METRO ETHERNET - CONHECENDO NA PRÁTICA OS SERVIÇOS ETHERNET LINE E ETHERNET LAN

Maiquel De Souza Dias
maiquel.dias@gmail.com
Matheus Herbstrith de Mattos
matheus.h.mattos@gmail.com
Ricardo Becker
ricardo.becker@senairs.org.br,
Vandersilvio da Silva
vandersilvio@senairs.org.br, vandersilvio@feevale.br

Faculdade de Tecnologia SENAI, RS; Ericsson do Brasil; Universidade de Caxias do Sul;
Centro Universitário Ritter dos Reis; Universidade FEEVALE

RESUMO: Este trabalho tem como objetivo, produzir um material prático de referência para o entendimento, implementação e teste de redes Metro Ethernet. Neste trabalho é apresentado uma revisão bibliográfica referente ao contexto evolutivo das redes, até o presente momento com a tecnologia Metro Ethernet. Como desenvolvimento do trabalho são propostos dois cenários, topologias, que servirão de base para as demonstrações dos dois principais serviços: Ethernet Line e Ethernet LAN. As configurações utilizadas e os resultados funcionais são apresentados.

Palavras-chave: Metro Ethernet; E-Line; E-Lan

ABSTRACT: The main objective of this paper is to produce a reference for understanding, implementing, and testing Metro Ethernet networks. This work presents a literature review regarding the evolutionary context of Ethernet networks until this moment, considering Metho Ethernet technology in this context. As development work we present two topologies, which are the basis for the statements of two main services: Ethernet Line and Ethernet LAN settings used and the functional results are presented.

Keywords: Metroethernet; E-Line; E-Lan

1 INTRODUÇÃO

Desde o seu surgimento, na década de 1970, o padrão Ethernet é o protocolo dominante em redes LANs (*Local Area Network*). A motivação para esse domínio se deve ao alto grau de padronização e integração desse protocolo. Atualmente existe a necessidade de migrar essa tecnologia para redes maiores, como MANs (*Metropolitan Area Network*) e WANs (*Wide Area Network*). O principal motivo é o crescimento exponencial do tráfego de dados por pacotes. Em face a essa exigência do mercado, especialmente das operadoras provedoras de serviços de dados, as mesmas se deparam com a necessidade de readequar suas redes metropolitanas. Neste sentido, as redes Metro Ethernet

são uma opção que se apresenta tanto pelo aspecto técnico quanto pelo econômico.

Segundo o MEF (*Metro Ethernet Forum*, 2002-2004), a Rede Metro Ethernet é definida por uma rede Metropolitana (MAN) que disponibiliza serviços de conectividade utilizando a Ethernet como o protocolo principal e permitindo aplicações em banda larga. É geralmente definida como a rede que conecta LAN´s espalhadas geograficamente através de WAN´s e *backbones* pertencentes a provedores de serviços

Por serem cada vez mais comuns as aplicações para redes Metro Ethernet, torna-se necessário o conhecimento prático destas redes. Neste sentido, esse artigo propõe a apresentação da tecnologia, de forma prática, para proporcionar, não só um guia teórico, mas também de implementação da tecnologia funcional, com os passos necessários para tanto.

2 Revisão bibliográfica

Nesta seção são apresentados os principais tópicos relacionados com a tecnologia Metro Ethernet, e alguns aspectos de configuração e protocolos envolvidos.

2.1. ETHERNET

No início da década de 1970 Norman Abransom e seus colegas da Universidade do Hawaii criaram uma rede sem fio para conectar usuários espalhados pelas ilhas vizinhas ao computador principal em Honolulu. Mais tarde Bob Metcalfe e David Boggs, funcionários da Xerox, aprimoram as idéias de Abransom e projetaram a primeira rede local utilizando cabo coaxial grosso. O sistema foi chamado de Ethernet (TANENBAUM, 2011). A Ethernet da Xerox foi se aprimorando e se difundindo, assim em 1978, a DEC, a Intel e a Xerox, criaram o padrão Ethernet de 10 Mbps, chamado padrão DIX. Em 1983 o padrão DIX se tornou o padrão IEEE 802.3 (*Institute of Eletrical and Eletronic Engineers*).

2.1.1. Padrão IEEE 802.3

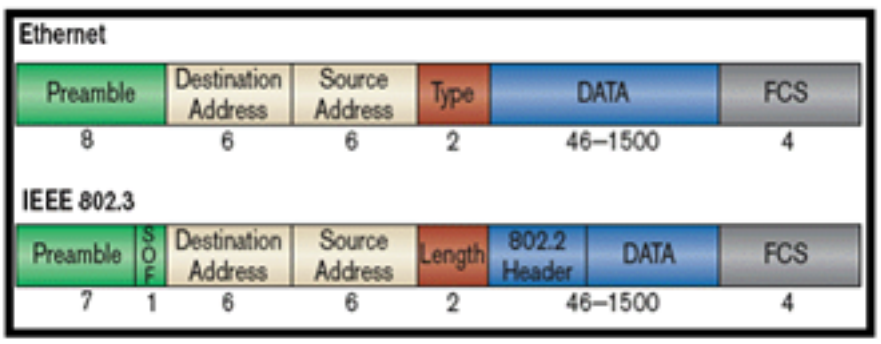
Segundo Filippetti (2008), a Ethernet proporciona o compartilhamento da mesma largura de banda de um enlace, entre todos os *hosts* de uma rede, através do seu método de acesso ao meio por concentração.

Conforme Gasparini (2004), o padrão IEEE 802.3 utiliza o método de acesso ao meio com detecção de portadora - CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*). O CSMA/CD especifíca que uma estação sempre "escuta" o meio antes de transmitir, e só transmite se o meio estiver desocupado.

2.1.2. Formato dos quadros Ethernet

De acordo com Tanenbaum (2011), a formatação dos quadros transmitidos segue o modelo da Figura 1. Os campos apresentados na Figura 1 têm a seguintes descrições:

Figura 1 - Formato do quadro Ethernet e IEEE 802.3.



Fonte: TANENBAUM, 2011, p. 177.

Preâmbulo (*Preamble*): Sequência alternada de 1 e 0 que provê um *clocking* de 5 MHz no início de cada pacote, permitindo ao recipiente "travar" a cadeia de bits sendo recebida. O *preamble* usa um campo de sincronização SFD ou SOF (*Start-of-Frame e delimiter*) para indicar a estação receptora que os dados da mensagem irá na sequência.

Destination Address: contém o endereço MAC do destinatário;

Source Address: contém o endereço MAC do remetente;

Type: indica qual protocolo da camada superior está no campo de dados;

Length: indica o tamanho, em Bytes, do campo de dados (*payload*);

Data: dados da camada superior, com tamanho entre 46 e 1500 bytes;

FCS – *Frame Check Sequence*: contém o *Cyclic Redundancy Check* (CRC).

2.1.3. Ethernet Comutada

Segundo Tanenbaum (2011), com a evolução da Ethernet clássica foi necessário aumentar a capacidade das redes. O *Hub* (repetidor), foi muito utilizado para dividir as redes e segmentá-las, mas não aumentava a sua capacidade. Com a utilização das *bridges* essa capacidade pode ser aumentada. Como as redes começaram a ter *N* segmentos, os "*bridges*" receberam o nome de *switch* (comutador). O *switch* melhora o desempenho em relação a um *hub* de duas maneiras: Primeiramente, como não existem colisões, a capacidade é usada de modo mais eficiente; Segundo, vários quadros podem ser envidados simultaneamente.

Conforme Kurose (2006), outro avanço da Ethernet comutada é a Ethernet *full-duplex*. *Full-duplex* é uma expressão que corresponde à capacidade de enviar e receber dados simultaneamente.

A Ethernet antiga não enviava e recebia ao mesmo tempo. Em uma rede comutada, os nós se comunicam com o *switch* e não diretamente com outro nó. As redes comutadas podem utilizar cabeamento de par trançado ou fibra ótica.

2.14. *Fast* Ethernet

De acordo com Tanenbaum (2011), em 1992 o IEEE reuniu o comitê 802.3 para produzir uma LAN mais rápida. O resultado foi o 802.3u, publicado em 1995, sendo conhecido como *Fast* Ethernet. Na camada física o Ethernet tem seus dados codificados no meio de transmissão em função do meio (cabo metálico ou fibra óptica). Para cada taxa de transferência, um padrão de codificação é utilizado. As especificações de codificação podem ser encontradas em Tanenbaum (2011).

Segundo Forouzan (2006), uma nova característica agregada ao padrão *Fast* Ethernet foi a autonegociação. A mesma possibilita a dois dispositivos negociar o modo ou a taxa de transmissão de dados. Permite ainda, a conexão de dispositivos com velocidades diferentes.

2.1.5. Gigabit Ethernet

Segundo Norris (2002), a criação do padrão IEEE 802.3z, deu origem ao Gigabit Ethernet. O objetivo do padrão IEEE 802.3z era abordar a necessidade de uma tecnologia de alta velocidade para interligar redes locais a *backbones* ou *Point of Presence* (POP) de uma rede. A Gigabit Ethernet funciona em *full duplex*, mantendo o protocolo e formatos idênticos ao 802.3. Como todas as tecnologias Ethernet, o Gigabit Ethernet é uma extensão do padrão IEEE 802.3 e inclui a camada de Controle de Acesso ao Meio (MAC - *Media Access Control*) e enquadramento, sendo a camada física e de Controle Lógico de Link (LLC – *Link Logical Control*) que lhe permitem maiores velocidades.

2.1.6. 10 Gigabit Ethernet

De acordo com Norris, (2002), o comitê IEEE 802.3ae descreve o padrão 10 Gigabit Ethernet quase da mesma maneira que o padrão Gigabit Ethernet, com diferenciais no aprimoramentos para altas taxas de transferência e operação apenas em modo *full-duplex*, normalmente ponto-a-ponto e através de fibras óticas. Isso encarece o padrão, mas traz ganhos de desempenho.

Segundo Tanenbaum (2011), as redes 10 Gigabit não vão substituir as redes atuais em médio prazo, mas sim complementar os padrões de modo a compartilhar as redes com as atuais tecnologias utilizadas nos *backbones*. Para tanto, foram especificados diferentes padrões para o 10 Gigabit Ethernet, de acordo com o tipo de mídia e no caso de fibras ópticas, também de acordo com o comprimento de onda usado.

2.2. VLAN

Segundo Odom (2003), VLAN (*Virtual LAN*) é um recurso que acompanha a maioria dos *switches* do mercado, tendo como objetivo obter um ganho de desempenho via a divisão da rede local em segmentos lógicos de rede. A divisão em pequenas redes lógicas (domínios lógicos – grupos de trabalho) limita o tráfego e as informações da rede àquele segmento de rede, otimizando a utilização da largura de banda e possibilitando uma maior segurança aos usuários destes segmentos. Pode-se dizer que as VLANs consistem numa solução alternativa ao uso de roteadores para conter o tráfego *broadcast*.

2.2.1. VLAN com Segmentação por Porta

Uma VLAN é criada via as configurações no *switch*. São especificadas as portas do equipamento que farão parte da VLAN, de modo a compartilhar somente as suas respectivas informações, não influenciando na banda dos demais usuários. Um aspecto a ser observado neste tipo de VLAN, é que caso alguma estação de trabalho passe para outro *switch*, em outro setor da instituição, a VLAN precisa estar configurada no mesmo (FILIPPETTI, 2008).

2.2.2. VLAN com Segmentação por MAC Address

Segundo Filippetti (2008), as VLANs com segmentação por endereço MAC são criadas a partir da informação destes próprios endereços que farão parte desta rede. Com isso o *switch* reconhece os endereços MAC das estações de trabalho pertencentes a cada VLAN.

Neste tipo de VLAN, caso exista a substituição da placa de rede da estação de trabalho, torna-se necessária a reconfiguração da VLAN para que possa aceitar o novo endereço MAC.

2.2.3. VLAN com Segmentação por Protocolo

De acordo com Filippetti (2008), as VLANs com segmentação por protocolo baseiam-se nos endereços da camada de rede. São informados ao *switch* os endereços de rede que comporão a VLAN. A segmentação por protocolo será válida somente se a rede possuir *switches* que contenham a tecnologia de camada 3 (*switch router*). Este tipo de *switch* executa também a função de roteador na rede.

Neste tipo de VLAN, os usuários podem mover as suas estações de trabalho sem existir a necessidade de reconfigurar o endereço de rede. O problema é que o tempo para o encaminhamento de pacotes, usando camada 3, é maior do que utilizando o endereço MAC.

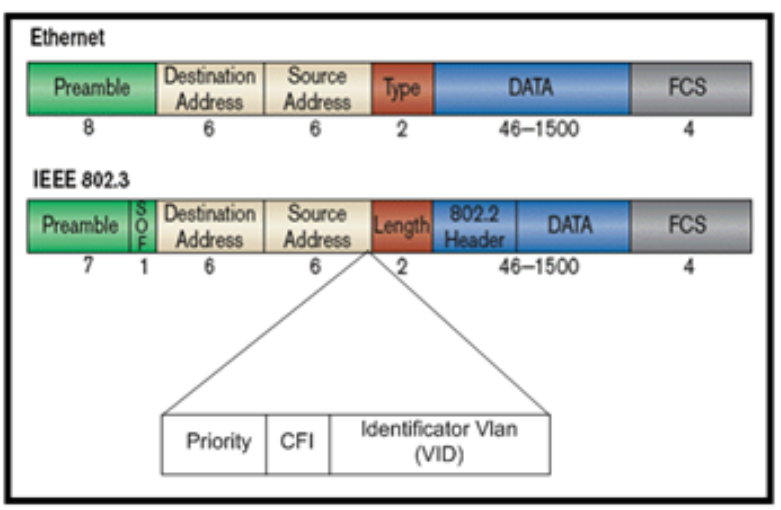
2.2.4. Padrão 802.1Q

Conforme Tanenbaum (2011), um *switch* que suporta o padrão IEEE 802.1q, recebe os quadros oriundos de uma estação de trabalho e os rotula (*tag*), indicando a VLAN ao qual o quadro pertence (VID – *VLAN Identification*). Este processo é chamado de marcação explícita (*explicit tagging*). O *switch* também é capaz de identificar qual é a VLAN de um quadro que é proveniente de uma porta (marcação implícita - *implicit tagging*). A marcação do quadro pode ser baseada na porta de origem do quadro, no campo do endereço MAC da fonte, no endereço de rede de origem ou algum outro campo ou combinação destes. Para ser capaz de rotular um quadro, utilizando um dos métodos citados, o dispositivo deve manter atualizada uma base de dados com o mapeamento entre as VLANs, com os caminhos possíveis e qual o campo é utilizado na marcação. Esta base de dados é chamada de *filtering database*, devendo possuir o mesmo conteúdo em todos os equipamentos. O *switch*, em uma LAN, é o responsável em determinar para onde o quadro deve ser encaminhado. Determinado o destino do quadro, deve-se verificar se o identificador VLAN deve ser adicionado ao quadro e enviado. Caso o destino do quadro seja um dispositivo com suporte a VLANs (*VLAN-aware*), o identificador VID é adicionado, mas caso ele não suporte o padrão IEEE 802.1q (*VLAN-unaware*), o quadro é enviado mesmo sem o VID.

2.2.5. Marcação de Quadros (*Tagging*)

De acordo com Tanenbaum (2011), é necessário que os quadros, ao serem enviados através da rede, possuam um meio de indicar a qual VLAN pertencem, de modo que sejam encaminhados somente para as portas que pertencem a esta rede virtual. Do contrário, os quadros são encaminhados para todas as portas. Isto é o que normalmente ocorre. Esta informação é adicionada ao quadro na forma de um rótulo ou marcação (*tag*) (Figura 2) em seu cabeçalho. Este rótulo permite especificar informações sobre a prioridade de um usuário, assim como indica o formato do endereço MAC.

Figura 2 - Formato do quadro Ethernet e IEEE 802.3 com a tag de VLAN.



Fonte: TANENBAUM, 2011, p. 218.

2.2.6. Tipos de Associações VLAN

Segundo Filippetti (2008), a associação de uma porta a uma VLAN pode ser realizada de duas maneiras: estaticamente ou dinamicamente. Na associação estática, cada porta do *switch* deverá ser designada para manter associação com uma determinada VLAN. Essa associação é realizada pelo administrador do ambiente na configuração do equipamento. Na associação dinâmica, as portas são designadas a uma VLAN automaticamente, através do uso de softwares de gerenciamento, como um Servidor Gerenciador de Políticas VLAN (VMPS), que irão mapear o endereço de *hardware* do cliente, protocolos e até mesmo aplicações ou *login* de usuários para uma VLAN específica.

2.2.7. Tipos de Conexão em VLANs

Conforme Filippetti (2008), as VLANs podem se espalhar em vários *switches* interconectados. Os *switches* dessa "malha" devem poder identificar a quais VLANs cada quadro pertence, possibilitando que uma VLAN envolva mais de um equipamento. As conexões entre os *switches* precisam trafegar dados que pertencem a diferentes VLANs, mesmo que elas não tenham comunicação direta entre si. Isso é feito via *links* de transporte (*trunk links*). Para que os quadros sejam corretamente identificados dentro do tronco é necessário que eles sejam marcados como pertencentes a alguma VLAN. Para tanto, é utilizado o recurso de etiquetamento de quadros (*frame tagging*). O outro tipo de *link* existente, além do de transporte, é o *link* de acesso. *Link* de acesso é a conexão até o computador de destino. Conexão essa que não possui qualquer tipo de etiquetamento, pois há conectividade para apenas uma VLAN. Ou seja, o recurso de *frame tagging* só é utilizado dentro dos *links* de transporte, e é retirado quando o quadro é entregue ao destino.

2.2.8. *Q-in-q* (IEEE 802.1ad)

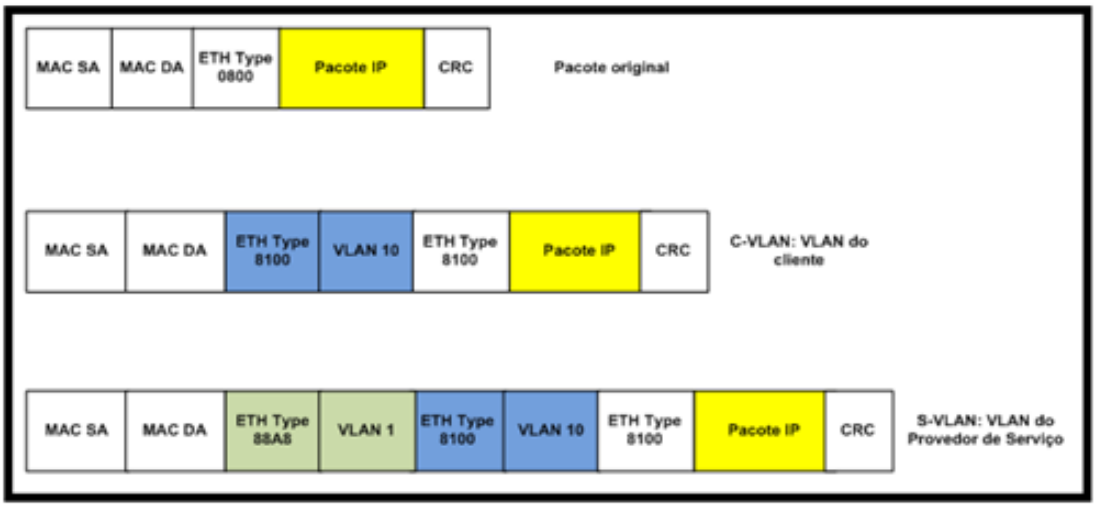
De acordo com a fabricante HUAWEI (2007), a cada VLAN é atribuído um identificador (VLAN-ID). Este recurso, já utilizado pelas LANs, é uma alternativa para as redes Metro Ethernet proverem isolamento de tráfego entre os diversos clientes. Porém, a utilização do 802.1q em redes Metro Ethernet esbarra na quantidade e administração dos VLAN-IDs. O operador de serviços não tem como gerenciar e assegurar que cada cliente utilize um VLAN-ID diferente dentro da rede metropolitana. Outra questão é que o número máximo de VLAN-IDs é de 4096, sendo este número limitado para as dimensões de uma rede metropolitana, além do fato de limitar o cliente na criação de suas próprias VLANs internas, o que não é aceitável.

Para solucionar esta questão, foi criado o tunelamento de VLANs (802.1ad – *Provider Bridge, Stacked VLAN, VLAN Tunneling, Q-in-q*). No tunelamento uma VLAN (C-VLAN – *Customer VLAN*) é encapsulada dentro de outra VLAN (S-VLAN – *Service VLAN*), conforme a Figura 3. Este tunelamento permite uma separação do tráfego do cliente. Desta forma, o cliente tem total liberdade

de gerenciar suas C-VLANs. O provedor tem à sua disposição até 4096 S-VLANs, suportando até 4 mil clientes/serviços (HUAWEI, 2007).

O formato do cabeçalho do 802.1ad é similar ao do 802.1q, conforme Figura 3.

Figura 3 - Tunelamento de VLANs – VLAN 10 dentro da VLAN1.



Fonte: Adaptado de MEDEIROS (2007).

A implementação da S-VLAN acrescenta 4 bytes ao cabeçalho Ethernet: após os campos de MAC de origem e destino, são inseridos 2 bytes correspondentes ao *EtherType* de S-VLAN e dois bytes correspondentes ao TCI (*Tag Control Information*). Diferentemente do 802.1q, o bit 4 do primeiro byte do campo TCI, passa a ser chamado de DEI (*Drop Eligeble Indicator*). A combinação dos 3 bits de prioridade mais o bit DEI formam o PCP (*Priority Code Point*), que é utilizado como parâmetro de descarte de pacotes (HUAWEI, 2007).

2.3. Arquitetura Metro Ethernet

2.3.1. Modelo de Camadas Metro Ethernet

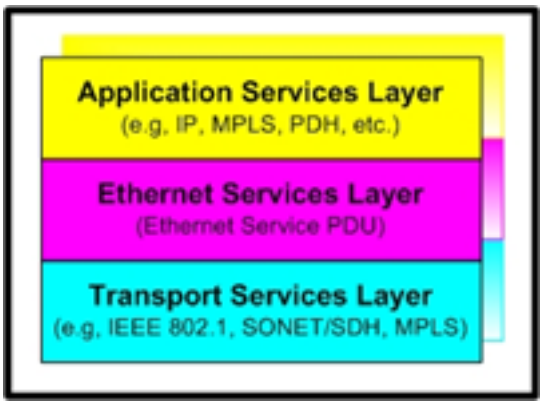
A Figura 4 mostra o modelo de camadas usado pelo MEF (*Metro Ethernet Forum*). A camada de serviços de aplicação (*Application Services Layer*) oferece suporte a aplicações baseadas nos serviços Ethernet através da MEN (*Metro Ethernet Network*). Serviços de aplicação podem ser suportados, como o uso da camada de serviços Ethernet como camada de serviços de transporte para outras redes (Metro Ethernet Forum, 2004).

A camada de serviços Ethernet (*Ethernet Services Layer*) é responsável pelos serviços do MAC e pela entrega dos quadros nas interfaces e nos pontos associados. O quadro pode ser *Unicast*, *Multicast* ou *Broadcast*, de acordo com o padrão IEEE 802.3 (MEF, 2004).

A camada de serviços de transporte (*Transport Services Layer*) oferece suporte para conectividade entre os elementos da camada de serviços Ethernet independentemente dos serviços. Várias redes podem ser utilizadas para suportar os requisitos de transporte para a camada de

serviços Ethernet (MEF, 2004).

Figura 4 - Camadas de referência usadas na rede Metro Ethernet.

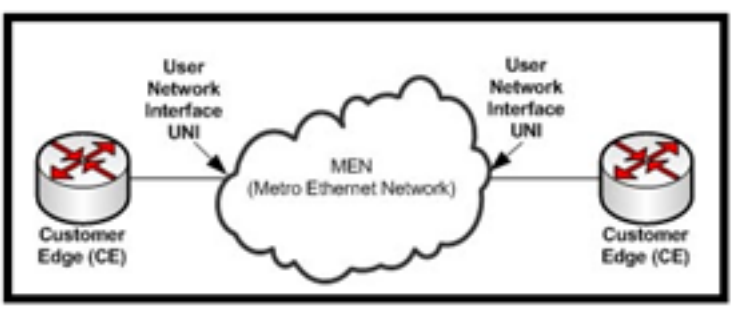


Fonte: MEF, (2002-2004).

2.3.2. Serviços Metro Ethernet

Serviços Ethernet compartilham atributos comuns, mas há diferenças. O modelo para serviços de Ethernet é mostrado na Figura 5, onde o provedor da MEN (*Metro Ethernet Network*) provê o serviço Metro Ethernet à seus clientes. O cliente CE (*Customer Equipment*) é conectado à MEN por meio da interface usuário (UNI) (SANTITORO, 2006).

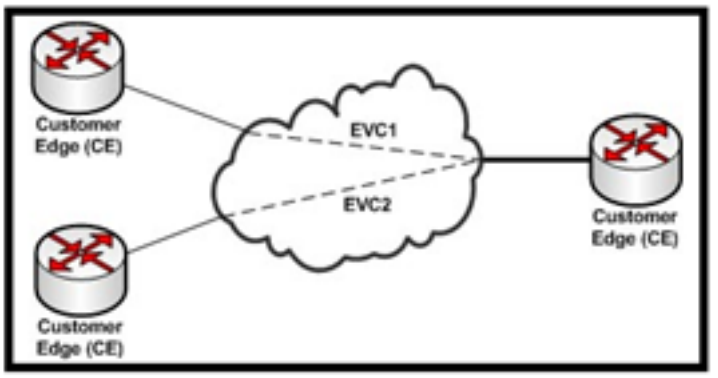
Figura 5 - Modelo básico para serviços Ethernet.



Fonte: MEF, (2002-2004).

Outro atributo (Figura 6) é a EVC (*Ethernet Virtual Conection*), que consiste na associação de uma ou mais interfaces de rede do usuário (UNIs). EVCs tem como função o estabelecimento de uma conexão (ponto a ponto ou multiponto) entre duas ou mais UNIs, transferindo quadros Ethernet e garantindo que não haverá comunicação entre sites que não façam parte da EVC. Um quadro não deve retornar a interface que o originou, e o quadro não deve ser alterado no caminho entre a sua origem até o seu destino.O MEF define dois tipos de serviços: Ethernet *Line* e Ethernet LAN (SANTITORO, 2006).

Figura 6 - Serviço Ethernet Line.



Fonte: MEF, (2002-2004).

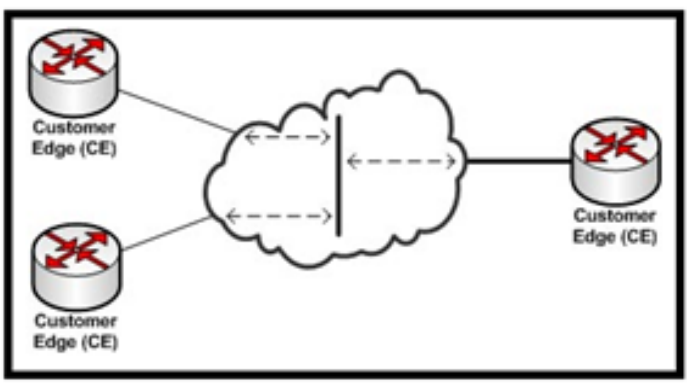
2.3.2.1. E- *Line*

Segundo MEF (Metro Ethernet Forum, 2004), o serviço Ethernet *Line* ou linha Ethernet, corresponde a comunicação ponto-a-ponto entre duas UNIs através de uma conexão Ethernet virtual, conforme é visto na Figura 6.

2.3.2.2. E-LAN

O serviço Ethernet LAN oferece conectividade multiponto entre duas ou mais UNIs. Sob a perspectiva do assinante a MEN assemelha-se a uma LAN. A Figura 7 exemplifica a conectividade entre 3 pontos, como se estivessem conectados ao mesmo barramento de rede (domínio). Quando uma nova UNI é integrada, simplesmente conecta-se essa nova UNI ao mesmo EVC para que esta UNI tenha conectividade multiponto (SANTITORO, 2006).

Figura 7 - Serviço Ethernet Lan.



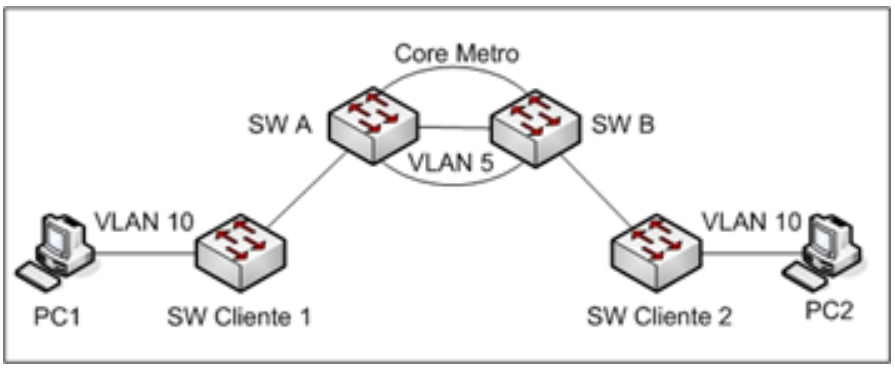
Fonte: MEF (2004).

3.1. Topologia E-*Line*

Na Figura 8, é mostrada a topologia proposta para o serviço E-*Line*. Na mesma o *Core* Metro Ethernet é formado por Sw (*switch*) *Core* A e Sw (*switch*) *Core* B. Como cliente foram definidos Sw Cliente 1 e Sw Cliente 2, conectados aos Sw clientes estão os computadores Cliente 1 e Cliente 2, que

são os usuários finais da rede.

Figura 8 - Topologia básica para o cenário de testes do serviço E-line.



Fonte: O próprio autor (2013).

3.1.1. Configuração dos *Switches* do *Core*

Foram utilizados dois *switches* do Fabricante Datacom, modelo DM Switch 3000, próprios para redes Metro Ethernet. O Switch DM 3000 possui 24 portas *Fast* Ethernet 10/100 e 4 portas Gigabit Ethernet SFP, conforme manual do fabricante (DATACOM, 2012).

Para configurar o equipamento no cenário da Figura 8, foi ativado o *q-in-q* e definida uma VLAN no *core* como VLAN 5. Foi configurada como membro *tagged* a interface Ethernet 1 (eth 1), pois esta é a de comunicação com o próximo *switch* do *core*, e como membro *untagged* a interface Ethernet 6 (eth 6), pois esta é a interface de acesso do cliente. No exemplo cada interface foi definida como nativa da VLAN 5. A interface de acesso do cliente (*eth* 6) ficou configurada como *q-in-q* externo (*external*), pois recebe pacotes oriundos da rede interna do cliente. Já a interface de comunicação com o *Core* Ethernet 1, configuramos com *q-in-q* interno (Figura 9). As configurações do *switch* SWA do *Core* são iguais ao *switch* SWB.

Figura 9 - Configurações dos Switches Datacom DM3000.

```
SWA>
SWA>enable
SWA#configure
SWA(config)#vlan qinq
SWA(config)#interface vlan 5
SWA(config-if-vlan-5)#set-member tagged eth 1
SWA(config-if-vlan-5)#set-member untagged eth 6
SWA(config-if-vlan-5)#interface ethernet 6
SWA(config-if-eth-1/6)#switchport native vlan 5
SWA(config-if-eth-1/6)#switchport qinq external
SWA(config-if-eth-1/6)# interface ethernet 1
SWA(config-if-eth-1/1)#switchport native vlan 5
SWA(config-if-eth-1/1)#switchport qinq internal
SWA(config-if-eth-1/1)#end
SWA#
```

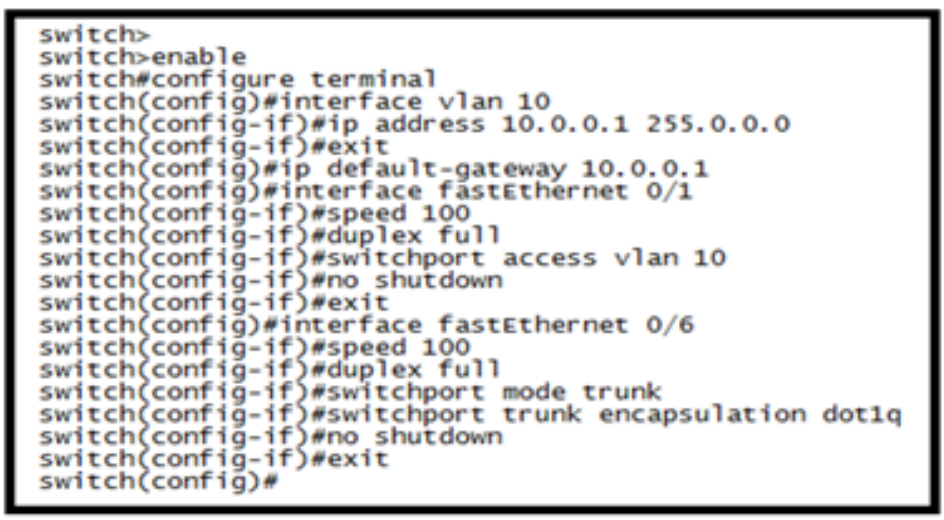
Fonte : O próprio autor (2013).

3.1.2. Configuração dos Switches do Cliente

No cliente foram utilizados dois Switches Cisco 3560. Estes equipamentos possuem 24 portas *Fast* Ethernet 10/10 e duas portas Gigabit Ethernet SFP (CISCO, 2012).

Para configurar o CISCO 3560, as mesmas foram realizadas conforme mostrado na Figura 10. Para o exemplo foi definido no *switch* do cliente a VLAN 10, configurado o IP 10.0.0.1 e máscara de rede 255.0.0.0 nesta VLAN, marcada como *default-gateway*.

Figura 10 - Comandos usados nos roteadores Cisco.



Fonte: O próprio autor (2013).

No exemplo, a velocidade da porta *Fast* Ethernet 0/1 (100 Mbps), operação *Full-duplex* e a qual VLAN ela pertence. Esta porta será conectada ao PC 1 da VLAN 10. A configuração da porta *Fast* Ethernet 6, que está conectada ao *core* Metro, também deve receber a velocidade de operação (100 Mbps) e operação *Full Duplex*. Como esta porta é a ligação com o *core*, ela pode ter que transmitir pacotes de mais de uma VLAN, por isso ela é definida como *trunk*. Este modo de operação deve ser usado sempre que acontecer comunicação entre *switches*, pois ele envia e recebe informações de múltiplas VLANs. É necessário também definir o protocolo *trunk* como IEEE 802.1q (dot1q). Este é o protocolo usado no *core*. Se não for definido nenhum protocolo, o padrão CISCO (ISL) é ativado automaticamente e não funcionará com *switches* de outros fabricantes.

3.1.3. Verificação do funcionamento

Para verificar o funcionamento das configurações implementadas, foi analisado a resposta do comando <*show*> em todos os *switches* da rede. Nos *switches* do *core*, tem-se a saída ao comando <*show running-config*> mostrada na Figura 11.

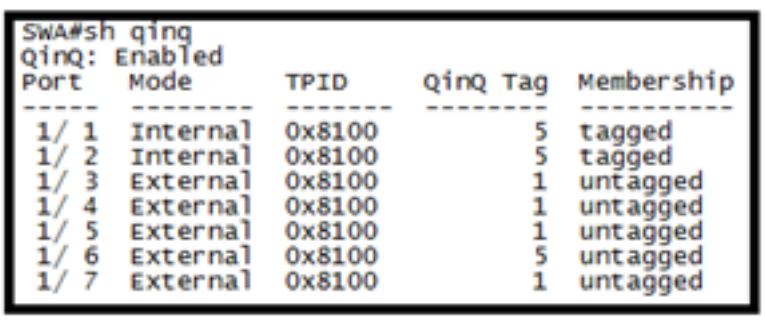
Figura 11 - Verificando as configurações que estão rodando nos Switches do Core.

```
SWA #show running-config
Building configuration...
!
! Board models in this configuration:
! Unit 1: DmSwitch3224F2
!
hostname SWA
!
username admin access-level 15
username admin password 7
d033e22ae348aeb5660fc2140aec35850c4da997
username guest access-level 0
username guest password 7
35675e68f4b5af7b995d9205ad0fc43842f16450
!
ip telnet server
ip http server
ip http secure-server
no ip ssh server
!
ip snmp-server
ip snmp-server community public ro
!
vlan qinq
!
interface vlan 1
 name DefaultVlan
 ip address 192.168.0.25/24
 set-member untagged ethernet range 1/1 1/28
!
interface vlan 5
 set-member tagged ethernet 1/1
 set-member untagged ethernet 1/6
!
vlan-group 1
vlan-group 1 vlan all
!
interface ethernet 1/1
 switchport native vlan 5
 switchport qinq internal
!
interface ethernet 1/6
 switchport native vlan 5
!
spanning-tree 1
spanning-tree 1 vlan-group 1
!
end
```

Fonte: O próprio autor (2013).

Outro comando é o <*show qinq*>. Este comando mostra uma lista com as portas, se são *tagged* ou *untagged* e se o *q-in-q* foi aplicado *internal* ou *external*. Na Figura 12 se verifica essa resposta, onde foram mostradas somente as portas de 1 a 7 utilizadas.

Figura 12 - Verificando o ***q-in-q*** implementado no equipamento.



```
SWA#sh qinq
QinQ: Enabled
Port    Mode       TPID     QinQ Tag  Membership
-----   --------   -------  --------  ----------
 1/ 1   Internal   0x8100          5  tagged
 1/ 2   Internal   0x8100          5  tagged
 1/ 3   External   0x8100          1  untagged
 1/ 4   External   0x8100          1  untagged
 1/ 5   External   0x8100          1  untagged
 1/ 6   External   0x8100          5  untagged
 1/ 7   External   0x8100          1  untagged
```

Fonte: O próprio autor (2013).

Verifica-se na Figura 12 que a porta Eth 1 está *tagged* com *qinq internal*. Já a porta Eth 6 está *untagged* com *q-in-q external*. Pode-se ainda verificar os contadores de cada interface/porta para

isso podemos usar o comando <*show interfaces counters*>.

Nos *switches* cliente pode-se analisar a saída ao comando <*show running-config*>.

Na Figura 13 verifica-se que no *switch* foi configurado a VLAN 10, e que a porta *Fast* Ethernet0/1 pertence a esta VLAN. Também pode-se conferir a velocidade *speed 100* e o modo de operação desta porta como *duplex full*. Já a porta *Fast* Ethernet 0/6, está configurada com a mesma velocidade e modo de operação, porém, está definida como tronco (*Switchport mode trunk*). Desta maneira, esta porta esta apta a comunicar-se com outros *switches* e utilizar o protocolo IEEE 802.1q definido pelo comando <*Switchport trunk encapsulation dot1q*>. Verifica-se que foi atribuído o IP: 10.0.0.10 e máscara 255.0.0.0 à VLAN 10.

Figura 13 - Verificando as configurações implementadas nos ***Switches*** do cliente.

Fonte: O próprio autor (2013)**.**

Com o comando <*show interfaces fastEthernet 0/1 e 0/6*>, mostrado na Figura 14a e Figura 14b, pode-se verificar as estatísticas de pacotes recebidos, transmitidos, perdidos, com erros e ainda se a porta está *up* e se o protocolo está *up*.

3.2. Topologia E-LAN

Tendo como base o referencial teórico, será elaborado um cenário de testes para o serviço E-LAN. Este cenário utiliza 3 *switches* DM 3000, interconectados entre si pelas portas Gigagit Ethernet, formando assim um Anel Metro Ethernet de 1 Gbps. Foram utilizados também, 3 *switches* Cisco 3560 V2, como *switches* do cliente. Como trata-se de um anel, foi utilizado o protocolo EAPS (*Ethernet Automatic Protection Switching*).

A utilização do EAPS se deu após estudo do manual do equipamento (DATACOM,2006) que sugere a sua utilização em anéis com *switches*. Este protocolo foi desenvolvido pela Extreme Networks, para ser tolerante a falhas. Como tem-se duas portas configuradas em cada *switch*, tem-se dois caminhos para trânsito de pacotes.

Figura 14 - As estatísticas de tráfego na fastEthernet 0/1 (a) e na fastEthernet 0/6 (b).

```
Switch#show interfaces fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is e840.4087.c303 (bia e840.40
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drop
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     881847 packets input, 59987346 bytes, 0 no buffer
     Received 881846 broadcasts (881846 multicasts)
     0 runs, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 881846 multicast, 0 pause input
     0 input packets with dribble condition detected
     956028 packets output, 68635916 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

(a)

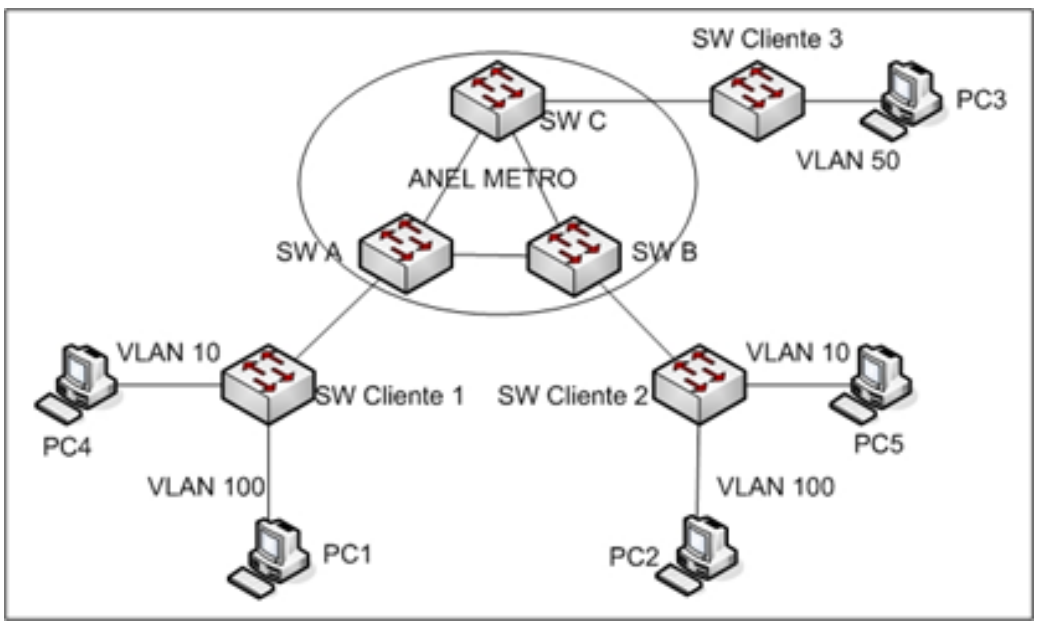
```
Switch#show interfaces fastEthernet 0/6
FastEthernet0/6 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is e840.4087.c308 (bia e840.408
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     881647 packets input, 56787546 bytes, 0 no buffer
     Received 881647 broadcasts 881647 multicasts)
     0 runs, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 881846 multicast, 0 pause input
     0 input packets with dribble condition detected
     958029 packets output, 67635816 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
Switch#
```

(b)

Fonte: O próprio autor (2013).

Para evitar o *loop* de rede, foi configurado o protocolo para selecionar um *switch* como *master* e os demais como trânsito. Nos *switches* foi especificada uma porta como primária e uma como secundária. O *master* bloqueia a porta secundária e utiliza somente a primária. Em caso de falha na rota da porta primária automaticamente a porta secundária é ativada. Essa ação ocorre em cerca de 50 ms. Na Figura 15, está a topologia mencionada.

Figura 15 - Topologia com anel Metro para testes do E-Lan.



Fonte: O próprio autor (2013).

Com a topologia da Figura 15 pode-se comprovar na prática o serviço E-LAN, onde tem-se uma rede multiponto-multiponto. Neste cenário usou-se duas VLANs de cliente, a VLAN 10 e a 100. Esta rede proporciona conectividade semelhante a uma rede local LAN. Para tanto, basta definir uma VLAN em todos os *switches* clientes, que o acesso ao anel comporta-se de maneira transparente não interferindo nas *tags* de pacotes oriundos do cliente.

3.3. Configuração dos switches do core

Na Figura 16 tem-se toda a configuração do switch SWA.

Figura 16 - Configuração dos Equipamentos membros do Anel.

```
SwA>enable
SwA#configure
SwA(config)#vlan qinq
SwA(config)#interface vlan 5
SwA(config-if-vlan-5)#name metrotag
SwA(config-if-vlan-5)#ip address 192.168.5.1/255.255.255.0
SwA(config-if-vlan-5)#set-member tagged ethernet 25
SwA(config-if-vlan-5)#set-member tagged ethernet 26
SwA(config-if-vlan-5)#set-member untagged ethernet 6
SwA(config-if-vlan-5)#exit
SwA(config)#interface vlan 99
SwA(config-if-vlan-99)#name vlancontrole
SwA(config-if-vlan-99)#interface ethernet 6
SwA(config-if-eth-1/6)#switchport native vlan 5
SwA(config-if-eth-1/6)#switchport qinq external
SwA(config-if-eth-1/6)#interface ethernet 25
SwA(config-if-eth-1/25)#switchport native vlan 99
SwA(config-if-eth-1/25)#switchport qinq internal
SwA(config-if-eth-1/25)#interface ethernet 26
SwA(config-if-eth-1/26)#switchport native vlan 99
SwA(config-if-eth-1/26)#switchport qinq internal
SwA(config-if-eth-1/26)#exit
SwA(config)#no spanning-tree
SwA(config)#vlan-group 15
SwA(config)#vlan-group 15 vlan range 5 20
SwA(config)#eaps 15
SwA(config)#eaps 15 name MetroTeste
SwA(config)#eaps 15 port primary ethernet 25
SwA(config)#eaps 15 port secondary ethernet 26
SwA(config)#eaps 15 control-vlan id 99
SwA(config)#eaps 15 protected-vlans vlan-group 15
SwA(config)#eaps 15 mode master
SwA(config)#end
```

Fonte: O próprio autor (2013).

A diferença aqui é o uso do protocolo EAPS. Para que o protocolo funcione foi necessário criar uma VLAN para controle, a VLAN 99, e criar um grupo de VLANs, o *VLAN-GROUP 15*. A este grupo foi adicionado um *range* de VLANs. No caso, somente a VLAN 5, mas foi gerado um *range* do 5 ao 20. Cabe salientar que não é obrigatório nomear as VLANs e o EAPS, tampouco endereçar a VLANs. Na Figura 16 está destacada a configuração do modo de operação do EAPS. Neste exemplo, o SWA será o *master* do anel. E recomendável desativar o protocolo Spanning-tree,[1] para que não haja interferência no funcionamento do EAPS. Esta configuração pode ser replicada de igual forma nos outros *switches* membros do anel com exceção do parâmetro *mode master*, que

[1] Protocolo desenvolvido pela *Digital Equipment Corporation* que foi padronizado pelo IEEE 802.1d. Serve para prevenir congestionamentos broadcast e outros efeitos colaterais nas ligações em loop (TANENBAUM, 2011).

nos demais deve ser definido como trânsito através do comando <*eaps 15 mode transit*>.

3.4. Configuração dos Switches do Cliente

Nos equipamentos do cliente foram aplicadas as configurações da topologia 1 (Figura 8), com a adição de alguns detalhes. Como no *switch* do cliente 3 nada mudará seguiremos a Configuração da Figura 9, pois este equipamento é membro apenas da VLAN 10. Para os *switches* SWA e SWB, que participam de duas VLANs tem-se a Figura 17.

Figura 17 - Configuração dos Switches do cliente 1 e 2.

```
Switch>enable
Switch#configure terminal
Switch(config)#interface vlan 10
Switch(config-if)#ip address 10.0.0.1 255.0.0.0
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#speed 100
Switch(config-if)#duplex full
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface vlan 100
Switch(config-if)#ip address 192.168.100.100 255.255.255.0
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#speed 100
Switch(config-if)#duplex full
Switch(config-if)#switchport access vlan 100
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/6
Switch(config-if)#speed 100
Switch(config-if)#duplex full
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#exit
```

Fonte: O próprio autor (2013).

3.5. Configuração dos Switches do Cliente

Para verificar o funcionamento das configurações implementadas, é analisada a resposta do comando show em todos os *switches* da rede. Na Figura 18especificamente tem-se um exemplo das configurações no anel, atravez do comando <*show running-config*>.

Conferir o EAPS é importante para ver se está funcionando corretamente, para isso temos o comando <*show eaps*>, que é mostrado na Figura 19a e Figura 19b.

Na Figura 19a verifica-se que o EAPS está rodando e completou seu tempo de convergência, pois seu *State* está *Complete*. Pode-se conferir também que este equipamento é o *master*, pois o Mode está como "M", a porta 1/25 é primária e a porta 1/26 é secundária. A VLAN de controle é a 99 e que temos um VLAN-GROUP com 16 VLANs sendo protegidas.

Na Figura 19b verifica-se o EAPS nos demais equipamentos do anel. Como são equipamentos trânsito (T), possuirão a mesma resposta ao comando <*show eaps*>. Neste caso o *State* será *Links-up* sinalizando que as conecções entre os membros do anel está estabelecida. A porta primária será a

1/25 enquanto que a secundária será a 1/26. A VLAN de controle é a mesma do mestre VLAN 99, e o número de VLAN-GROUP e VLANs protegidas deve ser o mesmo 1/16.

Pode-se conferir o *status* do *q-in-q*, através do comando <*show qinq*>, para isso basta seguir o exemplo da Figura 12 já comentado.

Figura 18 - Verificando as configurações nos Equipamentos do Anel.

```
SWA#show running-config
Building configuration...
!
! Board models in this configuration:
! Unit 1: DmSwitch3224F2
!
hostname SWA
!
!
monitor destination 1/10
!
vlan qinq
!
interface vlan 5
 name metrotag
 ip address 192.168.5.1/24
 set-member untagged ethernet 1/6
 set-member tagged ethernet range 1/25 1/26
!
interface vlan 99
 name vlancontrole
!
vlan-group 15
vlan-group 15 vlan range 5 20
!
interface ethernet 1/6
 switchport native vlan 5
 monitor source all
!
interface ethernet 1/25
 switchport native vlan 99
 monitor source all
!
interface ethernet 1/26
 switchport native vlan 99
!
eaps 15
eaps 15 mode master
eaps 15 name MetroTeste
eaps 15 port primary ethernet 1/25
eaps 15 port secondary ethernet 1/26
eaps 15 control-vlan id 99
eaps 15 protected-vlans vlan-group 15
!
end
```

Fonte: O próprio autor (2013).

Figura 19 - Verificando o EAPS (a) no SWA e (b) nos demais switches

```
SWA#show eaps
EAPS information:

 Mode: M - Master
       T - Transit

 ID      Domain          State        Mode  Pri Port  Sec Port  Ctrl VLAN
 --  --------------  --------------  ----  --------  --------  ----
 15  MetroTeste      Complete        M     1/25      1/26      99
```

(a)

```
SWB#show eaps
EAPS information:

 Mode: M - Master
       T - Transit

 ID      Domain          State        Mode  Pri Port  Sec Port  Ctrl VLAN
 --  --------------  --------------  ----  --------  --------  ----
 15  MetroTeste      Links-Up        T     1/25      1/26      99
```

(b)

Fonte: O próprio autor (2013).

4 APLICAÇÃO E RESULTADOS

Nesta etapa é verificado o funcionamento dos dois cenários propostos. É testada a conectividade da rede, e a sua convergência. Foi utilizado o teste de *ping* até o ponto remoto. Em seguida é analisado, com a ajuda o analisador de protocolos Wireshrark (COMBS,2012), os pacotes que estão trafegando no *Core* da rede, com o objetivo de visualizar o *q-in-q*.

4.1. Teste de conectividade - TOPOLOGIA 1

Com a configuração de todos os Switches realizada, e todos os cabos que conectam interfaces, conectados podem ser iniciados os testes de conectividade. Para isso, foi utilizada a topologia 1 descrita na Figura 8.

Para os testes foram utilizados dois PCs um em cada extremidade da topologia. O PC 1 foi configurado com IP 10.0.0.2 e o PC 2 com o IP 10.0.0.3. Foram disparados dois testes de *ping*, e verificou-se que a rede possuia conectividade fim a fim.

Verifica-se os contadores de cada interface do *switch*. Com isso é possível analisar a quantidade de pacotes que transitam na interface e ainda se há erros e perdas de pacotes. Basta utilizar o comando <*show interfaces couters Ethernet 1*>, como é visto na Figura 20.

Figura 20 - Análise das estatísticas da porta Ethernet 1.

```
SWA#show interfaces counters ethernet 1
Eth 1/1
  Octets input                    : 57848
  Octets output                   : 53428
  Unicast input                   : 172
  Unicast output                  : 173
  Discard input                   : 0
  Discard output                  : 0
  Error input                     : 0
  Error output                    : 0
  Unknown protos input            : 0
  QLen                            : 0
```

Fonte: O próprio autor (2013).

Outro teste sugerido é o rastreamento de tráfego para validar o encapsulamento dos pacotes que transitam por portas do *switch*. Para este teste é preciso realizar mais uma configuração nos *switches* do Core. É necessário fazer o espelhamento de porta ou monitoramento de porta (*port monitoring*). Para isso aplica-se os comandos da Figura 21.

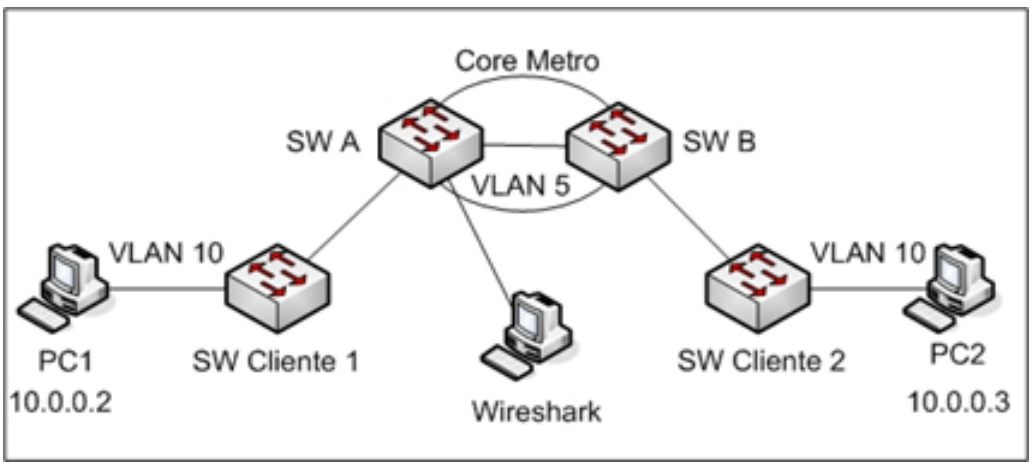
Figura 21 - Ativando o espelhamento de porta.

```
SWA#config
SWA(config)#monitor destination eth 10
SWA(config)#interface eth 1
SWA(config-if-eth 1/1)#monitor source all
SWA(config-if-eth 1/1)#end
SWA#
```

Fonte: O próprio autor (2013).

Com estes comandos, a porta Eth 10 será a porta destino para o tráfego que circula por Eth 1. Conecta-se um PC3 com o Wireshark, à porta Eth 10 do SWA (Figura 22).

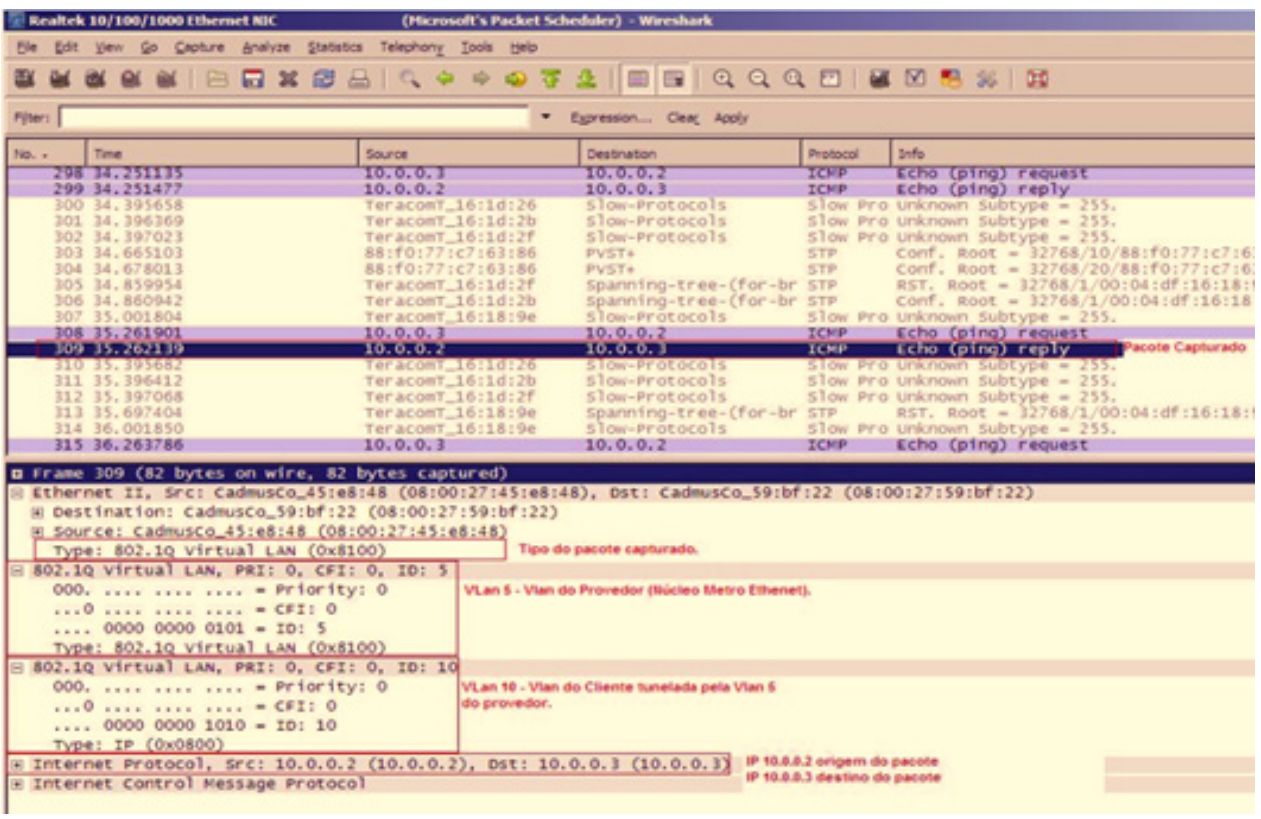
Figura 22 - Conectando o PC 3 para analise do protocolo com Wireshark.



Fonte: O próprio autor (2013).

Com isso podemos iniciar o analisador de protocolo Wireshark e ver se o tunelamento de VLANs está acontecendo. Na Figura 23 é visto que as configurações foram implementadas com sucesso nesta topologia, pois é possível rastrear os pacotes, e ver o que o formato do frame possui duas Tags de VLANs, a VLAN 10 (VLAN do cliente) e a VLAN 5 (VLAN do Core).

Figura 23 - Pacote capturado com Wireshark (Duas ***Tags*** de VLANs).



Fonte: O próprio autor (2013).

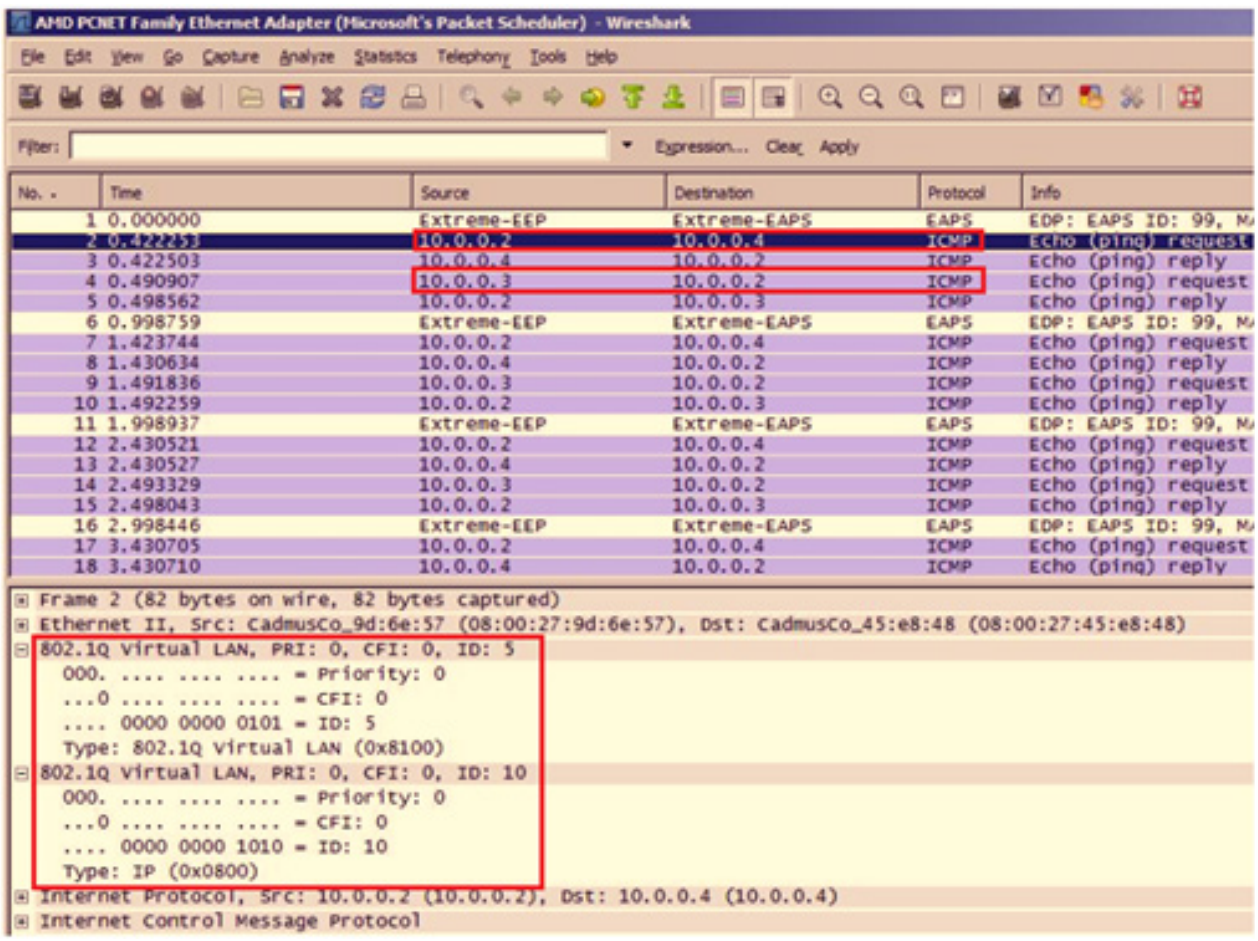
4.2. Teste de conectividade TOPOLOGIA 2

Para os testes de conectividade na topologia 2, considera-se a Figura 15. Para este cenários aplicaram-se os mesmos testes de conectividade aplicados na topologia 1.

Quanto a análise dos Pacotes Topologia 2, a análise do protocolo foi feita com o Wireshark. Nas Figura 24, Figura 25 e Figura 26, identifica-se que o tunelamento de ambas as VLANs do cliente aconteceu como esperado.

Na Figura 24 podemos analisar que o pacote capturado, tem como origem o endereço 10.0.0.2 (PC 1) e como destino o endereço 10.0.0.4 (PC 3). De forma simultânea o ping de origem 10.0.0.3 (PC 2) e destino 10.0.0.2 (PC 1). Sendo assim, comprova-se que a conectividade da rede entre PC 1 e PC3 e entre PC 2 e PC 1. Dentro do pacote podemos ver as duas Tags de VLAN, VLAN 10 (cliente) e VLAN 5 (anel).

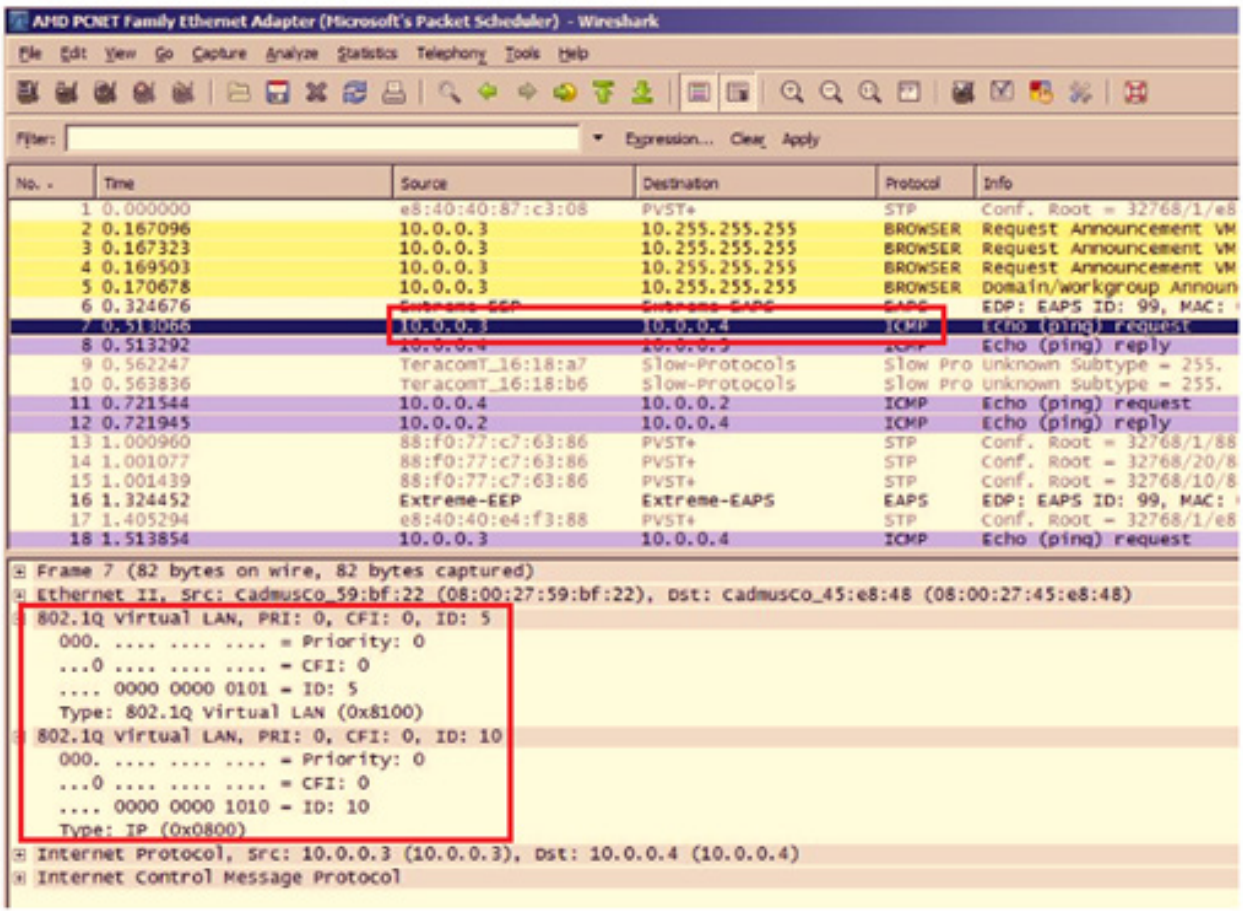
Figura 24 - Pacote capturado com duas VLANs na Tag.



Fonte: O próprio autor (2013).

Na Figura 25 ainda vemos as duas *tags* de VLANs, porém a origem é o endereço 10.0.0.3 e o destino 10.0.0.4, ou origem PC 2 e destino PC 3. Assim, comprovamos que a conectividade multiponto acontece na topologia para a VLAN 10 do cliente.

Figura 25 - Pacote capturado com duas VLANs na tag.

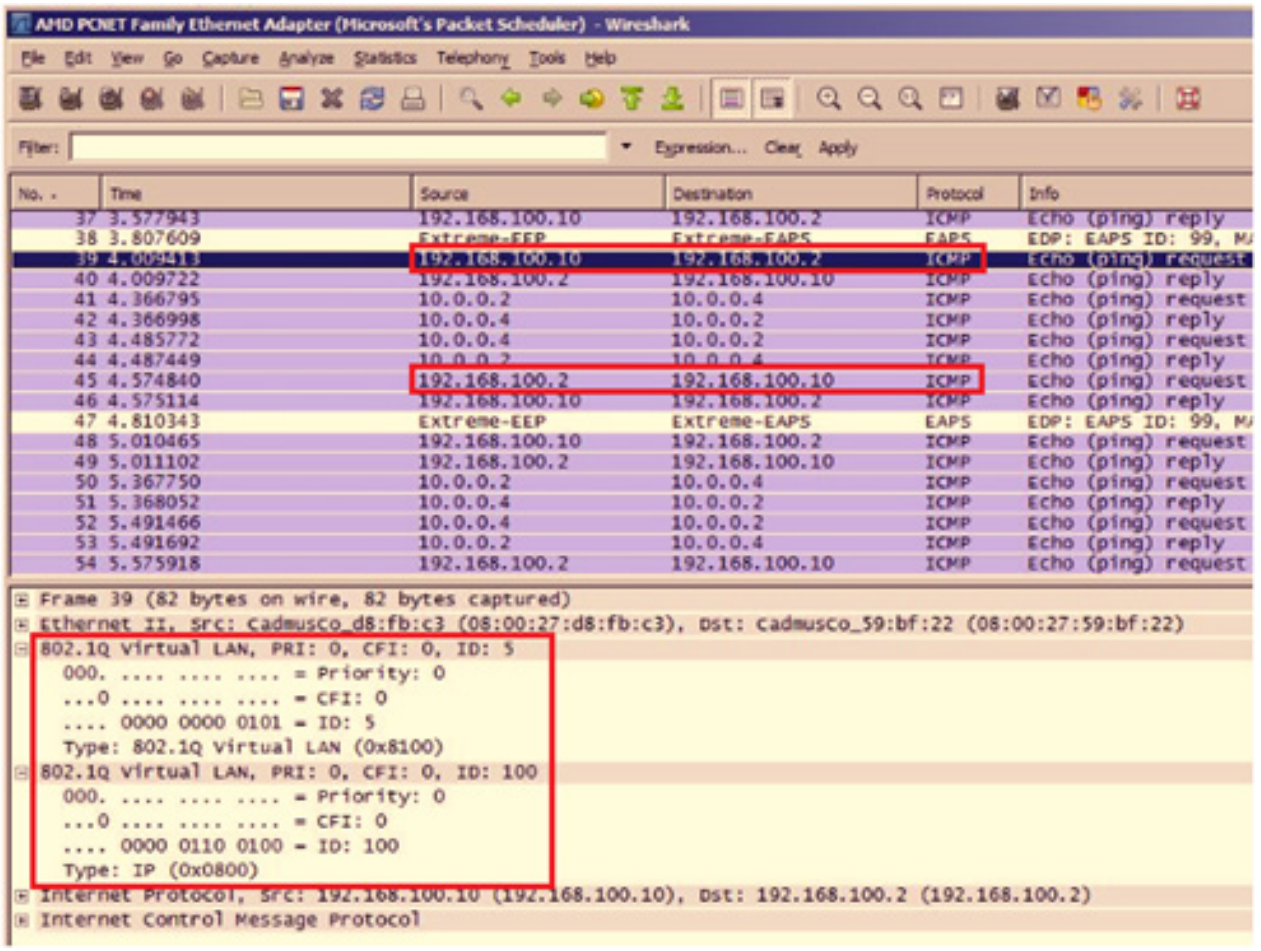


Fonte: O próprio autor (2013).

Ainda precisamos analisar a segunda VLAN do cliente, VLAN 100. Na Figura 26 faremos a análise desta segunda situação.

Na Figura 26 pode-se comprovar que a VLAN 100 também consegue passar através do anel e chegar ao seu destino. Identifica-se que o endereço 192.168.100.10 consegue realizar *ping* no endereço 192.168.100.2, e vice versa. Dentro do pacote estão as duas *tags*, 5 e 100.

Figura 26 - Pacote capturado com duas VLANs na ***tag***.



Fonte: O próprio autor (2013).

5 COMENTÁRIOS FINAIS

Cada vez mais os serviços das operadoras de telecomunicações chegam a uma quantidade maior de usuários. Seja pelas políticas econômicas mais favoráveis ao desenvolvimento, ou pelas novas tecnologias que chegam ao mercado, é verdade que o tráfego de pacotes ultrapassa o tráfego de voz. Com isso os provedores de acesso precisam utilizar tecnologias mais modernas, rápidas e acessíveis para atender essa demanda crescente.

Ao invés de utilizar linhas de circuitos dedicados a voz, está acontecendo a migração de serviços de voz para as redes de dados. Essa migração exige redes de dados robustas capazes de absorver novos serviços sem perder a qualidade. A difusão do protocolo Ethernet torna as redes Metro Ethernet um caminho simples e barato para o cliente, pois o mesmo já utiliza em sua rede local este protocolo. O fato de utilizar *switches* Ethernet facilita e diminui os custos da implementação pois o conceito de VLANs já está bem difundido não sendo novidade.

Com a necessidade de migrar as redes atuais para Ethernet, é de suma importância que um profissional da área de Comunicações conheça e opere tais redes. Assim, este trabalho visa contribuir com a complementação de formação de profissionais, e espera-se que possa ser um facilitador, especialmente nas rotinas de configuração e teste sugeridas.

Referências

CISCO, Cisco Systems Inc. Cisco Catalyst 3560 V2 Series Switches. Disponível em: <http://www.cisco.com/en/US/prod/collateral/Switches/ps5718/ps5528/at_a_glance_c45-527653.pdf>.

COMBS, Gerald. WireShark Analisador de Protocolos de Rede. Disponível em: <http://www.wireshark.org/>.

DATACOM, Datacom Telemática. Descritivo DM3000. Disponível em: <http://www.datacom.ind.br/new/>.

DATACOM, Datacom Telemática. DmSwitch Command Ref. Porto Alegre. 2006.

FILIPPETTI, Marco Aurélio. **CCNA 4.1** – Guia Completo de Estudo. Florianópolis: Ed. Visual Books, 2008.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 3. ed. Porto Alegre: Bookman, 2006.

GASPARINI, A. F. L. **Lans**: Redes Locais Infraestrutura Protocolos e Sistemas. São Paulo: Erica, 2004.

HUAWEI, Huawei Tech. Co., Ltd. Technical White Paper for QinQ. Disponível em: <http://www.huawei.com/products/datacomm/pdf/view.do?f=556>.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet**: Uma abordagem top-down. São Paulo: Ed. Addison Wesley, 2006.

MEDEIROS, L. C. L. L.; HABIB, I. B.: **Administração e projeto de redes** - Interconexão de redes de computadores. Escola Superior de Redes de Computadores – RNP, 2007. Disponível em: <https://esr.rnp.br/livro/adr4#p/1>.

MEF, Metro Ethernet Forum. Metro Ethernet Networks – A Technical Overview. Disponível em: <http://www.metroEthernetforum.org/PDFs/WhitePapers/metro-Ethernet-networks.pdf - 2002 - 2004>.

NORRIS, M. Gigabit Ethernet: **Technology and Applications**. Norwood: Artech House Telecomunications Library, 2002.

ODOM, W. Cisco CCNA - **Guia de Cert. do Exame**. 3. ed. Rio de Janeiro: Alta Books, 2003.

SANTITORO, Ralph. Metro Ethernet Services – A Technical Overview. Disponível em: <http://metroEthernetforum.org/metro-Ethernet-services.pdf>.

TANENBAUM, A. S. **Redes de Computadores**. 5. ed. São Paulo: Pearson P. Hall, 2011.