Centro Universitário de Brasília
Faculdade de Ciências Exatas e Tecnologia - FAET
Curso de Engenharia da Computação
Projeto Final

TRANSMISSÃO DE “TELEVISÃO” ATRAVÉS DE REDES METRO-ETHERNET, UTILIZANDO A TECNOLOGIA IPTV, EM UM CENÁRIO COM QoS

André Gustavo de Andrade Moreira
RA: 20024997

Orientador: Professor M.Sc. **Francisco Javier De Obaldía Díaz**

Brasília, 2° semestre de 2007

André Gustavo de Andrade Moreira

TRANSMISSÃO DE “TELEVISÃO” ATRAVÉS DE REDES METRO-ETHERNET, UTILIZANDO A TECNOLOGIA IPTV, EM UM CENÁRIO COM QoS

Trabalho apresentado ao
Centro Universitário de
Brasília (UNICEUB)
Como pré-requisito para a
obtenção de Certificado de
Conclusão do Curso de
Engenharia da Computação

Orientador: Professor M.Sc. **Francisco Javier De Obaldía Díaz**

Brasília, 2° semestre de 2007

Agradecimentos

A Deus por essa grande oportunidade concedida.

Aos meus pais que Ana Blandina e Francisco Lins que sempre acreditarem em mim.

A minha avó Maria Vieira Leite por ser um grande exemplo de simplicidade e sabedoria.

A minha irmã Thaís por sua amizade. A Minha Tia Maria Joaquina que sempre me ajudou.

A Larissa minha namorada que esteve ao meu lado sempre me fortalecendo e incentivando.

A minha tia Maria Joaquina que muito me ajudou em vinha vida.

Agradeço a todos os amigos da Vernet Comunicação de Dados pela credibilidade que me deram e por todos os recursos (laboratório e equipamentos) disponibilizados para esse estudo.

Ao orientador Javier que desde o primeiro momento acreditou neste estudo e se mostrou um grande amigo e guia nessa jornada.

Ao engenheiro Luciano Duque por sua ajuda e por suas idéias que enriqueceram esse trabalho.

Ao engenheiro e colega Wagner pelas suas idéias.

Resumo

Seguindo a tendência do mercado atual de redes convergentes, este projeto teve como norte a junção de duas tecnologias que atualmente despontam no mercado: IPTV e MetroEthernet.

Este trabalho apresenta a transmissão de televisão sobre IP, feita através de uma rede Metro Ethernet.

A fim de simular os serviços disponibilizados por um provedor de serviços, para este projeto foi desenhada e montada um rede com as características mais importantes que uma rede Metro Ethernet deve ter. Entre elas disponibilizar os meios necessários para que possa ocorrer a transmissão de IPTV com qualidade, disponibilidade e com uso de recursos de QoS (Qualidade de Serviço).

Palavras-Chaves: Redes convergentes, Metro Ethernet Network, IPTV.

Abstract

Following the trend of the current market for converging networks, this project has the northern junction of two technologies that currently dawn in the market.

The transmission of television over IP is done through a network Metro Ethernet.

In order to simulate the services provided by a service provider for this project was designed and assembled a network with the most important features that would have a Metro Ethernet. This should provide the wherewithal for it to happen the transmission of IPTV with quality and availability with the use of features such as QoS

Keywords: Convergent Network, Metro Ethernet Network, IPTV.

Sumário

Índice de Figuras

Índice de Tabelas

Lista de Símbolos

ABR – Area Border Router

ABR - Autonomous Border Router

ADSL - Assymetrical Digital Subscriber Line

ARP – (Address Resolution Protocol)

Arpanet – Advanced Research Projects Agency

ASBR – Autonomous System Border Router

ATM – Asynchrony Transfer Mode

BGP - Border Gateway Protocol

BPDU - Bridge Protocol Data Unit

BSR - Bootstrap Router

CBS – Committed Burst Size

CE - Customer Equipment

CE-VLAN – Custumer Edge Vlan

CIR – Committed Information Rate

CORE – Equipamento que fica no núcleo da rede

CoS – Class of Service

CPE - Customer Premises Equipment

CSMA – Carrier Sense Multiple Access

DBD - Database Description Packet

DMR - Digital Rights Management

DR – Designated Router

DVMRP – Distance Vector Multicast Routing Protocol

EBS – Excess Burst Size

Edge – Equipamento de borda

EIR – Excess Information Rate

E-Lan – Ethernet Private lan

E-Line – Ethernet Private Line

E-NNI – External Network-to-Network Interface

EPL – Ethernet Private Line

EVC – Ethernet Virtual Connection

EVPL – Ethernet Virtual Private Line

H.264 – Formato de compactação de vídeo

HDTV – High Definition

HOP – Ponto De Roteamento

HOST – Computador ligado em rede

IEEE – Institute of Electrical and Electronics Engineers

IGMP – Internet Group Management Protocol

IPTV – Internet Protocol Television

LAN – Local Area Network

LSA - Link State Advertisements

LSAck - Link State Acknowledgment

LSR - Link State Request

LSU - Link State Update

MAC - Media Access Control

MEF – Metro Ethernet Forum

MEN – Metro Ethernet Network

Mini-GBIC – Mini Gigabit Interface Converter

MPEG-2 – Motion Picture Experts Group 2

MPEG-4 – Motion Picture Experts Group 4

MPLS - Multi Protocol Label Switching

MTU - Multi-Tennant Unit

NAT – Network Address Translation

NI-NNI - Network Interworking Network-to-Network Interface

NSSA – Not So Stubby Area

OSPF – Open Shortest Path First

PBMR – Roteador PIM que de saída para Internet

PIM – Protocol Independet Multicast

QeS – Qualidade no uso do serviço

QoS – Qualidade de Serviço

RARP - Reverse Address Resolution Protocol

RFC - Request For Comments

RIP - Routing Information Protocol

RP – Root Port

RSTP – Rapid Spanning Tree Protocol

RSTP – Real Time Streaming Protocol

SD – Standard Definition

Set-top box – Equipamento para recepção e conversão de IP

SI-NNI - Service Interworking Network-to-Network Interface

SR – Strict Priority

SSH - Secure Shell

STP – Spanning Tree Protocol

Tagged – Interface que participa de várias VLANs

TCP/IP – Transmission Control Protocol/Internet Protocol

TDM - Time Division Multiplexing

Triple Play – Conjunto de serviços das empresas de telefonia

Trunk – Agregação de link

UNI – User network interface

UNI-C – Network User Interface Client

UNI-N - Internal Network-to-Network Interface

Untagged - Interface que participa de uma única VLAN

VLAN - Virtual LAN

VoD – Vídeo sob demanda

VoIP – Voz sobre IP

VPL – Virtual Private Line

WAN - Wide Area Network

WMV - Windows Media Vídeo

WRR – Weighted Round-Robin

CAPÍTULO 1 - Introdução

O foco deste trabalho se concentra nas tecnologias de IPTV e Redes Metro Ethernet, dois grandes expoentes da atualidade no setor de tecnologia da informação.

A seguir serão apresentados os motivos, objetivos e a estrutura que esta monografia segue, assim como o detalhamento das bases teóricas e os conceitos utilizados como diretrizes no desenvolvimento deste trabalho.

1.1) Motivação

De tempos em tempos vemos o surgimento e o declínio de novas tecnologias.

Atualmente vemos dois novos fenômenos no mundo das telecomunicações: o IPTV – transmissão de televisão por redes IP – e as redes convergentes. Se por um lado as empresas de televisão a cabo estão disponibilizando para os usuários o serviço de telefonia VoIP e, por isso, estão cada vez mais presentes em um mercado antes dominado exclusivamente pelas empresas de telefonia, por outro lado, surge o IPTV, uma nova opção para as operadoras de telefonia, que permite a elas a transmissão de televisão sobre redes IP, disputando um mercado com as operadoras de TV a cabo.

O IPTV dará um novo impulso às empresas de Telecomunicação, dotando-as da capacidade de atuar em uma nova frente, onde provavelmente os ganhos serão altos. No mundo corporativo atual o domínio de uma nova tecnologia pode gerar enormes lucros, do contrário, pode selar o fim de um segmento no mercado. As empresas de Telecomunicações têm mostrado que irão agir neste mercado. Muitas já estão testando soluções e pretendem disponibilizar esse serviço em breve para os consumidores.

Essas inovações estão se tornando realidade em virtude da convergência das redes. A convergência de redes busca aglutinar estruturas que antes atuavam separadamente, em estruturas únicas. Porém, para que isso seja viável, as estruturas devem garantir a transmissão dos dados de forma eficiente. Basicamente, o que uma rede convergente faz é enviar as informações da origem até o seu destino usando o protocolo IP.

O serviço denominado de “*Triple Play*” é um bom exemplo de utilização das redes convergentes. Neste tipo de serviço os provedores de serviços oferecem acesso a Internet em banda larga, telefonia IP e transmissão de imagem.

Tecnologias como DWDM (Dense Wavelength Division Multiplexing) e MPLS (Multi Protocol Label Switching) são usadas em redes convergentes. [Tanenbaum, 2003]

Um dos maiores expoentes das redes convergentes é a rede Metro Ethernet Network (MEN). Ela tem como características a escalabilidade, flexibilidade e confiabilidade; tudo isso a um preço acessível, quando comparados às tecnologias antecessoras. Além de serem capazes de suportar velocidades extremamente altas, desde algumas dezenas de Mbits/s, suportando facilmente 10Gbit/s, 40 Gbit/s e em breve 100Gbit/s

Estas redes, além de serem economicamente mais viáveis e terem grande desempenho, vêm crescendo rapidamente por serem compatíveis com a maioria das redes locais atuais. Assim, a rede Metro Ethernet, cada vez mais, vem ganhando espaço, antes ocupados por outras tecnologias e se tornando uma referência mundial em termos de rede de transmissão para sinais em alta velocidade.

Partindo do princípio que uma Metro-Ethernet Network já esta em produção anteriormente sem IPTV, é importante avaliar o impacto do acréscimo da transmissão simultânea do IPTV e de dados nesta rede, mostrando a viabilidade ou não, e as possíveis limitações existentes na busca das convergências de serviços em redes que utilizam esta tecnologia.

1.2) Objetivo

Este projeto propõe, a partir de um estudo sobre o IPTV e da rede Metro Ethernet Network (MEN), determinar a viabilidade da agregação destas duas tecnologias e transmitir sinais de TV. Será medido o impacto da transmissão de sinais *Internet Protocol Television* usando as redes Metro Ethernet Network como meio de transmissão. Ao final serão mostradas as condições em termos da qualidade desta transmissão e suas limitações.

Será considerado neste trabalho que a rede a ser analisada e avaliada para transmissão de IPTV, foi implementada com a função de trafegar dados convencionais e, principalmente, o IPTV. Consideramos que haverá tráfego de

dados e de IPTV e os dois fluirão por toda a estrutura simultaneamente. No primeiro momento não existe hierarquia entra essas duas transmissões.

Neste trabalho será avaliada a necessidade de alterações na rede Metro-Ethernet, para suportar a transmissão de IPTV. Tal avaliação será realizada com o uso de estrutura em ambiente de laboratório. Ou nos casos em que houver a necessidade de alteração do ambiente, essas alterações, configurações e programações serão citadas.

A viabilidade de se transmitir IPTV por esta rede será verificada através de simulações em laboratório. Será montado um ambiente de transmissão em Metro-Ethernet, onde serão gerados dados que representem o sinal de TV e transmitidos por este ambiente.

A seguir, após coletadas as informações, será verificada a viabilidade associada à qualidade desta transmissão de “televisão” através de redes Metro-Ethernet.

O fluxo de vídeo em uma rede é sempre um ponto crítico. Isso nos leva a crer que deverá ser agregado à estrutura montada para o transporte de IPTV um cenário com QoS (Qualidade de Serviço) para garantir o bom funcionamento de toda a estrutura.

O QoS será configurado para garantir a qualidade da transmissão de IPTV e as outras informações da rede terão tratamento de QoS, porém com uma importância bem reduzida. Com isso, pode-se determinar como uma rede irá se comportar quando for acrescentado um novo sinal.

Os parâmetros que serão usados para qualificar essa transmissão serão os padrões definidos por um comitê internacional (MEF – *Metro Ethernet Forum*) que trata sobre redes Metro Ethernet. Este comitê tem por função precípua a padronização dessas redes. Esta instituição é composta por mais de 120 empresas fornecedores/fabricantes, cientistas, pesquisadores engenheiros e técnicos. O MEF trabalha em conjunto com IEEE, determinando ou recomendando padrões que devem ser seguidos.

No ambiente será feita a simulação com transmissão de apenas um sinal de IPTV (simples), como um *broadcast* de um canal, que é uma das características do IPTV.

A captura dos vídeos será feita da forma que eles seriam vistos pelos usuários finais. Vários vídeos serão enviados para a estrutura MEN. Os primeiros, enviados sem QoS e os seguintes com QoS, para garantir a sua qualidade.

Em concorrência com o sinal de IPTV será iniciado o tráfego de dados convencionais.

Na criação da Metro Ethernet Network serão usadas tecnologias que estão em uso no mercado como: enlaces E-Line para ligação entre os equipamento do nó central, proteção contra falhas nas UNIs, acessos remotos para administração aos equipamento de forma segura, protocolos de roteamento, proteções contra degradação de processamento por loop, limitadores de tráfego inteligentes, E-Line montadas através de fibras óticas e cabos UTPs.

Um dos objetivos deste estudo é fazer com que a estrutura MEN chegue muito próxima do que seria uma estrutura real.

Como toda a estrutura que envolve uma transmissão real de televisão através de redes Metro-Ethernet é extremamente cara e complexa, todas as características das transmissões serão simuladas via *software*. Assim, serão utilizados *softwares* capazes de simular os dados que estariam sendo enviados pelos servidores de vídeo.

Este projeto não visa desenvolver serviços ou aplicativos de transmissão de imagem sobre redes.

1.3) Estrutura da monografia

Este trabalho será dividido em cinco capítulos principais e estes se subdividirão em tópicos conforme a conivência do tema abordado em cada capítulo.

O primeiro capítulo introduz o tema, especificando objetivos e a estrutura da monografia. No segundo capitulo será apresentada toda a parte teórica de referência que será usada no projeto. Nele, serão mostradas às principais características do IPTV, as ferramentas que compõem as redes Metro-Ethernet, serviços agregados a estas tecnologias e também os switches de camada dois e três.

Já no terceiro capitulo, será tratado todo o desenvolvimento do projeto, a estrutura laboratorial que será montada, escopos, ferramentas usadas nas simulações e também os *softwares* e *hardwares*. Todos estes vinculados às tecnologias abordadas no segundo capitulo.

Os resultados obtidos nas simulações serão apresentados no quarto capitulo. Também serão inseridos neste capítulo os gráficos, telas de configuração, telas dos aplicativos, tabela de valores e estatísticas.

No quinto e último capitulo, dar-se-á o fechamento ao trabalho. Nele, serão apresentados os comentários de todo o trabalho, também as conclusões obtidas e por fim sugestões para os trabalhos futuros.

1.4) Resultados esperados

Ao final do trabalho espera-se chegar a dois pontos. O primeiro será adquirir e apresentar uma boa base teórica sobre os assuntos tratados e solidificar os conhecimentos adquiridos durante o curso de Engenharia da Computação. O segundo trata da parte experimental. Após estas simulações, apresentar as condições de viabilidade para a transmissão de IPTV sobre os ambientes reais, para poder suportar o tráfego simultâneo de IPTV.

Serão considerados resultados satisfatórios as transmissões de IPTV e de dados que estiverem concorrentes no mesmo ambiente, porém, sem que uma influencie ou prejudique a outra. Será considerado um resultado insatisfatório caso o tráfego de informações de IPTV degrade as características de disponibilidade da rede.

CAPÍTULO 2 - Tecnologias de Redes, Metro-Ethernet e o IPTV

A transmissão de sinais utiliza infra-estruturas de redes baseadas em modelos amplamente estudados, quer seja a transmissão de dados convencionais, como a transmissão de vários tipos de tráfego em redes convergentes. A seguir serão apresentadas, brevemente, duas das arquiteturas mais utilizadas no estudo e implementação de redes: o modelo ISO/OSI e o TCP/IP. Além disso, será apresentada brevemente a tecnologia Ethernet, formação de redes e serviços associados, com o uso do protocolo IP.

2.1) Modelos ISO/OSI e TCP/IP

Para que haja comunicação entre computadores e dispositivos de rede é necessário estabelecer padrões. Esses conjuntos de padrões definem as estruturas, suas interfaces e protocolos.Dentre os protocolos mais conhecidos e usados temos os modelos ISO/OSI e TCP/IP.

O modelo TCP/IP é amplamente usado e bem difundido e atualmente está presente em boa parte das redes de computadores de todo o mundo.

Já o ISO/OSI não teve a sua utilização muito difundida, porém, por conseguir descrever bem as características de cada camada, ainda é muito válido como modelo de referência.

2.1.1) Modelo ISO/OSI

A sigla ISO significa (*International Organization for Standardization*), esta é uma organização internacional de padronização. A ISO criou um modelo em camadas para a comunicação em sistemas operacionais heterogêneos chamados OSI.

O modelo OSI é baseado em uma proposta desenvolvida pela ISO como um primeiro passo na direção à padronização internacional dos protocolos empregados nas diversas camadas. [Day e Zimmermann, 1983]. Ele trata da intercomunicação de sistemas abertos - ou seja, sistemas que estão abertos à comunicação com outros sistemas. [Tanenbaum, 2003]

Segundo Wendell Odom o modelo OSI pode assim ser definido – “Trata-se de um conjunto muito bem definido de especificações de protocolos com muitas opções para realizar tarefas similares”.

O modelo OSI proposto pela ISO é composto por 7 (sete) camadas, cada uma delas com tarefas bem definidas. [Tanenbaum, 2003]. As sete camadas deste modelo, na ordem da camada inferior até a superior, são:

Física (Camada um) – É a camada que trata sobre as características físicas da rede, tais como correntes elétricas, conectores, voltagens usadas na composição dos bits, modulação de luz, duração dos bits transmitidos. Nesta camada, como exemplo, temos as fibras óticas e os cabos de pares trançados UTP.

Enlace de dados (Camada dois) – A principal tarefa da camada de enlace de dados é transformar um canal de transmissão bruto de dados em uma linha que pareça livre de erros de transmissão não detectados na camada de rede. [Tanenbaum, 2003]

Nesta camada começa a ser feita uma verificação do controle de fluxo de informação entre receptor e transmissor. Com isso evita-se o aparecimento de erros.

Neste nível são detectados e corrigidos os erros na transmissão por meio da contagem de caractere, transparência de caractere, transparência de bit e detecção de quadros, verificando a violação do sinal no meio físico.

Nesta camada também é realizado o controle de fluxo. Este processo evita que o transmissor mande mais informação do que o buffer do receptor pode processar.

Rede (Camada três) – Esta camada é responsável pelo roteamento entre redes, ou seja, quando um pacote tem que trafegar de uma rede para outra até chegar ao seu destino é usada a camada 3. As informações da localidade de cada rede são guardadas em tabelas de roteamento, que podem ser estáticas ou dinâmicas.

Transporte (Camada quatro) – A função básica da camada de transporte é aceitar dados da camada acima dela, dividi-los em unidades menores, caso necessário, repassar essas unidades a camada de rede e assegurar que todos os fragmentos chegarão corretamente à outra extremidade. [Tanenbaum, 2003]

Neste nível já observamos a comunicação real entre os computadores (máquina de origem e máquina de destino), comunicação fim a fim. Nesta camada também existe um controle quanto ao envio excessivo de informação do transmissor para o receptor.

Sessão (Camada cinco) – Nesta camada ocorre a definição dos parâmetros que são usados para que os computadores possam estabelecer a comunicação entre si, ou seja, para iniciar, controlar e encerrar as sessões.

Entre as funcionalidades disponibilizadas por esta camada, as que mais se destacam são: gerenciamento de token, controle de diálogo e gerenciamento de atividades.

Apresentação (camada seis) **–** A função desta camada é a de definir formatos de dados, como textos ASCII e EBCDIC, Binário, BCD e JPEG. A criptografia também é definida pelo OSI como um serviço da camada de apresentação. [Wendell Odon, 2006]

A camada de apresentação está relacionada com a sintaxe e a semântica das informações transmitidas. [Tanenbaum, 2003]

Aplicação (Camada sete)– A camada de aplicação está diretamente ligada às formas como os aplicativos usam para estabelecer comunicação, ou seja, quando uma aplicação se comunica com outras máquinas em rede ela usa a camada de aplicação. Nesta camada também é tratada a diferença entre os sistemas de arquivos.

Está diretamente relacionada ao tipo de aplicação que está sendo usada, seja como aplicativos de rede como HTTP, SMTP, POP, FTP, etc.

A figura 2.1 apresenta o modelo ISO/OSI e suas sete camadas. Neste trabalho aspectos relacionados principalmente às camadas um, dois e três serão abordados.

Figura 2.1 Camada do modelo ISO/OSI **[Autor, 2007]**

2.1.2) Modelo TCP/IP

A sigla TCP/IP significa *Transmission Control Protocol/ Internet Protocol*. A arquitetura (TCP/IP) baseia-se principalmente em um serviço de transporte orientado à conexão fornecido pelo *Transmission Control Protocol* (TCP), e em um serviço de rede não orientado à conexão fornecido pelo IP. [Soares Luiz, 1997]

A arquitetura Internet TCP/IP dá uma ênfase toda especial à interligação de diferentes tecnologias de redes [Comer, 1991]. Esta arquitetura é composta por quatro camadas e uma subcamada.

Camada de Inter-redes - Esta camada é responsável pelo envio dos dados do ponto de origem até o destino final, trafegando por toda a rede, mesmo que esse ponto esteja em uma outra rede.

O trabalho realizado por essa camada pode ser ilustrado com o envio de correspondências através dos correios, onde as cartas são os pacotes e os correspondentes são computadores. Neste modelo é suficiente que se saiba o destinatário, pois o restante do trabalho é realizado pelo correio.

A tarefa da camada de inter-redes é entregar pacotes IP onde eles são necessários. O roteamento de pacotes é uma questão de grande importância nessa camada. [Tanenbaum, 2003]

Camada de transporte - A principal função desta camada é garantir que as aplicações tanto de origem como de destino tenham uma comunicação fim a fim.

Para realização desta tarefa pode ser usado o TCP ou o UDP. Com a utilização do TCP garante-se que os pacotes sejam entregues sem erros. Este protocolo pode ser caracterizado como orientado à conexão. O protocolo UDP utilizado por aplicações que não precisam de garantia de entrega. Este é caracterizado por não ser orientado à conexão.

Camada de aplicação - Esta camada está relacionada com os programas que acessam serviços de rede. As camadas de sessão, apresentação e aplicação do modelo OSI foram conglomeradas na camada de Aplicação do modelo TCP/IP. São exemplos de protocolos desta camada: TELNET, FTP, DNS, SMTP.

Camada de Host-redes - Abaixo da camada de inter-redes encontra-se um grande vácuo. O modelo de referência não especifica muito bem o que

acontece ali, exceto o fato de que o host tem que se conectar a rede utilizando algum protocolo para que seja possível enviar pacotes IP. [Tanenbaum, 2003]

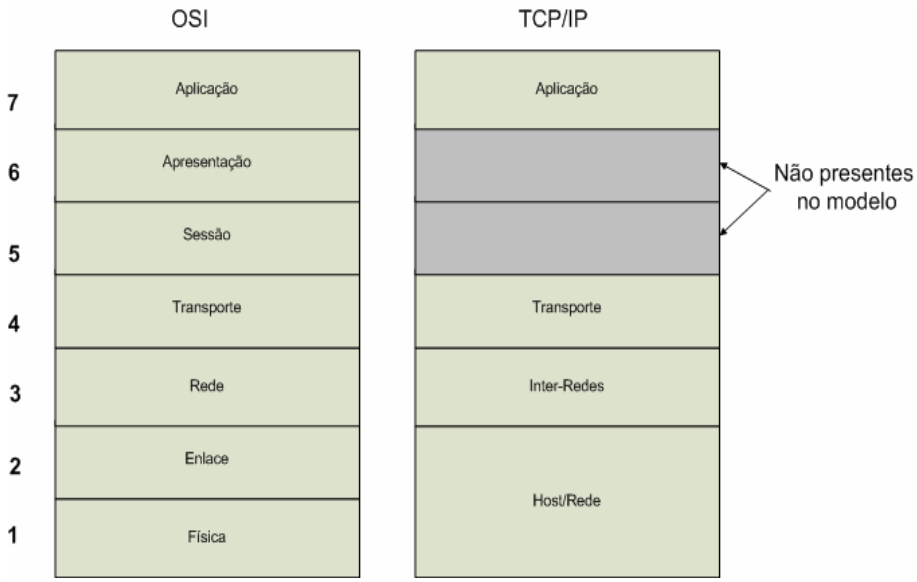


Figura 2.2 Modelos de Referência OSI x TCP/IP **[Tanenbaum, 2003]**

Neste trabalho serão abordados aspectos funcionais das camadas host de redes e inter-redes, com foco no protocolo IP e conectividade com redes ethernet, especificamente com o uso do protocolo IP em redes Metro Ethernet para a transmissão do sinal de TV.

2.2) O padrão Ethernet

Segundo os ensinamentos de Gabriel Torres “Ethernet é um padrão que define como os dados serão transmitidos fisicamente através dos cabos de rede. Dessa forma, essa arquitetura – assim como as arquiteturas *Token Ring* e FDDI – opera na camada 1 e 2 do modelo OSI” e complementa: “O papel do ethernet é, portanto, pegar os dados entregues pelos protocolos de alto nível e inseri-los dentro de quadros que serão enviados através da rede. O ethernet define também como fisicamente esses dados serão transmitidos”.

Os padrões mais usados em redes ethernet são 10BASE-T, 100BASE-T, 1000BASE-T. As velocidades mais usadas atualmente desta rede são 10 Mbit/s, 100 Mbit/s e 1000 Mbit/s, respectivamente. Porém esses não são os únicos; existem também o 10BASE2 e 10BASE5. Essa padronização foi feita pelo “Institute of Electrical and Electronics Engineers” (IEEE) e a norma que determina esses padrões é a IEEE 802.3. Essa norma aborda outros padrões que não foram

citados acima, porém nos atemos apenas a estes por serem os mais usados. [Tanenbaum, 2003]

Estas velocidades podem ser atingidas conforme a capacidade de cada equipamento ativo de rede ou placas de comunicação. O padrão para a maioria dos switches é que ocorra uma negociação da velocidade entre host e switch, assim de uma forma automática os equipamentos usam a melhor velocidade negociada. Porém, caso seja necessário uma velocidade estática, pode-se programar o switch para que não haja uma negociação entre o host. Desta forma, sempre será usada a velocidade programada.

É muito importante manter a padronização pois, através desta, consegue-se o incremento de velocidades, o que permite continuar evoluindo as taxas de transmissão e tornar possível o trabalho com as mesmas aplicações em redes diferentes desta.

2.2.1) Controle de colisões Ethernet CSMA/CD

Em um ambiente Ethernet, os computadores usam o mesmo barramento (meio) para trocar informações. Quando dois ou mais computadores, switches ou bridges tentam usar o mesmo barramento simultaneamente ocorre uma colisão de pacotes.

Um dos equipamentos usados nas redes é o *Hub*. Em um *Hub* todos os computadores estão no mesmo barramento. Uma das características destes é que eles criam um único domínio de colisão, ou seja, todos os equipamentos que estão diretamente ligados neste Hub competem pelo mesmo barramento.

Para evitar ou diminuir estas colisões foi criada uma forma de controle para acessar o barramento chamado CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*). Com esse algoritmo as máquinas começaram a reconhecer as colisões. Carrier Sense é a forma que é usada para verificar se o meio já está sendo usado. *Multiple Access* permite que vários equipamentos possam concorrer pelo uso do barramento e *Collision Detection* é o mecanismo que percebe se ocorreu alguma colisão durante as transmissões.

Com isso, antes dos dispositivos usarem o barramento eles escutam o seguimento para verificar se ele já esta sendo usado, caso esteja, eles esperam para transmitir os pacotes. Essa proteção não evita que ocorra uma colisão, porém os equipamentos são capazes de detectar essa colisão e tomar medidas caso elas ocorram.

Conforme os ensinamentos de Tanenbaum “Se duas estações perceberem que o canal está desocupado e começarem a transmitir simultaneamente, ambas detectarão a colisão quase de imediato” e finaliza “Em vez de terminar de transmitir os seus quadros que já estarão irremediavelmente adulterados, elas devem interromper a transmissão de forma abrupta tão logo a colisão seja detectada”. [Tanenbaum, 2003].

2.2.2) Controle de colisões Ethernet CSMA/CA

Outra forma de controle de colisão é o CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), que faz com que as estações transmitam as informações em intervalos de tempos pré-determinados. Desta forma, cada estação aguarda a sua vez para iniciar a transmissão de suas informações até que outra termine a sua transmissão.

Caso nenhuma estação faça uso do seu intervalo de transmissão, será fechado o ciclo a rede irá operar em CSMA normal.

2.2.3) Controle de colisões Ethernet – O uso de SWITCHES

Os switches são equipamentos muito mais eficientes e conseguem reduzir as colisões. Eles conseguem armazenar em seu buffer interno os pacotes que iriam concorrer pelo mesmo barramento.

Independente da quantidade de pacotes recebidos para diferentes portas o switch consegue armazenar na sua memória o pacote até que o meio esteja disponível para o envio. Assim eles conseguem criar múltiplos domínios de colisão.

A criação desses múltiplos domínios de colisão é realizado através da tabela de MAC (*Media Access Control*), esta contém o endereço IP e o endereço MAC referente a cada equipamento conectado ao switch.

Com esta tabela o switch consegue associar uma porta física a um equipamento. Desta forma quando os pacotes tiverem que ser transmitidos para uma estação X ligado na porta Y o switch enviará os dados apenas para a porta de destino Y.

Segundo a definição da RFC (*Request For Comments*) 826 “Este protocolo permite de forma dinâmica a distribuição das informações necessárias para construir as tabelas que traduzem um endereço IP em um endereço no espaço (endereço de *broadcast*)” [Plummer, 1982]

Para poder montar a sua tabela o switch precisa saber o endereço físico de cada máquina para isso ele pode usar o protocolo ARP (*Address Resolution Protocol*) ou RARP (*Reverse Address Resolution Protocol*).

Partindo do principio que a troca de informações do switch está sendo realizado pela primeira vez, sua tabela está vazia e deve ser preenchida. Como no inicio apenas o endereço IP esta disponível, então o switch envia o pacote para todas as máquinas do domínio de colisão excluindo a da porta de origem. A partir da resposta da maquina sabe-se qual é a porta de destino e seu MAC podendo assim ir montando a tabela com endereço de IP, porta e endereço de MAC correspondente.

O processo de preenchimento da tabela usando RARP é muito parecido com o ARP. O que é feito com RARP é o processo reverso do ARP.

“RARP representa a evolução dos protocolos definidos para ajudar os host de forma dinâmica descobrir o endereço IP. Esse protocolo requer que o cliente mande *broadcast* para começar a descoberta.” [Odon, 2006]

No RARP inicialmente temos apenas o MAC e queremos saber qual o IP.

“O RARP é uma requisição do próprio host para descobrir o seu próprio endereço IP. Assim RARP usa a mesma mensagem do ARP.” [Odon, 2006]

2.3) Metro-Ethernet

A idéia principal de Redes Metro-Ethernet está em utilizar a tecnologia Ethernet para áreas metropolitanas. Estas redes normalmente têm a dimensão de uma cidade e usam como principal meio de comunicação a fibra ótica.

Esta tecnologia está em franca expansão principalmente nos países desenvolvidos como Europa, Japão e Estados Unidos. Aqui no Brasil esta tecnologia já se encontra disponível em algumas das principais capitais.

Uma Rede Metro Ethernet é definida como uma rede MAN (*Metropolitan Area Network*) que conecta ou serve de ponte para redes LAN geograficamente separadas, usando a tecnologia ethernet como forma de comunicação. É conhecida como MEN (*Metropolitan Ethernet Network*).

Uma vantagem da MEN é a velocidade da taxa de transmissão por interface que podem ser alcançadas de 1 Mbps, 10 Mbps, 100 Mbps, 1 Gbps e 10 Gbps. E está em faze de teste, os incríveis 100 Gbps. Muitos prestadores de serviços de telecomunicação vêem a necessidades de passarem a usar portas de 100 Gbps para a comunicação com sua rede de transporte. Conforme a

necessidade de cada empresa esses taxas de transmissão podem ser aumentadas para 200 Gbp/s, 400 Gbps.

Quando falamos de Metro-Ethernet devemos lembrar que esta tecnologia é usada pelos provedores de serviços (na maioria empresas de telecomunicações), e não por pequenas ou médias empresas, por isso a necessidade de velocidades tão altas.

As tecnologias abordadas no item sobre Ethernet servem de norte para o uso em Metro Ethernet Network. É segundo Wagner L. Zucchi é importante salientar que ”Metro Ethernet não é simplesmente uma porta de um switch, com taxa de transmissão de 10 ou de 100 Mbit/s, e que aceita quadros com o formato utilizado em redes locais. Embora um acesso Metro-Ethenet seja fisicamente idêntico a um cabo Ethernet convencional, os dados que trafegam num cabo de uma rede Metro Ethernet são divididos em circuitos virtuais, uma entidade lógica que permite caracterizar o serviço oferecido a cada quadro transmitido.” [Wagner L. Zucchi, 2006]

A organização que estuda e padroniza as redes Metro Ethernet é a MEF (Metro Ethernet Forum). Na sua composição estão engenheiros, empresas de telecomunicação, empresas que desenvolvem equipamentos, cientistas e outros.

Entre as áreas de atuação do MEF os que mais se destacam são: especificações técnicas, implementações e certificações de equipamentos. [MEF, 2007]

O MEF trabalha em conjunto com instituições como IEEE. É uma organização sem fins lucrativos, formada com a missão de acelerar a utilização mundial das tecnologias de transporte por ethernet, classe de redes e serviços ethernet. [MEF, 2007]

Existem cinco atributos que são muito importantes nas redes metro. São eles: qualidade de serviço, gerenciamento de serviço, escalabilidade, padronização de serviços e confiabilidade.

2.3.1) Vantagem do uso de soluções em Metro-Ethernet

Como boa parte das redes locais utiliza Ethernet, apenas em casos muito específicos são utilizados protocolos diferentes nas redes locais. O uso de Ethernet facilita a migração para uma rede Metro-Ethernet, assim pode-se baixar o custo da migração; a migração pode ser feita de forma rápida.

A Ethernet, por ser uma tecnologia bastante difundida, quando usada em áreas metropolitanas, traz pontos importantes como facilidade no uso, custo e flexibilidade. Por ser largamente usado em redes locais, o conhecimento técnico também é aproveitado quando se migra para uma estrutura metropolitana.

A facilidade no uso se dá porque os equipamentos (computadores, ativos de rede, placas de rede) das redes já usam essa tecnologia, simplificando a estrutura da rede. Outra vantagem está no custo para aquisição de novos equipamentos, pois os custos em redes ethernet são menores que em redes ATM ou *Frame Relay*. [MEF, 2007]

Para os provedores de serviço a grande vantagem vem da velocidade do serviço, onde podem oferecer links com capacidades que variam de 1Mbps a até 1Gbps. Vários serviços podem ser agregados a um link nessas velocidades (de acordo com a necessidade de cada cliente),
e estes por sua vez a links de mais alta capacidade no núcleo da rede, como 10 Gbps.

Podem ter EVCs (*Ethernet Virtual Connection*) com circuitos dedicados, exclusivos, com garantia de taxa de transmissão, com redundância e com multiplexação.

2.3.2) Crescimento da Metro-Ethernet no mundo

Muitos estudos têm sido desenvolvidos sobre o mercado Metro-Ethernet. Estes estudos apontam um grande crescimento nesta área. De acordo com o site da *Infonetics Research* (empresa internacional especializada em estudos do mercado), a soma de todos os gastos para a aquisição de novos equipamentos no mundo nesta área será de 64 bilhões de dólares. Este valor acumula as estimativas com valores gastos entre os anos de 2005 até 2009.

A figura 2.3 mostra a previsão de gastos durante o período de 2006 até 2010. Deve-se observar que esta figura mostra o valor anual. Para obter-se o total do investimento até 2010 deve-se realizar a soma de todos os anos.

Michael Howard diretor de *Infonetics* acrescenta dizendo “A cada ano a ethernet chega mais perto de se tornar o modo dominante de transmissão de dados por todo mundo, com dezenas de milhões de portas de 1G, 10G prontas em redes metro e muitas mais projetadas.”

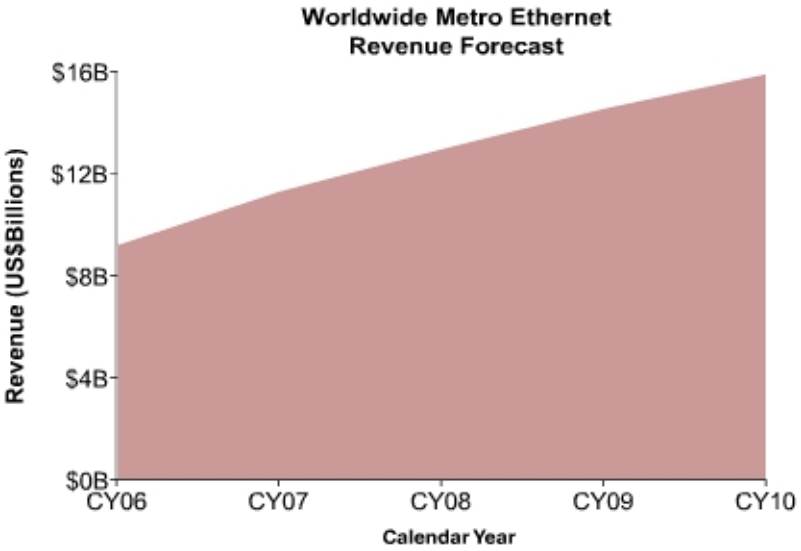


Figura 2.3 Previsão de gastos com rede Metro Ethernet **[Infonetics Research, 2007]**

2.3.3) Atributos a serem considerados na rede Metro-Ethernet

2.3.3.1) Qualidade de Serviço (QoS)

Deve-se conseguir monitorar a perda de pacotes, o uso de ferramentas para detecção de atrasos ou alteração no envio dos pacotes. Disponibilizar recursos de priorização de tráfego. Deve-se ter também recursos para garantir a taxa de transmissão. Tais aspectos deve ser utilizados para estabelecer-se um SLA (*Service Level Agreement*) que monitora a disponibilidade de recursos fim-a-fim, com performance baseada em CIR (*Committed Information Rate*), perda de pacotes, atrasos, variação de atraso.[MEF, 2007]. Em fim, que permita escolhas amplas entre a qualidade da banda e a qualidade do serviço. [MEF, 2007]

2.3.3.2) Gerenciamento De Serviço

As redes Metro-Ethernet podem ser gerenciadas de forma centralizada, mesmo os equipamentos estando a quilômetros de distância. Isso diminui custo de manutenção, dá celeridade aos novos processos que são implantados e facilita o gerenciamento.

Para o MEF essas redes devem ter “Habilidade de monitorar, diagnosticar e gerenciar centralmente a rede, usando bases de serviços padronizados independente do fornecedor dos equipamentos.” e “devem disponibilizar também recursos de manutenção, operação e administração” [MEF, 2007].

2.3.3.3) Escalabilidade

Essas redes devem ter capacidade de aumentar um link de comunicação de 1Mbps até 10 Gbps, conseguindo agregar mais portas aos equipamentos e mais equipamentos as redes.

Consegue transpor acessos metro para serviços nacionais globais por uma variedade de equipamentos. [MEF, 2007]

Uma rede com a capacidade para milhões de usuários utilizarem um serviço de rede que é ideal para as mais amplas variedades de negócios, informações, comunicação e entretenimento e aplicações com voz e dados. [MEF, 2007]

2.3.3.4) Padronização De Serviços

Deve ser suportado E-LAN, E-Line e VPL. A padronização dos serviços exige que não ocorram alterações nos equipamentos dos clientes para sua utilização. Esses padrões são usados em todos os pontos, seja no provedor de acesso ou no cliente.

Não deve requerer alteração nos equipamentos de rede local do cliente ou acomodações das redes atualmente existentes e conectadas como as time-sensitive sinalização de tráfego TDM. Para o MEF “E-Line, E-LAN provê de forma transparente, linhas privadas, linhas privadas virtuais e serviços de LAN” [MEF,2007]

2.3.3.5) Confiabilidade

Está associada à capacidade dessas redes disponibilizarem recursos que detectem e corrijam erros sem que esses problemas afetem a comunicação dos dados de toda a estrutura.

E exige mais, pois mesmo ocorrendo algum problema o tempo de recuperação da rede deve ser muito rápido. Esse tempo de recuperação não deve ultrapassar 50 ms.

Para o MEF uma das características mais importantes dessas redes é a forma de “encontrar os mais exigentes recursos de qualidades e disponibilidade.” [MEF, 2007]

2.3.4) Preservação dos atributos de CoS

Com o CE-VLAN CoS ocorre a preservação dos dados presentes no cabeçalho dos frames que contém os atributos de CoS 802.1p. Esse recurso faz com que as informações não sejam alteradas (preservadas) ao passar por EVCs.

Os dados que entram na MEN com informações de CE-VLAN CoS devem necessariamente sair idênticas como entraram.

2.3.5) Definição de Equipamentos e Dispositivos na Rede Metro-Ethernet

Nesta parte temos a descrição geral dos equipamentos e interfaces utilizadas, conforme os parâmetros do MEF, para a comunicação através da rede Metro-Ethernet. A figura 2.4 mostra o padrão de conexão entre o cliente e a MEN. A seguir são descritos os componentes dessa estrutura:

Customer Equipment (CE) – É o equipamento que está instalado na extremidade (borda) rede, normalmente fica no cliente e é responsável por interligar o cliente à rede. O equipamento usado para essa função é um switch/roteador. É indispensável ter um CE para se conectar a uma MEN.

User-Network Interface (UNI) – É a porta física (interface) que conecta o cliente ao provedor de serviço. Segundo a especificação da MEF é “uma demarcação física entre a responsabilidade do provedor de serviço e a responsabilidade do assinante”.

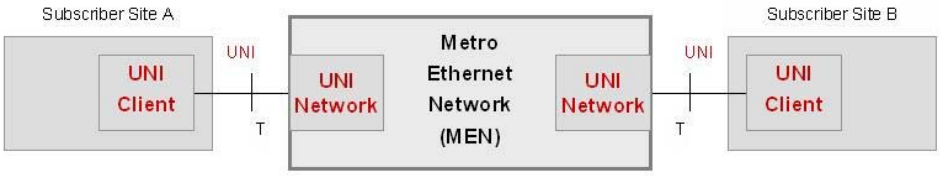


Figura 2.4 Diagrama de uma rede Metro Ethernet conforme o MEF **[MEF, 2007]**

Dependendo da localização e da funcionalidade agregada à UNI ela passa a ter outras classificações, tais como:

UNI *cliente* (UNI-C) - Quando está do lado do cliente é responsável por transmitir as informações para o domínio do provedor de serviço. Dependo da necessidade de cada cliente essa UNI-C pode ser gerenciada pelo provedor de serviço.

UNI *network* (UNI-N) – Este é o ponto de entrada para o domínio do provedor de serviço.

External Network-to-Network Interface (E-NNI) – Quando duas ou mais MEN precisam trocar informações de suas redes a interface usada é chamada de E-NNI.

Internal Network-to-Network Interface (I-NNI) – Interface usada para ligar a MEN aos elementos de rede.

Network Interworking Network-to-Network Interface (NI-NNI) – Ela esta associada às conexões ethernet virtual usadas para comunicação com outras redes que não sejam ethernet.

Service Interworking Network-to-Network Interface (SI-NNI) – Quando um MEN precisa trocar informações com outras redes e estas usam outras tecnologias (como ATM, *Frame Relay*, etc), o ponto de trocar de informações é chamado de SI-NNI

Neste trabalho entre as opções citadas acima utilizaremos interfaces UNI-C e UNI-N para a conexão entre os cinco switches que irão compor a estrutura de transmissão de IPTV.

2.3.5.1) Segmentações da Estrutura Física da MEN

Podemos dividir a estrutura física em quatro partes: *Core* (Núcleo), *Aggregation* (agregação), *Edge* (Borda) sendo que esta última se subdivide em outras duas categorias MTU ou CPE.

O *Core* ou Núcleo desta rede é composto por switches interligados como topologia anel através de portas de 10Gbps. Estas portas podem estar agregadas através de agregações de links que somados chegam a 40 Gbps, 80 Gbps dependendo da necessidade da rede. Por ter a capacidade de se comunicar em grandes velocidades o core têm como característica a velocidade de transmissão de pacotes, suporte a engenharia de tráfego e gerenciamento de congestionamento. Os protocolos de roteamento usados são OSPF, RIP, IBGP e outros. [Foundry, 2007]

Na camada de Agregação existe um grande fluxo de informações de entrada e saída. Neste segmento ocorre à agregação dos tráfegos e o gerenciamento de congestionamento. Este ponto fica localizado entre o Core da rede e a extremidade *Edge*. Este ponto também pode ser chamado de *Distribution* (Distribuição).

Edge – É o equipamento que esta na rede do cliente que contém todos os elementos necessários para que o cliente possa requisitar os serviços da MEN. Esse equipamento tem que suportar os requisitos mínimos para que possa

estabelecer uma relação com a MEN. Como esses equipamentos estão próximos das extremidades da rede recebem o termo *edge* (borda, extremidade).

De acordo com a forma que o equipamento de *Edge* estiver sendo usado, ele pode ter duas definições de MTU (*Multi-Tennant Unit*) e de CPE (*Customer Premises Equipment*).

O switch que faz a função do MTU fica no ponto mais extremo da rede. Pode ficar, por exemplo, em um prédio ou condomínio que contém vários escritórios ou residências, assim cada escritório ao invés de ter um único equipamento “aluga” apenas uma interface e esta interface é responsável pela entrega dos serviços contratados. As informações que trafegam por esta porta estão isoladas por VLANs. Assim todos os escritórios podem compartilham o mesmo equipamento (MTU) sem que isso afete a segurança dos dados que estão trafegando pelo equipamento. [Foundry, 2007]

A figura 2.5 exemplifica a estrutura de uma MEN composta por *Core*, *Distribution* e *Edge*.

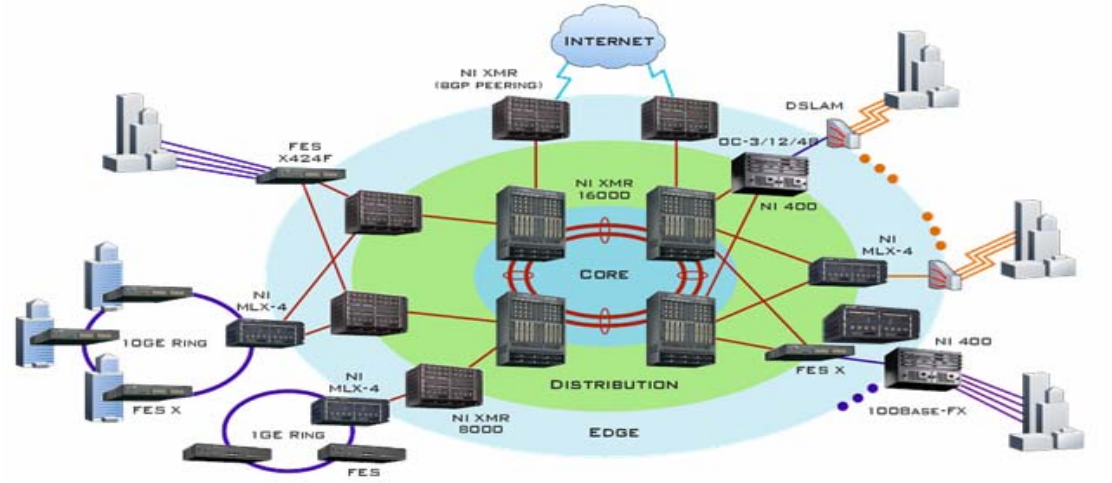


Figura 2.5 Topologia de uma MEN exemplificando Core, Distribution e Edge **[Foundry, 2007]**

O CPE tem as mesmas características do MTU, porém ao invés do equipamento ser compartilhado por várias empresas ou residências ele é usado por apenas um único escritório, por exemplo.

2.3.6) Serviços de transporte Ethernet

De acordo com as especificações da MEF um EVC (*Ethernet Virtual Connection*) é caracterizado por ser “uma associação de duas ou mais UNIs” e

completa “o aspecto fundamental dos serviços Ethernet está no *Ethernet Virtual Connection*” [MEF, 2007].

Um EVC pode trazer consigo duas características: uma ponto a ponto e a outra multiponto-multiponto.

Fazendo uma analogia a outros tipos de redes, um EVC age como um PVC em um *Frame Relay* ou uma SVC em um ATM.

2.3.6.1) Tipos de serviço

O serviço que roda ponto a ponto através de um EVC é conhecido como E-Line. Nele temos, basicamente, uma conexão entre duas UNIs interligadas. Assim, qualquer serviço Ethernet que for baseado em ponto a ponto por um EVC será designado como *Ethernet Line Service* (E-Line). [MEF, 2004]

O serviço E-Line pode prover largura de banda simétrica nas duas direções sem a garantia de performance. [MEF, 2004]

Este serviço pode-se subdividir de duas formas:

EPL (*Ethernet Private Line*) – Contém poucos recursos e a velocidade entre as duas UNIs sé igual. Não existe multiplexação.

EVPL (*Ethernet Virtual Private Line*) – Aqui já ocorre a multiplexação, vários circuitos podem ser usados simultaneamente.

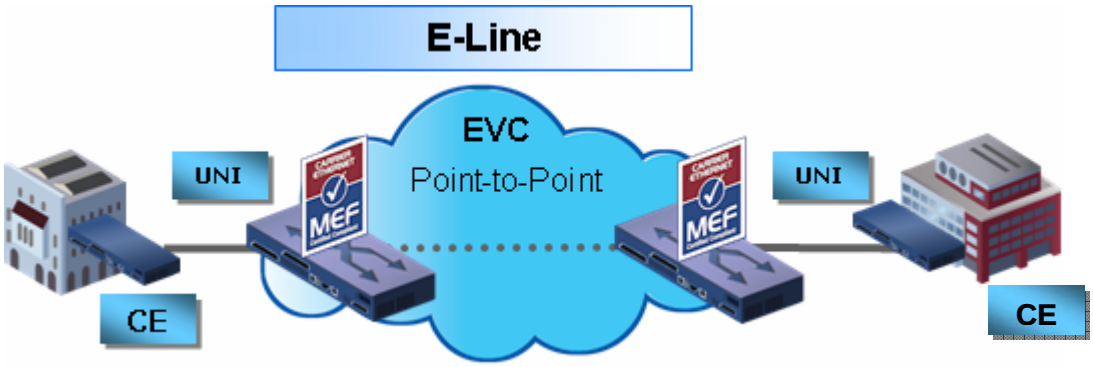


Figura 2.6 Diagrama de uma E-line conforme o MEF **[MEF, 2007]**

As conexões do tipo E-Line lembram os PVCs criados em circuito *Frame-Relay*.

Como pode ser observado na figura 2.6 existe apenas um EVC ponto a ponto que conecta os prédios. Esta topologia é indicada para MEN com poucos equipamentos.

O serviço E-LAN é caracterizado por ser multiponto-multiponto. Várias UNIs são usadas para interligarem vários pontos. As informações de uma UNI podem ser enviadas para uma ou mais UNIs simultaneamente.

Os serviços ethernet que forem baseados em multiponto-multiponto serão designados como E-LAN. Este recurso pode ser usado para criar um amplo leque de serviços. [MEF, 2004]

Com uma ligação E-LAN pode-se ter vários circuitos Ethernet virtuais. É importante ter vários métodos de garantia de banda, tais como CIR (*Committed Information Rate*), CBS (*Committed Burst Size*) e EIR (*Excess Information Rate*).

Para o tipo de serviço E-LAN pode ocorrer multiplexação em mais de uma UNI em um EVC. [MEF, 2004]

A vantagem de se utilizar essas tecnologias é que para o usuário, mesmo ele estando em uma MEN, aos seus olhos ele parece estar em uma LAN.

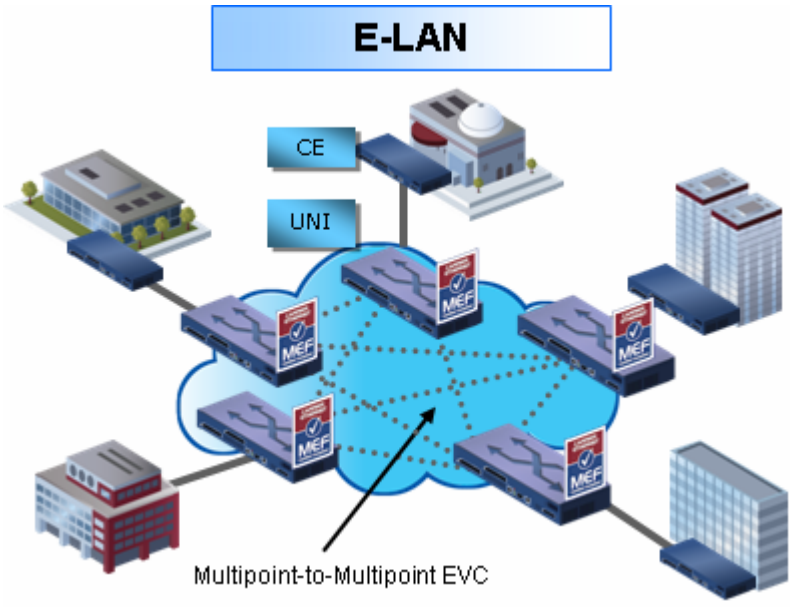


Figura 2.7 Diagrama de uma E-LAN conforme o MEF **[MEF, 2007]**

A figura 2.7 representa uma MEN que usa o serviço E-LAN, essa arquitetura é encontrada em grandes MENs.

O serviço E-TREE é parecido com o E-LAN só que a partir de um ponto existe a conexão para vários pontos. Já o **EPL** - (*Ethernet Private Line*) é um serviço especificado para ser usado com E-Line com UNIs dedicadas para fazerem conexões ponto a ponto .

Para o MEF “EPL prove um alto nível de transparência entre os serviços de frame entre as UNIs interconectadas ” e completa “O cabeçalho e o peso devem ser idênticos entre as UNIs de origem e destino” [MEF, 2004].

Só é permitido um único EVC entre as UNIs. Isso porque só passa informações do provedor de acesso e do cliente.

Com esse serviço temos várias características muito importantes como *Frame Delay*, *Frame Delay Variation* e *Frame loss*.

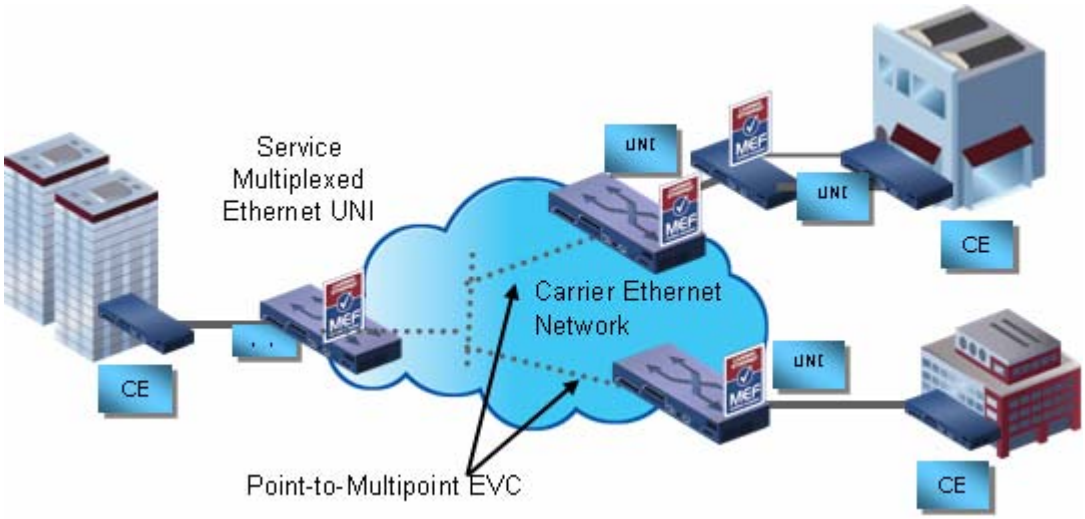


Figura 2.8 Diagrama de uma Ethernet Private Line conforme o MEF **[MEF, 2007]**

No serviço EVPL – (*Ethernet Virtual Private Line)* "é criado usando E-Line. Pode ser usado para criar serviços similares ao da Ethernet Private Line com algumas notáveis exceções. A primeira é que EVPL permite serviço de multiplexação para a UNI. Isto é, a capacidade de permitir que mais de uma EVC possa ser instalada em uma UNI, onde o EPL suportaria apenas uma". [MEF, 2004]

EVPL não tem transparência total dos dados que passam pelo EVC como no EPL e suporta Multiplexação. E isso faz com que uma UNI suporte mais de um EVC por multiplexação

Este serviço pode ser comparado com serviços *Frame-Relay* e o ATM. Caso ocorra a necessidade ele também pode substituir *Frame-Relay* ou serviços ATM.

Esses tipos de serviços serão extremamente importantes na estrutura laboratorial que será montada para os testes de transmissão de IPTV. Na ligação dos equipamentos centrais do laboratório será usado E-Line.

2.3.7) Métodos para Garantia de Largura da Banda de Transmissão

Conforme a necessidade de cada provedor de serviço ou cliente pode-se determinar a largura de banda disponível. O recurso usado para realizar esse

serviço é chamado de “*Rate Limit*”, este pode ser aplicado tanto na UNI como no CPE.

Os parâmetros usados são CIR, CBS, EIR e EBS. São eles que determinaram as características de largura da banda de transmissão.

Para o MEF o CIR define “A taxa média em bit/s para o service frame até a entrega na rede e executa os parâmetros definidos pelo CoS” [MEF, 2004].

O CBS define o número máximo de bytes disponíveis que podem ser enviados para uma UNI. [MEF, 2004]

A limitação de banda por CIR (*Committed Information Rate)* se subdivide em dois parâmetros, o “CIR rate” e o “CBS (*Committed Burst Size*) rate”. O CIR serve como limitador da quantidade máxima de bits que uma determinada interface (UNI) pode enviar ou receber durante um período de tempo, o padrão é 1 segundo. O valor é expresso em bits por segundo (bps). Se o tráfego for superior ao determinado pelo “CIR rate” entra o “CBS rate”. O CBS permite que a banda utilizada seja superior ao CIR. Normalmente o CBS é usado em períodos muito curtos, apenas quando existe um pico de utilização. Se os pacotes de entrada e saída forem maiores que os parâmetros de CIR e CBS, eles serão descartados ou será usado o EIR.

O EBS limita o número máximo de bytes disponíveis para estouro no ingresso de service frame enviados para uma UNI. [MEF, 2007] e o EIR é um parâmetro para largura de banda. Ele define a taxa média de bits/s que entram na rede. [MEF, 2007]

O EIR (*Excess Information Rate*) e o EBS (*Excess Burst Size*) trabalham de forma análoga ao CIR e o CBS. O EIR é requisitado quando o tráfego excede ao valor determinado para o CIR e CBS. A diferença entre o EIR e o CIR é que o EIR só é acionado quando os parâmetros do CIR são superados.

Quando o EIR é requisitado ele prove uma banda adicional para acomodar as requisições de entrada e saída. Se essa banda adicional também não for suficiente o CBS é acionado para liberar mais.

Vale observar que nenhum desses recursos pode ultrapassar a capacidade de transmissão das interfaces (UNI).

2.3.8) Estruturas e requisitos de proteção ethernet em MEN

“Proteção em Metro Ethernet Network (MEN) pode abranger várias idéias. Basicamente, é um tratamento próprio da rede que permite que esta continue em funcionamento com o mínimo ou sem impacto para os usuários da rede em

distribuição, parada ou degradação dos aparelhos ou equipamentos da MEN.” [MEF, 2004]

Essa proteção se subdivide em dois pontos. O primeiro é dos usuários que utilizam os serviços da MEN e o segundo é a visão do provedor de serviço.

Para os usuários existe um existe uma descrição técnica chamada de SLS (*Service Level Specification*), este contém os métodos e os mecanismos de proteção usados pelo provedor de serviço.

Para o provedor de serviço a união de todas as SLSs dos seus clientes compõe os requisitos que devem ser alcançados para a proteção da MEN.

Para que o provedor de serviço possa montar uma estrutura que atenda os requisitos de proteção, ele deve estar atento a três pontos: Detecção, Políticas e Restauração.

A detecção refere-se à habilidade de determinar falhas na rede. A política refere-se ao que pode ser feito quando falhas forem detectadas e a restauração é o componente que age para corrigir a falha; pode não ser uma recuperação total de todos os serviços e depende da natureza da falha e da política. [MEF, 2004].

Na maioria dos casos, um EVC implementando um serviço ethernet atravessa diferentes transportes de fim a fim e a proteção pode envolver mecanismos diferentes. [MEF, 2004]. Entre esses mecanismos de proteção estão o STP, RSTP, *Link Aggregation*, VRRP , entre outros.

Todos os EVCs que fazem parte de um mesmo trecho da rede devem ter os mesmos requisitos de proteção; só desta maneira a rede poderá cumprir com todos os requisitos de proteção.

2.3.8.1) Proteção de link baseado em agregação de link (802.3ad)

O LACP (*Link Aggregation Control Protocol*) é o protocolo usado pelos equipamentos para estabelecerem e monitorarem as agregações de link.

A “agregação de link” ou trunk é um grupo físico de interfaces (UNI) que agem como se fossem uma única interface. Esse tipo de ligação é montada entre dois switches/roteadores, ou até mesmo entre servidores. Em caso de falha em um dos links o conjunto não é afetado, ele apenas deixa de contar com o link que foi perdido.

Através da agregação de link consegue-se ter a soma da velocidade das interfaces, balanceamento de carga, redundância a falha. Essas agregações podem ser feitas com UNIs de 1000Mpbs e 10 Gbps.

As interfaces que fazem parte de uma agregação de link podem ser fibras ou cabos UTPs. Podem ser montadas agregações de link com duas, quatro, oito UNIs.

Depois de estabelecida a agregação entre as interfaces do trunk os equipamentos passam a trocar pacotes LAG (*Link Aggregation Group*) esta troca de pacotes é feita como os BPDU (*Bridge Protocol Data Unit*) do *Spanning Tree*.

Existem duas formas de monitoração dessas agregações: "*Slow mode*" e " *Fast mode*".

No *Slow mode* a troca de pacotes é feita a cada trinta segundos e a falha é corrigida em noventa segundos. Na *Fast mode* as mensagem de LACP são trocadas a cada um segundo e a falha é corrigida em três segundos.

2.3.8.2) IEEE 802.1D (Spanning Tree Protocol)

O *Spanning Tree Protocol* (STP) é uma algoritimo que impede a criação de *loop* entre as bridges ou switches, habilitando um único trajeto físico entre os switches.

STP usa mensagens entre os switches para estabilizar a rede para uma topologia livre de *loop* [Odon, 2006]

O *loop* na rede ocorre quando existem dois ou mais trajetos (redundantes) entre mesmos switches. Com isso o mesmo pacote é encaminhado infinitamente de um equipamento para outro. A topologia de uma rede em *loop* é mostrada na figura a seguir:

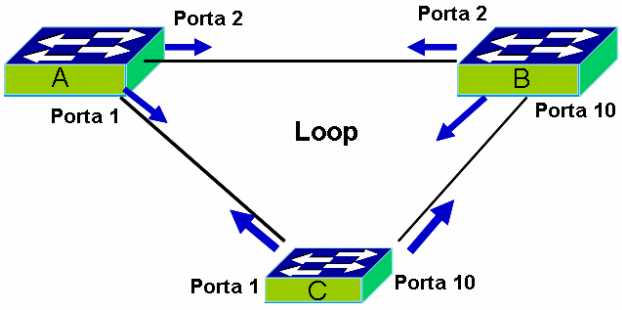


Figura 2.9 Diagrama de uma rede em loop **[FOUNDRY, 2007]**

O processador do switch usará 100% da sua capacidade para resolver a entrega deste pacote em *loop* e não conseguirá mais processar o resto dos pacotes. Uma rede em estado de *loop* fica completamente fora do ar.

Na resolução desse problema é usado o *spanning tree protocol*. Este protocolo troca informação entre os switches até que a rede se estabilize até um

estado de “*loop-free topology*” topologia livre de *loop*. Este objetivo só é atingido após vários passos. [Foundry, 2007]

O STP altera a forma como são “visualizadas” as interfaces (portas) de *up-link* entre os switches. Uma interface normal tem dois estados básicos: *forward ou receive*, para SPT as interfaces podem estar em vários estados:

Blocking – O protocolo STP bloqueia a porta, ela deixa de enviar pacotes para prevenir o loop.

Forwarding – A interface está enviando e recebendo pacotes do barramento de forma normal.

Disable – A porta não faz parte da proteção de STP.

Listening – Quando ocorre uma alteração na topologia, essa porta recebe BPDUs dos equipamentos próximos, assim podendo determinar a nova topologia.

Learning – Após o estado de listening ela passa para learning. Essa porta não envia nem recebe pacotes, porem aprende os MACs.

Para o STP deve existir um switch “principal” dentro desta rede. Só pode existir apenas um único switch com essa característica, este será chamado de “*switch root*”. Para determinar quem fará o papel do *switch root* ocorrerá um processo interno entre os switches de seleção. Todos os equipamentos presentes na rede participam dessa eleição. O primeiro passo a ser feito é determinar o *Switch Root*.

2.3.8.2.1) Determinação da Switch Root.

Apenas um switch pode ser o root do *spanning tree*; para selecionar o *root*, os switches organizam uma eleição. [Odon, 2006]. Neste processo de eleição todos os switches trocam entre si uma mensagem de “*olá*” chamada de BPDU (*Bridge Protocol Data Unit*), nela eles pedem para se tornar o *switch root* da rede.

Os switches ficam ouvindo as repostas uns dos outros. Quando o switch recebe uma resposta e nela tem um *Bridge ID,* se este for inferior ao seu, ele pára de enviar solicitações para ser o root da rede. Ganhará a eleição o switch com o menor *Bridge ID*.

O Bridge ID é composto por dois argumentos o *Bridge Priority* e o endereço MAC da interface

2.3.8.2.2) Determinação da Porta Root.

Depois de eleito o *Switch Root* inicia-se o processo de determinação da *Porta Root*.

Porta *root* de um switch é a porta que está diretamente conectada ao switch *root* ou porta na qual o switch pode se conectar ao *root* mesmo que de forma indireta.

Todos os switches devem informar qual será a sua porta *root*. Podemos dividir este processo em quatro passos principais.

- O switch *root* inicia o envio de "*Olá"* a cada 2 segundos.
- Todos os outros equipamentos respondem a esse "*Olá*". Nesta resposta também são enviadas informações sobre: o custo da porta; o *bridge ID*; prioridade da porta;
- Os equipamentos que não responderem, ficarão com suas portas em estado de *blocking*.
- A porta com o menor "custo" será a *Porta Root*.

O principal objetivo de determinar a porta root é saber qual é o melhor trajeto para os dados nesta nova topologia que será criada. Por isso leva-se em conta durante o calculo do custo do trajeto, a velocidade da porta e o número de estágios que serão necessários para chegar a esta porta.

Tabela 2.1 Diagrama do custo da interface em relação ao STP e RSTP **[FOUNDRY, 2007]**

Velocidade	Custo Original IEEE	Custo revisado pelo IEEE
10 Mbps	100	100
100 Mpbs	10	19
1000 Mbps	1	4
10 Gbps	1	2

2.3.8.2.3) Eliminação de caminhos redundantes.

Depois que os switches descobrirem e determinarem quais são as portas que os levam ao *switch root*, eles bloqueiam todas as portas que criam caminhos redundantes, assim garantem que não ocorra mais *loop*.

A figura 2.10 mostra como ficou a topologia livre de *loop* da figura 2.9.

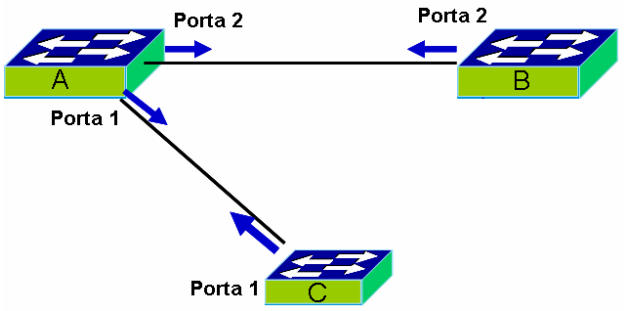


Figura 2.10 Diagrama mostra a nova topologia da fig. 2.9 sem loop **[FOUNDRY, 2007]**

O switch que ficar responsável de encaminhar os dados para a LAN será chamado de "*Designated Switch*" e a interface que ele usar neste encaminhamento será chamada de "*Designated Port*".

A partir do momento que os equipamentos já estiverem estáveis ficam ocorrendo alguns processos de monitoração. São eles:

- O *Switch Root* gera constantes mensagens de olá relacionado com o tempo.
- Todos os outros switches recebem estes olás.
- Eles atualizam esses olás e devolvem para o *Switch Root*
- O *Switch Root* recebe também a informação sobre todas as portas que estão em estado de *blocking*.

Quando não estiver mais ocorrendo nenhum processo de eleição entre os switches o *Spanning Tree Protocol* fica monitorando todos os olás enviados pelos switches.

Esta monitoração é necessária; caso algum olá chegue alterado o protocolo saberá que ocorreu uma alteração na topologia da rede e novos estudos deverão ser feitos para determinar a nova topologia. [Odon, 2006]

O STP lógico monitora o processo normal de troca de olá quando a topologia está estável; quando o processo de olá se altera, o STP precisa reagir e convergir para uma nova topologia. [Odon, 2006]

No caso de ter ocorrido uma alteração na topologia, o *Switch Root* perde essa característica e assim ele deixará de mandar os olás na rede e os outros switches perceberão a ausência do *Switch Root* e iniciarão um novo processo de eleição e determinação de topologia. Os fatos que geram esses novos estudos podem ser link *down*, o switch desligou, mais um novo caminho surgiu, entre outros.

O processo de eleição de novos equipamentos pode ser chamado de recalculo de *Spanning Tree*.

2.3.8.3) IEEE 802.1D (Rapid Spanning Tree Protocol)

O *Rapid Spanning Tree Protocol* (*RSTP)* traz várias melhorias para o já citado STP. Para disponibilizar essas melhorias o RSTP altera alguns parâmetros do *BPDU* (mensagens trocadas entre switches), acrescentam novos estados para as interfaces, novas regras nas interfaces. [Foundry, 2007]

A principal melhoria é a velocidade de convergência em novas topologias. Quando ocorre uma alteração na rede, o *RSTP* consegue estabilizar a rede em 2 ou 3 segundos. No SPT este processo pode chegar a 30 segundos.

Este protocolo espera apenas por três "*olás"* dos switches, se não tiver resposta já considera que ouve alguma alteração da topologia. No *SPT* o tempo de espera é de 10 "*olás".*

Outra alteração trazida pelo *RSTP* é o tratamento diferenciado entre os *links*. Quando o switch esta ligado em outro switch o *link* de conexão entre eles é chamado de *Point-to-Point*; quando está ligado a um *HUB* é chamado de *Shared*; e é chamado de *Edge* quando está ligado a um usuário final.

A importância de ter tratamento diferenciado por link está na velocidade alcançada. Por exemplo, os *links* que estão em estado de *Edge* são colocados em modo de *forwarding*, pois o switch já sabe que as portas ligadas a esse link não podem gerar *loop* na rede e por isso seria "perder tempo" fazer cálculos com estas portas. [Odon, 2006]

Os estados das portas se diferenciam das portas do SPT. Os novos estados são apresentados na tabela 2.2 abaixo:

Tabela 2.2 Tabela comparativa de estados de interfaces [FOUNDRY, 2007]

STP	RSTP
Disable	Disable
Blocking	Discarding
Listening	Discarding
Learning	Learning
Forwarding	Forwarding

As portas que estão em *Discarding* não encaminham nem recebem pacotes pela portas, não aprendem *MAC addresses. A* porta reage como se estivesse desligada. Se em algum momento essa porta precisar ser usada ela passará para o estado de *learning*. [Odon, 2006]

Nas portas Learning não ocorrem trocas de pacotes, ela apenas aprende MAC. Já as portas *Forwarding* estão enviando e recebendo pacotes e também aprendem MAC.

2.3.8.3.1) Estados das interfaces no RSTP

Root Port – tem as mesmas características no protocolo SPT tratado anteriormente.

Designated Port – tem as mesmas características no protocolo SPT tratado anteriormente.

Alternative Port – tem o conceito de UplinkFast

Backup Port – está ligada ao mesmo tipo de link compartilhado com outra porta no mesmo switch, a outra porta é a porta *Designated Port*, assim em caso de falha da *Designated Port* a porta de *backup* assume a sua função.

2.3.9) Identificação de VLAN 802.1Q padronização MEF

Como constantemente é necessário realizar uma diferenciação entre o fluxo de informações entre os EVCs de uma MEN, um importante ponto na diferenciação do tráfego de dados entre EVCs é o suporte a VLAN. Os serviços que passam por EVCs devem estar identificados com *Customer Edge* VLAN ID. [MEF, 2006]

No cliente essa diferenciação é feita a partir da UNI que está associada a uma EVC devidamente identificada pela VLAN ID.

As informações que saem do cliente são identificadas com CE-VLAN ID, onde CE identifica a borda do cliente (*Customer Edge*) e ID é um número inteiro. Nas duas UNI devem estar configuradas com os mesmos parâmetros de VLAN.

A numeração de ID dessas VLANs pode variar de 1 até 4094. Várias CE-VLAN ID podem estar passando ao mesmo tempo em um EVC.

Os CE-VLAN ID devem ter um valor de VLAN ID diferente de zero e devem estar configurados entre 1 a 4094. [MEF, 2006]

As UNIs que pertencerem à mesma CE-VLAN ID devem ter os parâmetros de tagged, *untagged* e de prioridade iguais nas UNIs que formam o EVC.

2.3.9.1) Padrão IEEE 802.1Q

Em determinado período ocorreu uma mudança de conceito sobre as VLANs. Percebeu-se que era mais importante identificar os quadros da VLAN e não a VLAN da máquina que enviava o sinal. Assim, o comitê IEEE mudou o formato e criou o padrão 802.1Q, esse novo formato acrescentou uma “tag de VLAN”. Essa mudança se deu porque quem usa os campos de VLAN são os switches e não as máquinas.

Para Tanenbaum “para usar VLANs, as pontes ou switches têm que estar conscientes das VLANs, mas isso já era uma exigência. Agora, só estamos introduzindo o requisito adicional de que eles devem reconhecer o 802.1Q, o que já acontece no caso dos novos dispositivos”. [Tanenbaum, 2003]

2.3.9.2) Virtual Local Área Network (VLAN)

Nas redes Ethernet e Metro Ethernet todos os equipamentos que conseguem enviar e receber *broadcast* estão no mesmo “Domínio de *Broadcast*”, ou seja, todos eles podem se comunicar.

VLAN é a abreviação do termo “*Virtual Local Área Network*”, ela é criada em um ou mais switches. Uma VLAN cria um único domínio de *broadcast* entre os hosts que fazem parte deste domínio. Com isso pode-se segmentar o tráfego ou fazer com que computadores, servidores que estão em switches diferentes participem do mesmo domínio de *broadcast*. Segundo os ensinamentos de Tanenbaum VLANs “se baseiam em switches especialmente projetados para reconhecer VLANs, embora também possam ter alguns *hubs* na periferia” e completa dizendo “para configurar uma rede baseada em VLAN, o administrador da rede decide quantas VLANs haverá, quais computadores estarão em cada VLAN e qual será o nome de cada VLAN” [Tanembaum, 2006]

As redes locais virtuais podem ser designadas de VLANs, essa é uma rede logicamente segmentada mesmo estando no mesmo equipamento. Várias VLAN's podem estar simultaneamente em um mesmo switch. O protocolo usado para realizar essa segmentação é o IEEE 802.1Q.

Existem switches que tem a capacidade de criar várias VLANs (domínios de *broadcast*) conforme a necessidade da rede. Os switches que não tem esse tipo de funcionalidade apenas enviam o *broadcast* para todas as interfaces com exceção apenas da que está enviando os pacotes.

Quando ligamos os switches ou hubs em cascata ou empilhados colocamos esses equipamentos no mesmo domínio de *broadcast*.

VLAN (*Virtual* LAN) é “um domínio de *broadcast* criado por um ou mais switches. A LAN é criada por configuração no switch. Assim, em vez de todas as portas formarem um único domínio de *broadcast*, o switch separa em várias de acordo com a configuração” [Wendell Odon, 2003].

Todas as portas que estão na mesma VLAN estão no mesmo domínio de *broadcast*. Uma porta pode participar de mais de uma VLAN ao mesmo tempo. Vários switches podem ter a mesma VLAN em suas configurações.

É importante lembrar que quando uma porta não faz parte de uma VLAN, essa não conseguirá se comunicar com as portas que estão presentes na VLAN, mesmo ela estando no mesmo switch.

2.3.9.2.1) VLAN em camadas 2 e 3

Pode ser que em uma topologia seja necessário enviar pacotes de uma VLAN para outra, para isso deverá ser usado outra abordagem. Quando criamos um domínio de *broadcast* não existe a necessidade de algum pacote ser enviado de uma LAN para outra, porém, se surgindo a necessidade de enviar pacotes entre uma LAN e a outra deverá ser usado um roteador.

Para que possa ser identificada a necessidade de cada topologia podemos citar três exemplos [Odon, 2006]

Exemplo 1 – Se em uma rede for preciso criar dois domínios de *broadcast* e os switches não têm suporte a múltiplas VLAN deve-se usar pelo menos dois switches para poder segmentar essa rede. Supondo que existe a necessidade de trocar quadros entre essas VLAN, esse equipamento não consegue rotear pacotes. Desta forma, esses switches só podem encaminhar pacotes para interfaces que estão no mesmo domínio de *broadcast*; será necessário usar um roteador para trocar essas informações. O papel do roteador nesta topologia é apenas encaminhar os pacotes entre as VLANs.

Exemplo 2 – Usando a mesma topologia do primeiro exemplo só que nesta os switches têm suporte a múltiplas VLAN. Seria necessário apenas um switch para segmentar essa rede já que é possível criar as duas VLAN no mesmo equipamento. Como esse switch não consegue rotear pacotes, é necessário acrescentar um roteador para que os pacotes possam ser enviados de uma rede para a outra.

Exemplo 3 – Nos switches atuais existe o suporte a múltiplas VLANs e a roteamento. Com um switch desse tipo podemos fazer todos os passos dos

exemplos acima só que todas as necessidades de VLAN e Roteamentos serão feitas pelo mesmo equipamento. Com isso podemos criar ambientes mais sofisticados e com menos equipamentos agregados.

No laboratório montado de Metro Ethernet onde será transmitido o sinal simulado de IPTV serão usados equipamentos com as características do exemplo 3 com recursos de OSPF e múltiplas VLANs.

2.3.9.2.2) Criação da tabela de endereço das VLANS

Para cada VLAN da rede, o switch cria uma tabela de endereço separada das demais. Quando uma porta recebe um quadro de uma VLAN qualquer, ele analisa a tabela que contém todos os endereços dessa VLAN. O endereço de origem é verificado, e caso ele não conste na tabela de endereços ele será adicionado na tabela de endereços. O endereço de destino também é verificado para que possa ser tomada a decisão de encaminhamento conforme a necessidade.

2.3.9.2.3) Portas tagged e untagged

O compartilhamento de VLANs entre Switches é conseguido introduzindo um TAG com um identificador de VLAN (VID).

Conforme a necessidade as portas podem ser programadas para agirem como *tagged* e *untagged*.

As portas *Tagged* são portas que podem participar ao mesmo tempo de dois ou mais domínios de *broadcast*, ou seja, várias VLANs. *Tagging* VLAN é um processo de acrescentar um cabeçalho adicional a um quadro de LAN com o intuito de identificar a qual VLAN o quadro pertence.

Já as portas *Untagged* só participam de um único domínio de *broadcast*, ou seja, uma única VLAN. Na maioria das vezes os computadores e servidores devem estar conectados em portas *untagged*.

2.3.9.3) IEEE 802.1ad QinQ

Um provedor de acesso pode precisar adicionar novas informações de *tag* aos dados de um cliente. Caso os pacotes desse cliente já venham com informações de *tag* é necessário usar recursos que preservem essas

informações. Esse recurso é conhecido como Q-in-Q. O MEF padronizou o uso do Q-in-Q.

CE-VLAN *Tag Preservation* mantém os parâmetros do CE-VLAN ID e a prioridade adicionados pelo cliente ou pelo provedor quando os dados passam por equipamentos diferentes ou por outros provedores que não sejam o provedor original. Essa preservação só ocorre caso todos os equipamentos essa função. Tem como propósito expandir o espaço de VLAN com ”*tageamento*” (marcação) de pacotes *tageados* (previamente marcados). Desta forma produz um pacote duplamente tageado. [Cisco, 2007]

Com esse dispositivo VLANs permitem que múltiplas VLANs sejam adicionadas umas as outras VLAN de forma que possam ser construídos caminhos e canais de camada 2. Cada caminho contém vários canais, cada um dedicado a um EVC.

A expansão de VLANs permite que o provedor disponibilize serviços, assim como acesso a Internet para VLANs de consumidores específicos e também permite o provimento de outros serviços para consumidores diferenciados. [Cisco, 2007]

Com esses recursos podemos aumentar a escalabilidade das VLANs, aumentando de 4095 IDs para 16 milhões, já que podem ser colocadas VLAN dentro de VLAN. Consegue-se, também, identificar todo o tráfego que vem do cliente dentro da MEN.

Q-in-Q é muito útil em aplicações como as que precisam de linhas privadas como VPNs. E isso é feito de forma transparente para as múltiplas redes.

No laboratório onde serão feitos os testes não será usado Q-in-Q. Porém essa tecnologia pode vir a ser muito útil em redes Metro Ethernet que estejam transmitindo IPTV.

2.3.10) Provider Backbone Bridges (PBB)

Também conhecido como MAC-in-MAC ou MinM tem como função estender a rede Ethernet do cliente e do provedor de acesso com um completo isolamento através de seus endereços MACs.

A norma IEEE que explica o PBB é 802.1ah. O que ocorre nesse conceito é uma alteração no frame ethernet onde é adicionado um cabeçalho MAC do provedor de serviço; é também adicionado o MAC de destino.

O endereço MAC do provedor de serviço e do cliente são verificados antes que sejam montadas as tabelas. Isso faz com que apenas os switches que estão nas bordas estejam preparados para PBB, porque só eles se comunicarão com os provedores de serviço.

Com isso os switches de *edge* passam a ser uma espécie de túnel para o backnone.

Pode ser usado o conceito de engenharia de tráfego para isolar as regiões da rede através de seus IDs de VLANs. [Cisco Press, 2007]

2.3.11) IEEE 802.1ag (Fault Management)

Pode ser chamado como *Ethernet Connectivity Fault Management*, esse protocolo está relacionado com a conectividade dos equipamentos.

Provê recursos que possibilita a descoberta de novos equipamentos, testes de conectividade, *loopback* e link trace.

Loopbacks são testes de camada dois que podem ser realizados a qualquer momento, são similares ao ping. A vantagem em usar *loopback* é que esta é uma porta virtual no switch que responde independente de configurações em UNI, é uma interface que está sempre ativa mesmo sem a conexão física. Alguns protocolos como o OSPF podem usar essas interfaces de *loopback* para otimização. Pode ser usado para testar os EVCs

O *Link trace* também é um teste de camada dois. Ele é parecido com o *traceroute* que mostra todos os nós (roteadores) que intermediários até chegar a um local.

Nos testes de conectividade são realizadas verificações continuas (*checks*) que verificam os serviços e por isso agem de forma pró-ativa na identificação de falhas. Esses testes podem ser feitos no mesmo domínio ou em domínios diferentes.

2.3.12) Medidores de performance

Os medidores de desempenho são importantes para determinar a qualidade da transmissão dos dados. Eles estão diretamente associados com o desempenho da rede. Quanto maior a criticidade dos dados mais importantes esses valores se tornam.

Frame Delay “Pode ser definido como o tempo transcorrido da recepção de entrada do primeiro bit na UNI de entrada, vindo do frame de serviço, até a

saída do último bit pela UNI de saída.” [MEF, 2004]. Para o melhor entendimento vejamos a figura abaixo:

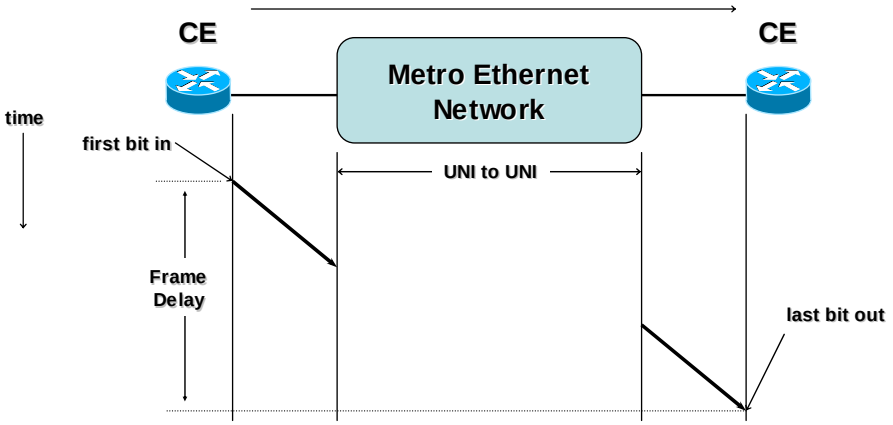


Figura 2.11 Diagrama de atraso no envio de pacotes conforme o MEF **[MEF, 2007]**

Podemos analisar a figura 2.11 dividindo-a em três partes; A primeira parte é a entrada do primeiro bit transmitido pela CE. Nesta parte o atraso é proporcional à velocidade da UNI (10Mbps, 100Mps e etc). Na segunda parte temos a MEN, nesse trecho é contado o atraso produzido pela própria MEN. Na terceira e última parte temos o atraso produzido pela última UNI, que também é proporcional à velocidade da UNI. O atraso total é calculado a partir da soma do atraso desses três períodos.

O **Frame Jitter** é responsável por medir a variação do atraso dos pacotes. Para aplicações que precisam de um alto desempenho como telefonia, transmissão de imagem e IPTV, não podem ocorrer variações de atrasos na transmissão dos dados. Por isso, nesses casos, o *jitter* é um parâmetro indispensável para avaliação da qualidade da transmissão.

O *Jitter* é calculado a partir dos valores medidos do *Frame Delay*.

2.3.13) Multiplexação em Ethernet Virtual Connection

Quando uma UNI precisa trafegar dados em mais de dois EVCs é usado o serviço de multiplexação para realizar esse envio.

O atributo de serviço de multiplexação é usado para que uma UNI suporte vários EVCs. [Santitoro, MEF - 2006]

Para melhor ilustrar o que ocorre na multiplexação, vejamos a imagem abaixo:

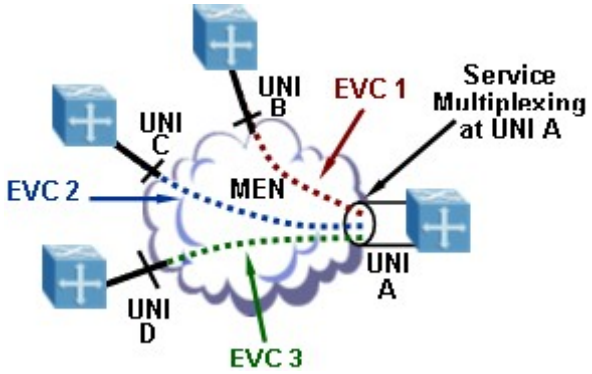


Figura 2.12 Serviço de multiplexação **[MEF, 2007]**

De acordo com a figura 2.12 a UNI **A** com capacidade de 10 Gbps, precisa trocar dados através de EVCs entre as UNIs **B, C** e **D** de 1 Gbps. A conexão entre eles é feita através de uma MEN. Para poder fazer essa troca de dados UNI **A** deve ter suporte a multiplexação e deve necessariamente ser configurada para aceitar as múltiplas EVCs. Programando o equipamento da UNI **A** para enviar todas as requisições pela UNI **A,** fechando com as UNI´s **B, C** e **D**.

Como a UNI **A** suporta multiplexação não é necessário acrescentar mais duas UNIs para fechar os canais de comunicação entre as UNIs **B, C** e **D** e a MEN.

A vantagem de usar multiplexação é dotar uma UNI da capacidade de receber dados de vários EVCs. Como uma interface age como se fosse várias intefaces, pode-se assim reduzir o número de interfaces nos clientes, isso faz com que o custo em equipamentos seja reduzido.

O serviço de multiplexação minimiza o número de interfaces dos switches ou roteadores dos clientes e maximiza a utilização de portas/slots. [MEF, 2006]

Estes serviços também reduzem o espaço, energia e cabeamento. Comparados com serviços não multiplexados os serviços multiplexados reduzem a ocupação no rack. [Santitoro, MEF 2006]

Partindo do princípio que já exista conexão entre todas as UNIs, pode-se adicionar novos EVCs sem a necessidade de agregar novos equipamentos, cabos e nem mesmo a presença física de técnicos.

O serviço de multiplexação permite que novos EVCs sejam estabelecidos sem a necessidade de novos equipamentos. [Santitoro, MEF 2006].

2.3.14) Padronização da MEF

A MEF montou uma tabela contendo os valores recomendados para que se tenha a melhor qualidade no envio dos dados em uma MEN. Essa tabela contém os parâmetros de classes de serviço.

Para Wagner A tabela 2.3 “mostra um possível portfólio de serviços combinando os parâmetros de uma rede Metro Ethernet com algumas aplicações mais utilizadas atualmente. A utilização de diferentes critérios para classificação de tráfego possibilita que os serviços. Metro Ethernet sejam oferecidos em diferentes níveis. Assim, um provedor de acesso poderia controlar o tráfego em cada VLAN individual e adquirir um serviço com taxa controlada na UNI de um provedor de rede metropolitana. Naturalmente, as demandas de tráfego em cada interface serão distintas, mas a partir do perfil de tráfego de entrada é possível obter-se uma boa estimativa do perfil de tráfego de saída e assim configurar corretamente cada acesso.” [Wagner L. Zucchi, 2006]

Tabela 2.3 Recomendação MEF sobre performance de MEN. **[MEF, 2006]**

Classe do Serviço	Características do service	CoS ID	Largura de Banda por EVC e por CoS ID	Performance
Premium	Telefonia IP em tempo real ou Aplicações de vídeo em IP	6, 7	CIR > 0 EIR = 0	Delay < 5ms Jitter < 1ms Loss < 0.001%
Silver	Aplicações de base de dados que requer baixa perda e atraso (Storage)	4, 5	CIR > 0 EIR ≤ Velocidade da UNI	Delay < 5ms Jitter = N/S Loss < 0.01%
Bronze	Aplicações que precisam de garantia de banda	3, 4	CIR > 0 EIR ≤ Velocidade da UNI	Delay < 15ms Jitter = N/S Loss < 0.1%
Standard	Serviço de melhor esforço	0, 1, 2	CIR=0 EIR=Velocidade da UNI	Delay < 30ms Jitter = N/S Loss < 0.5%

Alguns dos parâmetros que serão considerados neste projeto são os valores indicados para a classe premium; delay < 5 ms, Jitter < 1ms e perda de

pacotes < 0.001%. Os outros valores *Silver*, *Bronze*, *Standard* não serão utilizados neste trabalho.

Esses valores por serem estabelecidos pela MEF são de extrema importância para este estudo.

2.4) IPTV (Internet Protocol Television)

IPTV é o processo de transmitir sinal de televisão através de redes de dados IP. Esta rede IP pode ser gerenciada (xDSL ou óptica) ou não Se o sinal da televisão for analógico (Televisão padrão ou HDTV) o sinal de vídeo e áudio devem ser convertidos para a forma digital. Informações de pacotes de roteamento são adicionadas então ao sinal de vídeo e voz digital. Assim podem ser roteados pela Internet ou redes de dados. [Harte, 2007]

O IPTV pode ser definido como um serviço de transmissão de televisão digital com o uso da tecnologia IP através de rede de banda larga. O serviço foi especialmente desenvolvido para transmitir com alta qualidade o conteúdo da televisão através de redes IP para aparelhos de televisão e não apenas para os computadores.

Para ver uma transmissão de IPTV nas televisões normais precisa-se de um equipamento chamado de *Set-Top Box*, que é responsável pela conversão do sinal IP para a televisão.

Como esta transmissão de televisão está baseada em redes IP, pode-se associar a ela outros dois serviços baseados nessa tecnologia; o envio de dados convencionais e o serviço de voz (VoIP). A junção desses três serviços em uma única rede é conhecida como "*Triple-Play*".

Como o IPTV consome uma grande largura de banda da rede, esta tecnologia se mostrava inviável na era do dial-up onde as taxas de transmissão eram extremamente baixas, lentas e limitadas, impossibilitando o recebimento do seu conteúdo.

O IPTV se divide em duas área o *LiveTV* e o *VoD*. O *LiveTV* consiste basicamente a transmissão de televisão em tempo real. O *VoD* (Vídeo sobre Demanda) é a transmissão exclusiva para um único usuário.

Pelo fato de o IPTV consumir uma grande largura de banda leva-se a considerar a possibilidade da transmissão deste sinal em uma rede Metro Ethernet; que tem grande largura de banda, alto processamento e rapidez na comunicação.

A transmissão de IPTV não é exclusivista no que tange os meios de transporte. Os usuários podem receber a transmissão por uma rede ethernet ou rede ADSL. As premissas para a realização dessa transmissão estão associadas à largura de banda destinada que deve ser grande, á garantia da qualidade de serviço com a utilização de QoS e a uma medida subjetiva que é a qualidade na experiência QoE, além da necessidade de se reduzira quantidade de pacotes perdidos e o jitter. Tudo isso deve ser considerado em qualquer tipo de transmissão do IPTV. Com o uso de ADSL em alta velocidade (Internet de alta velocidade) essa realidade mudou, e agora já começamos a ver o início do processo de transmissão de televisão em redes IP.

A seguir são apresentadas as estruturas voltadas para a transmissão do sinal IPTV até o cliente final, No caso do presente trabalho, a demonstração da transmissão é sobre a rede Metro-Ethernet, mas o acesso ao usuário final poder ser feito com redes ethernet conectadas diretamente ou por estruturas de banda larga como abaixo descritas.

2.4.1) Estruturas e serviços agregados ao IPTV

Estruturalmente todo o sistema de transmissão e recepção é composto por equipamentos de visualização ou adaptadores; provedores de acesso de banda larga; provedores de serviço de IPTV; provedores de conteúdo. Cada um desses tem uma função especifica.

A função dos equipamentos de visualização é transformar o sinal digital em um sinal que possa ser visualizado pelos usuários. A dos provedores de acesso de banda larga é disponibilizar uma rede que possa ser capaz de transportar todas as informações de vídeo e som. Os provedores de serviços de IPTV ficam entre os equipamentos de visualização dos usuários e os provedores de conteúdo, Já os provedores de conteúdos armazenam, criam e organizam as informações que são transmitidas.

É importante ressaltar que o IPTV não consiste apenas em transmitir televisão. Essa solução agrega jogos interativos, acesso a bibliotecas, *t-commerce* e serviços de segurança.

Entre os serviços que podem ser agregados com esse novo conceito está *t-commerce*. Imaginemos que durante uma transmissão de um filme ou show apareça um produto qualquer. Se o telespectador quiser comprar este produto bastará clicar em cima da imagem que abrirá o recurso de compra e ele poderá

comprar este produto. Poderemos ter também a facilidade de comunicação, se durante uma entrevista o usuário desejar falar com o entrevistado, também bastará dar alguns cliques e poderá conversar com o entrevistado.

Entre outras facilidades pode-se juntar as contas, pois será possível a geração de uma única fatura que agregaria conta de telefone, Internet e TV a cabo, por exemplo.

2.4.2) Estatísticas de utilização de TV a cabo e ADSL

Para termos uma idéia do potencial de mercado do IPTV no Brasil temos que ver as estatísticas de número de usuários de TV por assinatura, total de conexões em banda larga com ADSL.

A seguir será apresentada a tabela 2.4 com o número de assinantes de TV a cabo.

Tabela 2.4 Usuários de TV por Assinatura [Anatel, 2007]

Fonte: Anatel	2004	2005	2006	1T07	2T07
TV a Cabo	2.270.297	2.510.883	2.841.900	2.924.447	3.016.942
DTH	1.350.410	1.437.943	1.479.554	1.541.508	1.644.529
MMDS	230.434	227.561	257.916	271.575	291.919
TVA	-	-	3.755	5.766	7.572
Total	3.851.141	4.176.387	4.583.125	4.743.296	4.960.962
Densidade*	2,11	2,26	2,45	2,52	2,63

Segundo a tabela 2.4 para o segundo semestre de 2007 teremos 4.960.962 assinantes de TV a cabo no Brasil. Esse número representa o total de consumidores que já estão habituados com a utilização de TV por assinatura e por isso podem ser futuros consumidores de um serviço de IPTV. É esta fatia do mercado que as operadoras de Telecomunicação disputam como clientes do serviço de TV.

Tabela 2.5 Total de conexões Banda Larga no Brasil **[Teleco, 2007]**

Milhares	1T06	2T06	3T06	4T06	1T07	2T07
ADSL	3.432	3.685	3.997	4.341	4.573	4.881
TV Assinatura	789	914	1.057	1.200	1.347	1.413
Outros(Rádio)	80	92	105	115	120	123*
Total	4.301	4.691	5.159	5.656	6.040	6.417*

Fonte: Operadoras, ABTA e Teleco, não inclui satélite e IP dedicado
* Estimativa preliminar do Teleco

A Tabela 2.5 mostra a quantidade de conexões em banda larga no segundo semestre de 2007. Esse número mostra o total de conexões possíveis para acesso a IPTV no mercado brasileiro.

2.4.3) Estatísticas de crescimento e investimento em IPTV no mundo

De acordo com pesquisas realizadas pela *Infonetics Research*, Inc. em 2005 estimava-se um total de 4.3 milhões de usuários de IPTV, sendo que as previsões mais pessimistas apontam um crescimento para 53 milhões de usuários para 2009.

No ano de 2005 os valores gastos na compra de novos equipamentos para a renovação do parque chegou a 400 milhões de dólares. Segundo previsões as empresas de telecomunicações devem gastar até o ano de 2009 um total de 6 (seis) bilhões de dólares, o que está motivando muito os investimentos e pesquisas nesta tecnologia [*Infonetics Research*, 2007]

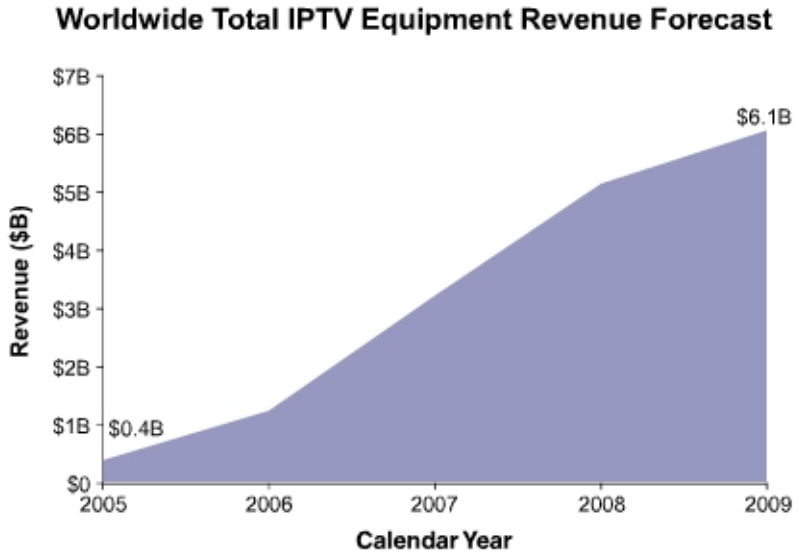


Figura 2.13 Gastos com novos equipamentos [Infonetics Research, 2007]

Na Bélgica atualmente existem mais de 200 mil assinantes de IPTV. A França pode ser considerada o país que detêm o maior número de assinantes da Europa. A fatia que ela ocupa no mercado mundial está próxima a 3 %.

“A ultima pesquisa feita pela empresa britânica *Canalys*, no início de 2007, mostra que o número de assinantes de IPTV na Europa e na Ásia aumentou 36% em 2006. Nos países europeus encontram-se dois terços de todo o sistema de IPTV do mundo, seguido pelo grupo formado pelo Leste Europeu e Ásia. A pesquisa demonstrou que ao final do ano passado eram cerca de 3,6 milhões de assinantes só na Ásia e Europa – quantidade que pode duplicar nos próximos dois anos.” [Correio Braziliense, 2007]

2.4.4) Cuidados iniciais na implementação.

Para garantir que esta tecnologia realmente seja utilizada, os provedores devem ter uma estrutura que comporte a transmissão de voz, dados, principalmente vídeos sobre demanda e televisão. Se a estrutura não for capaz de suportar todos estes aspectos certamente causará a insatisfação dos usuários que tentarem utilizar essa nova tecnologia.

Toda nova tecnologia que surge, ao ser implantada, tem um risco agregado. O sucesso depende de como será apresentada e da expectativa criada no usuário. No IPTV não será diferente, como já existem serviços de TV a cabo, TV aberta, TV via satélite que todos confiam, para o sucesso do IPTV deverão ser adotadas medidas de qualidade de serviço (QoS) que garantam que as expectativas dos usuários sejam alcançadas.

Quanto maiores forem as garantias de qualidade de serviço menores serão os riscos dos usuários não gostarem do serviço prestado. Estas garantias podem ser:

- Qualidade de serviço
- Diminuição nos erros de imagem e som
- Garantias de alta disponibilidade (tolerância a falhas).
- Fácil manuseio

2.4.5) Vídeos pela Internet e televisão sobre IP

Em uma análise rápida e superficial podemos confundir assistir vídeo pela Internet (por exemplo, os que assistimos no www.youtube.com) com o IPTV.

Quando vemos um vídeo por algum site, estamos usando a Internet como o meio de entrega e visualização. Nesse tipo de estrutura é muito difícil garantir a qualidade da recepção das imagens que estão sendo enviadas.

Quando falamos em IPTV estamos falando de transmissão de televisão baseada no protocolo IP, assim os provedores de serviços podem usar as suas estruturas para realizar essa transmissão baseada em IP. IPTV não é transmissão de televisão sobre Internet é transmissão sobre IP.

Um dos diferenciais do IPTV é que os usuários não necessariamente precisam de computadores para ter acesso à transmissão das imagens.

Como o IPTV é baseado no protocolo IP pode ser transmitido em uma rede fechada torna-se possível a transmissão de imagens de altas ou baixas definições, em detrimento as imagens enviadas pela Internet que em sua maioria está destinado à transmissão de imagens com baixa qualidade.

Uma forma fácil de identificarmos se a transmissão é de IPTV é verificar se esta transmissão tem como base uma rede IP e tem como destino final um aparelho de TV.

2.4.6) Set Top Box

Para que o usuário final possa visualizar as imagens que são transmitidas é necessário que haja a conversão do conteúdo transmitido em IP para um formato compatível com o seu aparelho de televisão. Na grande maioria dos casos quem faz esse trabalho é o *Set-Top box*.

Assim, “os equipamentos dos usuários finais de IPTV adaptam as mídias de comunicação IP para o formato acessível aos usuários finais” [Harte, 2007]

Esses equipamentos podem receber informações por Ethernet, xDSL, cabo, redes ópticas, redes sem fio.

A função do *Set Top Box* é converter os pacotes IP para um sinal analógico ou digital compatível com o televisor, esse sinal pode ser (NTSC, PAL, HDMI, HD).

Dentro dos STP existe um buffer, para amenizar possíveis falhas da transmissão. Esses dispositivos conseguem armazenar até 12 segundos de informação, o que da uma margem para possíveis atrasos de pacotes.

Algumas televisões já estão sendo produzidas com decodificadores IP internos, assim elas são capazes de receber as transmissões sem a necessidade de ter um STP.

2.4.7) Formatos de compressão de imagem

A viabilidade da transmissão de televisão por redes IP está diretamente associada a serviços de compressão de imagem. Os vídeos gerados com esta finalidade têm que passar por um processo extremo de compactação e depois de compactados devem ser encapsulados para o protocolo IP.

“Os vários formatos de compressão variam em quanto eles podem reduzir a ocupação da largura de banda.” [Joseph, 2006].

“No serviço IPTV, o sinal de vídeo deve ser compactado para sua transmissão, sendo esse, também, um elemento de escolha no projeto dessa arquitetura a ser implementado. Portanto, no projeto de uma arquitetura de rede IPTV, há várias opções de implementação, desde a distribuição até a entrega do vídeo ao usuário.” [Duque, 2007]

Mesmo os vídeos estando compactados, as taxas de ocupação da banda de transmissão são muito elevadas, e para garantir a qualidade do serviço é necessário ter uma grande largura de banda. Tudo isso afeta diretamente a disponibilidade da rede e devem ser estudados antes de serem implementados.

As tecnologias mais usadas são MPEG-2, H.264, MPEG-4, HD, VC-1, WMV (*Windows Media Vídeo 9*). Os algoritmos de compressão mais usados são o MPEG-2 e o MPEG-4.

Do ponto de vista de Joseph “MPEG-4 AVC, *Windows Media*/VC-1, *RealVideo* 10 esses formatos incluem ferramentas mais sofisticadas do que o MEPG-2 por isso alcançam uma compressão muito maior sem a perda da qualidade da imagem. Elas estão apenas começando a ser usadas no mercado comercial.” [Joseph, 2006]

A figura 2.14 mostra a relação entre a transmissão e a compactação de imagens em razão da largura de banda ocupada para imagens sem compactação e imagens compactadas em vários formatos.

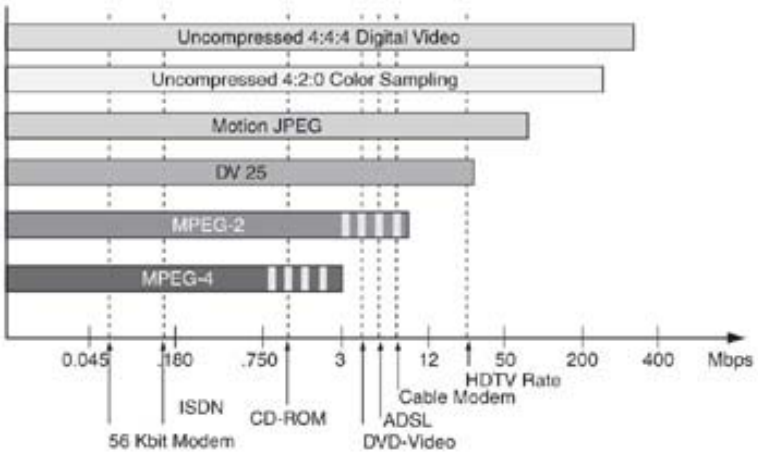


Figura 2.14 Taxa de ocupação da banda de transmissão **[IPTV Crash Course, 2006]**

A banda ocupada será diretamente proporcional ao tipo de compressão que será usada na transmissão. Um vídeo compactado com MPEG-2 ocupa algo em torno de 2 até 8 Mbit/s por canal, já a compactação por H.264 consegue reduzir a ocupação, esta passa a ocupar 2 Mbit/s por canal de TV. O VC-1 é um sistema proprietário da *Microsoft* e ocupa 1.5 Mbit/s. Os sinais em alta definição (HD) mesmo usando H.264 ocupam de 8 a 12 Mbit/s, os que usam MPEG-2 ocupam 15 Mbit/s.

Segundo Joseph o MEPG2 “em virtude da compressão pode ser reduzido de mais de 200 Mbps para algo em torno de 2 a 8 Mbps” [Joseph, 2006].

O formato que será usado em laboratório será o MPEG2 e os arquivos de vídeos usados serão oriundos de DVD, isto porque esse tem uma ótima qualidade de imagem e áudio; a mídia em DVD é de fácil mobilidade transporte; exigem alto desempenho dos equipamentos para a sua transmissão.

O sinal do laboratório será transmitido em alta definição (HD).

2.4.7.1) Ocupação de banda em relação à compressão

A ocupação da banda da rede de transporte está diretamente ligada à quantidade de canais de IPTV (*broadcast* de TV) transmitidos ou do somatório das transmissões simultâneas de VoD que estão passando na mesma rede. Caso esteja ocorrendo os dois tipos de transmissão deve-se realizar o somatório de tudo que está sendo transmitido.

A ocupação da banda envolve todos os equipamentos da rede até chegar ao usuário final que está assistindo a transmissão. O local onde a ocupação da banda é maior é no core da rede de transmissão.

No caso do IPTV no formato de *broadcast* de TV cada canal ocupa uma largura de banda de transmissão fixa, independente da quantidade de pessoas que estiverem recebendo as imagens desse canal. Na recepção, cada acesso via TV precisará de banda de acordo com a taxa de compressão que estiver sendo utilizada.

Já nas transmissões de VoD cada usuário ocupa um canal. Podemos considerar uma transmissão exclusiva. Assim a largura de banda ocupada é multiplicada pelo número de usuários que estiverem recebendo o *broadcast* de vídeo.

No VoD os usuários podem escolher e selecionar o conteúdo do vídeo e assistir a esse vídeo escolhido conforme a sua conveniência.

Para melhor explicar a diferença do IPTV e VoD em relação a taxa de ocupação podemos usar dois exemplos diferentes que mostram características de transmissão distintas.

No primeiro exemplo considerar-se-á transmissão de 50 canais de IPTV por uma rede e estes vídeos serão enviados apenas uma única vez. Por ser um tráfego de IPTV a banda ocupada independe do número de usuários que irá receber esta transmissão. Os canais serão comprimidos com H.264 e por isso ocuparão 2 Mbit/s cada um. Multiplicando o número de canais pela ocupação de 2 Mbit/s, concluímos que o total ocupado da banda será 100 Mbit/s. Assim o tráfego total que sairá do *backbone* até o meio de transmissão de banda larga do usuário será de 100 Mbit/s independente do número de usuários que estiverem assistindo os canais transmitidos, desta forma a transmissão não afeta drasticamente o *backbone* central Assim, se tivermos 2000 usuários assistindo programação serão utilizados os mesmos 100 Mbit/s.

No segundo exemplo considerar-se-á que cada assinante quer ver um filme que não está passando na programação normal daqueles 50 canais. Neste caso deverá ser usada uma transmissão de VoD *unicast* , ou seja cada usuário ocupará uma parte da banda de transmissão e essa não será compartilhada com os demais usuários; como uma transmissão exclusiva. Se for utilizado o mesmo esquema de compressão e formatação a 2Mbit/s, com 50 usuários seriam 100 Mbits/s, mas com 2000 usuários assistindo filmes diferentes ao mesmo tempo, teríamos um total de 4 Gbit/s de ocupação na rede de transporte, o que mostra que neste tipo de transmissão na há independência do número de usuários simultâneos. A partir deste calculo podemos ver o quando é crítica a transmissão de VoD em um *backbone*.

2.4.8) Recurso de RSTP para transmissões

Na medida em que as informações são enviadas para os assinantes é necessário agregar algumas funcionalidades para trazer mais conforto a transmissão. Para isso é usado o RSTP (*Real Time Streaming Protocol*).

O RSTP fornece a capacidade dar *play*, *stopping*, *pausar*, acelerar, voltar à transmissão que está sendo vista. Ele trabalha de forma muito parecida ao vídeo cassete. Normalmente esse recurso é mais usado em transmissões de *VoD*.

Este protocolo é compatível tanto com transmissões de *VoD* com o *LiveTV* (Transmissão do conteúdo da televisão aberta ou a cabo, em tempo real; novelas, jogos de futebol, seriados, telejornais são exemplos de *LiveTV*).

2.4.9) Arquitetura de redes para transmissão de sistemas em IPTV

São várias as arquiteturas que compõem a transmissão de IPTV. Podem ocorrer variações nessas arquiteturas. Todas essas estruturas podem ser mais detalhadas e se subdividir em várias subestruturas conforme a necessidade de transmissão de cada prestador de serviços, porém os pontos mais importantes são:

Headend – É o local onde os conteúdos estão armazenados; é também o local onde os vídeos são preparados, compactados, formatados para serem enviados para a Rede. Aqui neste ponto será determinando o tipo de compactação que será usada nos vídeos.

"Podendo ser centralizado ou distribuído. Serviços interativos como IPTV e o VoD são providos a partir de servidores de conteúdo em formato MPEG que enviam uma cópia ao usuário, quando requisitado." [Duque, 2007]

As informações podem ser armazenadas de forma centralizada em um Data Center, ou seja, todos os vídeos estarão armazenados no mesmo local. Outra forma é o armazenamento distribuído onde existem várias localidades armazenando os conteúdos de transmissão.

Parte deste conteúdo pode chegar através de redes metálicas, fibras ou por satélites.

Core Network – "Transporta todo o conteúdo do sistema (que são, vídeo, música, canais e dados). O core da rede é o "*backbone*" para o sistema *broadcast* de IPTV" [Joseph, 2006]. Este ponto também é conhecido como Core IP e pode ser considerado o coração de todo o sistema de IPTV. É o responsável pelo

transporte dos dados, do vídeo e voz que são transmitidos para os usuários. Neste ponto existe a presença dos roteadores, switches, *backbones*, etc.

Neste trabalho serão usados switches/roteadores tanto nas estruturas de core como de entrega. Estes equipamentos agregam todos os recursos necessários para comporem uma estrutura de rede MEN.

***Access* Net*w*ork (Rede de Acesso) –** “representando a ligação entre o fornecedor de serviço (operadora de Telecom) e a casa do usuário, ou seja, "a última milha”. A conexão do usuário pode ser realizada por meio de uma variedade de tecnologias de rede de acesso.” [Duque, 2007].

Entre as estruturas que estão sem utilizadas temos: DSL (linha digital de assinante) ou fibras óticas com velocidades superiores às do DSL.

O Digital Subscrieber Access Multiplexer (DSLAM) conecta os usuários através do par telefônico, e sua saída pode ser ATM ou *Ethernet*, a depender da tecnologia utilizada. O DSLAM ainda concentra os usuários e possui conectividade com o *Broadband Remote* Acess (BRAS). [Duque, 2007].

Home Network (casa) – Onde realmente o serviço é entregue (na casa). Neste ponto ocorre a distribuição de todas as informações (vídeo, voz, dados). As informações são entregues nos equipamentos IP (STP).

Aqui também ocorre a conversão da transmissão de *LiveTV* ou *VoD* que veio codificada e em pacotes, para o formato suportado pelos aparelhos de Televisão. O equipamento que realiza esse trabalho é o *Sep Top Box*.

Na figura 2.15 identificamos toda a estrutura de transmissão de IPTV, saindo do *Headend* passando pelo *Core Network* até chegar ao usuário final no seu *Home Network*.

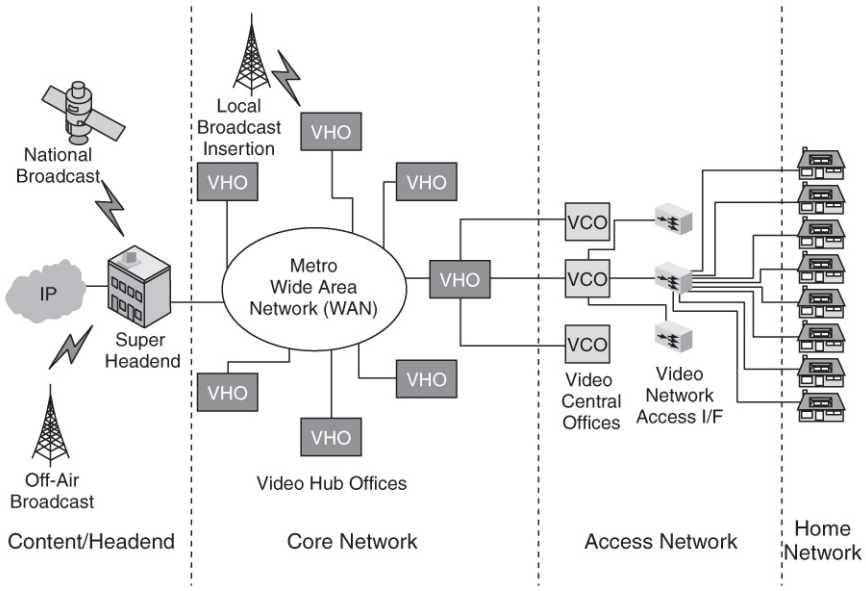


Figura 2.15 Estrutura de transmissão de IPTV **[IPTV Crash Course, 2007]**

2.4.10) IPTV em uma Metro-Ethernet

Na transmissão de IPTV em uma Metro-Ethernet os prestadores de serviços desta rede podem controlar o tráfego desta informação por toda a rede desde a origem até a entrega ao consumidor final, implementando serviços de QoS, segurança, estruturas de proteção contra falhas e alta disponibilidade.

A alta disponibilidade é um fator imprescindível nas redes que transportam IPTV. E no que tange a alta disponibilidade, as redes MEN (dependendo da arquitetura usada) conseguem se aproximar praticamente da taxa zero de indisponibilidade. E essa alta disponibilidade não é apenas no core de distribuição, se estende por toda a rede até o usuário final.

Se fosse utilizado um modelo de transmissão pela Internet, o sinal teria que trafegar por vários provedores, assim impossibilitando que os operadores desta rede tenham o mesmo controle de segurança e QoS que teriam em uma rede Metro Ethernet. Assim, neste modelo não seria possível garantir a qualidade do serviço de IPTV o que poderia até inviabilizar a transmissão desse serviço

Por ser uma rede heterogênea, para haver a comunicação entre as interfaces, seus equipamentos seguem os mesmo padrões, e com a sua administração centralizada facilita a padronização das estruturas disponibilizadas para prover o serviço de entrega de IPTV. O fato de uma MEN ser heterogênea não impede que estruturas anômalas a esta possam se comunicar com a MEN, se for necessário pode-ser incluir uma comunicação com uma rede ATM.

Com uma MEN não seria necessário agregar a estrutura DSLAM utilizada na rede que utiliza ADSL e ADSL 2. Para o usuário final apenas chegaria um cabo UTP, de forma que o usuário não se preocupasse com nada mais (*modens* ADSL).

Outro ponto muito importante do uso de MEN para esse tipo de transmissão é a velocidade. Enquanto nas redes que usam o sistema telefônico convencional para distribuição do sinal, o ADSL tem taxas que variam de 2 Mbps até 8 Mbps para *downstream* , para ADSL 2 pode chegar até 24 Mbps para o usuário final, em uma estrutura MEN poderia trabalhar com velocidades iniciais de 100 Mbps full duplex (envia e recebe na mesma velocidade), por exemplo.

Nas redes MEN a taxa de transmissão para IPTV no "*Core Network*" pode crescer conforme a necessidade podendo chegar facilmente (conforme a necessidade) na casa das centenas de Gibabits por segundo. Nas redes de que distribuem o sinal ADSL o core IP, na maioria das vezes trabalha com velocidades inferiores a essas suportadas pelas MEN, o que garante uma vantagem para as MENs.

Neste ponto do Core IP consideramos também a capacidade de processamento dos equipamentos que compõem essa estrutura central. De nada adiantaria velocidades de transmissão tão altas se esses equipamentos centrais não fossem capazes de processar todas essas requisições. Neste caso a opção de MEN é bem robusta de acordo com os dados dos fabricantes. Para a *Foundry* "disponibilizamos equipamentos que tem capacidade de processamento de 7.68 Tbps e dois bilhões de pacotes por segundo." [Foundry, 2007]

A topologia da rede MEN voltada para a entrega das transmissões de IPTV deveriam ter alguns pontos básicos e comuns tanto a estrutura IPTV como MEN, por exemplo:

Na *Edge* (Borda) da rede onde está o "*Headend*" seriam usados switches/roteadores com funções de CPE (uso exclusivo) recebendo as informações dos provedores de conteúdo. E por este CPE seria enviando as transmissões para o Core IP da MEN. A velocidade entre esses pontos poderia ser de 10 Gbit conforme a necessidade de cada *Headend*.

No Core IP certamente as taxas de transmissão iniciais seriam de 10 Gbps. Entre o *Core* IP e o *Home Network* seria usado uma camada MEN de Agregação que faria o papel de *Access Network* do IPTV e teria de 1Gbps a 10 Gbps para conexão ao core. Essa camada de agregação serve para fazer o intermédio entre o Core e o *Home Network*

Os equipamentos de borda responsáveis pela distribuição do sinal para o *Home Network* seriam switch/roteador agindo como MTU com velocidades que bem poderia ser de 100 Mbps até 1 Gbps sem a necessidade de fibras, o que pode reduzir os custo de implantação. No caso de uso de cabos metálicos haverá de se considerar a distância, que no caso do UTP não pode ultrapassar os 100 metros.

As tecnologias estudadas anteriormente, como segmentação de tráfego por VLAN, roteamento, QnQ e outras que tratam de MEN podem ser utilizadas no aprovisionamento do serviço de transmissão do sinal de TV com uso do protocolo IP.

Uma única MEN pode usada por várias emissoras (geradoras do sinal de TV) ao mesmo tempo de forma transparente e sem que uma transmissão influencie na outra.

Por exemplo, imaginemos que a Rede Globo de Televisão faça uso de uma MEN para distribuição do seu sinal IPTV para os usuários. Dentro da MEN a Globo teria a função de *Headend*, para que suas informações fossem propagadas para o Core IP da MEN seria usado um switch/roteador agindo como CPE (equipamento de conexão para MEN de uso exclusivo) de onde partiriam todas as informações da programação da televisão da rede Globo, seja *liveTV* ou *VoD*.

Para esta mesma MEN que a Rede Globo de Televisão usa para transmitir a sua programação poderiam ser acrescentadas novas empresas como Record, SBT, etc. Dessa forma elas usariam o mesmo conceito usado para a transmissão da Rede Globo propagar o seu sinal.

As transmissões de todas essas empresas seriam isoladas por todo o trajeto da MEN e o mais importante, mantendo as prioridades, velocidades de cada uma das emissoras.

Os testes em laboratório deste estudo seguiram alguns dos conceitos explicados acima. Para que possa ser melhor observado o impacto da transmissão de IPTV em redes MEN serão usado vídeos com alta resolução de DVD exatamente para ocupar o máximo de banda. Durante o processo de transmissão será verificado o recuperação do vídeo no usuário com mínimo de degradação.

2.4.11) Qualidade na experiência de transmissão QoE.

A viabilidade da transmissão de IPTV esta diretamente ligada à qualidade. Não basta transmitir televisão por redes IP é necessário adotar medidas que garantam uma qualidade no serviço prestado.

Para Luciano Duque QoE é “Definir a experiência que o usuário tem, em definir qualidade de imagem.” [Duque, 2007]

Vale lembrar que esta é uma medida subjetiva, feita por amostragem de um determinado grupo. Os usuários podem (e normalmente tem) opiniões diferenciadas sobre um mesmo ponto. Essa medida subjetiva está relacionada com a experiência que cada pessoa tem com os serviços já existentes.

A qualidade na experiência, dependendo do ponto de vista pode ser mais importante que os padrões numéricos de avaliação de qualidade (perdas de pacotes, atrasos, *jitter*). A satisfação do usuário final é o mais importante dos parâmetros de avaliação, porque se todos os usuários estiverem satisfeitos com a qualidade dos vídeos assistidos o QoS não importa no primeiro momento.

Um ótimo exemplo de qualidade na experiência é o MP3. Quando esse formato de compactação de áudio surgiu, foi testado e aceito pelo mercado. Para pessoas que não tem o ouvido absoluto é imperceptível a diferença entre um arquivo de áudio em MP3 e um CD com compactação convencional. Além de manter um padrão muito próximo ao áudio original o MP3 reduz o tamanho do arquivo. Por isso dificilmente uma pessoa recusa aparelhos que suportem leitura desse formato.

Podemos dividir em três grandes barreiras que deverão ser transpostas para que o IPTV vire uma realidade.

Na primeira fase deve-se provar que ela é viável, no que tange à estrutura a ser disponibilizada e aos serviços básicos. Este trabalho trata da viabilidade nesta fase;

Na segunda fase podemos destacar a importância da “qualidade na experiência”; avaliando-se se na percepção do usuário final a prestação do serviço, e o aumento dos serviços agregados, apresentam disponibilidade a qualquer tempo e se a estrutura disponibilizada suporta o crescimento da demanda gerando satisfação. Mesmo a tecnologia sendo muito boa, se os usuários não têm uma boa experiência pode inviabilizar o uso da tecnologia.

Na terceira fase, com a propagação em grande escala e o serviço praticamente aceito, verificar o impacto de agregar mais recursos. Um grande aumento de usuários é percebido.

Assegurar QoE para o IPTV vem se transformando rapidamente em prioridade entre vendedores e fornecedores de serviço. [Duque, 2007]

Existe uma grande dificuldade para medir o que seria a boa qualidade para os usuários finais. Por ser uma medida subjetiva cada pessoa pode ter um ponto de vista diferente. Por isso é importante ter parâmetros que direcionem essa avaliação.

Não é surpresa que a qualidade de experiência (QoE-*Quality of Experience*) do IPTV tem se tornado uma das expressões mais populares nas publicações dos mercados de Telecom e dos fornecedores dos produtos IPTV. [Duque, 2007]

Neste trabalho iremos tratar de medidas objetivas como atraso de rede, jitter e perdas de pacotes. O sinal transmitido será submetido á demonstração para algumas pessoas como forma de comprovação da transmissão.

2.4.11.1) Qualidade na banda de transmissão.

As redes originais não foram desenvolvidas para envio de televisão em tempo real. Quando ocorre um atraso na rede de alguns segundos os serviços de e-mail e web, por exemplo, poderão ser pouco impactados, mas, esse mesmo atraso em um transmissão de televisão pode ser bastante nocivo para a qualidade final da imagem. [Tanenbaum, 2006]

Para monitorar os possíveis erros devem ser medidos o atraso da rede, jitter e os pacotes perdidos.

Uma das formas de compensar o atraso de pacotes na rede é aumentar o buffer do set-top-box, assim ele consegue absorver os atrasos sem que os usuários percebam. Porém, se o atraso da rede for maior que o buffer pode suportar, ocorrerá perda da imagem; o congelamento de quadros.

A qualidade da banda de transmissão pode ser assegurada com a monitoração constante e correta da rede.

2.4.12) Digital Rights Management (DRM)

Existem vários aspectos de segurança que devem ser observados na transmissão de IPTV, seja na garantia segura ao acesso, seja a proteção contra

pirataria, proteção de propriedade intelectual, estruturas físicas que garantam a proteção.

O DMR está relacionado com os direitos que os assinantes têm em solicitar e receber os vídeos de forma segura. Segundo Harte “gerenciamento de diretos é o processo de organização, controle de acesso e acesso a usuários autorizados ao conteúdo. Gerenciamento de direitos pode envolver o controle do acesso físico as informações, validação de identidade, autorização de serviço, proteção da mídia e monitoração do uso”. [Harte, 2007]

O DRM é responsável pela criptografia dos dados, isso é necessário para proteger os dados contra acessos não autorizados. O DRM previne que ocorram cópias não autorizadas na rede, se não pessoas poderiam capturar os pacotes e ver toda a transmissão sem pagar.

Esse recurso criptografia os conteúdos que serão enviados e empacota antes da transmissão.

> “Quando os usuários quiserem visualizar o conteúdo que tiver sido protegido por DMR, o equipamento do cliente deverá se comunicar com o DMR servidor de licença. [Joseph, 2006]

Se considerados os aspectos apresentados de disponibilidade, largura de banda, presença de erros, proteções contra falhas na rede, a utilização da rede Metro Ethernet para distribuição do sinal de IPTV seja ele *LiveTV* ou *VoD* em relação a distribuição por redes ADSL, torna-se mais vantajosa.

Esses aspectos serão observados, medidos, estudados e apresentados nos capítulos 3 e 4 deste trabalho.

2.5) PROTOCOLOS DE ROTEAMENTO

A função dos protocolos de roteamento é conduzir os pacotes da máquina de origem para a máquina de destino que estão em redes diferentes. Basicamente o que eles fazem é divulgar as rotas (caminhos) e atualizar as tabelas de roteamento. Para realizar essa função os protocolos de roteamento usam os algoritmos de roteamento.

Para Tanenbaum “algoritmo de roteamento é a parte do *software* da camada de rede responsável pela decisão sobre a linha de saída a ser usada na transmissão de pacotes de entrada. Se a sub-rede utilizar datagramas internamente, essa decisão deverá ser tomada mais de uma vez para cada

pacote de dados recebido, pois a melhor rota pode ter sido alterada desde a última vez". [Tamenbaum, 2003]

Existem vários protocolos de roteamento, entre os mais importantes podemos citar o RIP, OSPF, BGP e o IGRP. Cada um desses tem suas especificações e são usados conforme a necessidade de cada rede. Alguns usam rotas estáticas e outros rotas dinâmicas; uns são usados no mesmo sistema autônomo, outros em sistemas autônomos diferentes.

2.5.1) Protocolo de roteamento RIP

O significado de RIP é "*Routing Information Protocol*" com este protocolo é possível criar tabelas de roteamento com o endereço de cada rede. Para poder montar essas tabelas é usado o algoritmo "vetor-distância". [Tanenbaum, 2003]

"O protocolo de *gateway* interior da Internet original era o protocolo de vetor distância (RIP) baseado no algoritimo de Bellman-Ford, herdado da *ARPANET*" [Tanenbaum, 2003]

O vetor quer dizer direção, as interfaces definem as direções de entrada e saída para as redes. E a distância está relacionada com o número de roteadores que o pacote deverá passar até chegar ao seu destino.

Com essas duas informações de vetor e distância o algoritmo escolhe qual a rota que será melhor para encaminhar os pacotes.

HOPs são os saltos ou quantidade de roteadores que os pacotes deve passar até conseguir chegar ao seu destino.

No RIP os roteadores enviam suas tabelas de roteamento para todos os roteadores adjacentes. Essas tabelas contêm todas as redes conhecidas e a forma que essa rede pode ser alcançada. Informações de atualização de tabelas são enviadas a cada 30 segundos ou quando a topologia da rede muda, isso faz com que todos os roteadores tenham suas tabelas atualizadas.

Se um roteador receber uma tabela que contenha uma nova rota, ele adiciona esta nova rota a sua tabela, porém o valor do trajeto é acrescentado de 1 ponto. Se o valor do trajeto chegar a 16, esta rota é descartada e passa a ser considerada inatingível.

Após receber uma tabela ele realiza uma verificação para ver se existe alguma rede com o caminho mais curto do que ele esta usando no momento.

Caso exista um caminho melhor ele passa usar essa rota ou no caso existam duas rotas que levem para o mesmo destino, a opção usada pelo RIP

será pelo trajeto que tiver o menor caminho, ou seja, o caminho que tiver o menor número de roteadores em todo o trajeto.

Uns dos problemas do RIP é que ele não realiza uma verificação mais completa de todo trajeto, como salienta Gabriel Torres: O problema é que os caminhos mais curtos nem sempre são os melhores, já que o protocolo RIP não implementa nenhum modo para verificar o desempenho do caminho. Ele também não verifica o congestionamento ou se o caminho é realmente confiável. Portanto, uma rota mais longa pode acabar sendo mais rápida. [Gabriel Torres, 2001].

2.5.2) Protocolo de roteamento OSPF

O significado de OSPF é "*Open Shortest Path First*".

"O OSPF funciona transformando um conjunto de redes, roteadores e linhas reais em um grafo orientado, no qual se atribui um custo (distância, retardo etc.) a cada arco. Em seguida o OSPF calcula o caminho mais curto com base nos pesos dos arcos. Uma conexão serial entre dois roteadores é representada por um par de arcos, um em cada sentido. Seus pesos podem ser diferentes. Uma rede de multiacesso é representada por um nó da rede e os roteadores têm peso 0 e foram omitidos do grafo." [Tanenbaum, 2003]

A métrica usada pelo OSPF está associada ao custo do trajeto.

Entre as principais diferenças encontradas em relação ao RIP temos que o OSPF procura o caminho mais rápido e não o menor caminho. Assim ele evita usar um trajeto menor que tenha uma velocidade baixa ou que esteja saturado.

Como o OSPF calcula muito mais rotas para determinar qual o melhor trajeto conseqüentemente é usado mais processamento e memória. Atualmente não é mais significativa essa preocupação, porém há alguns anos atrás esse uso excessivo de memória e CPU era um ponto de cuidado nas redes.

2.5.2.1) Troca de informações entre roteadores OSPF

A troca de informações entre roteadores OSPF é feita por pacotes que contém informações sobre o link, solicitações, entre outras.

O LSA significa (*Link State Advertisements*). É através dos LSA que os roteadores de mesmo domínio OSPF trocam informações. Para cada tipo de informação existe um padrão de LSA. Assim, os roteadores trocam informações e identificam os tipos de pacotes, como:

Pacote *Hello* – Este pacote é trocado sempre que dois roteadores precisam estabelecer ou manter suas adjacências. Esses pacotes são usados para os roteadores saberem se são vizinhos. O pacote Hello inicia e mantém as adjacências entre os roteadores. [Foundry, 2007]

Os pacotes DBD (*Database Description Packet*) contêm a base de dados do roteador que enviou o DBD. Ele também trás uma visão superficial de cada LSA, assim o roteador conhece a lista de LSA vizinhos.

O pacote DBD descreve o LSA, que está contido na base de dados original do roteador. [Foundry, 2006]

LSR (L*i*nk *State Request*) – Quando um roteador precisa de uma informação específica de LSA de um link. Com isso ele identifica uma ou mais LSAs. E mostra que o roteador que envio quer mais informações sobre LSA.

O pacote LSU (*Link State Update*) – Pode conter uma reposta a uma requisição LSR ou uma informação de alteração na topologia.

LSAck (*Link State Acknowledgment*) – Transmite informações de reconhecimento de adjacência.

2.5.2.2) Divisões em áreas OSPF

O OSPF dependendo da topologia usada pode ser configurado para trabalhar com hierarquia. Conforme a necessidade de hierarquia pode-se dividir os roteadores em áreas.

Essas áreas representam grupos de roteadores que conseguem informar os caminhos que um pacote deve percorrer até alcançar um determinado ponto.

Podemos usar a mesma concepção das sub-redes IP para entender as áreas OSPF que consiste em um grupo de redes logicamente vinculadas que trocam informações das suas bases de dados.

As áreas são identificadas por um número inteiro, para cada área existe um endereço de rede e o endereço IP de entrada.

O número da área não necessariamente é similar ao endereço IP da rede. Por exemplo, a área 0 pode ter endereço 172.22.2.0/16. Porém quando o endereço de rede segue o número da área facilita a identificação.

2.5.2.3) Tipos de áreas OSPF

O LSA se divide em vários tipos, os mais importantes são: Tipo 1 que são enviados por qualquer todos os roteadores; Tipo 2 são originados apenas pelos DR (*Designated Router*); os do Tipo 3 e 4 são originados pelos ABR (*Autonomous Border Router*); o Tipo 5 é enviado ASBR (*Autonomous System Border Router*); o Tipo 7 NSSA são para as áreas –

Backbone Area – Esta área é normalmente conhecida como área 0. De forma direta ou indireta todas as outras áreas se conectam a esta área. A área 0 propaga as tabelas de roteamento para as outras áreas.

Normal – Aceita todas as LSA.

Stub – Está área não recebe e também não envia LSA de áreas externas. Ela usa uma rota estática para o ABR para mandar o tráfego de saída de sua área. Esse tipo de área pode ser usada para direcionar um trafego para uma determinada saída e garante que esse roteador não aprenda rotas que ele não deva acessar. Essa área recebe LSA do tipo 3 e 4.

NSSA – Vem da abreviação (Not So Stubby Area) é uma área que não é totalmente Stubby. Nessa área passa LSA do tipo 5 e 7. Esta também se parece com uma área stub, só estas podem enviar informações para a área central de *backbone*, porém não recebem rotas dos roteadores centrais.

Totally Stubby – Apenas a rota default é enviada para o ABR. Esta área é bem parecida com a área stubby, ela não propaga a sumarização de rotas externas. Para que os pacotes posam sair dessa área utiliza-se uma rota default de saída.

Existe uma hierarquia entra as áreas. É possível criar várias áreas entre roteadores OSPF, em cada área existe um agrupamento de roteadores. O roteador que está entre duas áreas de OSPF é chamado de ABR (*Area Border Router*), por estar entre essas duas áreas sua base de dados é maior do que a dos demais roteadores e por isso tem um número maior processamento de tabelas.

2.5.3) Protocolo de roteamento BGP

O significado de BGP é *Border Gateway Protocol*. “O BGP é fundamentalmente um protocolo de vetor distância, mas é bem diferente da maioria dos outros, como o RIP. Em vez de apenas manter o custo para cada destino, cada roteador BGP tem o controle de qual caminho está sendo usado. Da mesma forma, em vez de fornecer periodicamente a cada vizinho seu custo estimado para cada destino possível, o roteador BGP informa a seus vizinhos o caminho exato que está sendo usado.” [Tanenbaum, 2003]

Este protocolo quando foi projetado optou-se para que ele aceita-se vários tipos de políticas de roteamento entre os sistemas autônomos.

2.5.4) Roteamento IP em multicast IGMP

No envio de pacotes de algum ponto da rede para outro ponto pode-se usar o método conhecido como o *broadcast*. No caso de vários pontos estarem envolvidos o método é *Multicast*.

Porém, quanto maior o número de pontos mais difícil fica a realização desse envio. E as aplicações exigem, cada vez mais, o envio de pacotes de um ponto para vários (vídeo, voz, música), daí surge à necessidade do roteamento IP em *Multicast*.

O uso de roteamento IP em *Multicast* é indicado quando um *host* precisa mandar pacotes de uma origem até um grande grupo selecionado de destinatários e estes estão separados da origem por roteadores. [Odon Wendell, 2006]

2.5.4.1) Ocupação da Rede em Relação ao Modo de Transmissão.

Existe outro método de transmissão que é o *unicast*. Odom Wendell explica que “O método *unicast* requer que as aplicações de vídeo mandem uma cópia de cada pacote para todos os membros do grupo de endereço de *unicast*” e exemplifica dizendo “Para uma garantia de máxima emoção, em tela cheia, um vídeo *stream* requer 1.5 Mbps de banda para cada receptor. Se apenas alguns receptores existirem, este método funciona bem, mas continua requerendo n*1.5 Mbps de banda, onde o n é o número de usuários” [Odon Wendell, 2006].

Para melhor exemplificar segue a figura 2.16:

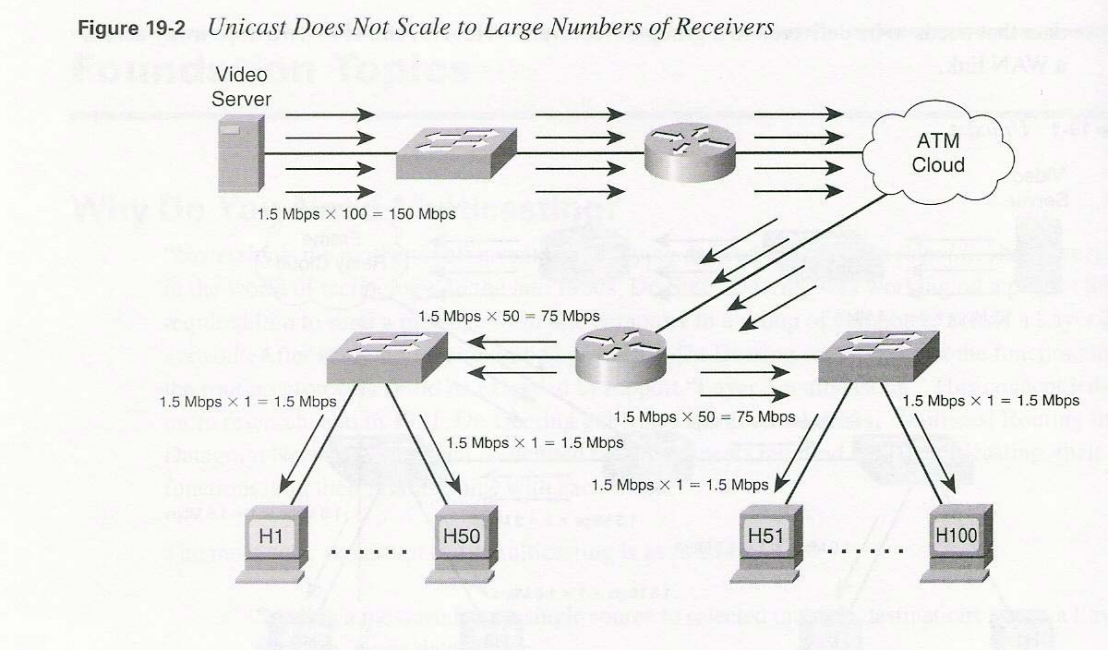


Figura 2.16 Fluxo e ocupação da banda de transmissão em unicast **[Cisco Press, 2006]**

Nesta forma de transmissão quanto mais cresce o número de usuários solicitando transferência de dados, mais os servidores e a rede (rotedores e switches) são requisitados para processar essas requisições. Isto porque a cada nova solicitação o servidor tem que enviar a mesma informação para todos os pontos. Se na figura 2.16 acima tivessem 200 usuários acessando essa rede, a taxa de utilização seria de 300 Mbps. Se fosse o total de usuários passa-se para 2000, essa taxa aumentaria para 3 Gbps.

Para tráfegos em *broadcast* ocorre outro problema. Mesmo o servidor transmitindo apenas um vídeo para os primeiros switches/roteadores os que estiverem mais para o final receberão um grande número de requisições.

Entre o *broadcast* e o *unicast* o que trará mais problemas do que benefícios será o *broadcast*. Como o *broadcast* envia os pacotes para todos os usuários independente da vontade de receber o que esta sendo transmitido, ocorrerá um grande desperdício de banda e processamento.

Na figura a 2.17 mostra-se como ocorre esse desperdício na rede:

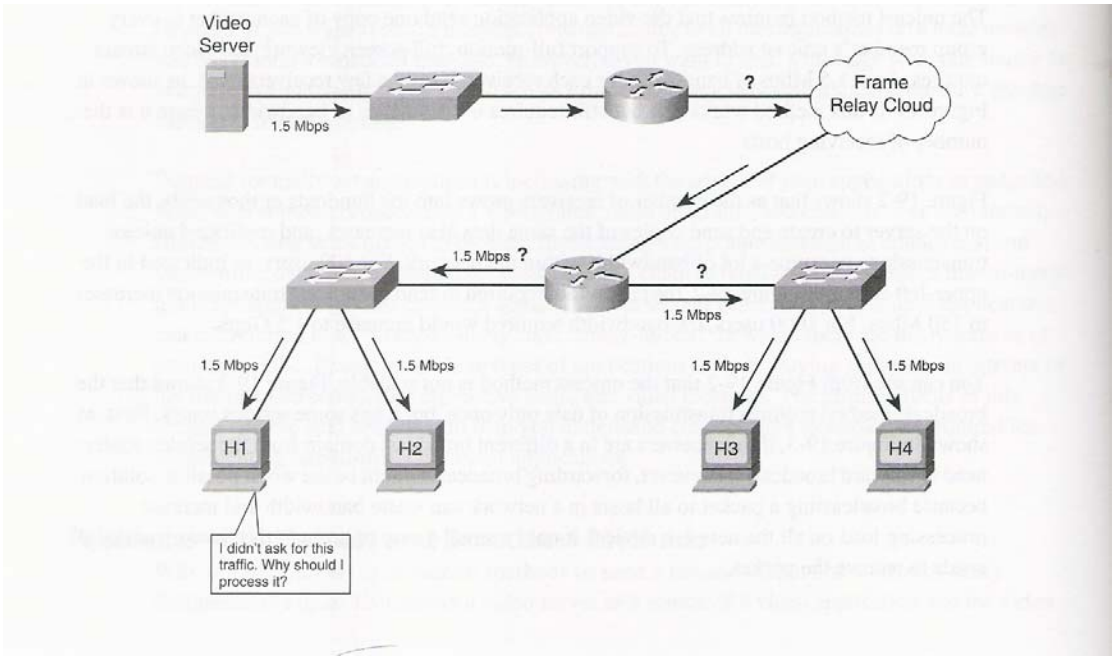


Figura 2.17 Fluxo e ocupação da banda de transmissão em broadcast **[Cisco Press, 2006]**

A figura 2.17 mostra como o *broadcast* pode enviar informações desnecessárias para a rede. O computador H1 recebe o fluxo de informações mesmo não tendo solicitado esse envio. Com isso ocorre um aumento de pacotes entre os roteadores e switches. Neste exemplo existia apenas um equipamento recebendo informações desnecessárias, porém se fossem cinqüenta computadores boa parte do processamento do switch seria ocupada desnecessariamente.

2.5.4.2) Ocupação da rede com transmissão em Multicasting

Nesta transmissão devem-se levar em conta vários pontos; dois deles são o IP de origem e o IP de destino. O IP de origem pode ser considerado um servidor de *IPTV*, e o IP de destino o *host* que irá receber a transmissão.

Partindo do ponto que existe um servidor de IPTV e está transmitindo um canal de televisão qualquer por Liv*e*TV. O servidor usa na sua transmissão a camada 3 (três) e o seu IP de destino é o 255.5.5.5. Quando qualquer um desses usuários desejar receber o que esta sendo transmitido, eles devem “entrar” no grupo de *multicasting*, isso implica que eles irão receber a partir daquele momento os pacotes de *multicasting* que estão sendo transmitidos para o IP 255.5.5.5.

Na figura 2.18 acima podemos ver vários pontos deste tipo de transmissão. Os computadores H50, H51 até H100 desejam receber as informações que são

transmitidas em tempo real. Para isso entram no grupo solicitando as informações do endereço IP 225.5.5.5. O grande diferencial que pode ser observado na figura está na ocupação do roteador R2, mesmo transmitindo informações para mais de 50 máquinas o fluxo não passa de 3 Mbps, isso faz com que seja preservado recursos como processamento nos roteadores, taxa de ocupação de interfaces.

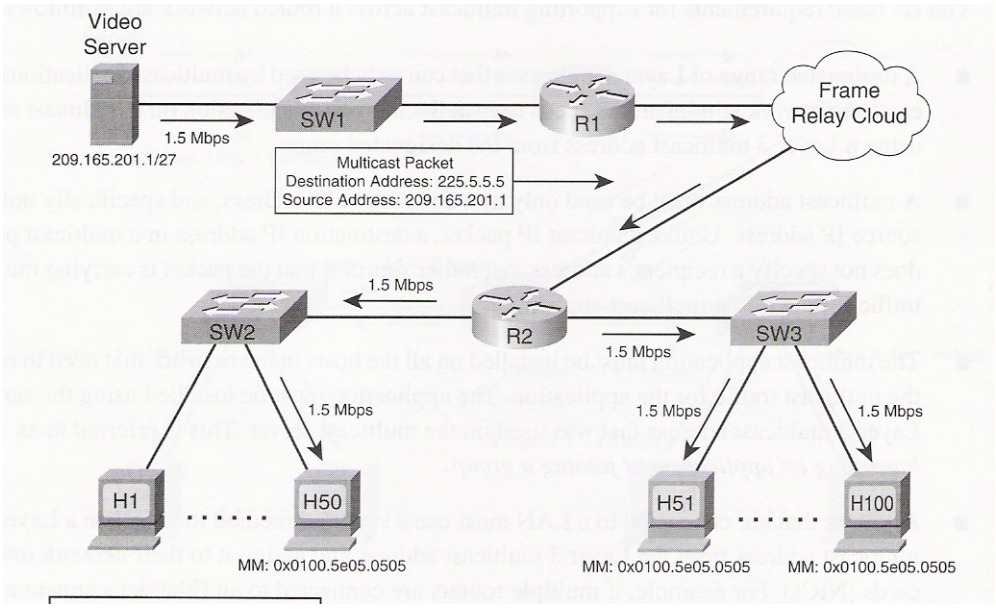


Figura 2.18 Fluxo e ocupação da banda de transmissão em multicast **[Cisco Press, 2006]**

2.5.4.3) Características da transmissão em Multicasting

No *multicasting* ocorre um tratamento diferenciado entre IP de origem e IP de destino. No endereçamento de *multicasting* é usado exclusivamente o IP de destino e não se usa como IP de origem. Isto porque ele não é usado como um único IP mais sim um range de destino.

Todos os *hosts* que desejam receber este tipo de transmissão da rede devem entender *multicasting*.

2.5.5) Protocol Indepedent Multicast – PIM

Este pode ser considerado o de mais fácil configuração e utilização entre os protocolos de roteamento *multicast*. [Cisco, 2006]

O *Protocol Independent Multicast* usa a própria tabela de roteamento que está sendo usada no equipamento seja OSPF, RIP ou rota estática.

O protocolo PIM pode operar de duas maneiras: *Dense Mode* que é indicado para ambientes de rede local o *Sparce Mode* é usado para redes WAN.

Os roteadores estão na mesma “vizinhança” e que estão configurados para trabalharem com PIM criam um domínio.

Para que um *host* comece a receber informações de um determinado grupo de *Multicast* dos roteadores, eles devem mandar uma solicitação para mostrar o seu interesse em receber essas informações.

Estes roteadores podem assumir três tipos de configuração: PMBR, BSR, RP. Os equipamentos

O PMBR tem algumas interfaces no domínio de PIM e pelo menos uma interface fora deste domínio. Esta configuração é usada quando é preciso que o domínio PIM possa ser acessado pela Internet.

O RP é um ponto central para origem e destino para as requisições de *Multicast*. O switch onde está ligado o servidor gerando o sinal de *Multicast* deve estar programado para ser o RP. [Foundry, 2007]

Cada grupo de *Multicast* tem um RP. Um domínio PIM pode ter múltiplos RPs. Os BSR são responsáveis por distribuir informações sobre os RPs do domínio, existe apenas um BSR ativo em um domínio. [Foundry, 2007]

2.5.6) Distance Vector Multicast Routing Protocol (DVMRP)

O protocolo que o DVMRP usa é IGMP, ele é responsável por gerenciar os grupos de *Multicast* IP. O DVMRP é um protocolo de *Multicast*
que faz uma espécie de “poda” nos galhos das arvores de *Multicast*. O DVMRP é um protocolo de *Multicast* de poda que entrega pacotes IP de *Multicast* que aos usuários demonstram interesse na recepção. [Foundry, 2007]

Quando os usuários querem receber os dados eles se registram no grupo usando IGMP, e o DVMRP monta a árvore de *Multicast*. No início, todos os pacotes são enviados para todos os nós da árvore, os nós que não tem grupos que desejam receber as informações mandam informações de *prune message* (mensagem de podar, cortar) e vão se desligando do grupo.

Essas mensagens de poda são importantes para reduzir o tráfego de informação desnecessário nos roteadores e equipamentos da rede.

O DVMRP constrói arvores de *Multicast* para cada grupo de origem e destino [Foundry, 2007]

Na implementação do *prune* no DVMRP o fluxo das informações de *Multicast* são direcionadas para que a topologia entre roteadores mantenha as árvores de entrega de *Multicast* com o número mínimo de ramos.

Para cada grupo receptor que estiver presente em um galho existe um transmissor que está no topo da árvore.

2.6) SSH (Secure Shell)

O SSH é a mistura de um programa com um protocolo. Através desse programa é possível acessar, monitorar e gerenciar computadores, switches, roteadores, e outros elementos de rede uma rede de forma segura. Esta segurança é conseguida através de criptografia.

A comunicação por SSH é muito parecida com TELNET. A principal diferença é que por TELNET as informações trafegam pela rede sem segurança, por não estarem criptografadas. Dependendo da criticidade das informações trafegadas o uso do TELNET deve ser evitado.

As conexões do SSH são criptografadas e, por isso, mais seguras. Se você tem de gerenciar um servidor remotamente, opte por usar o SSH em vez do Telnet. [Torres, 2007]

Como existem várias versões de protocolo de SSH, é necessário que o switch consiga diferenciar e tratar as versões de SSH. Para garantir o acesso do usuário ao equipamento, o switch negocia com o programa da máquina do usuário (tudo isso de forma transparente) qual versão de SSH a máquina está usando e a versão mais atual suportada pelos dois equipamentos será usada na comunicação.

2.7) NAT (Network Addess Translation)

No NAT não existe um protocolo nem mesmo uma padronização, basicamente o que o NAT faz é uma série de tarefas para converter o IP entre redes diferentes.

Tanembaum explica com muita clareza o conceito de NAT. Ele disse: “a idéia básica por trás do NAT é atribuir a cada empresa um único endereço IP (ou, no máximo, um número pequeno deles) para o tráfego na Internet. Dentro da empresa, todo computador obtém um endereço IP exclusivo, usado para o roteamento do tráfego interno. Porém quando o pacote sai da empresa e vai para o ISP, ocorre uma conversão do endereço. Para tornar esse esquema possível, três intervalos de endereços foram declarados como privativos. As empresas podem utilizá-los internamente como desejarem. A única regra é que nenhum

pacote contendo esses endereços pode aparecer na própria Internet". [Tanembaum, 2003]

Os endereços privativos e que não podem ser usados na Internet estão distribuídos em redes privativas. São elas: A rede 10.0.0.0 que disponibiliza 16.777.216 hosts; as redes de 172.16.0.0 a 172.31.0.0 que disponibilizam 1.048.576 hosts; e por fim as redes 192.168.0.0 a 192.168.255.0 com 65.536 *hosts*.

Essa técnica que consiste em reescrever os endereços IP dos computadores em rede é chamada de NAT (*Network Address Translation*). Nesta o endereço IP de origem de um pacote é alterado quando passa por um roteador ou *firewall* tornando possível que um computador de uma rede interna tenha acesso ao exterior, como por exemplo, a Internet.

O Processo de conversão do endereço IP é feito da seguinte forma: O Pacote que precisa deixar a rede interna e sair para Internet deve passar em uma "caixa NAT" que converte o endereço de origem "rede interna" para um endereço válido na Internet. Em cada pacote é adicionado a porta de origem e a porta de destino para informar aonde devem ser entregues os pacotes.

Um computador atrás de um roteador *gateway* NAT tem um endereço IP dentro de uma gama especial, própria para redes internas. Como tal, ao aceder ao exterior, o *gateway* seria capaz de encaminhar os seus pacotes para o destino, embora a resposta nunca chegasse, uma vez que os roteadores entre a comunicação não saberiam re-encaminhar a resposta (imagine-se que um desses routeadores estava incluído em outra rede privada que, por ventura, usava o mesmo espaço de endereçamento). Duas situações poderiam ocorrer: ou o pacote seria indefinidamente re-encaminhado, ou seria encaminhado para uma rede errada e jogado fora. [Wikipédia, 2007].

2.8) Utilização de Quality of Service (QoS)

Os técnicos e engenheiros de rede devem usar valores (objetivos) numéricos para avaliarem as condições do tráfego em uma rede. Para que as informações trafeguem conforme as determinações dos engenheiros devem ser usado padrões de QoS.

Quando analisamos o QoS devemos observar certos parâmetros como largura de banda requerida, atraso no envio dos pacotes, jitter e a perda dos pacotes.

Esses parâmetros medidos são informações objetivas (valores numéricos). Já os valores de QoE (*Quality of Experience*) são subjetivos.

Conforme pensamento de Wagner L. Zucchi “sem dúvida, a possibilidade de transmissão de informação com QoS sobre redes de comutação de pacotes é uma das razões da popularidade do serviço Metro-Ethernet, já que mensagens originadas e destinadas a esse tipo de acesso podem ser transmitidas sobre a Internet com um mínimo de mudanças de formato.” RTI dez 2006.

As ferramentas de QoS (*Quality of Service*) são usadas para priorizar o uso da largura de banda em um roteador. O tráfego é classificado quando chega a um roteador e processado através de fundamentos previamente programados. [Foundry, 2007]

No fluxo, os dados podem ser descartados, priorizados, ter a sua entrega garantida, ter a sua entrega limitada, conforme a criticidade de cada aplicação.

Entre as ferramentas existentes usadas para realizar essa priorização estão WRR (*Weighted Round-Robin*), SP (*Strict Priority*) e *Hybrid* WRR + SR que pode ser usado para a priorização de vídeo, com garantia para dados. Esses recursos trabalham com fila de priorização.

O WRR garante que todas as filas serão processadas durante ciclos. Para cada processo é atribuído um peso que é usado para alterar no serviço garantindo que todos consigam enviar e receber suas requisições. [Foundry, 2007]

O SP garante ao serviço uma alta prioridade no tráfego. O *software* determina peso máximo para essas filas de pacotes. [Foundry, 2007]

Hybrid WRR + SR usa a combinação das duas características, assim pode-se dar alta prioridade a um determinado trafego como o IPTV e garantir que os restantes sejam entregues, porém, com uma prioridade inferior.

Na tabela 2.6 observamos os valores de ocupação da banda em relação à prioridade. Para os valores Qosp7 e Qos6 será usado *Strict Priority* para priorização dos pacotes. Para os valores de zero a cinco será usado WRR.

Tabela 2.6 Largura de Banda combinada com SP e WRR com mecanismos de fila **[Foundry, 2007]**

Fila	Largura de Banda Padrão
Qosp7	Strict priority (Alta prioridade)
Qosp6	Strict priority
Qosp5	25%
Qosp4	15%
Qosp3	15%
Qosp2	15%
Qosp1	15%
Qosp0	15% (Baixa Prioridade)

No capítulo seguinte será abordado entre outras coisas os parâmetros de QoS Roteamento OSPF, segmentação por VLAN.

Para QoS será utilizado será o Hybrid WRR + SR com os pacotes que IPTV saindo com prioridade 7 e os outros dados com prioridade 3. O protocolo de roteamento usado neste projeto para comunicação nível 3 entre os equipamentos será o OSPF, a utilização deste protocolo justifica-se por ser amplamente usado pelos provedores de serviço.

CAPÍTULO 3 - Implementação de projeto para Transmissão de IPTV em redes Metro-Ethernet.

Conforme os estudos apresentados no segundo capitulo sobre a IPTV e a Metro-Ethernet, este projeto fará uso dos mesmos em um ambiente de laboratório, que permitirá o tráfego de TV encapsulado no protocolo IP utilizando uma rede Metro-Ethernet.

A concepção deste projeto está em simular a transmissão de televisão baseada em IP através de um *backbone* metro-ethernet, que será a parte central da rede, passando pelas bordas da rede, que representa a parte intermediária da comunicação, até chegar ao usuário final, que será um computador.

Esta Metro Ethernet Network foi montada no laboratório da sede da empresa Vernet Comunicação de Dados, localizada em Brasília, no Distrito Federal.

Note que, em uma aplicação real, o usuário final receberia essa transmissão de TV em seu aparelho de TV ligado à rede. Neste projeto está-se considerando o computador no usuário final, pois não está disponível um *Set Top Box* necessário para a conexão da TV à rede. Contudo, as funcionalidades do *Set Top Box* serão agregadas ao computador que receberá o sinal.

O Projeto está estruturado da seguinte forma:

i) Estudo e levantamento de requisitos para a transmissão do sinal de TV com uso do protocolo IP. Estes requisitos foram apresentados no capítulo 2;
ii) Definição da estrutura para a rede Metro Ethernet a ser utilizada na implementação;
iii) Programação dos switches da estrutura de rede. Este ponto se subdivide em outros dois estágios, são eles:
    (a) A Criação, programação e simulação do *backbone*
    (b) A Criação, programação e simulação das estruturas de borda (*Edge*) e usuários finais.
iv) Inserção e transmissão do sinal simulado de IPTV na Metro Ethernet criada;
v) Cópia do sinal gerado para apresentação;
vi) Análise dos dados coletados.

A topologia da rede que foi criada segue o modelo da figura 3.1:

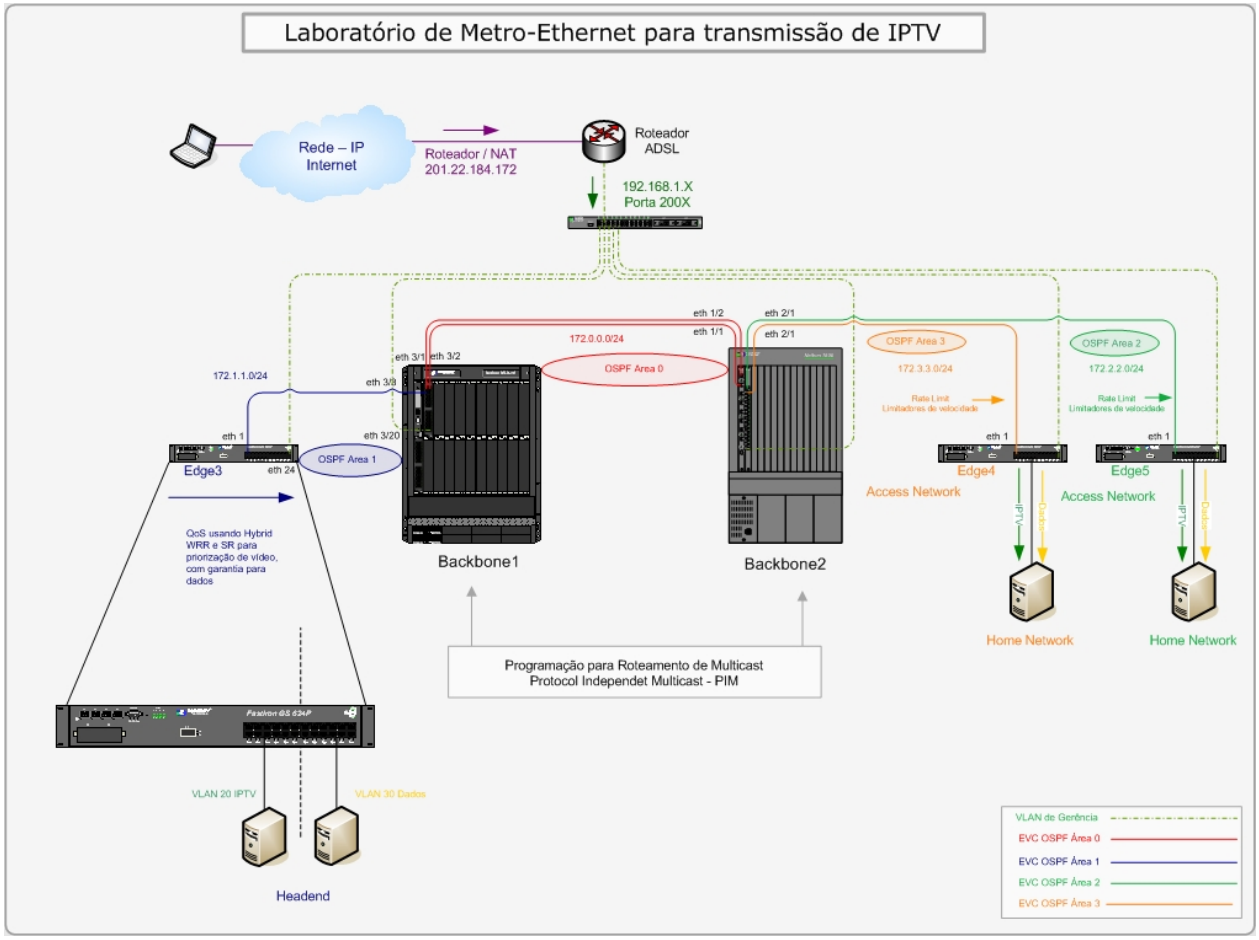


Figura 3.1 Topologia do laboratório de Metro Ethernet

A figura 3.1 representa a estrutura montada para a transmissão de IPTV em uma rede Metro Ethernet. Vários pontos devem ser observados nessa figura. Essa ilustração pode ser observada de duas maneiras, uma sob o ponto de vista de uma MEN e a outra do sistema de distribuição de IPTV.

Para a estrutura de Metro Ethernet temos cinco switch/roteadores responsáveis por transmitir todas as informações da rede. Desses cinco equipamentos, dois são usados para compor a estrutura central, pois estes são responsáveis pelo recebimento e distribuição das informações da rede. Esses dois equipamentos podem ser identificados na parte central da figura 3.1 com os nomes de *Backbone1* e *Backbone2*.

Os outros três equipamentos são responsáveis pela entrega e recebimento das informações aos equipamentos centrais. Foram denominados por *EDGE3*, *EDGE4* e *EDGE5*. O *EDGE3* está à esquerda na figura os outros dois estão localizados à direita.

Para a transmissão de IPTV o(s) computador(es) ligado ao *EDGE3* fará o papel de *Headend*, representado no lado esquerdo do desenho. Já os equipamentos que se encontram no lado direito da figura 3.1 fazem o papel de

Access Network e *Home Network*. Estes ultimos recebem a transmissão de IPTV enviada pelo *Headend*.

Durante o processo de transmissão será buscado a maior qualidade de imagem suportada, por isso as imagens processadas pelo *Headend* terão como origem mídias de DVD originais.

Para o acesso remoto aos equipamentos da MEN optou-se pela utilização de um roteador ADSL. Este roteador segue o mesmo padrão dos equipamentos residenciais. A presença deste recurso justifica-se apenas para o acesso remoto a este laboratório; em uma MEN real não teríamos a presença deste equipamento.

Todas essas estruturas serão detalhadamente descritas nos próximos tópicos deste capitulo.

3.1) Equipamentos usados na montagem da rede Metro Ethernet.

Será criado e simulado um ambiente composto por equipamentos que farão o papel de *backbone*, agregação e bordas, onde será inserido o sinal que simula uma transmissão de IPTV e também a comportamento de uma rede real.

Para a criação deste ambiente foram necessários:

- Um switch (camada 2 simples) para ser o concentrador da VLAN de gerência;
- Dois switches/roteador para fazer o papel de *backbone* (camada 2 e 3);
- Três switches/roteador para realizar o papel de *edge* (camada 2 e 3);
- Um roteador ADSL com acesso a Internet, com um endereço IP fixo;
- Módulos de interfaces ethernet para os chassis;
- Oito computadores para transmitir o sinal através da MEN e receber o sinal transmitido.

As conexões entre os switches e computadores foram feitas através de cabos UTPs e as placas de rede ethernet dos computadores suportam velocidades de 1Gbp/s.

Os cabos que ligam os equipamentos uns aos outros e por onde passaram as EVC (Ethernet Virtual Conection) são cabos UTP categoria 5e.

As conexões entre os equipamentos, em pouquíssimos casos foram feitas por fibras ópticas. Isto porque a conectorização com fibras, para fins deste projeto, ficaria muito cara e as distâncias utilizadas são inferiores a 100 metros. Apenas entre os equipamentos centrais da MEN foram usados UNIs que suportam velocidades de 10Gbps.

A título de ilustração, pode-se citar que o valor de um conector RJ45 de qualidade é em média um real, já as MiniGbics que são necessárias para ligar as fibras aos equipamentos podem custar até dez mil reais.

A opção de cabos UTPs também se justifica, pelo menor valor agregado. Como em distâncias menores que 100 metros, os cabos podem trabalhar com velocidades iguais ou menores a 1000 Mbps, poderíamos substituir essas fibras sem alterar a qualidade da estrutura, tendo a mesma velocidade que teríamos usando com as fibras.

Um dos switch/roteador que fazia papel do *backbone* não tinha módulo com interfaces ethernet com padrão UTP categoria 5, apenas interfaces de fibra óptica. Para manter o mesmo modelo foi usado o Mini-GBIC metálico que possui conector padrão RJ-45.

A rede montada seguiu características de uma Metro Ethernet real, conforme normatizações do MEF estudadas no capítulo 2.

Um dos objetivos do laboratório foi aproximar tanto os equipamentos como as suas programações do que seria usado atualmente em ambientes de produção.

A distância entre os equipamentos montados no laboratório não passa de alguns metros, porém nada impede que os equipamentos estivessem separados por quilômetros (neste caso a fibra passa a ser necessária). Eles ficaram próximos apenas pela facilidade.

3.1.1) Ferramentas usadas para gerência, administração e programação dos equipamentos da Metro-Ethernet.

3.1.1.1) Secure Shell (SSH)

Duas ferramentas de SSH Secure Shell foram escolhidas para serem usadas neste projeto. A primeira é o SSH Secure Shell Client versão 3.2.9. A segunda é o PuTTY release 0.60. Estas ferramentas foram escolhidas porque são amplamente utilizadas atualmente pelas empresas de rede de computadores para administração e gerência, o que dá maior credibilidade.

Estas duas ferramentas podem ser adquiridas de forma gratuita nos sites do fabricante. Além de usarem pouca memória e processamento, são de fácil utilização, e principalmente agregam segurança na comunicação dos dados transmitidos durante o acesso os switchs/router conforme descrito no capítulo 2.

Para o uso desse recurso, a programação mais complexa foi realizada nos nós de acesso e no roteador ADSL. Em ambas as ferramentas de SSH só foram configurados alguns parâmetros de acesso. Nos próximos tópicos será descrita a programação de cada equipamento.

Este tipo de acesso pode ser feito localmente ou remotamente. Para que um computador possa estabelecer comunicação com um equipamento por SSH ambos devem estar ligados através cabos UTP. Pode-se também usar conexões pela Internet, na qual não é necessário que o computador esteja diretamente conectado ao equipamento. Para o acesso através da Internet são necessários alguns recursos além do padrão. Esses recursos adicionais serão tratados posteriormente neste capítulo.

No desenvolvimento deste projeto utilizou-se os dois tipos de acesso. O acesso através da Internet será demonstrado durante a apresentação para a banca examinadora.

Na utilização do PuTTY para acesso externo era informado o endereço IP 201.22.184.172 (válido na Internet), porta de comunicação e um nome para essa conexão caso fosse necessário salvá-la. Usando essa opção de salvar, não é preciso lembrar de todas as portas de acesso, porque elas já ficam armazenadas em memória. Com esses parâmetros preenchidos, fez-se a requisição de acesso ao nó e quando solicitado, informou-se o usuário e senha para concluir a autenticação.

A utilização da ferramenta SSH Secure Shell Client também é muito parecida com a PuTTY. Nessa ferramenta informa-se o endereço IP, usuário e porta. A única desvantagem entre o PuTTY e o SSH Secure Shell Client é que a SSH Secure Shell Client não guarda as informações de endereço IP, porta e usuário; isso pode dificultar o acesso se não for lembrado todos os endereços e portas que precisam ser acessadas.

3.1.1.2) TELNET

As características da requisição TELNET são um pouco parecidas com SSH. Como não agrega segurança, esta opção de acesso foi muito pouco usada no projeto

Todos os equipamentos ficaram habilitados para receber acesso por TELNET, mesmo não sendo esta muito utilizada. Essa opção justificou seu uso nas eventualidades, como acesso por um computador que não tinha ferramenta de SSH instalada.

Para usar o TELNET basta abrir o *Prompt* de comando do *Windows* XP e digitar "*telnet* 192.168.1.X" onde o X é o número final do endereço IP de cada equipamento.

3.1.1.3) Acesso por cabos de console através de portas seriais

O fabricante fornece um cabo para acesso direto aos switchs/roteadores. Na utilização desses cabos é preciso ter um computador com porta serial. Conectados diretamente no switch/roteador em seu módulo de gerência.

No uso dessa solução é necessário instalar uma ferramenta de "*hyper terminal*". O *Windows* disponibiliza esse aplicativo gratuitamente. Porém essa ferramenta se mostrou um pouco limitada, sem recursos, e por isso foi preterida neste projeto.

A ferramenta que melhor se adaptou ao projeto foi a Teraterm que será descrita no item 3.1.1.4 deste capítulo.

O recurso de acesso por cabos de console foi amplamente usado durante a montagem e testes do laboratório. A velocidade de acesso por console é menor que a por SSH, mais não influencia na programação de nenhum equipamento. A utilização dessa solução se justifica por ser mais segura e prática, com ela não existe o risco de perda da conexão com o equipamento durante a programação, o que pode ocorrer no SSH e Telnet.

Os switches/roteadores têm recursos visuais (leds) que mostram a conexão, link, velocidade, ligado/desligado, esses recursos podiam também ser usados já que, para trabalhar com cabos de console, necessariamente precisa-se estar próximo dos equipamentos.

3.1.1.4) Ferramenta Teraterm

Essa ferramenta é muito utilizada pelos profissionais que trabalham com redes de computadores e também é gratuita, podendo ser facilmente obtida no site da empresa desenvolvedora.

Seguindo as especificações dos equipamentos fornecidas pelo fabricante, o terminal de acesso aos equipamentos foi configurado desta forma:

- 9600 bps
- 8 data bits
- 1 stop bit
- No parity

- No flow control

Depois de configurados esses parâmetros os equipamentos já se tornam acessíveis. Não foi necessário programar os switches/roteadores para este acesso.

Todas as programações dos equipamentos foram feitas com o uso dessa ferramenta. Este recurso permite abrir apenas uma janela por vez. Caso fosse necessário abrir mais de uma janela, deve-se usar outro tipo de acesso.

3.1.1.5) Ferramentas de TFTP

A atualização dos sistemas operacionais e o *backup* da programação dos equipamentos foi feita através das ferramentas PumpKIN versão 2.7.2 Fabricante Klever Group ou 3CDaemon Versão 2.0 Fabricante 3Com Corp.

Na parte inicial da montagem do laboratório foi definida a topologia da Metro-Rede e nela descrita cada recurso de rede que os equipamentos deveriam disponibilizar. Depois de definidos os recursos, foram inseridas nos equipamentos switches/roteadores as imagens do sistema operacional a fim de torná-los capazes de trabalhar como switch, roteadores, switch/roteadores e de disponibilizar as funcionalidades de camadas 2 e 3 .

Esta ferramenta também foi útil para realização dos *backup*s das configurações bem como restauração dessas configurações.

Os sistemas operacionais são disponibilizados pelo fabricante para *download* através do seu site.

Depois de adquiridas as imagens de boot, sistemas operacionais SXR04000.bin, sxz04000.bin por exemplo, os equipamentos eram atualizados com essas imagens. Estas ficavam armazenadas no computador servidor de TFTP. Para este projeto foi utilizado o mesmo computador, tanto para este recurso de TFPT como para programação.

Dentro do aplicativo de TFPT é apontado o diretório onde estão essas imagens.

Para que os equipamentos possam ser atualizados, tanto o equipamento como o servidor devem ter endereços IP na mesma rede e na padronização desse acesso, a todo momento foi usada a rede de gerência (192.168.1.0/24) para estas atividades.

Finalizado esses procedimentos, quando foi necessário fazer alguma atualização, foi utilizado o acesso por console para informar a ação a ser executada (*backup*, atualização, restauração) passando os parâmetros de origem

(da informação), destino, endereço IP da origem, nome da imagem e local de armazenamento.

3.1.2) Backbone Central.

Na abordagem da transmissão de IPTV a empresa provedora do serviço é responsável por receber o sinal dos provedores de conteúdo e disponibilizar meios para que a transmissão ocorra com sucesso até os usuários finais. E sem dúvida um dos pontos mais importantes que esta transmissão passa é o *backbone* central da MEN.

A estrutura montada (conforme figura 3.1) foi projetada para processar todas as informações de Televisão sobre IP e o tráfego de rede de uma rede normal. Para conseguir esse objetivo os equipamentos usados no *backbone* chegam a ter a capacidade de processamento de 3.84 Tbps. Embora não fossem necessários, para atender os objetivos do projeto equipamentos com tão elevada capacidade de processamento foram utilizados por estarem disponíveis na empresa/laboratório. Porém, um *backbone* montado com tais equipamentos tem as principais características que um *backbone* de uma prestadora de serviços de telecomunicações teria, passando por ele todas as informações entre computadores, switches e roteadores.

Na criação do *backbone* da rede foram usados dois switches/roteadores fabricados pela FOUNDRY, um deles modelo XMR 16000. Este ficou definido como *Backbone1,* e um outro, que é um NetIron 15000, que foi definido como o *Backbone2*. O site do fabricante desses equipamentos é www.foundrynet.com. Neste podem ser consultadas mais especificações técnicas.

Esses dois equipamentos podem ser vistos na parte central do esboço do laboratório, apresentado na Figura 3.1. Para facilitar a visualização eles estão interconectados por linhas vermelhas.

A opção do uso desses equipamentos neste ponto da rede vem do fato que eles são capazes de rotear pacotes entre as redes com alta velocidade além de terem uma grande capacidade para armazenar rotas. Trabalham com um grande range de redes. Eles são indicados para *backbones* que precisam de alta disponibilidade.

Todos eles são capazes de trabalhar com velocidades de 10/100/1000/10Gbps e já estão preparados para 100Gbps. Outro ponto é que

estes equipamentos também são capazes de trabalhar com as principais tecnologias estudadas no capitulo 2.

Juntos, esses dois equipamentos compõem a Metro Ethernet. Conforme ilustrado no capítulo 2, eles formam uma “nuvem” MEN onde os outros dispositivos serão ligados.

O tipo de EVC usado para ligação entre os dois nós centrais foi uma E-Line (representado no diagrama do laboratório pela linha vermelha). Por não ser preciso ter muitos equipamentos, esta opção se mostrou a melhor para o laboratório e também por ser uma conexão ponto-a-ponto. Isso porque se fossemos usar E-LAN o número de equipamentos necessários seria tão grande que inviabilizaria o projeto.

Como uma das intenções desse estudo é aproximar ao máximo a MEN criada em laboratório a uma estrutura real, usa-se uma configuração de proteção para a E-Line criada, que consiste na agregação de link. Com essa abordagem, em caso de falha de qualquer uma das fibras, os equipamentos centrais não teriam o seu EVC desfeito.

Estes dois equipamentos, que podem ser classificados como nós centrais, foram ligados entre si, como se fosse uma ligação de topologia anel. E a partir deles foram ligados os outros switches/roteadores que são os equipamentos de edge da rede. A ligação ao *backbone*, destes equipamentos que atuam como edge, segue uma topologia estrela.

Nos primeiros testes, os nós centrais foram programados exclusivamente com VLANS. Entre elas, a VLAN de vídeo, a VLAN gerência, a VLAN dados. O roteamento entre os nós era feito por rotas estáticas. Cada uma destas VLANS tinha uma função especifica para que o comportamento de cada uma dessas redes pudesse ser estudado de forma independente.

Só que esta opção distanciou-se da realidade usada no mercado. Para corrigir essa distorção foi alterado o conceito usado no *backbone* central e este passou a operar em camada três usando o protocolo de roteamento OSPF, sendo criadas as áreas de roteamento OSPF. No desenho do laboratório a área OSPF está na cor vermelha.

Para a conexão entre os dois nós centrais foi criada a área 0 (zero). O endereço de rede para esta área é 10.0.0.0 e a máscara 255.255.255.0.

Em cada interface ethernet que se ligava à área 0 foi adicionado um endereço IP. Para o *Backbone1* ficou o endereço 10.0.0.1/24 e endereço de *Loopback* 10.0.0.10/24.

Já o *Backbone2* ficou com 10.0.0.2/24 e sua *Loopback* responde em 10.0.0.20/24. Para facilitar e criar um padrão, a primeira e a segunda interface dos nós centrais foram usadas para conexão na área 0.

Essas interfaces (UNI) que formam o EVC do core da rede são respectivamente 3/1 para o *Backbone1* e a 1/1 para *Backbone2*.

A interface que fará o papel de UNI-N para o *Backbone1* e será responsável por receber as requisições de entrada da área OSPF 1 será a 3/3 e responde pelo endereço IP 10.1.1.2/24.

No *Backbone2* tem uma UNI-N a mais que o *Backbone1*, as interfaces são 2/1 e 2/2 respectivamente. A interface 2/1 responde pelo endereço de rede 10.3.3.12 máscara de rede 255.255.255.0 respondendo na área três e a interface 2/2 ficou com 10.2.2.13 respondendo na área dois.

Foram criadas duas VLANs nos dois nós centrais para tráfego de dados de IPTV e de rede convencional.

A VLAN de Dados ficou com os seguintes parâmetros: ID de identificação 30 interface taggeada 3/3, nome DADOS.

A VLAN de IPTV ficou com os seguintes parâmetros: ID de identificação 20 interface taggeada 3/3, nome IPTV.

O EVC formado entre os dois nós centrais da rede, passaram informações da VLAN de IPTV, de DADOS, LSA do OSPF e informações de taggeamento de VLAN.

A figura 3.2 mostra os dois equipamentos centrais usados na estrutura MEN montada em laboratório.

Figura 3.2 Foto do Backbone1 e Backbone2

3.1.2.1) Rede de gerência nos equipamentos centrais.

A última interface de cada equipamento foi adicionada na VLAN 10 de gerência. Mesmo não precisando de mais interfaces para acesso remoto, se necessário fosse poderiam ser adicionadas novas interfaces.

A conexão dos equipamentos com a VLAN de gerência é representada pela linha verde tracejada na Figura 3.1. Vale lembrar que esta passa por todos os equipamentos da MEN.

No ponto que trata sobre a rede de gerência, no *Backbone1,* a porta de acesso SSH foi alterada para 2001 e o endereço IP que ele responde dentro da VLAN de gerência é o 192.168.1.101/24, e por padronização, a última interface do equipamento 3/20 ficou responsável pelas requisições de gerência.

A porta SSH usada pelo *Backbone2* foi a 2002 e sua gerência por SSH é feita pelo endereço IP 192.168.1.102/24. A interface que recebe essas requisições é a 2/16.

3.1.3) Borda/Edge.

Nas transmissões de redes precisa ter equipamentos que recebam os dados e os encaminhem para o *Backbone* e, este, por sua vez, encaminhe para todos os nós da rede até que a transmissão chegue ao destino.

Para realizar a função de borda da Metro-Ethernet foram usados os equipamentos FastIron, que são switches/roteadores; estes foram usados tanto para transmitir informações para o core da rede como receber as transmissão de IPTV do core . As principais características destes equipamentos são a flexibilidade, as opções de segurança, alto nível de desempenho e a grande capacidade de processamento. Além disso, têm suporte das especificações da MEF para se ligar a uma MEN.

Todos os equipamentos de borda têm opções de velocidades das interfaces que são 10/100/1000 Mbps e também podem ter interfaces que suportam a utilização de fibra óptica. Estes equipamentos estão nas extremidades do diagrama do laboratório (ver Figura 3.1) e podem ser identificados por seus nomes “*EDGE*”.

Estes equipamentos também possuem suporte às tecnologias de camada dois e camada três, assim como ao protocolo de roteamento OSPF, todos abordadas no Capitulo 2, além de suportarem funcionalidades de QoS.

Estes equipamentos são os Customer Equipment (CE) da rede Metro-Ethernet. No total são três CEs se conectando ao núcleo da rede. Como o uso desses CEs não será compartilhado, cada um deles fará o papel de CPE. Esses CPEs podem ser encontrados no desenho do laboratório com o nome de *EDGE*

Durante a construção da MEN havia a opção de fazer com que os equipamentos das bordas atuassem como CPE ou MTU. Como era desejável a segmentação do tráfego de informações e observação do comportamento pontualmente, a melhor opção foi o CPE, pois este possui as mesmas características do MTU. Entretanto, ao invés do equipamento ser compartilhado por vários nós, ele foi usado por apenas um único nó.

Cada provedor de serviço de IPTV ou provedores de conteúdo precisam ter ou compartilhar a utilização do equipamento de borda, para, a partir deste, encaminhar sua transmissão para o núcleo da rede, de forma que toda a sua transmissão possa ser distribuída para todos os outros nós que desejassem receber esses dados.

Buscando se aproximar ao máximo dessa realidade, na estrutura de transmissão de IPTV montada na Figura 3.1, usamos um switch/roteador (CE) de

borda ligado ao *backbone*, para fazer o papel do equipamento da emissora de televisão.

No laboratório considera-se que apenas uma emissora estará gerando o sinal. Por isso considera-se que apenas um nó será responsável por esta tarefa. Esta emissora pode ser observada no lado esquerdo da figura do laboratório

Foram criadas mais três áreas OSPF além da área zero de *backbone*. Uma responsável pela transmissão de IPTV e as outras duas para recebimento de todos os tráfegos gerados. Para cada área foi colocado um novo nó, totalizando três novos equipamentos.

Ficou definido como 1 (um) a área que recebe os dados de IPTV e o endereço de rede para esta área ficou como 10.1.1.0/24. As outras duas áreas ficaram como 2 (dois) e 3 (três), sendo elas responsáveis pelo recebimento da transmissão; seus endereços de rede ficaram 10.2.2.0/24 e 10.3.3.0/24, respectivamente.

Por convenção o *Custumer Edge* (CE) que forma um EVC com o *Backbone1* foi chamado de *EDGE3*. A interface que faz o papel de UNI-C é a 1.

O *EDGE3* ficou com o endereço IP 10.1.1.3/24 e sua *loopback* responde em 10.1.1.11/24.

Os fluxo de informações saem do *EDGE* 3 pela sua interface 1, sendo transmitidas ao *backbone1* através do EVC formado entre sua UNI e a UNI do *EDGE* 3. Este fluxo passa através do *Backbone1* até o *Backbone 2*, e deste é distribuído entre o *EDGE4* e *EDGE5*.

Existem dois equipamentos de *Custumer Edge* (CE) que formam um EVCs com o Backbone2. Eles chamados de EDGE4 e EDGE5. Tanto no *EDGE4* como no *EDGE5* as interfaces que fazem o papel de UNI-C é a 1.

O *EDGE4* ficou com o endereço IP 10.2.2.22/24 e sua *loopback* responde em 10.3.3.33/24. Este não terá recurso de QoS, isso porque conforme abordado no capítulo 2 a prioridade é colocada no pacote quando ele é enviado ao seu destino. Como os pacotes de IPTV saem pelo *EDGE* 3, apenas este insere informações de QoS nos pacotes.

O *EDGE5* ficou com o endereço IP 10.2.2.3/24 e sua *loopback* responde em 10.2.2.22/24. Este também não terá recurso de QoS pelo mesmo motivo apresentado para o *EDGE* 4 no parágrafo acima.

Para cada VLAN criada nos equipamentos definiu-se um endereço de rede e uma interface virtual de roteamento. No total foram criadas seis redes e seis interfaces virtuais nos equipamentos de borda.

Para o *EDGE3*, o endereço de rede da VLAN de IPTV ficou definido como 20.20.20.0/24 e sua interface virtual de roteamento VE (virtual interface) tem o número identificador 20 e esta reponde pelo endereço IP 20.20.20.1/24. A VLAN de dados responde pelo endereço 30.30.30.0/24 e sua VE é a 30 com endereço 30.30.30.1/24

No *EDGE4* o endereço de rede é o 40.40.40.0/24 para IPTV com saída pela VE 40 com endereço 40.40.40.1/24. Para a VLAN de DADOS usou-se o endereço 50.50.50.0/24, VE 50 endereço 50.50.50.1/24.

Para o *EDGE* 5 o endereço de rede é o 60.60.60.0/24 para IPTV com saída pela VE 60 com endereço 60.60.60.1/24. Para a VLAN de DADOS usou-se o endereço 70.70.70.1/24, VE 70 endereço 70.70.70.1/24.

Na figura 3.3 temos os equipamentos de borda. O equipamento acima é o *EDGE3* o do meio é o *EDGE4.* O último equipamento na foto é o concentrador para acesso remoto por SSH.

Figura 3.3 foto dos equipamentos de borda o *EDGE3, EDGE4 e concentrador*

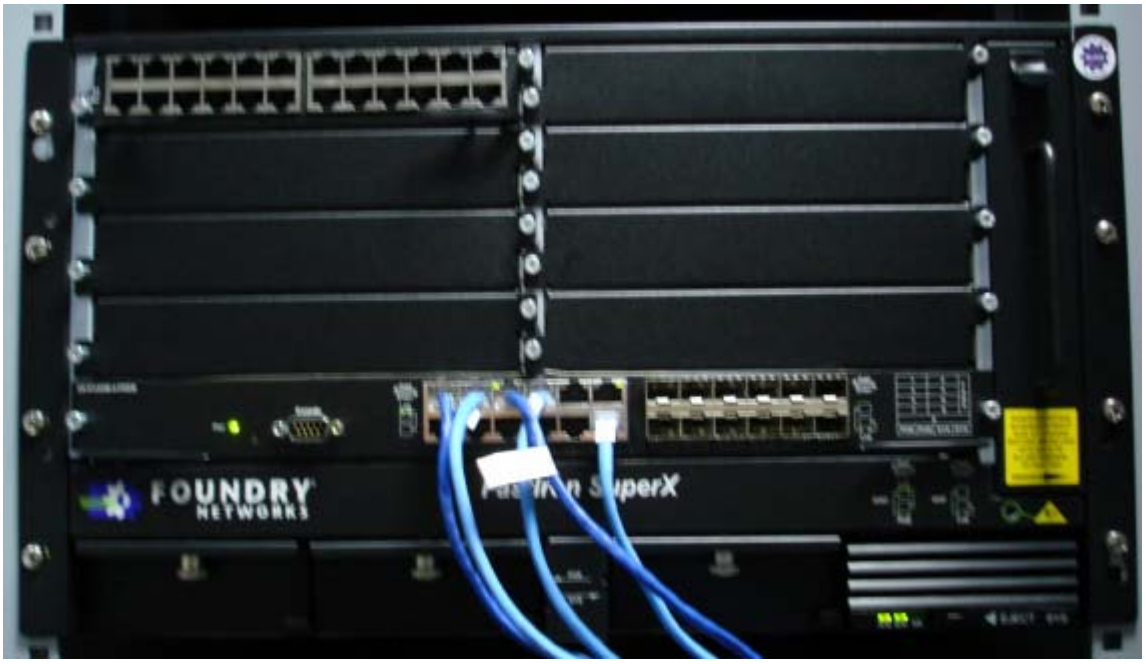


Figura 3.4 foto o equipamento de borda o *EDGE5*

3.1.3.1) Rede de gerência nos equipamentos de borda.

Assim como nos equipamentos centrais a última interface de cada equipamento foi adicionada na VLAN10 de gerência (ver no diagrama – Figura 3.1- a linha verde tracejada).

Buscou-se usar uma lógica de usar sempre o mesmo número de identificação do *EDGE* (porta SSH e endereço IP).

No *EDGE3* a porta de acesso SSH foi alterada para 2003 e o endereço IP que ele responde dentro da VLAN de gerência é o 192.168.1.103/24. EGDE4 porta 2004, endereço IP 192.168.1.104; EGDE5 porta 2005, endereço IP 192.168.1.105

Em todos esses a conexão com a VLAN de gerência é representada pela linha verde tracejada.

3.2) Áreas OSPF.

Como era necessário dividir o domínio de roteamento OSPF em áreas, foram criadas 4 áreas no total.

Para a área 0 (zero) - está entre os dois nós centrais (*Backbone1* e *Backbone2*) - foi atribuído o endereço de IP 10.0.0.0/24.

Para a Área 1, que compreende a área entre o *EDGE* 3 e o *Backbone1*, foi atribuído o endereço IP como 10.1.1.0/24.

A Área 2 compreende a área entre o *EDGE5* e o *Backbone2*, e o endereço IP deste trajeto é 10.2.2.0/24.

A Área 3 compreende a área entre o *EDGE4* e o *Backbone2*, o endereço IP deste trajeto é 10.3.3.0/24.

Para facilitar a identificação das áreas elas foram divididas por cores no desenho do laboratório (Figura 3.1). A área 0 ficou com a cor vermelha, área 1 com a cor azul, a área 2 com a cor verde e por fim a área 3 com a cor laranja.

3.3) Segmentação do tráfego por VLANs.

Outra forma usada para aproximar a MEN a uma estrutura real de uma provedora de serviços, foi segmentar os dados enviados e recebidos através de VLAN.

Além de aproximar a uma estrutura real, essa abordagem facilita o estudo das informações geradas e coletadas.

No total foram criadas 3 VLANs.

A VLAN de Dados: responsável por transmitir as informações de DADOS por toda a MEN.

A VLAN de IPTV: responsável por transmitir o sinal de IPTV por todo a MEN.

A VLAN de gerência: responsável por transmitir as requisições de acesso remoto por todo a MEN.

Todas as UNIs que formavam EVCs tiveram que ser programadas para estarem ao mesmo tempo em mais de um VLAN. Isso pode ser feito informando a todas elas que seriam "*tagged* ethernet X/X" e acrescentando essas UNIs em todas as VLANs.

Todas as outras interfaces que não formavam EVCs ficaram como "*untagged* ethernet X/X".

Por definição, nos equipamentos de borda, as interfaces de 2 até 10 fazem parte da VLAN 20 e são interfaces *untagged* e as de 11 até 20 são da VLAN 30 e também são *untagged*.

3.3.1) VLAN exclusiva de gerência "Acesso Remoto".

Para termos completo acesso a Metro-Ethernet montada em laboratório, foi criada uma VLAN só para esta função. Em um ambiente real poderia não existir uma VLAN exclusiva para Gerência, porém visando facilitar o acesso externo optou-se por criar essa VLAN. Um ponto que justifica esta opção é o fato das

informações que trafegam nesta VLAN não influenciarem nos dados da transmissão de IPTV.

Outro ponto importante foi a facilidade que agregou no acesso por SSH. Esta opção foi determinante para que todos os equipamentos estivessem disponíveis simultaneamente, uma vez que nos primeiros testes ocorria acesso apenas em um equipamento, os demais eram acessados por TELNET depois de realizada a conexão, e tendo apenas uma única janela de gerenciamento.

Por convenção a VLAN de gerência e o ID de identificação é o número 10 (dez), o seu nome é “Acesso-Remoto” e o endereço da rede é 192.168.1.0 com máscara 255.255.255.0. O uso deste endereço de rede é necessário porque ele também é usado pelo roteador ADSL que é o responsável pela troca de informações com a Internet. O uso de ADSL neste ponto se justifica exclusivamente pelo acesso remoto. A única função deste roteador ADSL é receber as requisições de gerência vindas da Internet e direcionar para os equipamentos da MEN.

Todas as interfaces de todos os equipamento que faziam parte dessa VLAN foram programadas para serem *untagged*, porque elas não fariam parte de mais nenhuma outra VLAN.

Seguindo os parâmetros da rede o *Backbone1* ficou programado para responder no endereço 192.168.1.101 máscara de rede 255.255.255.0 com rota estática de saída para o roteador ADSL. A rota criada foi “ip route 0.0.0.0/0 192.168.1.1”.

Dentro desta VLAN foram adicionadas as interfaces responsáveis por responder as requisições. Para padronizar a topologia, foram colocadas as duas últimas interfaces de cada switch/roteador.

Estas programações tiveram de ser realizadas em todos os nós da Metro-Rede que deveriam ser acessadas.

Ao final obtemos a seguinte tabela de endereços IP:

Tabela 3.1 Relação entre equipamentos e endereços IP

Nome do nó	Endereço IP de gerência	Máscara
Backbone1	192.168.1.101	255.255.255.0
Backbone2	192.168.1.102	255.255.255.0
Edge3	192.168.1.103	255.255.255.0
Edge4	192.168.1.104	255.255.255.0
Edge5	192.168.1.105	255.255.255.0

Como o roteador ADSL não tinha interface ethernet suficiente (apenas uma) para receber todos os cabos UTP que vinham dos switch/roteadores, foi adicionado mais um switch básico de camada dois, que passou a exercer a função de um concentrador. Este equipamento pode ser facilmente identificado observando o destino das ligações feitas pelas linhas tracejadas na cor verde, onde todos os cabos convergem para este equipamento. Todos os cabos da VLAN de gerência foram conectados neste concentrador. Por fim foi ligado um cabo de *up-link* entre o concentrador e o roteador ADSL.

3.4) Proteção da MEN contra loop

Conforme tratado no capítulo 2, um dos pontos importantes das redes MEN é a capacidade de proteção e recuperação contra falhas.

Um dos recursos usados é o protocolo STP para proteger a estrutura montada contra possíveis *loops*.

Optou-se por habilitar Spanning Tree Protocol em vários pontos da MEN montada e em algumas UNI foi usado o RSTP. Todos os equipamentos usados são compatíveis com essa tecnologia.

A VLAN que poderia apresentar mais ocorrências de *loop* era a VLAN 10 de gerência, nesta foi programada com 802.1w (Rapid Spanning Tree Protocol). Isto porque ela trabalha basicamente em camada dois e tem conexão direta com todos os equipamentos.

Em todas as interfaces (UNI) que faziam parte de EVCs foram habilitadas 802.1w, mesmo que na topologia não tivesse *loop*. Essa opção foi feita por ser uma boa prática em MEN.

As portas que não faziam parte de EVCs e que estavam sendo usadas por computadores e servidores foram programadas para “rstp admin-edge-port”, assim é garantido que essas interfaces passem direto para *forwarding* sem a necessidade de esperar o calculo de STP para ficarem ativas. Isso faz com que o impacto para os usuários seja amenizado.

Nas outras VLANS também foi habilitado o STP, mas isso como uma boa prática pois não era obrigatória essa opção.

3.5) Dados convencionais de rede.

Para gerar um tráfego que fosse parecido com o de uma rede convencional usamos duas formas:

- Transferência de arquivos por pastas compartilhadas.
- Transferência de arquivos por ftp.
- Acesso remoto

A mais utilizada foi a transferência de arquivos através de pastas compartilhadas. As transferências eram feitas entre uma máquina que ligava-se ao *EDGE3* e transferia os arquivos por toda estrutura da MEN, chegando ao usuário final.

A VLAN de DADOS do *EDGE3* responde pelo endereço IP 30.30.30.0/24 com o *gateway* de saída 30.30.30.1/24. Desta forma, a máquina que enviava os dados respondia no endereço IP 30.30.30.3/24.

A recepção dos dados transmitidos foi feita por uma máquina ligada ao *EDGE4* conectada a VLAN DADOS que respondia pelo endereço 50.50.50.0/24 com *gateway* 50.50.50.1/24. O endereço da máquina era o 50.50.50.3/24.

Os dois computadores que realizavam essas troca de informações ligavam-se ao switches/roteadores placas de rede que suportavam velocidades de 1Gbps.

Esses dados foram gerados para concorrerem com os dados de IPTV que passam pelo mesmo EVC entre os equipamentos *Backbone1* e *Backbone2*. Porém, quando usados os parâmetros de QoS esses dados têm importância inferior aos dados de IPTV. Isto porque em uma transmissão real o IPTV tem prioridade; para a recuperação o sinal não admite variações de atrasos ou que já não ocorre com o sinal de dados.

Como o fluxo dessas informações não é objeto de estudo deste trabalho, apenas garantimos que este estivesse em funcionamento.

3.6) Monitoramento de interfaces por espelhamento.

Conforme apresentado no capitulo 2, switches/roteadores não propagam as informações para todas as portas do barramento, sendo por isso necessário utilizar uma abordagem mais específica quando deseja-se coletar os pacotes trafegados em determinadas UNIs.

A abordagem usada foi programar os equipamentos com espelhamento de interfaces. Nesses espelhamentos ficou padronizado que a penúltima interface de cada equipamento seria usada para espelhamento. O único switch que não foi habilitado com espelhamento foi o concentrador da VLAN de Gerência, pois os dados que trafegam por ele não necessitavam ser observados.

Além de programar as interfaces (UNI) para encaminhar uma cópia dos pacotes trafegados entre determinadas interfaces, foi necessário, também, o uso de *software* específico para a coleta dessas informações. O *software* usado para realizar a captura dos pacotes foi o **WireShark** (Network Protocol Analiser) Version 0.99.6a (SVN Rev 22276). A opção pela utilização dessa ferramenta se justifica por ela ser gratuita e amplamente utilizada no mercado.

Dentro de todas as interfaces que irão monitorar (receber) os pacotes gerados deve ser passado o seguinte parâmetro “mirror ethernet X/Y”, aonde o X determina o módulo e o Y à porta. Assim ela se prepara para ser uma porta espelho.

Foi necessário direcionar o tráfego de pacotes gerados pelas interfaces que formavam EVCs e também das interfaces onde estavam ligados os servidores, para as portas espelho criadas em cada equipamento. Cada switch/roteador havia apenas uma interface responsável pelo espelhamento.

Com os procedimentos citados acima os dados são encaminhados para a interface espelho, porém ainda não estão sendo capturados para análise. O processo de captura é feito com um computador e a ferramenta de captura de pacotes, ligando a placa de rede do computador à interface espelho. Com o programa Wireshark aberto, informa-se em qual placa de rede (caso tenha mais de uma) que será realizada a captura. Com esses procedimentos já se consegue ver os dados.

Inicialmente o programa captura todas as informações que estão trafegando nas portas espelhadas. Conforme a necessidade alguns filtros podem ser inseridos. Por exemplo, captura de apenas informações que derivam para um

determinado destino ou alteração da cor de apresentação dos pacotes conforme suas características TCP, UDP.

Vale lembrar que sem essas programações nos equipamentos nada seria capturado. E quando ocorre espelhamento todos os dados apontados são transferidos, mesmo que por definição estivessem em VLANs diferentes.

3.7) Acesso aos equipamentos por Secure Shell (SSH).

Um dos pontos importantes deste projeto é garantir que os switches e roteadores estejam accessíveis para gerenciamento e configuração sem restrições. E esta é uma das vantagens da utilização de Metro Ethernet. A opção escolhida para isso foi o SSH, por se tratar de uma conexão mais segura e rápida.

Para poder interagir com os equipamentos, mesmo que remotamente, foi necessário agregar algumas soluções que tornassem possíveis os acessos vindos da Internet.

Para que os equipamentos pudessem ser acessados pela Internet foi necessário disponibilizar um IP fixo (201.22.184.10) responsável por receber e encaminhar as requisições de SSH para os equipamentos apontados.

O fluxo que se segue para o acesso remoto poder ser observado na topologia do laboratório (canto superior esquerdo) a partir do *notebook*, passando pela nuvem Internet até chegar ao roteador ADSL.

O equipamento usado para prover o acesso à Internet com um IP válido na Internet foi um roteador ADSL convencional que tem capacidade de realizar NAT e DHCP. Este roteador ADSL foi conectado a um switch por meio de cabos de rede ethernet.

Posteriormente, o roteador ADSL foi configurado para realizar um NAT, que converte o IP público da requisição que vem da Internet em um IP privado 192.168.1.X com acesso pela porta 22 (SSH) e encaminha as solicitações de acesso para a rede com esse endereço traduzido.

O uso do roteador ADSL se justifica única e exclusivamente para disponibilizar um endereço válido na Internet e realizar o NAT para prover o acesso remoto aos equipamentos. Em uma estrutura MEN não seria necessário agregar um roteador ADSL. Vale lembrar também que este não faz parte da estrutura de transmissão de IPTV.

Este endereço IP 192.168.1.X pertence a um dos switch/roteador. Cada switch/roteador foi previamente configurado para ter um endereço IP de gerência.

Além do endereço IP de gerência foi necessário programar todos os equipamentos com uma série de parâmetros para que estes pudessem responder as requisições de SSH. O primeiro passo foi criar um usuário e definir uma senha; o próximo, foi gerar uma chave criptográfica responsável por criptografar os dados transmitidos durante o acesso; e por fim criar uma rota de saída do equipamento para o roteador ADSL.

Com essas configurações o acesso remoto foi concluído. O *software* de SSH usado foi “SSH Secure Shell Client” versão 3.2.9. Neste *software*, basta informar qual o endereço IP de destino, porta (padrão 22) e o usuário que fez a requisição. Quando esta requisição de acesso chega ao equipamento, ele verifica se o usuário é autorizado; caso seja, é permitido verificar as configurações, gerenciar e programar os switches/roteadores da Metro-Ethernet.

Nos primeiros testes foi utilizado apenas um único acesso SSH para um determinado nó do *backbone* central. Essa solução foi se mostrando inadequada, pois todos os outros nós de borda ou o outro *backbone* tinham que ser acessados por TELNET dentro da mesma janela de SSH. Assim, acabava ficando muito confuso o acesso e gerava grandes dificuldades para as programações e gerenciamentos.

Para aperfeiçoar essa solução acrescentou-se um switch de camada 2 simples apenas para ser um concentrador das requisições de acesso remoto de todas as VLANs de gerência. Duas grandes alterações foram feitas para nessa nova solução. Na primeira, todas as portas de SSH foram alteradas para não mais responderem para a porta 22. Assim, cada nó da Metro-Rede foi programado para responder em porta diferente; de forma que o *Backbone1* passou a responder na porta 2001, o *Backbone2* responde as requisições de SSH na 2002, e os de borda nas 2003, 2004 e 2005.

A segunda configuração foi feita no Roteador ADSL. Foram criadas várias entradas, uma para cada equipamento. Por exemplo, as requisições de acesso remoto para a porta 2001 devem ser traduzidas e encaminhadas para o endereço de IP (192.168.1.101/24) do *Backbone1*. As requisições para a porta 2002 são direcionadas para o *Backbone2* da mesma forma feita para o *Backbone1*, com a diferença do endereço IP (192.168.1.102/24). Assim, cada requisição era apontada para o endereço IP de gerência de cada equipamento. Ao final tínhamos o seguinte mapa de endereços e portas:

Tabela 3.2 Relação dos equipamentos associados aos endereços e portas para acesso pela Internet.

Nome do nó	Endereço IP válido na Internet	Endereço IP de gerência	Máscara	Porta SSH
Backbone1	201.22.184.172	192.168.1.101	255.255.255.0	2001
Backbone2	201.22.184.172	192.168.1.102	255.255.255.0	2002
Edge3	201.22.184.172	192.168.1.103	255.255.255.0	2003
Edge4	201.22.184.172	192.168.1.104	255.255.255.0	2004
Edge5	201.22.184.172	192.168.1.105	255.255.255.0	2005

O grande diferencial dessa solução usada foi que, por um único IP fixo válido na Internet, pôde-se gerenciar todos os equipamentos da Metro-Ethernet.

Assim, quando for necessário acessar um nó pela Internet basta trocar a porta padrão de acesso (22) pela porta previamente programada (ex: 2001, 2002, 2003, 2004 e 2005) do equipamento que deve ser acessado. Caso seja necessário pode-se abrir uma janela para cada equipamento.

O acesso remoto será um recurso a mais a ser usado durante a apresentação para a banca. Com este recurso poderão ser observados e testados alguns recursos da MEN montada em laboratório para enriquecer a apresentação. Este acesso remoto não tem por objetivo a comprovação da transmissão de IPTV. O uso deste tipo de acesso justifica-se por trazer uma das características fundamentais apresentada no capitulo 2

A comprovação da transmissão será feita com a apresentação dos vídeos coletados durante a transmissão, pacotes capturados e fluxo de informação de forma idêntica ao observado no laboratório durante as transmissões.

3.8) Priorização dos dados por QoS.

Conforme estudos realizados no capitulo 2, a opção implementada na MEN foi WRR (Weighted Round-Robin) + SP (Strict Priority).

Agregou-se funcionalidades de qualidade de serviço para garantir a prioridade dos dados de IPTV. Utilizou-se também recursos de QoS para os outros dados convencionais de rede com uma prioridade reduzida.

As prioridades determinadas foram:

- QoS 7 para IPTV (alta prioridade)
- QoS 3 para os demais.

Como a transmissão de IPTV estava com QoS 7 ela sai do equipamento com Strict Priority, já os dados convencionais saem com Weighted Round-Robin.

Os parâmetros de QoS são informados diretamente nas interfaces dos switches/roteadores.

As interfaces foram programadas para identificar os pacotes com o QoS 7 foram as do *EDGE3* que faziam parte da VLAN de IPTV.

Com as configurações acima realizadas a estrutura já esta pronta para a transmissão de IPTV.

A utilização de desses parâmetros de QoS segue o modelo proposto na tabela 2.6 presente no capítulo 2. Os dados da VLAN de IPTV saem identificados com prioridade 7, com isso garante-se prioridade total dentro da MEN para estes dados; já os que saem com prioridade 3 entram em uma fila e são transmitidos com prioridades reduzidas.

3.9) Transmissão de IPTV

Seguindo a proposta inicial deste o trabalho, após montada toda a estrutura da MEN, será feita uma transmissão de IPTV através desta rede metro-ethernet e serão observados os impactos da transmissão deste sinal na rede. Ao final pode-se verificar a qualidade dos vídeos e imagens transmitidas no ambiente criado.

Para a transmissão da televisão usando a tecnologia de IPTV será transmitido um sinal que simule as características de um sinal de IPTV.

Vale lembrar que, conforme estudos do capítulo 2, esta não é uma transmissão de vídeo pela Internet e sim uma transmissão de vídeo baseado no protocolo IP.

Na comprovação da transmissão será utilizado sinal de vídeo oriundo de DVD, que apresenta características mais exigentes de largura de banda e qualidade. Para a demonstração será apresentado um sinal com as mesmas características desta transmissão.

3.9.1) Software para transmissão de IPTV

Durante o processo de pesquisa sobre a ferramenta que realizaria o processamento e encapsulamento dos vídeos para transmissão na rede MEN, buscou-se um *software* que permitisse gerar um sinal que se aproximava ao

máximo com as características de uma transmissão de IPTV, com a qualidade necessária que esta transmissão requer.

Esta ferramenta é capaz de gerar e transmitir vídeo a partir de um computador, que quando conectado à Metro-Ethernet, simula a parte geradora do sinal de vídeo localizada no *Headend*. Ela trata de um sinal já gerado, armazenado em vários formatos e que podem ser processados para a transmissão, no formato MPEG2, conforme requisitos do projeto.

O *software* que mais se adequou às necessidades do estudo foi o “VLC Media Player” versão 0.8.6c. Além de se adequar às expectativas, este *software* é gratuito e tem o código aberto.

Entre os recursos disponibilizados pela ferramenta os que são de maior relevância são a capacidade de processar vídeos em vários formatos e transmiti-los em formato MPEG2, com a opção de alta definição.

O ”VLC Media Player“ suporta o envio feito por VoD (*Unicast*) ou LiveTV (*Multicast*), lembrando que estas duas características são as duas das mais importantes na propagação do sinal de IPTV.

Este *software* foi instalado em um computador que estava diretamente ligado ao switch/roteador *EDGE3* por uma interface que fazia parte da VLAN de IPTV. Tanto a máquina servidora como a interface tem velocidades de transmissão de 1Gbps.

Como o escopo desse projeto não está voltado para a segurança na transmissão, não foi acrescentada nenhuma ferramenta de DMR. O que se buscou realizar foi a comunicação entre o *Headend* e o *Home Network*.

3.9.2) Armazenamento e preparação do vídeo

Um dos objetivos deste trabalho é realizar a transmissão de IPTV por intermédio de uma rede MEN. Para isso simulou-se um *Headend* que deu início à transmissão das imagens

Uma das características do *Headend* está no armazenamento e preparação dos vídeos que serão distribuídos. Os computadores que realizavam o papel de *Headend* estavam ligados ao *EDGE* 3 através de placas de rede que suportavam taxas de transmissão de 1 Gbps.

O responsável pelo armazenamento será a própria máquina servidora (que está ligada ao *EDGE* 3) onde foi instalado o *software* para distribuição de IPTV.

Entre as origens das imagens pode-se considerar o DVD, VCD, SVCD 2, DVB, Satélite, TV Digital, TV a cabo, todos eles podendo gerar nos formatos MPEG2.

A figura 3.5 mostra as opções de entrada de vídeo, o fluxo que a informação segue e as possíveis formas de visualização da transmissão.

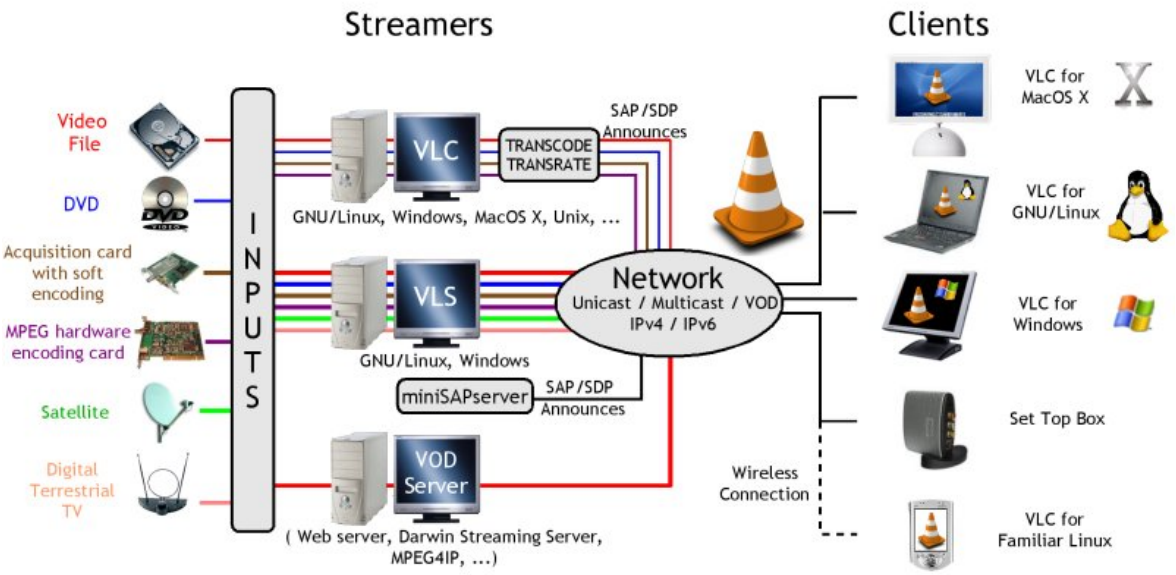


Figura 3.5 Diagrama mostra as opções de entrada, tipos de distribuição e equipamentos de recepção **[VideoLAN, 2007]**

Para melhor visualizar o local onde o computador que atua como *Headend* foi instalado, optou-se por aumentar o desenho do *EDGE* 3 (canto inferior esquerdo da Figura 3.1).

A opção escolhida foi DVD. A máquina servidora usa a leitora de DVD para ler os arquivos de uma mídia em DVD. O DVD foi usado por ser um arquivo de vídeo em alta resolução.

Poderíamos armazenar o filme do DVD dentro do HD do servidor, por uma questão de direitos autorais preferiu-se usar o próprio disco DVD.

Duas opções de IPTV poderiam ser utilizadas em laboratório: O VoD ou LiveTV. A opção escolhida foi de VoD, por ser uma transmissão que ocupa muito mais banda da rede, e com isso conseguir observar a transmissão mais impactante.

Como o sinal gerado para a LiveTV é comum a todos os usuários usar o recurso de *Multicast* para reduzir a quantidade de sinal gerado. Caso fosse usada, ocorreria uma redução de informação para análise posterior. Por isso o LiveTV seria passível de transmissão com maior facilidade nessa rede.

Outro ponto levado em consideração na escolha de VoD em relação ao LiveTV foi a indisponibilidade de recursos que captassem o conteúdo em tempo real (LiveTV) gerado pelas emissoras.

Para geradora do sinal o VoD é o sinal mais importante porque consome uma enorme largura de banda. Este sinal será encapsulado com em IP e posteriormente transmitido pela Metro Ethernet até chegar ao usuário final, representado pelos equipamentos ligados ao *Home Network*.

Com o VoD poderá ser realizada várias transmissões simultâneas, passando pelo mesmo EVC e ocasionando uma concorrência entre o conteúdo gerado para cada usuário, trazendo assim mais informações sobre pacotes enviados, recebidos e perdidos.

Após ler os dados, a ferramenta converte as imagens em pacotes de forma que estes possam ser enviados pela MEN usando o protocolo IP. Os vídeos serão transmitidos em MPEG2. A partir daí os pacotes já estão prontos para serem transmitidos, de modo que, logo após a preparação dos dados, eles passam a ser enviados pela rede.

O *Headend* responde pelos endereços de rede 20.20.20.4/24, 20.20.20.5/24 e 20.20.20.6/24.

Os dados são enviados para a MEN através do equipamento *EDGE3* (lado esquerdo do desenho), e a partir desse os dados são transmitidos para o Core até que cheguem ao *Home Network*.

Vale ressaltar que uma das preocupações desse trabalho foi utilizar apenas mídias de filmes de DVD originais, nenhum dos testes foi realizado com imagens “pirateadas”. Em momento algum foram aferidos lucros com os testes.

3.9.3) Recebimento da transmissão do vídeo

Por fim, após iniciadas as transmissões, estas deveriam ser recebidas na outras extremidade da MEN através nós *EDGE* 4 e 5 que estão fazendo o papel de Access (ver figura 3.1).

Os usuários desejam receber e converter as imagens que estão sendo transmitidas em IP através da MEN, e precisam de um equipamento especial. O equipamento que realiza essa tarefa é o *Set Top Box*.

O papel do *Set Top Box* (do usuário) será simulado pelo mesmo programa que realiza a parte de transmissão. Ele é responsável por receber e converter os pacotes IP que contém as imagens transmitidas para o formato de vídeo.

Os computadores que realizavam o papel de *Home Network* estavam ligados ao *EDGE* 4 e ao *EDGE* 5 através de placas de rede que suportavam taxas de transmissão de 1 Gbps.

Os usuários que desejam receber a transmissão devem externar a sua vontade requisitando o recebimento do vídeo ao *Headend* através de seu endereço IP, para isso deve-se entrar no grupo de transmissão e informar o seu endereço IP.

Para o usuário do *Home Network* que recebia a transmissão através do *EDGE4* ficou com o endereço IP 40.40.40.4. Para o *EDGE5* os endereços de rede foram 60.60.60.4/24, 60.60.60.6/24.

Com todos esses procedimentos realizados o ambiente laboratorial tornou-se completo e já possibilitando dar prosseguimento à última etapa da parte laboratorial.

No próximo capítulo serão apresentados os testes realizados para comprovar o funcionamento dos recursos propostos, a metodologia seguida durante os testes e também os resultados obtidos com as simulações.

CAPÍTULO 4 - Simulações e Resultados

Este capítulo engloba os testes realizados na rede Metro Ethernet, as simulações na transmissão de IPTV realizadas e também resultados obtidos.

Para reduzir a ocorrência de erros na estrutura, sejam eles de topologia, programação, configuração e transmissão, utilizou-se uma metodologia para os testes, onde todos os procedimentos iniciavam-se com o menor número de variáveis: um switch/roteador, apenas um acesso remoto, uma transmissão de VoD e assim por diante.

A cada nova variável, como o acréscimo de equipamentos, transmissões e programações, foram realizados testes para garantir a funcionamento do serviço. Caso resultados satisfatórios não fossem obtidos, não se daria prosseguimento a novas atividades.

Existem três grandes grupos de testes. Eles foram segmentados e testados de forma isolada e ao final todos foram testados simultaneamente. Estes grupos são:

- **Acesso Remoto** – Acesso aos equipamentos através da Internet de forma segura por SSH (Secure Shell);
- **A comunicação dos switches/roteadores nas camadas de nível dois e três da MEN** – Verificação da conectividade entre todos os nós, servidores de IPTV e resoluções da tabela de roteamento.
- **A transmissão do VoD** – Transmissão do sinal de IPTV Vídeo sob Demanda – VoD – e recebimento pelo usuário (*Headend*).

Como cada um desses três grupos tem características diferentes, os testes foram realizados de forma diferenciada.

Todos esses procedimentos buscaram validar as especificações propostas no capitulo 3.

4.1) Simulações de estruturas segmentadas

4.1.1) Acesso Remoto por SSH

Depois de realizadas as programações para o acesso remoto descritas no capitulo 3, cada switch/roteador foi testado unitariamente.

Posteriormente, os switch/roteadores foram acrescentados um de cada vez até obter todos os cinco, formando a MEN proposta no capítulo 3.

4.1.1.1) Acesso por SSH interno unitário

A base da gerência remota está no acesso por SSH interno. O acesso remoto só é possível se o acesso local estiver funcionando corretamente. Por este motivo, o teste de acesso local foi realizado anteriormente ao remoto.

Estes procedimentos foram realizados diretamente nos switches/roteadores.

Para se realizar o teste local, um computador foi conectado diretamente à interface destinada ao acesso remoto através de cabo UTP. Adicionou-se o endereço IP 192.168.1.2/24 à interface do computador.

Seguindo a tabela 3.2, apresentada no capítulo 3, usou-se o endereço IP, a porta SSH e o nome do usuário para iniciar a conexão com o equipamento. Passados esses parâmetros informou-se a senha anteriormente definida. Vale lembrar que neste ponto foi usado o endereço IP 192.168.1.10X e não o endereço válido na Internet.

A figura 4.1 mostra os parâmetros passados para o acesso ao equipamento *EDGE5*. Estando todos os procedimentos corretos o acesso ao equipamento era concedido.

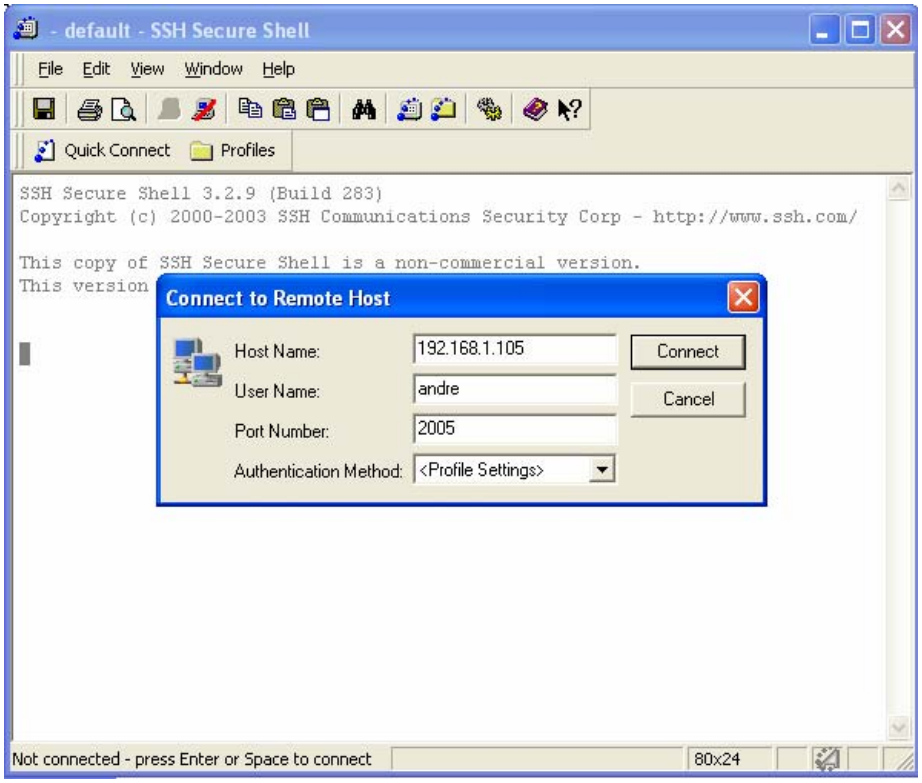


Figura 4.1 Tela de acesso local por SSH usando a ferramenta SSH Secure Shell.

4.1.1.2) Acesso por SSH interno conjunto

Após a validação dos testes unitários em todos os equipamentos, iniciou-se o teste conjunto com todos os equipamentos.

Conforme proposto no capitulo 3, todos os equipamentos foram conectados ao concentrador.

Para realizar o teste em conjunto o computador que antes se ligava à última interface de cada equipamento foi ligado ao switch que realizava o papel de concentrador.

A realização da requisição de acesso passando pelo concentrador segue o mesmo parâmetro da requisição unitária. A partir daí, informa-se o endereço IP, nome do usuário e porta SSH.

Todos os equipamentos responderam conforme o planejamento. Após essa confirmação já poderia ser feito o acesso remoto por meio da Internet.

4.1.1.3) Acesso unitário SSH por meio da Internet

Alcançados os resultados satisfatórios no acesso local, já era possível iniciar os testes de acesso por meio da Internet.

O teste de acesso remoto por meio da Internet consiste em realizar uma requisição de gerência a um equipamento, só que ao invés de conectar-se diretamente, usa-se a Internet como meio de comunicação.

No teste unitário ligava-se a última interface do equipamento ao roteador ADSL, responsável por enviar as requisições de acesso vindas da Internet para os equipamentos. Verificada a ligação entre equipamento e roteador ADSL, solicita-se o acesso passando os parâmetros previamente configurados.

Após a passagem dos parâmetros da requisição, o switch/roteador valida os objetos passados e libera o acesso para a gerência.

O endereço IP e porta usada para o acesso seguem o padrão determinado pela tabela 3.2. Vale observar que neste momento o endereço IP que era solicitado era o válido na Internet.

Na figura 4.2 são apresentados os parâmetros usados para acessar o equipamento pela Internet. Observa-se que é usado o endereço 201.22.184.172 válido na Internet e não mais o endereço local 192.168.1.10X.

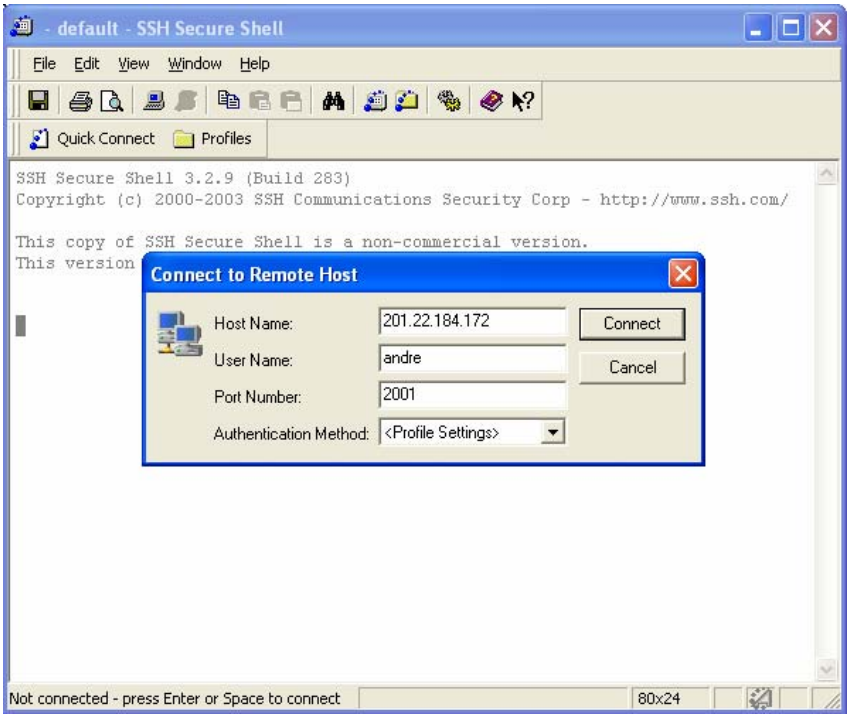


Figura 4.2 Tela de acesso através da Internet por SSH usando a ferramenta SSH Secure Shell.

4.1.1.4) Acesso conjunto SSH por meio da Internet

Após a validação unitária fez-se necessário realizar a validação conjunta por meio da Internet.

A topologia final testada para o acesso pela Internet pode ser observada pela figura 3.1 do capítulo 3. Todos os equipamentos ligavam-se ao concentrador e este por sua vez conectava-se ao Roteador ADSL.

Neste ponto, o fator que diferencia os equipamentos não é mais o endereço IP e sim a porta SSH anteriormente programada em cada equipamento.

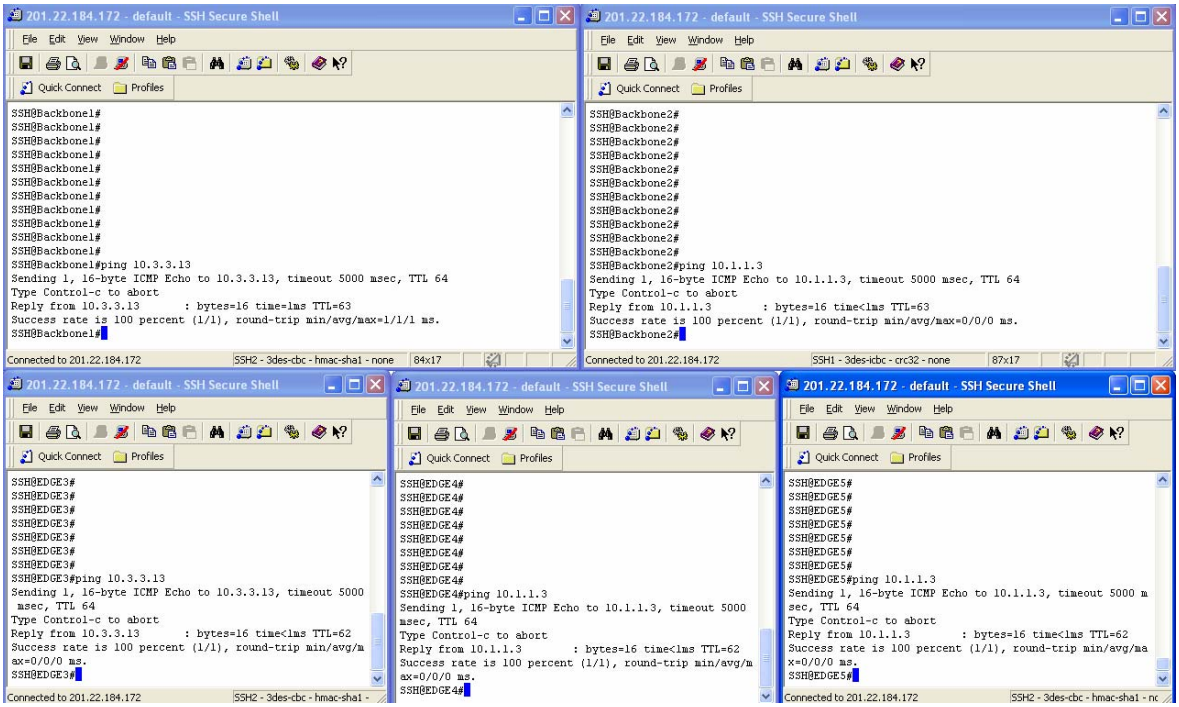


Figura 4.3 Todos os equipamentos sendo acessados simultaneamente pela Internet usando a ferramenta SSH.

A figura 4.3 mostra os cinco acessos simultâneos pela Internet aos equipamentos da MEN. Nas duas janelas superiores estão os switchs/roteadores centrais *Backbone1* e *Backbone2*. As três janelas inferiores da esquerda para a direita mostram o acesso aos equipamentos de *EDGE*3, *EDGE4* e *EDGE*5. Cada um desses equipamentos está respondendo a porta determinada no capítulo 3.

O último teste que validou em definitivo esse modelo de acesso por SSH foi realizado nas dependências do UNICEUB, distante a aproximadamento quatro quilômetros do laboratório.

Com um *notebook* conectado na rede wireless, requisitou-se o acesso externo aos equipamentos no laboratório e todos responderam às solicitações de gerência conforme as expectativas. Como o UNICEUB utiliza firewall, solicitou-se para os administradores da rede que fossem liberadas as portas 2001 até 2005 para o 201.22.184.172.

Após todos esses testes sabia-se que a estrutura montada responderia corretamente a todos os tipos de acesso, tanto internos como externos.

Esse acesso externo tem grande importância para este projeto. Com ele poderá ser demonstrado à conveniência de se gerenciar uma rede desta magnitude remotamente, que é uma das características de uma MEN. E também suprirá a necessidade de demonstrar as configurações e topologias para validação deste projeto.

4.1.2) Comunicação dos equipamentos da Metro Ethernet

Nos testes de comunicação entre os equipamentos da MEN utilizou-se o protocolo ICMP através da ferramenta muito conhecida, o ping. Em um primeiro momento pensa-se que o ping é uma ferramenta simples, porém ela se mostra extremamente útil ao verificar a comunicação em redes.

Em todos os testes de conectividade era usada a ferramenta **Prompt de comando** que já vem nativo no *Windows* XP. Dentro do Prompt de comando usa-se o **ping** passando o parâmetro (endereço IP) a ser testado. Com esses testes tinha-se certeza que tanto o caminho de ida como o de volta estavam funcionando.

Os primeiros testes unitários realizaram-se no *EDGE*3, com o *notebook* diretamente conectado à interface do *EDGE* 3.

Deve-se observar que os equipamentos estão segmentados em VLANs e isso implica que deveriam ser feitos vários testes dentro do mesmo equipamento. Foram feitos teste em cada VLAN e na interface responsável pela saída/entrada na área OSPF.

Para testar a conectividade de cada VLAN, fez-se necessário ligar o *notebook* em uma interface que estivesse associada àquela VLAN.

Por exemplo, para testar a VLAN de IPTV ligou-se o *notebook* a interface 5 do *EDGE3*, configurava-se o endereço IP do *notebook* com um endereço da rede válido para esta VLAN, a partir daí pingava-se a interface virtual de roteamento da VLAN de IPTV.

A figura 4.4 mostra uma resposta positiva ao teste de conectividade do *EDGE3* feito a partir do *notebook* que estava diretamente conectado ao switch/roteador.

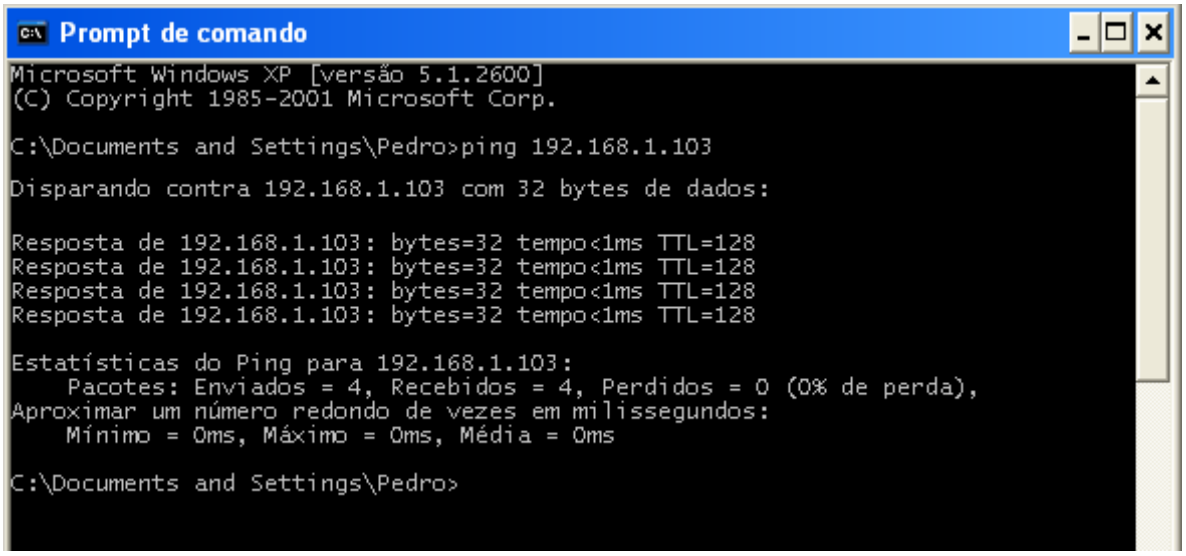


Figura 4.4 Resposta do teste de conectividade ao EDGE3.

Concluídas todas as programações de endereços IP, ligações físicas, VLANs, rotas, áreas OSPF descritas no capitulo 3, cada switch/roteador foi testado em conjunto com todos os cinco nós na Metro Ethernet.

Neste último teste todos os endereços IP de cada equipamento foi verificado. Este teste é considerado o mais importante porque valida a comunicação de toda a estrutura da MEN, iniciando pelo equipamento de borda, onde fica o *Headend*, chegando até a outra extremidade da rede no usuário no *Home Network*.

Figura 4.5 Teste de conectividade do EDGE3 por toda a estrutura MEN.

Na figura 4.5 pode ser visto o resultado do teste de conexão do *EDGE* 3 com toda a estrutura da MEN. O primeiro endereço IP acesso é o 20.20.20.1 correspondente a interface virtual e *gateway* de saída da VLAN de IPTV. O teste segue para o endereço IP da área OSPF 1, passando pelos principais Hops da área 0 até chegar na área 2.

4.1.3) Transmissão de VoD

Para a simulação, transmissões e testes do vídeo sob demanda (VoD) foi usada a ferramenta VLC Media Player conforme descrito no capitulo 3.

Durante os testes a ferramenta VLC mostrou-se robusta e de grande confiabilidade, além de ser gratuita.

Nos trabalhos iniciais usaram-se imagens de baixa resolução, pois o foco não era a qualidade, mas sim conseguir realizar o envio do VoD pela MEN e garantir o seu recebimento pelo *Home Network*.

O primeiro teste foi realizado apenas com um switch e dois computadores. O switch operava apenas em camada dois e não realizava funções de roteamento, QoS, nem VLANs. Essa opção justificou-se para diminuir os números de variáveis que poderiam aparecer caso a transmissão falhasse.

O objetivo deste teste era conseguir enviar e receber a transmissão por computadores diferentes. Neste teste conseguiu-se transmitir e receber de um computador para o outro com o vídeo passando pelo switch.

Alcançados os objetivos do primeiro teste, iniciaram-se os testes que agregavam novas funcionalidades. Para isso o switch começou a realizar a segmentação interna por VLAN das informações de IPTV.

Como os dados de IPTV estavam segmentados, agregou-se o uso de interfaces virtuais para que ocorresse o fluxo das informações entre VLAN. Com essa nova programação foi realizada nova transmissão de VoD. Esse teste validou a transmissão de VoD usando o roteamento interno.

Nos primeiros testes realizados com dois switches/roteadores, onde o *Headend* ligava-se em um deles e o *Home Network* ligava-se no outro, foram usadas rotas estáticas entre os switches/roteadores para evitar problemas de roteamento. Com esse teste observou-se o comportamento e da qualidade da transmissão fluido entre os dois equipamentos.

O próximo teste realizado envolvia OSPF seguindo a estrutura apresentada no capítulo 3, que usava o *EDGE*3 e o *Backbone1*. Com estes dois equipamentos a transmissão de VoD usando OSPF passando por um EVC foi verificada.

À medida que os testes avançavam verificou-se através das medições que a qualidade das imagens poderia ser ampliada. Mesmo não sendo a objetivo principal deste estudo, para enriquecer ainda mais as informações, agregaram-se então as medições para transmissões de VoD em alta definição (HD).

Vale lembrar que na transmissão de IPTV existem duas áreas; o LiveTV e o VoD. A opção de transmissão dos vídeos em laboratório foi o VoD, por se tratar de uma requisição sob demanda, onde os vídeos eram transmitidos em alta definição (HD) compactados com o formato do vídeo e MPEG2.

Os filmes transmitidos com essas características descritas acima ocupavam na banda de transmissão valores entres 8Mbps até 12Mbps.

A título de ilustração alguns dos filmes e shows em DVD usados foram: filme CRUZADAS produzido pela “Twentieth Century Fox”; filme LENDAS DA VIDA produzido por “Twentieth Century Fox”; show ANDREA BOCELLI Under The Desert Sky produzido pela “Universal”

A partir desse momento usaram-se apenas imagens em alta definição oriundas de DVDs (originais)

Durante todos os testes foram realizadas coletas e armazenamento dos pacotes enviados entre o Haedend e o *Home Network*. A partir desses dados foram gerados os gráficos, estatísticas, médias de utilização, perdas e etc.

Com todos os resultados de conectividade esperados obtidos principalmente com os testes de OSPF passou-se para o teste conjunto com todas as estruturas agregadas.

4.2) Simulações de estruturas agregadas

Finalizados os testes unitários com sucesso, começaram os testes com todos os recursos de IPTV, Metro Ethernet e acesso remoto. A topologia criada para esta parte segue o diagrama 3.1 explicado no capítulo 3.

Como primeira atividade, todos os servidores de IPTV foram ligados ao switch/roteador *EDGE3*, onde fica localizado o *Headend*. Posteriormente, os clientes que iriam receber as informações de VoD forma ligados nos switches/roteadores *EDGE4* e *EDGE5*.

Quando todos os computadores estavam conectados, os testes de conectividade entre eles foram realizados. Para isso foi usado o mesmo processo descrito no item 4.1.2 deste capítulo, só que neste já se considerava as estruturas de roteamento válidas.

Para realizar esse teste foi usado um total de nove computadores, todos trabalhando. Três transmitiam as requisições de VoD, outros três recebiam o fluxo de informação de vídeo, dois trocavam dados de rede convencionais e o último era responsável pela coleta das informações.

Estando todos os servidores respondendo corretamente, começaram a ser disponibilizadas as transmissões de VoD para os usuários, uma de cada vez. O número total de requisições de VoD incrementava-se de uma a uma.

Tabela 4.1 Relação de testes realizados e recursos agregados.

Teste	Recurso	Resultado
Primeiro	Uma requisição de VoD	Positivo
Segundo	Duas requisições de VoD	Positivo
Terceiro	Três Duas requisições de VoD	Positivo
Quarto	Três requisições de VoD sem QoS	Positivo
Quinto	Três requisições de VoD com QoS	Positivo
Sexto	Três requisições de VoD + dados sem QoS	Positivo
Sétimo	Três requisições de VoD + dados com QoS	Positivo

Para que fosse melhor observado o comportamento de todos os equipamentos switch/roteadores, servidores, EVCs, *Home Network* envolvidos durante a transmissão de IPTV, foram realizados sete testes evolutivos.

Considerava-se o resultado positivo quando as requisições de VoD chegavam ao usuário final conforme solicitado sem a presença de erros durante todo o trajeto. O trajeto considerado foi desde o *Headend* passando pelo Core IP até chegar ao usuário final.

A realização novos testes só seria feita quando todos os resultados obtidos no teste presente fossem considerados positivos para os padrões citados no parágrafo acima.

O teste de acesso remoto foi executado quando todas as estruturas de *Headend* já estavam enviando as requisições de VoD e todos os *Home Network* recebendo os dados envidados. Esse acesso remoto realizou-se durante o sétimo teste.

4.3) Coleta dos dados das simulações

Foram várias as ferramentas usadas na coleta e tratamento dos dados. As ferramentas são: a WireShark, Tracebuster e WinEyeQ estas duas últimas fabricadas pela empresa Touchestone. A ferramenta WireShark é gratuita e pode ser adquirida no site do fabricante. As ferramentas da Touchestone são pagas mas podem ser testadas gratuitamente.

Com esta ferramenta WireShark tornou-se possível verificar o fluxo das informações que passavam em cada equipamento, além de mostrar em tempo real o tráfego da rede. Esta ferramenta também dá a opção de salvar os dados coletados para posterior análise.

Essa ferramenta foi instalada em duas máquinas. Optou-se por instalar em *notebooks* pela mobilidade que trazem, facilitando as trocas de interfaces monitoradas. Porém o único teste que utilizando as duas maquinas simultaneamente foi o último.

A principal coleta/monitoramento foi feita no EVC do *Backbone2*, porque por este EVC passavam necessariamente todas as informações da MEN. Outras capturas foram feitas em pontos distintos da MEN, tais como no *EDGE4* e *EDGE5* onde estavam ligados os equipamentos de *Home Network*, podendo assim observar a qualidade no usuário.

Foram coletados os pacotes das transmissões dos testes enumerados na tabela 4.1. Após a coleta, as informações de ocupação da banda, total de pacotes enviados, perdas, atrasos foram analizadas. Todas as informações puderam ser observadas com sucesso através dessas ferramentas.

Para que esses dados fossem coletados, um computador foi ligado à penúltima interface do *Backbone2*.

A ferramenta WireShark também foi de grande utilidade para identificação de erros na estrutura, caso uma transmissão não estivesse chegando a um determinado ponto. Com os dados coletados por essa ferramenta conseguiu-se diagnosticar erros de transmissão, tais como endereços IP de destino errados e transmissões enviadas para redes erradas.

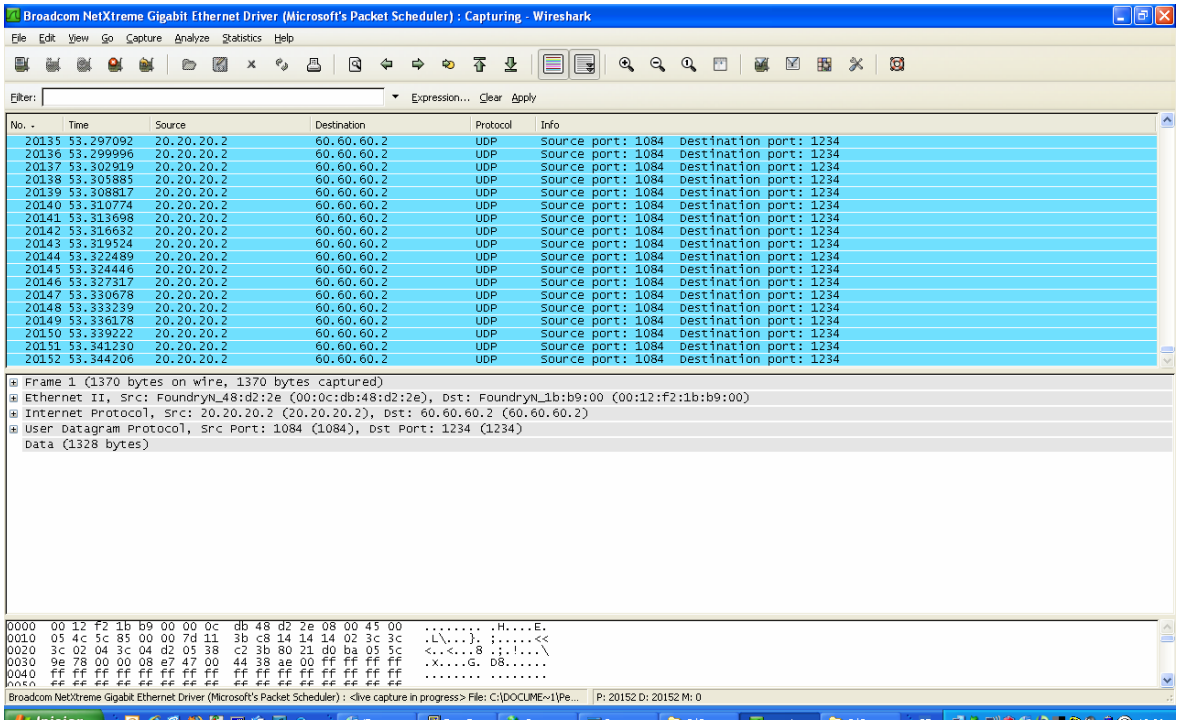


Figura 4.6 Coleta do tráfego da transmissão de VoD.

A figura 4.6 mostra os dados coletados de uma transmissão de VoD com o uso da ferramenta WireShark. Pode ser observado que o endereço IP de origem da transmissão é o 20.20.20.2 e o endereço de destino é 60.60.60.2.

Após a captura dos pacotes, com o auxílio da ferramenta TraceBuster versão 1.0.0 do fabricante Touchstone Technologies analisou-se os dados coletados.

Além de gerar os gráficos de ocupação da banda de transmissão o TraceBuster calcula a perda de pacotes e jitter. Nas suas estatísticas ocorre uma segmentação das informações de transporte de vídeo, voz e dados.

A figura 4.7 mostra a ocupação da banda e o número de pacotes durante a transmissão de VoD em alta definição. Neste gráfico ocorria apenas uma única requisição de VoD sendo enviada. Para esta transmissão a taxa média de ocupação da banda foi de 8.5 Mb/s com picos de transmissão de 9.6 Mb/s. A média de pacotes transmitidos foi de 800 pacotes por segundo, em determinados momentos alcançou-se 936 pacotes por segundo.

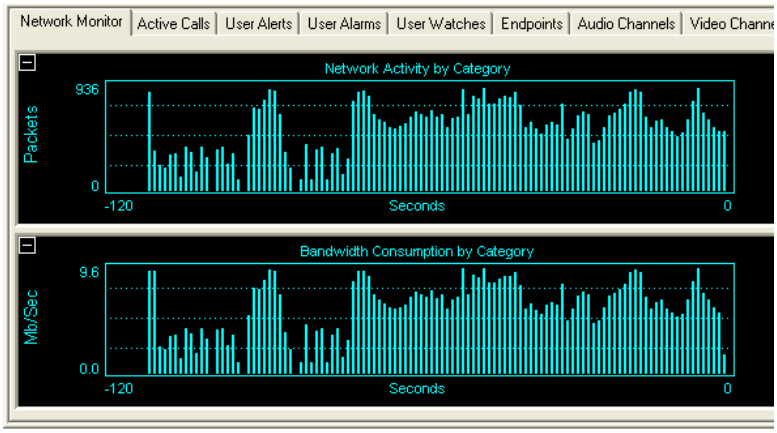


Figura 4.7 Gráfico da ocupação da banda de transmissão.

Cada pacote capturado neste segmento tinha um tamanho médio de 1356 Bytes.Durante a transmissão dos dados que compõem o gráfico acima não existia a priorização por QoS.

Esse gráfico apresenta exclusivamente a real taxa de ocupação do sinal gerado de VoD, por isso considerou-se que o sinal de VoD gerado em alta definição no ambiente criado ocupa uma taxa média de 8.5 Mbps. Este transmissão de VoD serve de parâmetro para todas as outras transmissões enviadas, sejam elas sem QoS, com QoS, transmissões de duas requisições de VoD ou VoD com dados.

Protocol	Packets	Bytes
IP	54,032	73,267,392
ICMP	0	0
UDP	54,032	72,186,752
TCP	0	0

Figura 4.8 Total de pacotes e total de Bytes recebido.

Os dados da figura 4.8 mostram o total de pacotes recebidos durante a mesma transmissão da figura 4.7

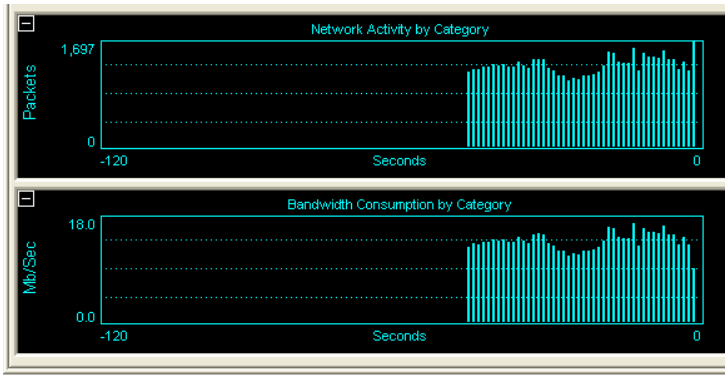


Figura 4.9 Duas transmissões simultâneas de VoD.

O gráfico da figura 4.9 mostra uma ocupação média de 17 Mbps na saída do Core IP da rede de IPTV durante a requisição de VoD.

De todos os tráfegos gerados os mais importantes foram os da transmissão simultânea de três requisições de VoD com prioridade garantida por Qualidade de Serviço. Isto porque esses tráfegos foram os que mais exigiram processamento dos equipamentos, por se assemelharem mais ao modelo que seria usado em uma transmissão de um provedor de acesso, por ter o maior número de funcionalidades agregadas.

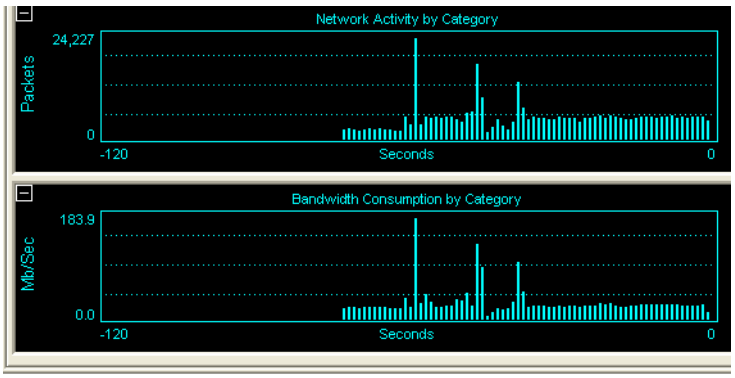
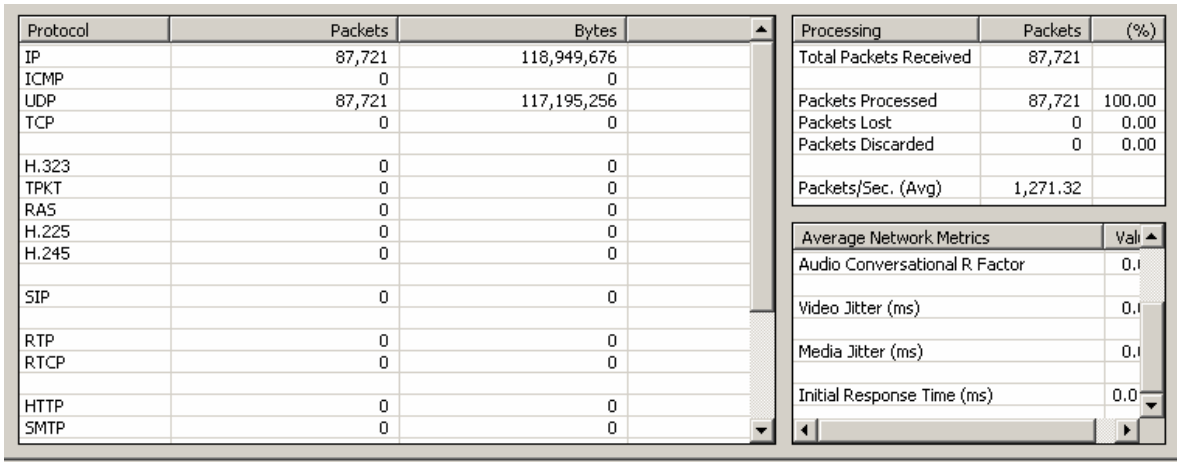


Figura 4.10 Três transmissões simultâneas de VoD e dados com QoS.

A figura 4.10 mostra a ocupação da banda e o número de pacotes durante a transmissão de VoD em alta definição. Neste gráfico ocorria apenas uma única requisição de VoD sendo enviada.

Durante a transmissão dessas informações ocorriam picos próximos de 200 Mbps e picos de transmissão que chegavam a 24.227 pacotes por segundo. Durante o período de coleta foram transmitidos 332.778 pacotes que totalizaram 261.709.957 Bytes.



Protocol	Packets	Bytes
IP	87,721	118,949,676
ICMP	0	0
UDP	87,721	117,195,256
TCP	0	0
H.323	0	0
TPKT	0	0
RAS	0	0
H.225	0	0
H.245	0	0
SIP	0	0
RTP	0	0
RTCP	0	0
HTTP	0	0
SMTP	0	0

Processing	Packets	(%)
Total Packets Received	87,721	
Packets Processed	87,721	100.00
Packets Lost	0	0.00
Packets Discarded	0	0.00
Packets/Sec. (Avg)	1,271.32	

Average Network Metrics	Val
Audio Conversational R Factor	0.
Video Jitter (ms)	0.
Media Jitter (ms)	0.
Initial Response Time (ms)	0.0

Figura 4.11 Calculo do Jitter para três transmissões simultâneas de VoD e dados com QoS.

Nesta figura 4.11 são apresentadas as estatísticas da transmissão de três sinais simultâneos de VoD concorrendo no mesmo EVC pelo o envio de dados convencionais. Nesta transmissão ocorria priorização de ambos os tráfegos por QoS.

Durante um minuto transmitiu-se um total de 87.721 pacotes e um total de 118.949.676 Bytes. Em momento algum nas transmissões de VoD concorrendo com dados ocorreu perda de pacotes.

A transmissão representada na figura 4.11 tem as mesmas características de IPTV da figura 4.10, porém na primeira buscou-se avaliar o Jitter, perda de pacotes e pacotes descartados.

Como pode ser observado na figura 4.11 não ocorreu a presença de jitter na rede em nenhum momento durante a transmissão, inclusive as casas decimais do cálculo de jitter também apresentam valor zero.

Essa informação é de grande importância, pois os pacotes perdidos, descartados e o Jitter estão diretamente associados à perda de qualidade na transmissão.

As informações de Jitter, perda de pacotes e pacotes descartados foram geradas em tempo real pela ferramenta WinEyeQ. O armazenamento dessas informações só pode ser feito com a versão paga do *software* usado.

Durante esse teste o computador responsável pela coleta das informações chegou muito próximo de sua capacidade máxima de processamento. Chegou-se a ocupar 95% dos recursos de CPU e acesso a disco. Caso fossem acrescentadas mais requisições de VoD o computador coletor não seria mais capaz de processar todas as informações recebidas.

As coletas dos pacotes não podiam superar mais de 3 minutos, pois o fluxo de informação capturado era tão grande que o computador não processava. Por isso as capturas giravam em torno de 2 minutos.

Após as coletas, o tempo de processamento das informações por este computador chegou a cinco minutos.

O último ponto analisado durante essa última transmissão era a qualidade para os usuários finais que estavam no *Home Network*. Nesses também não deveriam ocorrer erros enquanto estivessem recebendo as suas requisições de VoD.

Protocol	Packets	Bytes
IP	54,115	73,379,940
ICMP	0	0
UDP	54,115	72,297,640
TCP	0	0

Figura 4.12 Total de pacotes e total de Bytes recebidos.

Processing	Packets	(%)
Total Packets Received	54,115	
Packets Processed	54,115	100.00
Packets Lost	0	0.00
Packets Discarded	0	0.00
Packets/Sec. (Avg)	1,136.95	

Average Network Metrics	Val
Audio Conversational R Factor	0.(
Video Jitter (ms)	0.(
Media Jitter (ms)	0.(
Initial Response Time (ms)	0.0

Figura 4.13 Cálculo do Jitter durante recebimento das transmissões no usuário final.

Para que fosse feita uma análise global de toda a transmissão, realizou-se uma coleta simultânea no equipamento do Core IP (apresentada nas figuras 4.10 e 4.11) e no *Home Network* para os usuários finais, durante a transmissão de três VoD, com dados e QoS.

Essa abordagem mostra a qualidade da transmissão nos pontos mais importantes do trajeto até a entrega do vídeo ao usuário final.

Os dados apresentados na figura 4.13 mostram as informações referentes à recepção das requisições de VoD de dois usuários finais. As casas decimais do cálculo de jitter também apresentam valor zero.

Durante o período de coleta de informações foram recebidos pelos dois usuários um total de 54.115 pacotes que juntos trafegaram 73.379.940 Bytes de informações. Como pode ser verificado pela figura 4.13 neste ponto também não ocorreu a presença de jitter e perdas de pacotes.

Após a análise dos dados coletados, gráficos gerados, estatísticas verificou-se que todos os parâmetros estabelecidos pelo MEF de qualidade foram atendidos tanto para os usuários finais como para os equipamentos do Core IP, mesmo quando as transmissões foram realizadas com vídeos em alta definição.

4.4) Dificuldades e evoluções do projeto.

Os recursos implementados no laboratório, citado neste trabalho, quer sejam da Metro-Ethernet, da transmissão de IPTV ou do acesso remoto por SSH, são resultados de processos evolutivos. Inicialmente, essas três estruturas não tinham essas características apresentadas no presente capítulo. Antes de se chegar ao resultado final deste projeto várias etapas de problemas tiveram que ser superadas. A seguir são apresentadas as principais dificuldades:

4.4.1) Evolução do Acesso Externo

Inicialmente tinha-se um acesso, realizava-se as requisições através de um computador que ficava diretamente conectado a um equipamento por um cabo de console. Esta abordagem apresentou muitos pontos de falhas e sem segurança.

Apenas um equipamento sendo acessado por SSH os demais eram acessados por TELNET a partir do acesso por SSH. Essa opção não muito prática e dificultava quando era necessário interagir com vários equipamentos simultaneamente.

E na ultima evolução todos os equipamentos sendo acessados simultaneamente. Para que isso pudesse ocorrer foram agregados a estrutura de um roteador ADSL, NAT, rota, endereço IP da rede de acesso remoto, switch concentrador.

4.4.2) Evolução Metro-Ethernet

Na primeira topologia do laboratório existia apenas um equipamento central e dois equipamentos de borda; com esta opção não seria formado um EVC no backbone central de forma que todo o processamento interno seria internamente dificultando a análise das informações transmitidas.

A seguir foi utilizada a topologia com dois equipamentos centrais e dois de borda. Nesta opção já foi possível construir um EVC entre os equipamentos centrais para formar um E-Line. Esta opção já era boa, porém poderia ser melhorada.

No final da topologia foram usados dois equipamentos centrais e três de borda. Com a utilização desta topologia pode-se aproximar ao modelo real que poderia ser usado na transmissão de IPTV por redes Metro, com pontos bem definidos de segmentação de IPTV e Metro tais como Headend, CoreIP, Homenetwork.

4.4.3) Rotas estáticas X OSPF

Os primeiros laboratórios da Metro-Ethernet foram feitos com rotas estáticas. Mesmo esse modelo funcionando corretamente sofreu uma evolução para se aproximar ao modelo que bem pode ser usado pelas operadoras de telecomunicação.

A evolução consiste na utilização de rotas dinâmicas, sendo usado o protocolo de roteamento OSPF.

Anteriormente quando trabalhava-se apenas com os equipamentos em camada 2, para que as informações fossem transportadas entre os nós da rede, usava-se dentro de cada VLAN uma porta tagged que era usada como ponte entre VLANs.

Quando o OSPF foi inserido nos roteadores criou-se uma nova dificuldade de passar várias informações pelo mesmo EVC, pois a interface que era usada para a saída para as áreas OSPF não suportava agir como tagged, não podendo então ser usada diretamente pela VLANs como saída para o domínio OSPF.

Para que as informações pudessem passar todas pelo mesmo EVC foram agregadas às VLANs estruturas de interfaces virtuais de roteamento. Estas passaram a realizar as funções de roteamento, direcionando o fluxo de informações de saída das VLANs para as interfaces de OSPF.

4.4.4) Evolução do sinal IPTV

A primeira opção usada para simular a transmissão do sinal de IPTV foi o Gerador de tráfego IPERF, com ele é possível gerar um fluxo de informações com as características do IPTV, porém, mesmo sendo um sinal simulado ainda existia uma diferença entre uma transmissão real. Por isso, decidiu-se melhorar a características dos sinais transmitidos.

Existem softwares específicos de simulação de IPTV na grande maioria desenvolvidos por empresas Européias. Realizaram-se vários contatos com estas empresas para solicitar versões de teste, porém todos os contatos foram infrutíferos.

A última opção foi VideoLAN pelas vantagens apresentadas neste estudo.

CAPÍTULO 5 – Conclusões e Projetos

5.1) Conclusão

Este estudo buscou unir duas novas tendências que vêm crescendo no mercado mundial: a transmissão de televisão sobre o protocolo IP e a rede Metro Ethernet Network. Esta última seria o meio usado para a transmissão de IPTV.

Para o desenvolvimento desse projeto foi necessário estudar novos conceitos de diversas áreas aqui abarcadas, principalmente redes em geral, o IPTV e, especificamente, as redes Metro Ethernet. Foi necessário um grande trabalho de pesquisa de material nessas áreas.

Com esse projeto foi possível verificar bem de perto os processos e as estruturas que estão por trás da transmissão de televisão em uma MEN, podendo identificar o seu comportamento, a sua influência com a inserção deste sinal e ao final indicar o que é mais viável para essa estrutura.

Pesquisar novas tecnologias não é uma tarefa fácil. Exige uma grande dedicação e esforço. Existe a dificuldade de encontrar material referente ao assunto, os documentos são em sua grande maioria em língua estrangeira, o que acabou atrasando um pouco o desenvolvimento do trabalho. Mas todo o esforço vale à pena quando vemos que o conhecimento adquirido começa a mostrar seus frutos.

No segundo capítulo deste trabalho, foram mostrados todos os recursos que são de extrema relevância para o potencial de crescimento do mercado, os componentes mais importantes de cada estrutura, as topologias que cada um deve ter e as formas de proteção que garantem a qualidade do serviço.

Todas as tecnologias estudadas e implementadas eram muito novas e, como no mercado de tecnologia tudo que é novo é muito caro, algumas partes desse projeto tiveram que ser simuladas, outras, substituídas por soluções mais baratas. Mas as restrições foram superadas e vencidas de forma satisfatória sem que estas influenciassem no resultado final do trabalho.

Ao iniciar o estudo não se tinha a idéia de como seria o comportamento da transmissão de IPTV, se a rede era compatível, se a capacidade de processamento dos equipamentos suportaria o IPTV, se a banda disponível

suportaria a taxa de ocupação da transmissão. À medida que o estudo foi se aprofundando, essas respostas foram aparecendo de forma gradual.

Através da estrutura montada, mesmo sendo real ou simulada, consegue-se demonstrar toda a divisão do processo, seja pelos componentes da MEN (*Backbone*, *Edge*, EVCs, etc) ou para os de Transmissão de IPTV (*Headend*, Access Network, Core, *Home Network*).

Além disso, a transmissão de IPTV requer que sejam observados vários parâmetros de QoS, principalmente os que garantem a prioridade através de toda a estrutura de distribuição, feita nos switches e roteadores, fundamentalmente.

Ao final, foi possível observar que a viabilidade não se resume apenas no fato de a Metro Ethernet ter capacidade de transmitir o IPTV. Existem outros fatores agregados a essa realidade que devem ser considerados, tais como: os custos de se montar uma estrutura tão grandiosa, o risco, sob ponto de vista empresarial, no que se refere ao retorno do capital investido, o uso da rede metálica já existente. Por isso, no primeiro momento, é mais viável a utilização de estruturas já montadas.

Porém, quando os custos da montagem da estrutura já tiverem sido superados (compra de equipamento, distribuição de fibra óptica nos pontos de recepção), ou seja, uma rede metro que já está em produção, ao final desse estudo acredita-se que atualmente não haja recurso melhor para transmissão de IPTV do que as redes Metro Ethernet.

5.2) Projetos Futuros

Algumas das sugestões aqui descritas podem ter caráter apenas acadêmico pela sua concepção original, outras têm um grande potencial e podem vir a se tornar bons projetos comercias.

Como as tecnologias envolvidas nesse projeto são muito novas, existem várias idéias que podem servir como propostas para projetos futuros:

- O uso de enlaces de rádio para comunicações entre equipamentos de última milha da rede de distribuição, quando não existir a opção da fibra. Verificar como pode ser feita essa comunicação e quais são os melhores recursos a serem utilizados.

- A melhoria no tempo de Zapping de canais, desenvolvendo recursos (*software* ou *hardware*) que minimizem o tempo necessário para a

troca de canais. De uma forma geral, reduzir o tempo necessário para que os equipamentos troquem de canal.

- Melhorias na comunicação entre o *Set Top Box* Wireless, roteadores ADSL, e a televisão, fazendo com que os dois equipamentos trabalhem de uma forma integrada e sem fio.

- O desenvolvimento de um aplicativo gratuito, em um *software* de simulação de IPTV, que possa simular os dois tipos de transmissão de IPTV (LiveTV e VoD) ao mesmo tempo, com recursos do total de usuários conectados, largura de banda ocupada, estatísticas de perdas de pacotes, Jitter e que também simule o *Set Top Box* fazendo a troca de canais.

- O desenvolvimento de um *software* (com interface web) de gerência para redes Metro Ethernet para monitoramento específico para transmissões de IPTV.

- A proposição de um estudo sobre direitos autorais, onde novas ferramentas poderão ser agregadas às soluções já existentes.

- A transmissão de IPTV para dispositivos portáteis (como IPod Touch), no desenvolvimento de uma ferramenta que os tornem aptos a receber transmissões de televisão por IP. Vale lembrar que esse IPod já vem com wireless integrado, o que facilita o desenvolvimento. Essa é uma boa oportunidade de desenvolver um *software* com o ponto de vista comercial.

- Comparação da qualidade da imagem transmitida em relação à codificação do sinal pelos formatos MPG1, MPG2, MPG4, H264. Neste estudo pode ser determinado o melhor custo benefício entre os vários formatos para a transmissão de IPTV.

Em continuidade a este trabalho, passado o estudo da viabilidade e já comprovada a capacidade de transmissão de IPTV pela Metro Ethernet Network, poderá ser feito um estudo bem aprofundado e longo, onde poderão ser estudadas as perdas gradativas da qualidade do sinal em relação à distância da fibra até o ponto de entrega ao usuário em transmissões de IPTV em alta qualidade e junto desse teste, cálculos de perdas na qualidade de transmissão em virtude de fibras saturadas com um número alto de transmissões simultâneas de IPTV sejam elas VoD ou LiveTV.

REFERÊNCIAS BIBLIOGRÁFICAS

DUQUE Luciano Henrique; IPTV: Avaliação de Arquiteturas em Redes de Banda Larga – 2007

FERGUSON, Paul; **HUSTON** Geoff. Quality of Service, Delivering on the Internet and in Corporete Networks – Editora Wiley Computer Publishing, 1998.

HARTE, Lawrence; IPTV basics technology, operation and services – Althos Publishing; Fuquay – Varina 2007.

JOSEPH Weber; IPTV Crash Course ,MacGraw - Hill, June 2006.

METRO ETHERNET FORUM, MEF 1, “Ethernet Services Model, Phase 1” Novembro 2003.

METRO ETHERNET FORUM, MEF 10, “Ethernet Services Attributes, Phase 1.” Novembro 2004.

METRO ETHERNET FORUM, MEF 10.1 "Ethernet Services Attributes Phase 2" Novembro 2006

METRO ETHERNET FORUM, MEF 11 “User Network Interface (UNI) Requirements and Framework” Novembro 2004

METRO ETHERNET FORUM, MEF 2, “Requirements and Framework for Ethernet Service Protection in Metro Ethernet Networks”, Fevereiro 2004.

METRO ETHERNET FORUM, MEF 3, “Circuit Emulation Service Definitions, Framework and Requirements in Metro Ethernet Networks” Abril 2004.

METRO ETHERNET FORUM, MEF 4, “MEN Architecture Framework – Part 1: Generic Framework.” May 2004.

METRO ETHERNET FORUM, MEF 5, “Traffic Management Specification: Phase I” Maio 2004

METRO ETHERNET FORUM, MEF 6, “Ethernet Services Definition, Phase 1.” Junho 2004.

MOY, John T.; OSPF Anatomy of a Internet Routing Protocol – Editora Addison Wesley; Indianápolis 1998

ODON, Wendell; Cisco CCNA; Cisco Press; Janeiro de 2003

ODON, Wendell; GEIER, Jim ; MEHTA, Narem. CCIE Rounting and Switching; Cisco Press, Indianapolis fevereiro de 2006.

OLMAR, Rolf; Testing iptv delivery from the head-end to the home

RALPH Santitoro; Metro Ethernet Services – A Technical Overview – 2006

SOARES, Luiz; **LEMOS** Guido; **COLCHER** Sérgio. Redes de Computadores – Elsevier Editora - 1995

STEVENS, Comer; Interligação com Redes TCP/IP – Editora Campus – 2006

TANENBAUM Andrew S. Redes de Computadores – Editora Campus

TORRES, Gabriel; Redes de Computadores: Curso Completo – Editora Axcel Books – 2001.

WHALLEY, Mark; **MOHAN**, Dinesh. Metro Ethernet Networks – A technical Overview

ZUCCHI Wager L.; Revista RTI – Aranda Editora – Ano VII, n° 78 – Novembro de 2006

Suplemento Especial **IPTV**, Correio Braziliense quarta-feira 10 de outubro

Sites citados

http://www.infonetics.com

www.clubedohardware.com.br

www.youtube.com

www.foundrynet.com

www.wireshark.org

www.touchstone-inc.com

Sites consultados

www.foundrynet.com acessado em 19 de março de 2007

www.clubedohardware.com.br acessado em 15 de abril de 2007

www.cisco.com.br acessado em 19 de março de 2007

http://www.metroethernetforum.org acessado em 20 de março de 2007

http://en.wikipedia.org/wiki/Metro_Ethernet acessado em 21 de março de 2007

http://www.gta.ufrj.br/grad/04_2/metro/metro.html acessado em 02 de abril de 2007

http://www.infonetics.com/resources/purple.shtml?ms06.vid.1.nr.shtml acessado em 03 de abril de 2007

http://www.folha.com.br acessado em 26 de fevereiro de 2007

http://www.books24x7.com acessado em 17 de março de 2007

http://metroethernetforum.org/PDF_Documents/metro-ethernet-services.pdf acessado em 8 de setembro de 2007

http://www.vivaolinux.com.br/artigos/impressora.php?codigo=227 acessado em 14 de maio de 2007

http://metroethernetforum.org/_root/members/bostonmeeting/updates/archref-mod-mef_f103001.pdf acessado em 18 de maio de 2007

http://www.ietf.org/Internet-drafts/draft-balus-l2vpn-vpls-802.1ah-01.txt acessado em 28 de junho de 2007

http://www.teleco.com.br/tutoriais/tutorialiptv/pagina_1.asp acessado em 27 de setembro de 2007

www.teleco.com.br acessado em 22 de novembro de 2007

Palestras

MOLINARI, Marcelo; Uso de Metro-Ethernet - Mostra de Soluções em Tecnologia da Informação e Comunicações Aplicadas ao Setor Público, 29 de março de 2007.

DUQUE, Luciano; IPTV:uma plataforma com garantias de QoE – IV Semana Da Engenharia - 6 de novembro de 2007

APÊNDICE - Programações

As informações entre # # são comentários que não fazem parte da programação dos equipamentos.

Programação Backbone1

```
SSH@Backbone1>
SSH@Backbone1>sh ru
Current configuration:
!
ver V3.3.0dT163
module 3 ni-xmr-20-port-1g-100fx
!
mirror ethernet 3/1      # Portas espelhadas para monitoração #
mirror ethernet 3/3      # Portas espelhadas para monitoração #
!
!
no spanning-tree
!
vlan 10 name Acesso-Remoto       # Criação da VLAN de acesso remoto #
 untagged ethe 3/20      # Portas adicionadas a VLAN#
 router-interface ve 10     # Criação da interface virtual #
!
vlan 1 name DEFAULT-VLAN  # VLAN padrão existente em todos os
equipamentos #
!
!
aaa authentication web-server default local      #  Parâmetros para o acesso
remoto #
aaa authentication enable default local     #  Parâmetros para o acesso remoto #
aaa authentication login default local        #  Parâmetros para o acesso remoto #
username andre password .....                  #  Parâmetros para o acesso remoto #
ip route 0.0.0.0/0 192.168.1.1 #  Rota de saída padrão para o SSH #
!
```

```
!
!
!
!
ip dns domain-name iptv.com.br     #  nome do domínio dos equipamentos #
hostname Backbone1  #  nome do equipamento #
!
router ospf     #  criação do domínio OSPF #
 area 0    #  criação do domínio OSPF #
 area 1    #  criação do domínio OSPF #
 redistribution connected
!
router pim
!
!
!
interface loopback 1 #  loopback de saída para o domínio OSPF #
 ip ospf area 0
 ip address 10.0.0.10/24
!
interface management 1
 enable
!
interface ethernet 3/1          #  interface de saída para o domínio OSPF #
 port-name EVC_backbone2
 enable
 ip ospf area 0
 ip address 10.0.0.1/24
 ip pim-sparse
!
interface ethernet 3/3  #  interface de saída para o domínio OSPF #
 port-name EVC_EDGE3
 enable
 ip ospf area 1
 ip address 10.1.1.2/24
 ip pim-sparse
```

```
!
interface ethernet 3/4
 enable
 rstp admin-edge-port
!
interface ethernet 3/5
 enable
 rstp admin-edge-port
!
interface ethernet 3/6
 enable
 rstp admin-edge-port
!
interface ethernet 3/7
 enable
 rstp admin-edge-port
!
interface ethernet 3/8
 enable
 rstp admin-edge-port
!
interface ethernet 3/9
 enable
 rstp admin-edge-port
!
interface ethernet 3/10
 enable
 rstp admin-edge-port
!
interface ethernet 3/11
 enable
 rstp admin-edge-port
!
interface ethernet 3/12
 enable
 rstp admin-edge-port
```

```
!
interface ethernet 3/13
 enable
 rstp admin-edge-port
!
interface ethernet 3/14
 enable
 rstp admin-edge-port
!
interface ethernet 3/15
 enable
 rstp admin-edge-port
!
interface ethernet 3/16
 enable
 rstp admin-edge-port
!
interface ethernet 3/17
 enable
 rstp admin-edge-port
!
interface ethernet 3/18
 enable
 rstp admin-edge-port
!
interface ethernet 3/19
 enable
 rstp admin-edge-port
 mon ethernet 3/1 both
!
interface ethernet 3/20
 port-name Ligacao-Concentrador
 enable
!
interface ve 10  #  saída da interface virtual #
 ip address 192.168.1.101/24
```

```
!
!
router pim
 rp-address 10.1.1.3
!
!
!
!
ip ssh  port 2001     #  porta de saída de SSH #
!
!
end

SSH@Backbone1>
```

Programação Backbone2

```
SSH@Backbone2>sh ru
!Building configuration...
!Current configuration : 3161 bytes
!
ver 09.4.00T53
!
module 1 bi-jc-8-port-gig-m4-management-module
module 2 bi-jc-16-port-gig-copper-module
!
global-protocol-vlan
!
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 10 name Acesso_remoto by port    # Criação da VLAN de acesso remoto #
 untagged ethe 2/16
 router-interface ve 10
!
!
```

```
aaa authentication web-server default local     #  Parâmetros para o acesso
remoto #
aaa authentication enable default local      #  Parâmetros para o acesso remoto #
aaa authentication login default local     #  Parâmetros para o acesso remoto #
hostname Backbone2       #  Nome do equipamento #
ip dns domain-name iptv.com.br
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
mirror ethernet 2/15    #  Porta de espelhamento #
!
username andre password .....
route-only
!
router ospf #  criação do domínio OSPF #
 area 0
 area 2
 area 3
 redistribution connected
!
router pim
 rp-address 10.1.1.3 0
!
interface loopback 1     #  Loopback de saída para o domínio OSPF #
 ip ospf area 0
 ip address 10.0.0.20/24
!
interface ethernet 1/1    #  Porta de saída para o domínio OSPF #
 port-name ECV-Backbone1
 enable
 ip address 10.0.0.2 255.255.255.0
 ip pim-sparse
 ip ospf area 0
 mon ethe 2/15 input
 mon ethe 2/15 output
!
```

```
interface ethernet 2/1     #  Porta de saída para o domínio OSPF #
 port-name EVC-EDGE 5
 enable
 ip address 10.2.2.13 255.255.255.0
 ip pim-sparse
 ip ospf area 2
!
interface ethernet 2/2    #  Porta de saída para o domínio OSPF #
 port-name EVC-EDGE 4
 enable
 ip address 10.3.3.12 255.255.255.0
 ip pim-sparse
 ip ospf area 3
!
interface ethernet 2/3
 enable
rstp admin-edge-port
!
interface ethernet 2/4
 enable
rstp admin-edge-port
!
interface ethernet 2/5
 enable
rstp admin-edge-port
!
interface ethernet 2/6
 enable
rstp admin-edge-port
!
interface ethernet 2/7
 enable
rstp admin-edge-port
!
interface ethernet 2/8
 enable
```

```
rstp admin-edge-port
!
interface ethernet 2/9
 enable
rstp admin-edge-port
!
interface ethernet 2/10
 enable
rstp admin-edge-port
!
interface ethernet 2/11
 enable
rstp admin-edge-port
!
interface ethernet 2/12
 enable
rstp admin-edge-port
!
interface ethernet 2/13
 enable
rstp admin-edge-port
!
interface ethernet 2/14
 enable
rstp admin-edge-port
!
interface ethernet 2/15
 enable
rstp admin-edge-port
!
interface ethernet 2/16
 port-name Acesso-Concentrador
 enable
rstp admin-edge-port
!
interface ve 10
```

```
 ip address 192.168.1.102 255.255.255.0
!
!
!
!
!
! # Criação da chave criptográfica #
crypto key generate rsa public_key "1024 33
118339734377256649706001030003397824238929589876392833392807409781915970716630678622260468731581673187599409050890601603694221443666744287190359123093665767190342422269660437662517006641668009309862038893666074815169472615406833350456376810047057541686300219908713217999521704884264912002486566823392321821217
Backbone2@iptv.com.br"
!
crypto key generate rsa private_key "**********"

!
ip ssh port 2002
!
end

SSH@Backbone2>
```

Programação EDGE 3

```
SSH@EDGE3>sh ru
Current configuration:
!
ver 03.2.00aT3e3
!
!
!
!
vlan 1 name DEFAULT-VLAN by port
!
```

```
vlan 10 name Acesso-Remoto by port  # Criação da VLAN de acesso remoto #
 untagged ethe 48
 router-interface ve 10
!
vlan 20 name IPTV by port  # Criação da VLAN de IPTV #
 untagged ethe 2 to 10
 router-interface ve 20
!
vlan 30 name DADOS by port  # Criação da VLAN de DADOS #
 untagged ethe 11 to 20
 router-interface ve 30
!
!
!
!
!
qos mechanism mixed-sp-wrr
!
aaa authentication web-server default local   #  Parâmetros para o acesso remoto
#
aaa authentication enable default local   #  Parâmetros para o acesso remoto #
aaa authentication login default local   #  Parâmetros para o acesso remoto #
enable telnet authentication   #  Parâmetros para o acesso remoto #
hostname EDGE3   #  Nome do equipamento #
ip dns domain-name iptv.com.br   #  Nome do domínio #
ip route 0.0.0.0 0.0.0.0 192.168.1.1   #  Rota de saída para o acesso SSH #
!
username andre password .....    #  Criação do usuário para o acesso remoto #
router ospf     #  criação do domínio OSPF #
 area 1
 redistribution connected
!
router pim
 rp-address 10.1.1.3 0
!
interface loopback 1 #  Porta de saída padrão para o OSPF #
```

```
 ip ospf area 1
 ip address 10.1.1.11/24
!
interface ethernet 1 #  Porta de saída padrão para o OSPF #

 port-name EVC_Backbone1 #  Porta de saída padrão para o OSPF #

 ip address 10.1.1.3 255.255.255.0
 ip pim-sparse
 ip ospf area 1
!
interface ethernet 3 #  Portas com flags de prioridade QoS #

 priority 7
!
interface ethernet 4 #  Portas com flags de prioridade QoS #
 priority 7
!
interface ethernet 5 #  Portas com flags de prioridade QoS #
 priority 7
!
interface ethernet 18 #  Portas com flags de prioridade QoS #
 priority 2
!
interface ethernet 48
 port-name Acesso-Concentrador
!
interface ve 10     #  Endereços de saída para as interfaces virtuais #
 ip address 192.168.1.103 255.255.255.0
!
interface ve 20 #  Endereços de saída para as interfaces virtuais #
 ip address 20.20.20.1 255.255.255.0
 ip pim-sparse
!
interface ve 30 #  Endereços de saída para as interfaces virtuais #
 ip address 30.30.30.1 255.255.255.0
```

```
!
!
router pim
 bsr-candidate e 1 30 255
 rp-candidate e 1
!
!
!
!
!
ip ssh  port 2003
!
!
end

SSH@EDGE3>
```

Programação EDGE 4

```
SSH@EDGE4>sh ru
Current configuration:
!
ver 03.2.00aT3e3
!
!
!
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 10 name Acesso-Remoto by port
 untagged ethe 24
 router-interface ve 10
!
vlan 20 name IPTV by port
 untagged ethe 3 to 10
 router-interface ve 20
```

```
!
vlan 30 name DADOS by port
 untagged ethe 11 to 20
 router-interface ve 30
!
!
!
!
!
!
aaa authentication web-server default local #  Parâmetros para o acesso remoto #
aaa authentication enable default local #  Parâmetros para o acesso remoto #
aaa authentication login default local #  Parâmetros para o acesso remoto #
!
hostname EDGE4
ip dns domain-name iptv.com.br
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
username andre password .....
router ospf
 area 3
 redistribution connected
!
router pim
 rp-address 10.1.1.3 0
!
interface loopback 1 #  Porta de saída padrão para o OSPF #
 ip ospf area 2
 ip address 10.2.2.22/24
!
interface ethernet 1 #  Porta de saída padrão para o OSPF #
 ip address 10.3.3.13 255.255.255.0
 ip pim-sparse
 ip ospf area 3
!
interface ve 10  #  Endereços de saída para as interfaces virtuais #
```

```
 ip address 192.168.1.104 255.255.255.0
 ip pim-sparse
!
interface ve 20 #  Endereços de saída para as interfaces virtuais #
 ip address 40.40.40.1 255.255.255.0
 ip pim-sparse
!
interface ve 30
 ip address 50.50.50.1 255.255.255.0 #  Endereços de saída para as interfaces
virtuais #
!
!
!
!
!
!
!
ip ssh  port 2004 #  Porta para SSH para acesso remoto #
!
!
end

SSH@EDGE4>
```

Programação EDGE 5

```
SSH@EDGE5>sh ru
Current configuration:
!
ver 04.0.00T3e3
!
module 1 fi-sx4-24-port-gig-copper-module
module 9 fi-sx4-12-combo-port-management-module
!
!
!
```

```
vlan 1 name DEFAULT-VLAN by port
!
vlan 10 name Acesso-Remoto by port # Criação da VLAN de Acesso Remoto #
 untagged ethe 9/12
 router-interface ve 10
!
vlan 20 name IPTV by port # Criação da VLAN de IPTV #
 untagged ethe 9/2 to 9/6
 router-interface ve 20
!
vlan 30 name DADOS by port # Criação da VLAN de DADOS #
 untagged ethe 9/7 to 9/11
 router-interface ve 30
!
!
!
!
!
!
aaa authentication web-server default local
aaa authentication enable default local
aaa authentication login default local
enable telnet authentication
hostname EDGE5
ip dns domain-name iptv.com.br
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
username andre password .....
router ospf
 area 2
 redistribution connected
!
interface loopback 1 #  Porta de saída padrão para o OSPF #
 ip ospf area 0
 ip address 10.3.3.33/24
!
```

```
interface ethernet 9/1 #  Porta de saída padrão para o OSPF #
 port-name EVC_Backbone2
 ip address 10.2.2.14 255.255.255.0
 ip ospf area 2
!
interface ethernet 9/3
 port-name Home-network
!
interface ethernet 9/12
 port-name Acesso-Concentrador
!
interface ve 10
 ip address 192.168.1.105 255.255.255.0
!
interface ve 20
 ip address 60.60.60.1 255.255.255.0
!
interface ve 30
 ip address 70.70.70.1 255.255.255.0
!
!
!
!
!
!
!
ip ssh  port 2005
!
!
end

SSH@EDGE5>
```