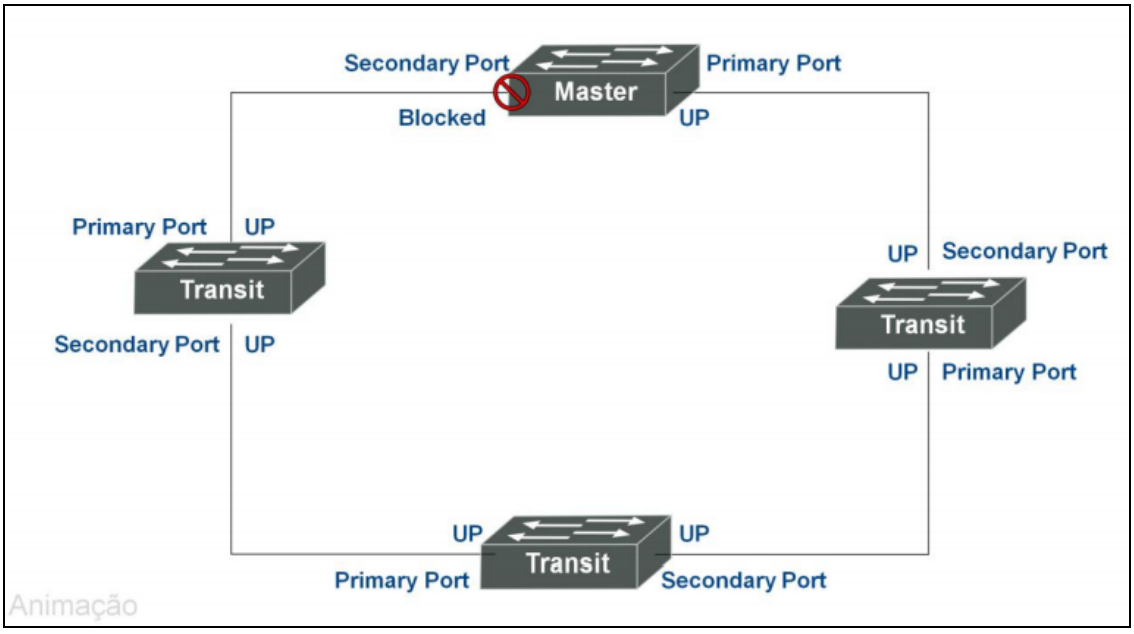
O protocolo EAPS, semelhante ao STP também previne as redes de camada 2 dos *loops* ocasionados pelo uso de conexões redundantes, falha essa que já foi explicada no capitulo sobre o protocolo STP.

## 4.1 RECONHECIMENTO DA REDE

O protocolo EAPS, diferentemente do STP, não faz o reconhecimento da rede automaticamente nos equipamentos que possuem o protocolo habilitado, caso exista um erro de configuração, *loops* podem ocorrer e derrubar a rede devido o aumento da utilização de CPU causado pelo *brodcast storm*, conforme explicado no capítulo anterior.

O mapeamento da rede é feito totalmente manual, ocasionando assim um grande *handwork* no processo de configuração do protocolo. Como podemos ver na Figura 6, necessitamos indicar para o protocolo qual é a interface primária – interface que ficará ativa, e será por onde o trafego irá passar – e a interface secundária – interface essa que ficará bloqueada no *switch master*, e entrará em atividade para assumir o transporte do tráfego quando alguma falha ocorrer com a interface primária.

**Figura 6 – Topologia EAPS**




**Fonte: Datacom, 2013**

Semelhantemente ao STP, o EAPS também possui um *switch* principal que será o responsável pelo controle do protocolo e o monitoramento da rede. Segundo

afirma a empresa DATACOM (2013, p. 72), o “[...] EAPS tem um equipamento designado como "MESTRE". Todos os outros equipamentos do anel são referidos como equipamentos "TRANSITO"”. No EAPS o monitoramento da rede é feito pelo *switch* mestre utilizando-se de frames de sinalização, similares aos BPDUs, porém, não os utiliza para mapeamento da rede.

Apesar de se perder em agilidade na expansão da rede, devido à necessidade de mapeamento manual, ao utilizar o protocolo EAPS ganha-se em segurança da rede e controle das alterações realizadas. Também devido à configuração manual do EAPS, podemos ativá-lo sem a necessidade de parar a rede ou derrubar o tráfego, diferentemente do STP onde o processo automático de convergência interrompe o tráfego na rede até que toda a rede esteja mapeada.

## 4.2 ELEIÇÃO DO *SWITCH* MASTER, PORTA PRIMÁRIA E SECUNDÁRIA

Conforme já explicitado anteriormente, todo o mapeamento da topologia do EAPS é feito manualmente. Portanto, após uma minuciosa análise da topologia, o administrador da rede define qual o *switch* será o *master*, e os equipamentos restantes serão os *switches transit*. Essa definição é normalmente baseada na capacidade de processamento e na capacidade de *throughput* dos *switches* que compõem a rede, ou seja, o *switch* mais robusto e com maior capacidade será o escolhido como o *switch master*. Esse *switch* é colocado em uma posição estratégica na rede, onde controlará as ações do protocolo EAPS.

Assim como a eleição dos *switches master* e *transit*, as portas primária e secundária da cada equipamento são definidas manualmente pelo administrador. Essa definição segue uma lógica básica como também pode-se ver na Figura 6, a porta primária de um *switch* sempre é conectada a porta secundária do próximo, e assim sucessivamente com os outros.

## 4.3 ESTADOS DAS PORTAS NO EAPS

Nos equipamentos rodando o protocolo EAPS temos basicamente dois estados onde as portas podem se encontrar *up* e *blocked*. Onde naturalmente *up* é o estado em funcionamento normal, onde a porta envia e recebe os *frames* referentes ao tráfego de dados e também os *frames* de controle do EAPS. Já a porta no estado *blocked*, tem seu tráfego bloqueado para os *frames* de dados, mas envia e recebe os *frames* de controle do EAPS.

O estado *blocked* só pode ocorrer em uma das portas do *switch master*, pois a porta designada como primária ficará *up* e porta secundária ficará *blocked*, evitando assim os *loops* de camada 2. Já nos equipamentos *transit*, ambas as portas estarão sempre *up*. Vemos esse cenário também na Figura 6.

## 4.4 FUNCIONAMENTO DO EAPS

“O funcionamento do EAPS consiste na criação inicial de um domínio EAPS para um anel” (Datacom, 2013, p. 73). O domínio EAPS é baseado em uma *VLAN* de Controle, onde essa *vlan* será a mesma em todos os *switches* envolvidos na topologia desse domínio. É necessário que esse domínio seja o mesmo em cada equipamento da topologia, pois um *switch* pode pertencer a mais de um domínio por vez, ou seja, pode fazer parte de mais de uma topologia EAPS ao mesmo tempo. Isso pode ocorrer por diversos motivos, como balanceamento de carga em uma mesma topologia ou duas topologias com funcionamento apartado que tenham um *switch* em comum, como visto na Figura 2.

Após a criação desse domínio, é feito a definição do tráfego de dados que será protegido por essa topologia EAPS. Tráfego esse que também é definido com o uso de *vlans*, conhecido como *PROTECTED VLANS*. Em seguida, como visto anteriormente, é feito a indicação do *switch master* e dos *switches transit*. Também são definidas as portas primárias e secundárias de cada *switch*, onde no *switch master* a primária fica em funcionamento normal e a secundária bloqueada para o tráfego de dados. Após todo esse processo, a rede entra em funcionamento.

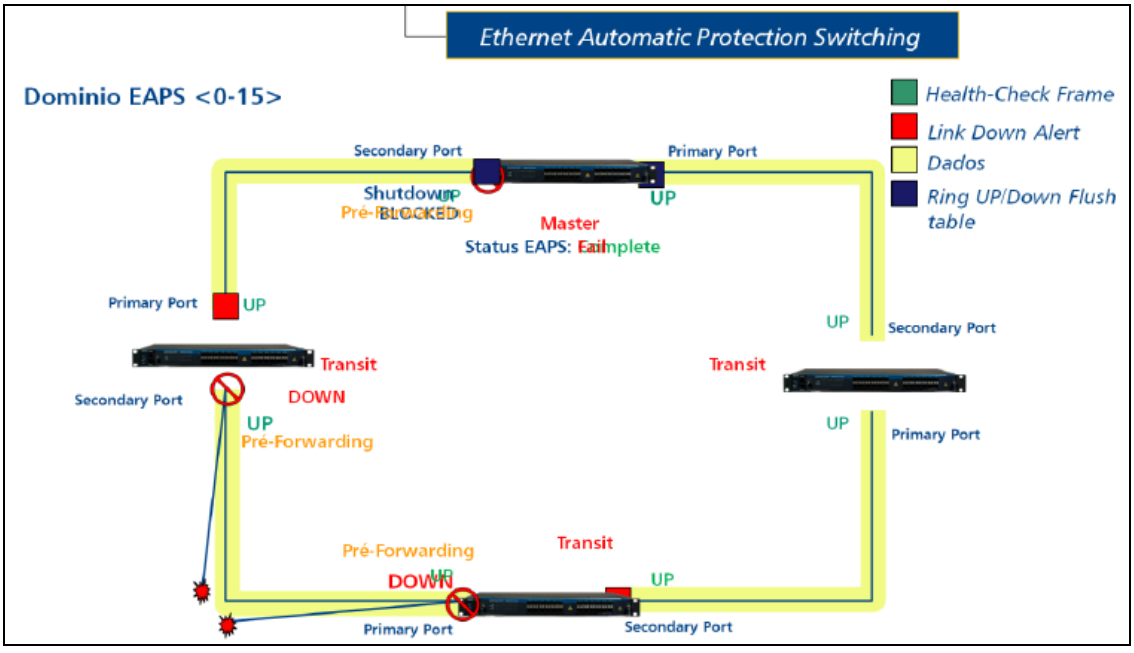
Com a rede em funcionamento como se pode ver na Figura 7, o *switch master* começa a exercer a sua função de “[...] “MASTER NODE”, enquanto todos os outros *switches* do anel serão designados “TRANSIT NODES”” (Datacom, 2013, p. 73). O *switch master* através da *vlan* de controle monitora a rede a procura de falhas, então “se o MASTER NODE detecta uma falha no link (failed state), ele desbloqueia a SECONDARY PORT e permite o encaminhamento do tráfego de dados por esta porta.” (Datacom, 2013, p. 73).

Essa ação fica clara na afirmação da empresa Datacom (2013, p. 74)

> Quando uma falha de link ocorre uma TRAP Msg é enviada pelos TRANSIT NODES através da vlan de controle e o estado de falha é declarado pelo MASTER NODE, o que acarreta no desbloqueio da SECONDARY PORT [...].

Após o chaveamento do tráfego para porta secundária, o *switch master* continua monitorando a rede. Caso o *switch master* receba uma sinalização de restabelecimento da topologia, ele retorna o tráfego para a porta primária, normalizando a rede.

**Figura 7 – Funcionamento EAPS**




**Fonte: Datacom, 2013**

Todo o processo entre a detecção de falhas e o chaveamento do tráfego para a porta secundária é muito rápido, “[...] sendo este da ordem de mili segundos (< 50m), o que o torna um protocolo altamente seguro e escalável” (Datacom, 2013, p. 72).

# 5 CONFIGURAÇÃO DOS PROTOCOLOS

Neste capitulo, será visto a configuração básica dos protocolos STP e EAPS, para isso será usado como base o equipamento DM4100 do fabricante Datacom. Como se pode ver na Figura 8, o DM4100 possui várias versões de *hardware* disponíveis, mas o modelo de configuração não se altera entre eles.

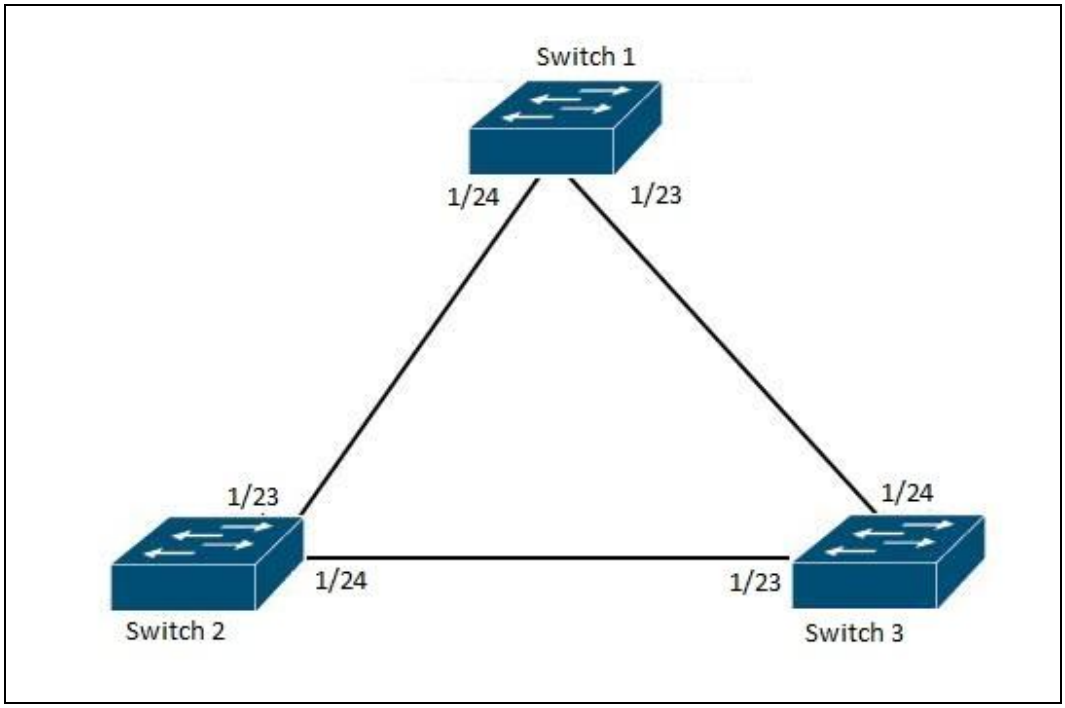
O DM4100 pode atuar tanto com o protocolo STP como com o EAPS, ou caso seja necessário com os dois protocolos ao mesmo tempo.

Para a demonstração dos *scripts*, será usada como base a topologia demonstrada na Figura 9.

**Figura 8 – DM4100**


**Fonte: Datacom, 2013**

**Figura 9 – Topologia Modelo**




**Fonte: Autoria Própria**

## 5.1 CONFIGURAÇÕES STP

Por ser o protocolo de proteção padrão dos *switches*, o STP já vem habilitado por *default* no DM4100. Porém, pode ser modificado para atender as necessidades do administrador.

Nosso *script* de configuração tomará como base uma rede nova e sem tráfego.

Usando como cenário a topologia da Figura 9 e assumindo que todos os *switches* sejam DM4100, é possível ver as configurações necessárias para que o STP funcione corretamente.

### 5.1.1 Configurações *Switch* 1

**Passo 1**

Habilitar o modo se configuração.

**DM4100_SWITCH-01# *configure***

**Passo 2**

Criar um conjunto de *vlans* de dados, ou seja, criar um grupo com as *vlans* destinadas ao tráfego de dados.

**DM4100_SWITCH-01(config)# *vlan-group 1 vlan all***

**Passo 3**

Definir o modo de operação do STP criando a instância 1. Depois forçar o *Switch* 1 como *root-bridge* configurando a sua prioridade como 0. Após isso, atribuir o grupo de tráfego criado pelo *vlan-group* 1 a instância 1 do STP para que sejam protegidas nela.

**DM4100_SWITCH-01(config)# *spanning-tree mode stp***

**DM4100_SWITCH-01(config)# *spanning-tree 1 priority 0***

**DM4100_SWITCH-01(config)# *spanning-tree 1 vlan-group 1***

**Passo 4**

Habilitar o modo configuração em todas as interfaces e habilitar o *spanning tree* para atuar em todas as interfaces do *switch*.

**DM4100_SWITCH-01(config)# *interface ethernet all***

**DM4100_SWITCH-01(config-if-eth-1/1-to-1/24)# *spanning-tree 1***

### 5.1.2 Configurações *Switch* 2 e *Switch* 3

**Passo 1**

Habilitar o modo se configuração.

**DM4100_SWITCH-0X(config)# *configure***

**Passo 2**

Criar um conjunto de *vlans* de dados, ou seja, criar um grupo com as *vlans* destinadas ao tráfego de dados.

**DM4100_SWITCH-0X(config)# *vlan-group 1 vlan all***

**Passo 3**

Definir o modo de operação do STP criando a instância 1. Após isso, atribuir o grupo de tráfego criado pelo *vlan-group* 1 a instância 1 do STP para que sejam protegidas nela. Obs.: Não alteramos a prioridade do STP no *Switch* X, pois definimos que o *Switch* 1 será o *root-bridge* da rede.

**DM4100_SWITCH-0X(config)# *spanning-tree mode stp***

**DM4100_SWITCH-0X(config)# *spanning-tree 1 vlan-group 1***

**Passo 4**

Habilitar o modo configuração em todas as interfaces e habilitar o *spanning tree* para atuar em todas as interfaces do *switch*.

**DM4100_SWITCH-0X(config)# *interface ethernet all***

**DM4100_SWITCH-0X(config-if-eth-1/1-to-1/24)# *spanning-tree 1***

## 5.2 CONFIGURAÇÕES EAPS

A configuração do EAPS é bem simples, e diferentemente do STP não vem habilitado nos equipamentos, e caso se queira usá-lo é necessário realizar toda a sua configuração.

Nosso *script* de configuração toma como base uma rede nova e sem tráfego.

Usando também como cenário a topologia da Figura 9 e assumindo que todos os switches sejam DM4100 com suas portas 23 e 24 ligadas ao anel, serão vistas as configurações necessárias para que o EAPS funcione corretamente.

### 5.2.1 Configurações Switch 1

**Passo 1**

Habilitar o modo se configuração.

**DM4100_SWITCH-01(config)# *configure***

**Passo 2**

Criar a *vlan* de controle do EAPS e definir um nome para identificação.

**DM4100_SWITCH-01(config)# *interface vlan 4094***

**DM4100_SWITCH-01(config-if-vlan-4094)# *name EAPS01***

**Passo 3**

Criar um conjunto de *vlans* de dados, ou seja, criar um grupo com as *vlans* destinadas ao tráfego de dados. Após isso, remover a *vlan* de controle do grupo de *vlans* destinadas ao tráfego de dados.

**DM4100_SWITCH-01(config)# *vlan-group 1 vlan all***

**DM4100_SWITCH-01(config)#** ***no vlan-group 1 vlan 4094***

**Passo 4**

Criar o domínio EAPS 1 e definir um nome para identificação do EAPS. Após isso, definir o *Switch* 1 como *master* da topologia EAPS. Definir a porta primária e a secundária da topologia, e depois indicar qual a *vlan* destinada para controle do EAPS. Por ultimo, informamos qual será o grupo de *vlans* a ser protegido pelo EAPS.

**DM4100_SWITCH-01(config)#** ***eaps 1***

**DM4100_SWITCH-01(config)#** ***eaps 1 name EAPS1***

**DM4100_SWITCH-01(config)#** ***eaps 1 mode master***

**DM4100_SWITCH-01(config)#** ***eaps 1 port primary ethernet 1/23***

**DM4100_SWITCH-01(config)#** ***eaps 1 port secondary ethernet 1/24***

**DM4100_SWITCH-01(config)#** ***eaps 1 control-vlan id 4094***

**DM4100_SWITCH-01(config)#*eaps 1 protected-vlans vlan-group 1***

5.2.2 Configurações Switch 2 e Switch 3

**Passo 1**

Habilitar o modo se configuração.

**DM4100_SWITCH-0X(config)#** ***configure***

**Passo 2**

Criar a *vlan* de controle do EAPS e definir um nome para identificação.

**DM4100_SWITCH-0X(config)# *interface vlan 4094***

**DM4100_SWITCH-0X(config-if-vlan-4094)# *name EAPS01***

**Passo 3**

Criar um conjunto de *vlans* de dados, ou seja, criar um grupo com as *vlans* destinadas ao tráfego de dados. Após isso, remover a *vlan* de controle do grupo de *vlans* destinadas ao tráfego de dados.

**DM4100_SWITCH-0X(config)# *vlan-group 1 vlan all***

**DM4100_SWITCH-0X(config)# *no vlan-group 1 vlan 4094***

**Passo 4**

Criar o domínio EAPS 1 e definir um nome para identificação do EAPS. Após isso, definir o *Switch* X como *transit* da topologia EAPS. Definir a porta primária e a secundária da topologia, e depois indicar qual a *vlan* destinada para controle do EAPS. Por ultimo, informamos qual será o grupo de *vlans* a ser protegido pelo EAPS.

**DM4100_SWITCH-0X(config)# *eaps 1***

**DM4100_SWITCH-0X(config)# *eaps 1 name EAPS1***

**DM4100_SWITCH-0X(config)# *eaps 1 mode transit***

**DM4100_SWITCH-01(config)# *eaps 1 port primary ethernet 1/23***

**DM4100_SWITCH-01(config)# *eaps 1 port secondary ethernet 1/24***

**DM4100_SWITCH-01(config)# *eaps 1 control-vlan id 4094***

**DM4100_SWITCH-01(config)#*eaps 1 protected-vlans vlan-group 1***

# 6 ESTUDO DE CASO

A empresa utilizada no estudo de caso é uma empresa de origem brasileira, atua no setor de telecomunicações e será tratada pelo nome fictício de ETHRIO. A ETHRIO atua em âmbito nacional e possui mais de 6 mil funcionários, entre colaboradores e parceiros. A empresa em questão possui milhares de quilômetros de redes, de vários tipos: fibra óptica, rádio micro-ondas, satélite. A ETHRIO também possui interconexões internacionais, o que facilita o escoamento do trafego internacional de dados e a diminuição dos custos, devido a não necessidade de contratação de circuitos terceiros.

Parte de um grupo internacional de telecomunicações, a ETHRIO é uma das mais expressivas e a mais experiente das empresas que atuam no mercado brasileiro. Acostumada a grandes projetos, é a empresa mais atuante no fornecimento de soluções de conexão para grandes eventos e fornecedora regular do governo nacional.

A ETHRIO é uma corporação extremamente preocupada com os avanços tecnológicos e o seu atual foco são redes ethernet metropolitanas, conhecidas como rede *Metro Ethernet*. As redes Metro Ethernet ganharam adeptos, por trazer o já conhecido modelo de redes *ethernet* dos ambientes *LAN* (*Local Area Network*) para os ambientes *WAN* (*Wide Area Network*). As redes *Metro Ethernet* crescem no mundo todo e a sua utilização é vista com bons olhos por grande parte das empresas de telecomunicações, devido a seu baixo custo de implantação e altas taxas de transferência de dados atingidas com elas.

Pode-se ver que a ETHRIO é uma empresa extremamente dinâmica, que investe em seu futuro e acredita fielmente no crescimento do mercado brasileiro.

## 6.1 HISTÓRICO

1965 – É fundada no Rio de Janeiro como empresa do setor público.

1967 – A ETHRIO inicia a criação da sua estação de comunicação por satélites.

1969 – Primeira transmissão comercial de televisão via satélite.

1970 – Primeira transmissão de uma Copa do Mundo ao vivo no Brasil.

1972 – Primeira transmissão de TV em cores no Brasil.

1975 – Inicia a operação de ligações internacionais do Brasil para outros países.

1980 – Criação da primeira rede de dados exclusivos da América do Sul.

1984 – Inaugura sua rede de Comutação por Pacotes.

1985 – Coloca em órbita seu primeiro satélite.

1986 – Coloca em órbita seu segundo satélite.

1993 – Inaugura a primeira rede de Fibra Óptica.

1994 – Inaugura sua primeira interconexão por fibras ópticas internacional, interconectando Brasil e Estados Unidos da América.

1997 – Inicia um processo de ampliação de duas redes, a fim de atender a crescente demanda de acessos para o uso da Internet.

1998 – A empresa é privatizada.

1999 – A Internet chega às residências, e isso faz com que a empresa siga com o aumento e modernização de suas redes.

2003 – Inicia seu investimento em redes MPLS.

2004 – A empresa é incorporada por um grupo de investidores focado no mercado de Telecomunicações.

2013 – Anuncia inicio da sua operação no mercado de Cloud Computing.

2014 – Inicia um grande processo de modernização da rede. Foco em redes Metro Ethernet, com acessos em Ethernet e GPON.

## 6.2 REDES *ETHERNET* DE ACESSO

Chamamos de rede de acesso, as redes que interligam o cliente final ao ponto de concentração da operadora. Pode-se entender claramente esta definição na afirmação, “As redes de acesso interligam os usuários com a rede mundial. Sua função principal é prover o acesso dos mesmos a informações de dados, voz e vídeo através de serviços prestados por operadoras.” (BARROS, 2007; TELECO, 2010).

As redes de acesso que mais recebem investimento na ETHRIO são as redes GPON (*Gigabit Passive Optical Network*) e *Ethernet*. O foco do nosso estudo serão as topologias de redes de acesso *ethernet* da ETHRIO. A rede de acesso *ethernet*, não é nada mais do que a mesma topologia de *switches* utilizada em ambientes *lan*, porém, em uma escala maior, com equipamentos mais robustos e confiáveis. O cabeamento usado são fibras ópticas. Essa troca ocorre devido à limitação de até 100 metros do cabo *ethernet* elétrico e também a total ausência de interferência dos campos eletromagnéticos. Fibras ópticas quando combinada com interfaces potentes, podem atingir quilômetros sem a necessidade de repetidor.

A ETHRIO está migrando gradativamente as suas redes SDH/SONET para o ambiente *ethernet*, e tem adquirido um grande número de equipamentos. Sua rede de acesso *ethernet* é basicamente composta por *switches* do fabricante Datacom.

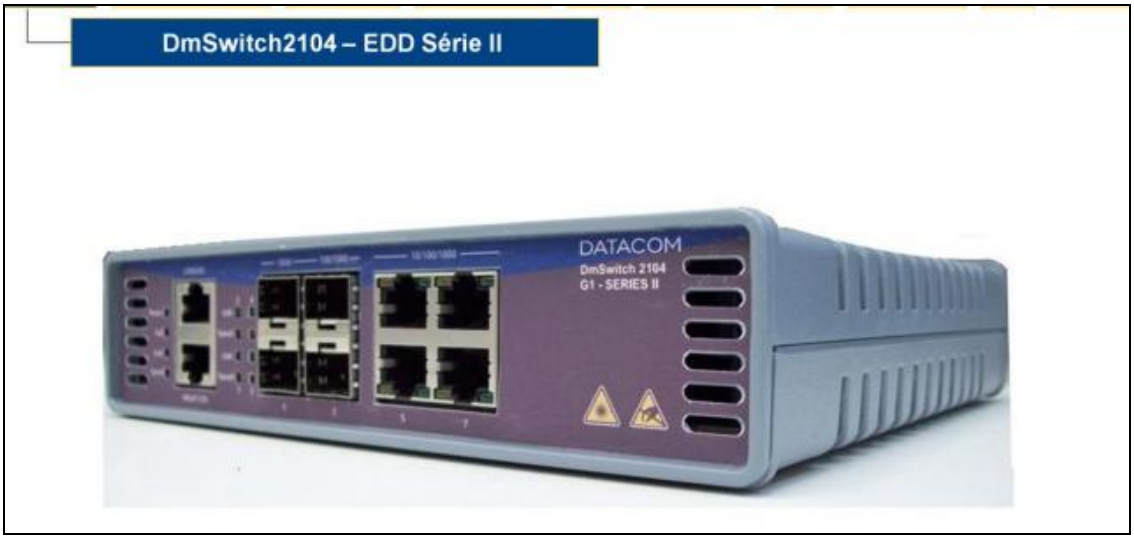
Para instalações nos clientes, é utilizado o equipamento DM2104 G2 – EDD Series II. O DM2104 possui as seguintes especificações:

- 4 portas 10/100/1000Base-TX (RJ45)
- 2 portas ópticas 1000Base-X (SFP)
- 2 portas ópticas 100Base-FX/1000Base-X (SFP)
- 1 porta CONSOLE para gerência via serial RS232

- 1 porta MNGT 10/100Base-TX (RJ45) para gerência
- Entrada POWER AC/DC com seleção automática

O *bayface* do equipamento é apresentado na Figura 10:

**Figura 10 – DM2104 G2 – EDD Series II**




**Fonte: Datacom, 2013**

Para instalações nos pontos de concentração, é utilizado o equipamento DM4001 chassis. O DM4001 como visto na Figura 11, é um equipamento modular. E possui as especificações:

- Compatível com todas as placas de interfaces da linha DM4000
- Chassis suporta 1 placa de interface
- Entrada redundante de alimentação -48VDC, com fontes redundantes em cada módulo de interface

**Figura 11 – DM4001 Chassis**


**Fonte: Datacom, 2013**

Equipamentos modulares são extremamente importantes em operações de grande porte, pois podem ser customizados da maneira mais adequada para cada ponto de concentração. Com equipamentos modulares, a expansão da rede também é facilitada e mais dinâmica.

A placa mais utilizada na topologia da ETHRIO é a DM4000 ETH24GX + 2x10G – MPLS, apresentada na Figura 12. Seguem especificações:

- 24 portas ópticas 1000Base-X (SFP)
- 2 portas ópticas 10G (XFP)

**Figura 12 – DM4000 ETH24GX + 2x10G – MPLS**

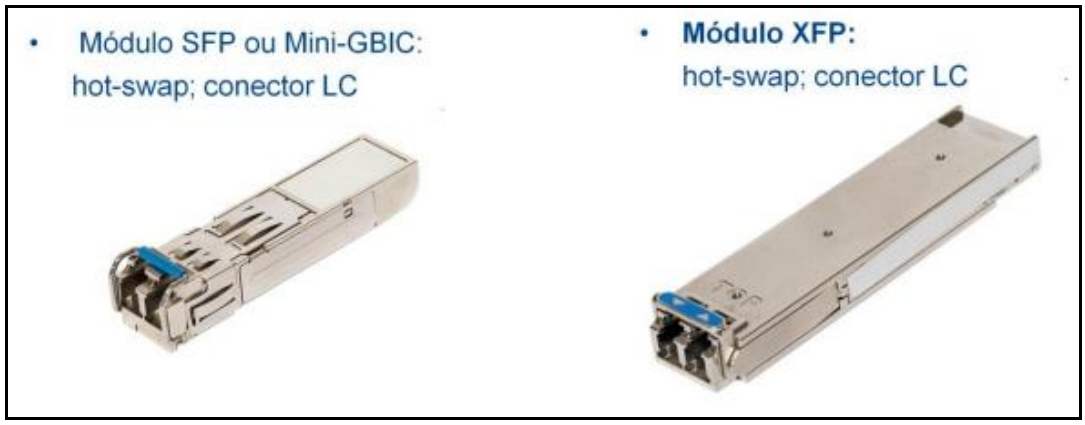

**Fonte: Datacom, 2013**

Os módulos SFP e XFP são adquiridos e utilizados pela ETHRIO de acordo com a necessidade de banda, distancia e quantidade de conexões.

Módulos SFP e XFP para operações de grande porte são de extrema importância, pois não limita o equipamento e podem ser trocados de acordo com as necessidades dos projetos. Cada interface também pode usar um módulo diferente, deixando assim o switch extremamente versátil.

A ETHRIO utiliza diversos tipos, alguns deles podem ser vistos nas Figuras 13, 14 e 15.

**Figura 13 – Módulos SFP e XFP Ópticos**




**Fonte: Datacom, 2013**

**Figura 14 – Módulo SFP Elétrico**


**Fonte: Datacom, 2013**

**Figura 15 – Módulos SFP Ópticos Bidirecional**


**Fonte: Datacom, 2013**

Os equipamentos do fabricante Datacom, assim como a maioria dos equipamentos fabricados para empresas de Telecomunicações, são *hot-swap*. Equipamentos *hot-swap* aceitam troca de módulos SFP, placas e em alguns casos fontes de energia redundantes, com o equipamento em operação. Isso facilita a ativação de novas conexões, expansões de *links* e principalmente as manutenções nos equipamentos em produção.

## 6.3 PROBLEMA ENCONTRADO

A topologia utilizada pela ETHRIO em sua rede de acesso *ethernet* é composta basicamente anéis entre os concentradores, com anéis ou conexões lineares com os seus clientes. A definição da conexão redundante até o cliente é definido pelo pedido feito, ou seja, o quanto o cliente tem de recursos para pagar pela alta disponibilidade do serviço.

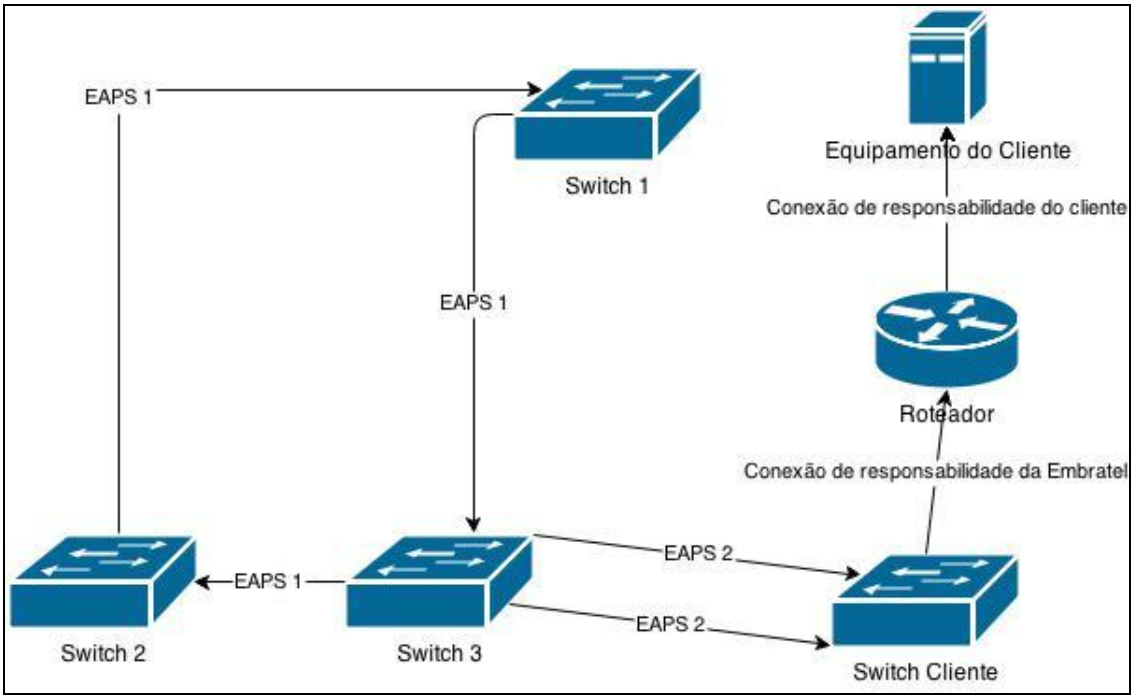
Para conexões redundantes o SLA (*Service Level Agreement*) acordado é de retorno do serviço em até 2 horas, ou seja, após a notificação da queda a ETHRIO tem esse prazo para restabelecer o serviço. Para conexões não redundantes, esse o SLA acordado é de 4 horas.

O foco do trabalho são os clientes que possuem conexões totalmente redundantes. Clientes esses que seus negócios dependem da alta disponibilidade do serviço e para isso pagam mais.

Como se pode ver na Figura 16, toda a topologia de acesso dos concentrados até os clientes são redundantes, ou seja, possuem dupla abordagem até o *switch* instalado no cliente. Toda a topologia de *switches* é protegida pelo protocolo EAPS, o que garante um chaveamento menor que 50 milissegundos. Esse tempo ínfimo de chaveamento faz com que o cliente não sinta uma possível queda de um *link* e permite a ETHRIO que recupere esse *link* sem maiores problemas. Tendo em vista que toda a rede é monitorada e casos de queda são tratados através de alarmes gerados.

Porém, a última conexão do *switch* com o roteador (equipamento que também pertence à ETHRIO) não possuem dupla abordagem. Esse é um ponto de falha extremamente frágil. Apesar de toda a topologia possuir conexões redundantes, caso um problema ocorra nessa conexão, dificilmente a ETHRIO conseguirá cumprir o SLA de 2 horas.

**Figura 16 – Topologia ETHRIO Atual**




**Fonte: Autoria Própria**

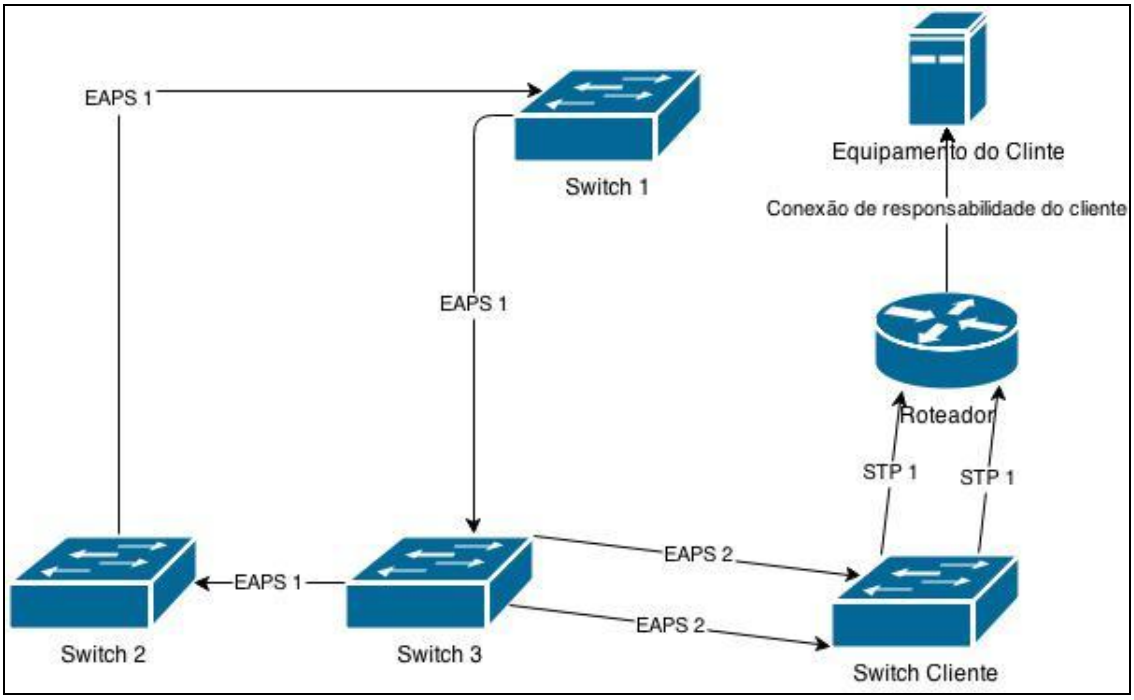
## 6.4 SOLUÇÃO PROPOSTA

Para solucionar esse problema, o ideal seria adicionar conexões redundantes também entre o *switch* no cliente e o roteador. Fazendo com que se mantenha a alta disponibilidade do serviço em todos os trechos de responsabilidade da ETHRIO.

Ao adicionar conexões redundantes, será necessária a aplicação de um protocolo de proteção. O protocolo EAPS é descartado, pois devido a ETHRIO utilizar roteadores de vários fabricantes, alguns não possuem a função EAPS disponível. Já o STP é um protocolo extremamente difundido e está disponível em todos os equipamentos utilizados pela ETHRIO. Como visto anteriormente, o STP pode ser utilizado em conjunto com o EAPS no mesmo *switch*, contanto que sejam em interfaces distintas. Apesar de o tempo de convergência do STP não ser baixo, devido à topologia simples de apenas dois equipamentos esse tempo com certeza ficará abaixo da média.

Portanto, como se pode ver na topologia proposta na Figura 17, pode-se usar o STP para a conexão dentro do cliente e o alto tempo de chaveamento é compensado pela alta disponibilidade dos serviços.

**Figura 17 – Topologia ETHRIO Proposta**




**Fonte: Autoria Própria**

# 7 CONSIDERAÇÕES FINAIS

O objetivo geral desse estudo foi conhecer os funcionamentos básicos dos protocolos STP e EAPS do ponto de vista de suas utilizações como meio de controlar conexões redundantes em redes *ethernet*.

Ambos os protocolos possuem muito mais funcionalidades do que as tratadas por esse trabalho, porém, não foram aprofundados devido ao foco proposto.

No decorrer da pesquisa foi visto um pouco da evolução das redes *ethernet* e seus principais colaboradores. Também foi possível apreciar o quanto essa evolução foi baseada pelo crescimento do uso das redes de computadores e da necessidade de confiabilidade das empresas e organizações nessas redes.

Apesar de a segurança das redes de comunicação ser uma constante, a disponibilidade é a maior preocupação existente para as corporações, pois não adianta investir dinheiro na segurança de uma rede que não “para em pé”. Portanto, os protocolos apresentados nesse estudo e suas funcionalidades são de extrema importância para que as corporações não percam a comunicação com suas filiais, seus clientes e também com o mundo.

Por fim, no estudo de caso foi possível analisar a aplicação dos protocolos de proteção de redes *ethernet* em um cenário real, implementado por uma grande empresa no atendimento de seus clientes.

Na topologia da ETHRIO, foi identificado um ponto de falha na proteção da topologia de acesso *ethernet*. Foi visto que essa falha acarretaria na demora do restabelecimento do serviço do cliente em caso de falha na infraestrutura interna, ocasionando muitos problemas à empresa. A solução proposta para a resolução desse problema foi o uso da topologia mista STP e EAPS, e isso se mostrou eficiente, pois se conseguiu sanar o problema deixando toda a topologia da ETHRIO completamente redundante. Com isso, se pode ver que com projetos bem estruturados a aplicação desses protocolos podem suprir as necessidades e transformar redes simples em redes robustas e de alta disponibilidade.

## REFERÊNCIAS


BRAINMATICS. **Braintutor CCNA.** Disponível em: http://www.brainmatics.com/braintutor/ccna2/fig/fig3-2.gif. Acesso em 13 de Outubro de 2014.

CISCO SYSTEM. **Entendendo e Configurando o Spanning Tree Protocol (STP) em Switches Catalyst.** Disponível em: http://www.cisco.com/cisco/web/support/BR/8/82/82594_5.html. Acesso em 25 de Setembro de 2014.

CISCO SYSTEM. **Leran Cisco.** Disponível em: http://www.learncisco.net/assets/images/icnd2/008-broadcast-storms.jpg. Acesso em 10 de Outubro de 2014.

CPqD TECNOLOGIA. **Arquitetura de rede Ethernet robusta e de baixo custo. Campinas. CPqD Tecnologia.** Disponível em: http://www.cpqd.com.br/cadernosdetecnologia/Vol4_N1_jan_jun_2008/pdf/artigo5.pdf . Acesso em 07 de Outubro de 2014.

DATACOM. **Treinamento de Configuração, Operação e Manutenção da Linha de equipamentos Switches Ethernet.** Eldorado do Sul. Datacom. 2013.

DIAS, BEETHOVEM ZANELLA; ALVES JR., NILTON. **Evolução do Padrão Ethernet.** Disponível em: http://www.rederio.br/downloads/pdf/nt00202.pdf. Acesso em 07 de Outubro de 2014.

EXTREME NETWORKS, INC. **Ethernet Automatic Protection Switching (EAPS).** Disponível em: http://www.ntnu.no/telematikk/_media/studies/courses/tm8106/weaps_1293.pdf. Acesso em 15 de Outubro de 2014.

EXTREME NETWORKS, INC. **Summit X250e Series.** Disponível em: http://www.extremenetworks.com.br/site/files/DSSX250e_1341.pdf. Acesso em 15 de Outubro em 2014.

FIGUEIREDO, IRIA LUPPI. **História das Redes de Computadores.** Dispoível em: http://www.oficinadanet.com.br/post/10123-historia-das-redes-de-computadores. Acesso em 03 de Outubro de 2014.

FILIPPETTI, MARCO AURÉLIO. **CCNA 4.1 – Guia Completo de Estudo.** Florianópolis. Visual Books. 2008.

IEEE COMPUTER SOCIETY. **Media Access Control (MAC) Bridges.** Disponível em: http://standards.ieee.org/getieee802/download/802.1D-2004.pdf. Acesso em 11 de Setembro de 2014.

TELECO. **Fibra Óptica I.** Disponível em: http://www.teleco.com.br/tutoriais/tutorialsolfo1/pagina_1.asp. Acesso em 23 de Outubro de 2014.

# GLOSSÁRIO

**ENDEREÇO MAC** – *Media Access Control Address* – Endereço físico associado à interface de comunicação que conecta um dispositivo à rede.

**ETHERNET** – Arquitetura de redes baseadas em pacotes e protocolos de controle para a camada 2 do modelo OSI.

**FIBRA ÓPTICA** – Cabeamento de rede composto de núcleo de vidro ou plástico extrudido, usado para transportes de dados de alta capacidade através de luz.

**FRAME BROADCAST** – Frame enviado para o endereço FF:FF:FF:FF:FF:FF, endereço este que se destina a todos os elementos conectados a rede.

**IEEE** – *Institute of Electrical and Electronics Engineers* – O Instituto de Engenheiros Eletricistas e Eletrônicos é uma organização de profissionais que tem como meta disseminar o conhecimento no campo da engenharia elétrica, eletrônica e computação. Sua principal função é criar padrões para computadores e equipamentos afins.

**ITU** – *International Telecommunication Union* – A União Internacional de Telecomunicações é a agência da ONU voltada para comunicação e tecnologia da informação. Destinada a padronizar e regular as ondas de rádio e telecomunicações internacionais.

**LAN** – *Local Area Network* – Conceito de redes de dados aplicado à infraestrutura de comunicação destinada a redes de alcance local.

**MEF** – *Metro Ethernet Forum* – Consórcio internacional de indústrias, dedicada à padronização e incentivo a implementação mundial de redes e serviços Carrier Ethernet.

**METRO ETHERNET** – Conceito aplicado a redes metropolitanas baseadas em padrões ethernet.

**MODELO OSI** – Modelo de referência em camadas, criado pelo ISO com o intuito de padronizar o desenvolvimento de aplicações e equipamentos mantendo assim a interoperabilidade entre fabricantes e desenvolvedores.

**RFP** – *Request for Proposal* – Tipo de licitação feita por empresas ou órgãos públicos que necessitam adquirir um produto ou serviço. Este documento informa todas as necessidades e exigências mínimas do solicitante para que o fornecedor esteja apto a entrar na concorrência.

**SDH/SONET** – *Synchronous Digital Hierarchy* – Rede de transporte de dados que utiliza multiplexação determinística.

**SLA** – *Service Level Agreement* – Acordo de Nível de Serviço, normalmente utilizado entre empresas de TI para definir o tempo de restabelecimento de um serviço com problema ou tempo para o atendimento de uma solicitação.

**SWITCH-RAIZ** – *Root Bridge* – Switch responsável por controlar e definer a topologia do Spanning Tree Protocol.

**UTP** – *Unshielded Twisted Pair* – Cabeamento de rede par trançado, tipo de cabo composto por filamentos entrelaçados com o intuito de anular as interferências eletromagnéticas.

**WAN** – *Wide Area Network* – Conceito de redes de dados aplicado à infraestrutura de comunicação destinada a redes de longo alcance. Redes essas que podem abranger várias regiões geográficas, podendo se estender por mais de um país.

**TTL** – *Wide Area Network* – Conceito