

OUTROS TRABALHOS EM:
www.projetoderedes.com.br



UNIVERSIDADE
ESTADUAL DE LONDRINA

MARCELO HENRIQUE ALVES

ENGENHARIA DE TRÁFEGO METRO ETHERNET

**LONDRINA - PARANÁ
2008**



UNIVERSIDADE
ESTADUAL DE LONDRINA

MARCELO HENRIQUE ALVES

ENGENHARIA DE TRÁFEGO METRO ETHERNET

Monografia apresentada ao Curso de Especialização em Redes de Computadores e Comunicação de Dados, Departamento de Computação da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Especialista, sob orientação do Prof. Dr. Juergen Rochol.

LONDRINA - PARANÁ
2008

Alves, Marcelo Henrique

Engenharia de Tráfego – Redes Metro Ethernet / Alves, Marcelo Henrique. Londrina: UEL / Universidade Estadual de Londrina, 2008.

Orientador: Juergen Rochol.

Dissertação (Especialização) – UEL / Universidade Estadual de Londrina, 2008.

Referências bibliográficas: f. 01-51

1. Engenharia de Tráfego. 2. VLAN. 3. WAN - Monografia. I. Juergen Rochol. II. Universidade Estadual de Londrina Especialização em Redes de Computadores e Comunicação de Dados, III. Engenharia de Tráfego – Redes Metro Ethernet.

MARCELO HENRIQUE ALVES

ENGENHARIA DE TRÁFEGO METRO ETHERNET

Esta monografia foi julgada adequada para obtenção do título de Especialista, e aprovada em sua forma final pela Coordenação do Curso de Especialização em Redes de Computadores e Comunicação de Dados, do Departamento de Computação da Universidade Estadual de Londrina.

Banca Examinadora:

Prof. Dr. Juergen Rochol - Orientador
Universidade Federal do Rio Grande do Sul

Prof. Dr. Mario Lemes Proença Jr.
Universidade Estadual de Londrina

Prof. Msc. Fabio Sakuray
Universidade Estadual de Londrina

Londrina, 30 Agosto de 2008.

DEDICATÓRIA

Dedico este trabalho de conclusão de curso à meus amáveis e eternos pais , que, no decorrer da minha vida, proporcionaram-me, além de extenso carinho e amor, os conhecimentos da integridade, da perseverança e de procurar sempre em Deus à força maior para o meu desenvolvimento como ser humano.

Por essa razão, gostaria de dedicar e reconhecer à vocês, minha imensa gratidão e sempre amor.

AGRADECIMENTOS

Agradeço minha esposa pela paciência e colaboração nos momentos difíceis, pela minha ausência quando necessário nos períodos de estudo.

A Deus, quando algumas vezes, sentindo-me desacreditado e perdido nos meus objetivos me deu forças para a conclusão deste curso.

Aos meus professores que por diversas vezes entenderam minhas dificuldades, e com sabedoria souberam transmitir seus conhecimentos.

Agradeço também à Universidade Estadual de Londrina por permitir que eu me qualificasse para juntos trabalharmos por uma Universidade cada vez mais competente.

RESUMO

Cada vez mais o mercado tem buscado por soluções de rede que garantam qualidade de serviço, propiciando interconexão entre as redes corporativas geograficamente distribuídas e também com a internet, e que tenham um baixo custo. As redes Metro Ethernet tem se mostrado uma escolha óbvia, por propiciar simples administração, baixo custo, fácil interconexão e boa granularidade de banda. Novos protocolos têm sido propostos de maneira a atribuir a estas redes qualidade de serviço, segurança e robustez, de modo a se aproximar das características das redes de circuito tradicionais, mantendo as vantagens de uma rede de pacotes.

Palavras-chave: Metro Ethernet. Engenharia de Tráfego. VLAN.

ABSTRACT

Each time more the market has searched for net solutions that guarantee quality of service, propitiating interconnection also enters the corporative nets geographically distributed and with the Internet, and that they have a low cost. The nets Ethernet Meter if have shown an obvious choice, for propitiating simple administration, low cost, easy interconnection and good granularidade of band. New protocols have been considered in way to attribute to these nets quality of service, security and robustness, in order to come close itself to the characteristics of the traditional nets of circuit, keeping the advantages of a net of packages.

Key-words: Metro Ethernet. Traffic Engineering. VLAN.

LISTA DE ILUSTRAÇÕES

| | |
|---|----|
| Figura 1 - Rede Metro Ethernet..... | 14 |
| Figura 2 - 802.3 Ethernet em relação ao modelo OSI..... | 18 |
| Figura 3 - Padrões IEEE 802.x..... | 19 |
| Figura 4 - Tecnologias Ethernet mapeadas no modelo OSI..... | 20 |
| Figura 5 - Formato do quadro Ethernet..... | 21 |
| Figura 6 - VLAN Trunk..... | 23 |
| Figura 7 - VLAN Stacking..... | 24 |
| Figura 8 - Modelo básico de referência..... | 27 |
| Figura 9 - Topologia típica de Metro Ethernet..... | 29 |
| Figura 10 - Arquitetura Metro Ethernet ponto-a-ponto e multiponto-multiponto..... | 31 |
| Figura 11 - Tipo de serviço E-Line..... | 31 |
| Figura 12 - Tipo de serviço E-Lan..... | 32 |
| Figura 13 - Atributos de Bandwidth Profile..... | 34 |
| Figura 14 - Marcação dos quadros de serviço através de cores..... | 35 |
| Figura 15 - Metro Ethernet - topologia básica..... | 39 |
| Figura 16 - Rede Metro com Firewall..... | 41 |
| Figura 17 - Gerência da Rede Metro - Visualização completa dos elementos..... | 43 |
| Figura 18 - Gerência da Rede Metro - Criação de VLANS..... | 44 |
| Figura 19 - Gerência da Rede Metro – Criação de VLANS..... | 44 |
| Figura 20 - Gerência da Rede Metro – Tráfego em interfaces..... | 45 |
| Figura 21 - Gerência da Rede Metro – Tráfego em equipamentos..... | 45 |
| Figura 22 - Gerência da Rede Metro - Administração de operadores..... | 46 |
| Figura 23 - Visualização instantânea dos protocolos que trafegam na rede..... | 47 |
| Figura 24 - Aplicação de regras para tráfegos prejudiciais à rede..... | 48 |
| Figura 25 - Conexões HTTP..... | 49 |
| Figura 26 - Requisições HTTP..... | 49 |
| Figura 27 - Uso da CPU do Cache..... | 49 |

LISTA DE TABELAS

| | |
|---|----|
| Tabela 1 - Exemplo de SLA baseado em COS..... | 36 |
|---|----|

LISTA DE ABREVIATURAS E SIGLAS

ARP - Address Resolution Protocol
ATM - Asynchronous Transfer Mode
CBR - Constant Bit Rate
CBS - Committed Burst Size
CE - Customer-Edge
CE-VLAN - Customer-Edge VLAN
CIR - Committed Information Rate
CoS - Class of Service
CSMA/CD - Carrier Sense Multiple Access/Collision Detection
DIX - DEC, Intel, Xerox
DoS - Denial of Service
DWDM - Dense Wavelength Division Multiplexing
EBS - Excess Burst Size
EGP - External Gateway Protocol
EIR - Excess Information Rate
EVC - Ethernet Virtual Connection
FDDI - Fiber Distributed Data Interface
ICMP - Internet Control Message Protocol
IDF - Intermediate Distribution Frame
IEEE - Institute of Electrical and Electronics Engineers
IGMP - Internet Group Management Protocol
IP - Internet Protocol
IPX - Internetwork Packet Exchange
EoMPLS - Ethernet over Multi Protocol Label Switching
HTTP - HyperText Transfer Protocol
L2TP - Layer 2 Transport Protocol
LAN - Local Area Networks
LDAP - Lightweight Directory Access Protocol
LLC - Logical Link Control
MAC - Media Access Control
MAN - Metropolitan Area Networks

MDF - Master Distribution Frame
MEF - Metro Ethernet Forum
MEN - Metro Ethernet Network
MPLS - Multi Protocol Label Switching
MSPP - Multi-Service Provisioning Platform
NIC - Network Interface Card
ODBC - Open Data Base Connectivity
OSI - International Standards Organization
P2P - Peer-to-Peer
PC - Personal Computer
PHB - Per-Hop Behaviors
PPPoE - Point-to-Point Protocol over Ethernet
QoS - Quality of service
RSVP - ReSerVation Protocol
SDH - Synchronous Digital Hierarchy
SFD - Start Frame Delimiter
SLA - Service Level Agreement
SNMP - Simple Network Management Protocol
SONET - Synchronous Optical Network
TCP - Transmission Control Protocol
TDM - Time Domain Multiplexing
TOS - Type Of Service
UNI - User Network Interface
UNI-C - User Network Interface Client
UNI-N - User Network Interface Network
VC - Virtual Channel
VLAN - Virtual Local Area Networks
VPLS – Virtual Private LAN Service
WAN - Wide Area Networks

SUMÁRIO

| | | |
|-------|--|----|
| 1 | INTRODUÇÃO | 14 |
| 2 | ETHERNET..... | 16 |
| 2.1 | Conceitos Básicos..... | 16 |
| 2.2 | Componentes de uma Ethernet | 18 |
| 2.3 | Quadro Ethernet..... | 20 |
| 2.4 | Endereçamento | 21 |
| 3 | VLAN | 22 |
| 3.1 | Conceitos | 22 |
| 3.3 | VLAN Trunk | 23 |
| 3.3 | VLAN Stacking | 24 |
| 4 | REDES METRO ETHERNET | 26 |
| 4.1 | Descrição de redes Metro Ethernet..... | 26 |
| 4.2 | Arquitetura de Redes Metro Ethernet..... | 26 |
| 4.3 | Topologias de redes Metro Ethernet..... | 27 |
| 5 | SERVIÇOS METRO ETHERNET | 30 |
| 5.1 | Serviços | 30 |
| 5.2 | Interoperabilidade..... | 33 |
| 5.3 | Parâmetros de Tráfego..... | 33 |
| 5.4 | Identificadores de Classes de Serviços (CoS) | 35 |
| 5.5 | Desafios das Redes Metro Ethernet..... | 36 |
| 6 | EQUIPAMENTOS EMPREGADOS EM REDES METRO ETHERNET | 38 |
| 6.1 | Equipamentos para transporte de dados | 38 |
| 6.1.1 | Core da Rede | 39 |
| 6.1.2 | Switch de Agregação | 39 |
| 6.1.3 | Switch de Acesso..... | 40 |
| 6.2 | Equipamentos para segurança e gerência | 40 |
| 6.2.1 | Segurança - Firewall..... | 40 |
| 6.2.2 | Segurança – IDP (Intrusion Detection and Prevention) | 41 |

| | | |
|-------|---|----|
| 6.2.3 | Gerência..... | 42 |
| 6.3 | EQUIPAMENTOS PARA OTIMIZAÇÃO DA REDE..... | 46 |
| 6.3.1 | Disciplinador de Tráfego | 46 |
| 6.3.2 | Cache de Conteúdo HTTP | 48 |
| 7 | CONCLUSÃO | 50 |
| 8 | REFERÊNCIAS | 51 |

1 INTRODUÇÃO

Por muitos anos, o padrão Ethernet tem sido o protocolo dominante em redes LAN; hoje, mais de 98% do tráfego corporativo passa por interfaces Ethernet. Isto é motivado pela simplicidade, facilidade de operação, alto grau de integração e padronização do protocolo Ethernet, o que torna esta tecnologia extremamente atrativa em termos de custo. Por outro lado, o mesmo não acontece com as redes MAN e WAN, com as operadoras oferecendo serviços baseados em ATM, Frame Relay e linhas privativas, todos significativamente mais complicados e com custo mais elevado.

Atualmente, os mais importantes serviços demandados pela área corporativa e que mais tem crescido são a interconexão das redes LAN geograficamente distribuídas e a conectividade com a internet. Em face a estes serviços e à crescente exigência do mercado por baixos custos, as operadoras de serviços se deparam com a necessidade de readequar suas redes metropolitanas, sendo as redes Metro Ethernet uma escolha de destaque tanto pelo aspecto técnico quanto pelo econômico.

Uma Rede Metro Ethernet (MEN – Metropolitan Ethernet Network) é definida basicamente como uma rede que interconecta LANs corporativas geograficamente separadas, interconectando-se ainda a uma rede WAN ou backbone operados pelo provedor de serviços, conforme ilustrado na Figura 1.

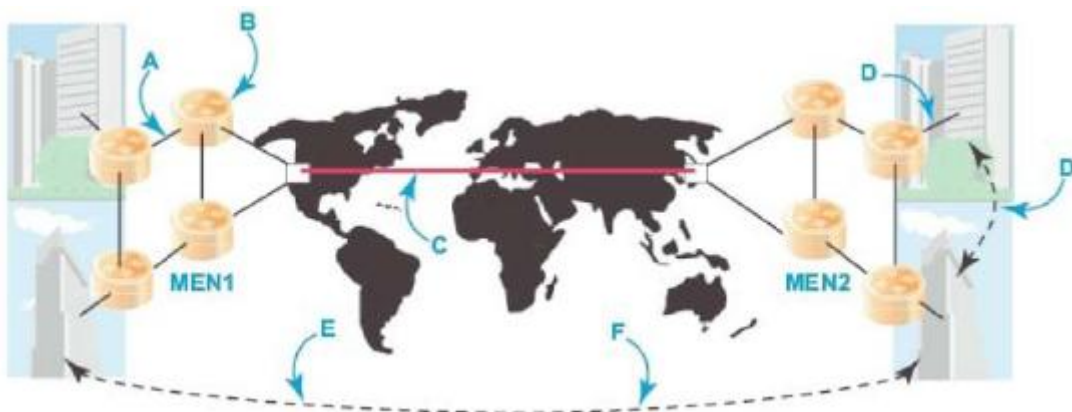


Figura 1 - Rede Metro Ethernet

As principais vantagens de uma rede Metro Ethernet são:

- Redução do custo operacional e de planejamento da rede, o qual é significativamente menor que para redes comutadas tradicionais.
- Equipamentos de menor custo; a economia de escala oriunda da base de equipamentos Ethernet instalada leva à redução do custo dos insumos, assim como à redução dos custos de desenvolvimento.
- Melhor granularidade e facilidade de aumento de banda, em comparação às redes de circuito comutado (E1/T1, E3/T3, SDH/SONET), permitindo, por exemplo, o aumento da banda do assinante de 1Mbps a 1Gbps, em passos de 1Mbps.
- Transmissão baseada em pacotes, o que permite um uso otimizado dos recursos da rede quando comparado com transmissão baseada em circuitos.
- Interoperabilidade com as redes LAN; permite a interconexão direta com as redes LAN, sem a necessidade de protocolos de adaptação, uma vez que praticamente a totalidade das redes LAN é baseada em Ethernet.

2 ETHERNET

2.1 Conceitos Básicos

A maior parte do tráfego na Internet origina-se e termina com conexões Ethernet. Desde seu início nos anos 70, a Ethernet evoluiu para acomodar o grande aumento na demanda de redes locais de alta velocidade. Quando foram produzidos novos meios físicos, como a fibra ótica, a Ethernet adaptou-se para aproveitar a largura de banda superior e a baixa taxa de erros que as fibras oferecem. Atualmente, o mesmo protocolo que transportava dados a 3 Mbps em 1973 está transportando dados a 10 Gbps.

Esse sucesso da Ethernet deve-se aos seguintes fatores:

- Simplicidade e facilidade de manutenção
- Capacidade de introdução de novas tecnologias
- Confiabilidade
- Instalação e atualização econômicas

Com a introdução da Gigabit Ethernet, aquilo que começou como uma tecnologia de redes locais, agora se estende a distâncias que fazem da Ethernet um padrão para MAN (Rede Metropolitana) e para WAN (Rede de longa distância). A idéia original para Ethernet surgiu de problemas de permitir que dois ou mais hosts usem o mesmo meio físico e de evitar que sinais interfiram um com o outro. Esse problema de acesso de vários usuários a um meio físico compartilhado foi estudado no início dos anos 70 na University of Hawaii. Foi desenvolvido um sistema denominado Alohanet para permitir o acesso estruturado de várias estações nas Ilhas do Havaí à banda compartilhada de radiofrequência na atmosfera. Esse trabalho veio a formar a base para o método de acesso Ethernet conhecido como CSMA/CD.

A primeira rede local do mundo foi a versão original da Ethernet. Robert Metcalfe e seus colegas na Xerox fizeram o seu projeto há mais de trinta anos. O primeiro padrão Ethernet foi publicado em 1980 por um consórcio entre a Digital Equipment Company, a Intel, e a Xerox (DIX). Metcalfe quis que a Ethernet fosse um padrão compartilhado que beneficiasse a todos e foi então lançada como padrão aberto. Os primeiros produtos desenvolvidos que usavam o padrão Ethernet foram vendidos durante o início dos anos 80. A Ethernet transmitia até 10 Mbps através de cabo coaxial grosso a uma distância de

até 2 quilômetros. Esse tipo de cabo coaxial era conhecido como thicknet e era da espessura de um pequeno dedo.

Em 1985, o comitê de padronização de Redes Locais e Metropolitanas do Institute of Electrical and Electronics Engineers (IEEE) publicou padrões para redes locais. Esses padrões começam com o número 802. O padrão para Ethernet é 802.3. O IEEE procurou assegurar que os padrões fossem compatíveis com o modelo da International Standards Organization (ISO)/OSI. Para fazer isso, o padrão IEEE 802.3 teria que satisfazer às necessidades da camada 1 e da parte inferior da camada 2 do modelo OSI. Como resultado, no 802.3, foram feitas algumas pequenas modificações em relação ao padrão Ethernet original.

As diferenças entre os dois padrões eram tão insignificantes que qualquer placa de rede Ethernet (NIC) poderia transmitir e receber quadros tanto Ethernet como 802.3. Essencialmente, Ethernet e IEEE 802.3 são padrões idênticos.

A largura de banda de 10 Mbps da Ethernet era mais do que o suficiente para os computadores pessoais lentos (PCs) dos anos 80. No princípio dos anos 90, os PCs tornaram-se mais rápidos, os tamanhos dos arquivos aumentaram e ocorreram gargalos no fluxo de dados. A principal causa era a baixa disponibilidade de largura de banda. Em 1995, o IEEE anunciou um padrão para 100 Mbps Ethernet. A esse, seguiram-se padrões para Ethernet de gigabit por segundo (Gbps, 1 bilhão de bits por segundo) em 1998 e 1999.

Todos esses padrões são essencialmente compatíveis com o padrão Ethernet original. Um quadro Ethernet podia sair de uma placa de rede Ethernet de cabo coaxial mais antiga de 10 Mbps instalada em um PC, ser colocado em um link de fibra Ethernet de 10 Gbps e ter seu destino em uma placa de rede de 100 Mbps. Contanto que o pacote permaneça em redes Ethernet, não será modificado. Por essa razão, a Ethernet é considerada bem escalável. A largura de banda da rede poderia ser aumentada muitas vezes sem modificar a tecnologia Ethernet subjacente.

O padrão Ethernet original tem sido atualizado várias vezes com a finalidade de acomodar novos meios físicos e taxas mais altas de transmissão. Essas atualizações proporcionam padrões para as tecnologias emergentes e mantêm compatibilidade entre as variações da Ethernet.

2.2 Componentes de uma Ethernet

A Ethernet opera em duas áreas do modelo OSI, a metade inferior da camada de enlace de dados, conhecida como subcamada MAC, e a camada física. (Figura 2)

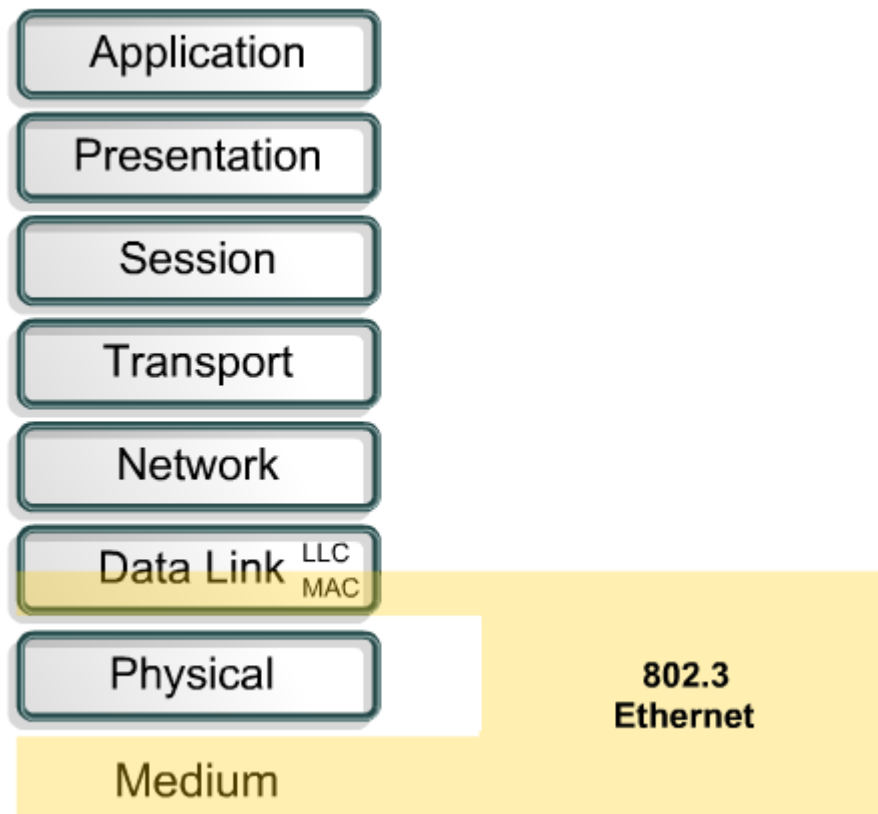


Figura 2 - 802.3 Ethernet em relação ao modelo OSI

Para mover dados entre uma estação Ethernet e outra, os dados freqüentemente passam através de um repetidor. As demais estações no mesmo domínio de colisão vêem o tráfego que passa através de um repetidor. Um domínio de colisão é, portanto, um recurso compartilhado. Quaisquer problemas originados em uma parte do domínio de colisão geralmente afetam o domínio de colisão inteiro.

Um repetidor é responsável pelo encaminhamento de todo o tráfego a todas as outras portas. O tráfego recebido por um repetidor jamais será enviado à porta de origem. Qualquer sinal detectado por um repetidor será encaminhado. Se o sinal for degradado pela atenuação ou pelo ruído, o repetidor tentará reconstruir e regenerar o sinal.

Os padrões garantem um mínimo de largura de banda e operacionalidade, ao

especificar o número máximo de estações, o comprimento máximo do segmento, o número máximo de repetidores entre estações, etc. As estações que são separadas por repetidores estão dentro do mesmo domínio de colisão. As estações separadas por bridges ou roteadores estão em domínios de colisão diferentes.

A Figura 3 mapeia uma variedade de tecnologias Ethernet para a metade inferior da camada 2 do modelo OSI e toda a camada 1. A camada 1 da Ethernet envolve as interfaces entre meios físicos, sinais, fluxo de bits que se propagam nos meios físicos, componentes que colocam sinais nos meios e várias topologias. A camada 1 da Ethernet realiza um papel importante na comunicação que ocorre entre dispositivos, mas cada uma de suas funções tem limitações. A camada 2 trata dessas limitações.

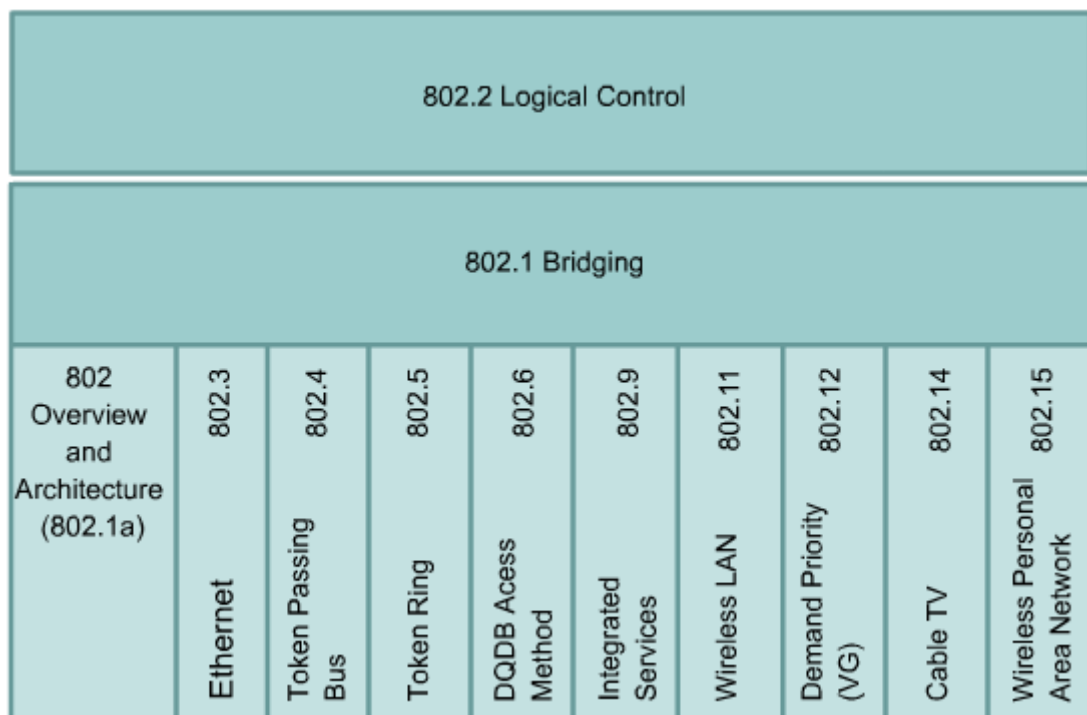


Figura 3 - Padrões IEEE 802.x

As subcamadas de enlace de dados contribuem significativamente para a compatibilidade da tecnologia e a comunicação entre computadores. A subcamada MAC trata dos componentes físicos que serão usados para comunicar as informações. A camada LLC (Logical Link Control) permanece relativamente independente do equipamento físico que será usado para o processo de comunicação.

A Figura 4 mapeia uma variedade de tecnologias Ethernet para a metade inferior da camada 2 e para toda a camada 1 do modelo OSI. Já que existem outras variedades

de Ethernet, aquelas exibidas aqui são as mais universalmente usadas.

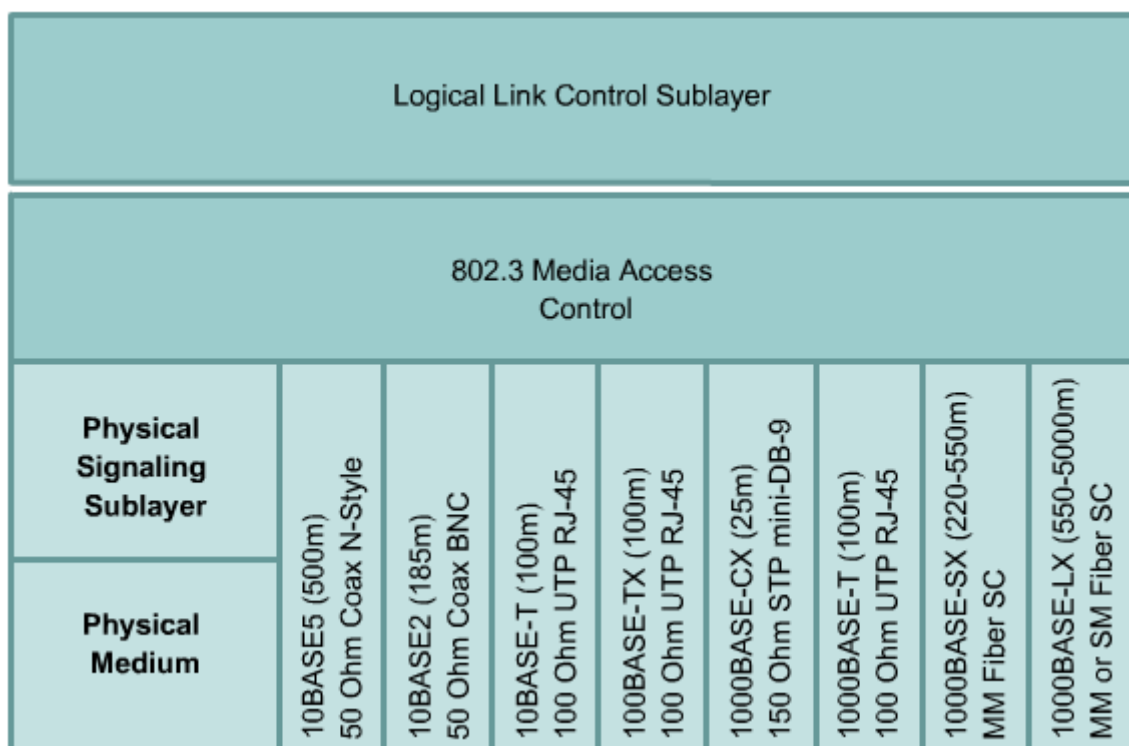


Figura 4 - Tecnologias Ethernet mapeadas no modelo OSI

2.3 Quadro Ethernet

Na camada de enlace de dados, a estrutura do quadro é quase idêntica para todas as velocidades da Ethernet, desde 10 Mbps até 10 Gbps. No entanto, na camada física, quase todas as versões de Ethernet são substancialmente diferentes umas das outras, com cada velocidade tendo um diferente conjunto de regras de projeto de arquitetura.

Na versão da Ethernet que foi desenvolvida por DIX antes da adoção da versão IEEE 802.3 da Ethernet, o Preâmbulo e o SFD (Start Frame Delimiter) foram combinados em um único campo, apesar do padrão binário ser idêntico. O campo denominado Comprimento/Tipo foi identificado apenas como Comprimento nas primeiras versões do IEEE e apenas como Tipo na versão DIX. Esses dois usos do campo foram oficialmente combinados em uma versão mais recente do IEEE, pois os dois usos do campo são comuns por toda a indústria.

O campo Tipo da Ethernet II está incorporado na definição de um quadro no padrão 802.3 atual (Figura 5). O nó receptor precisa determinar qual é o protocolo de camada superior que está presente em um quadro de entrada, examinando o campo

Comprimento/Tipo. Se o valor dos dois octetos é igual ou maior que 0x0600 (hexadecimal), 1536 em decimal, então o conteúdo do campo de dados (data field) do quadro é decodificado de acordo com o protocolo indicado. Ethernet II é o formato de quadro Ethernet utilizado em redes TCP/IP.

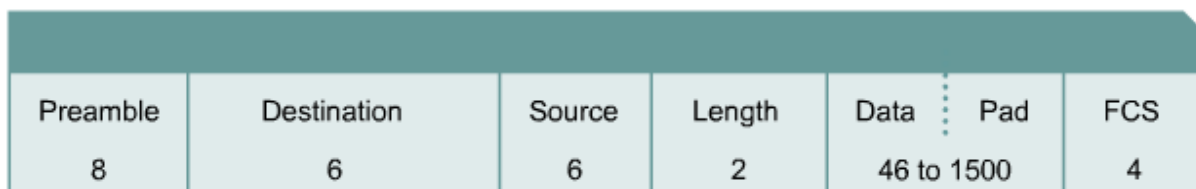


Figura 5 - Formato do Quadro Ethernet

2.4 Endereçamento

MAC refere-se aos protocolos que determinam qual dos computadores em um ambiente de meios físicos compartilhados, ou domínio de colisão, tem permissão para transmitir os dados. O MAC, com o LLC, compreende a versão IEEE da Camada 2 do OSI. O MAC e o LLC são subcamadas da Camada 2. Há duas abrangentes categorias de Controle de Acesso aos Meios, determinístico (revezamento) e não determinístico (primeiro a chegar, primeiro a usar).

Exemplos de protocolos determinísticos incluem Token Ring e FDDI. Em uma rede Token Ring, os hosts individuais são organizados em um anel e um token especial de dados circula ao redor do anel, chegando a cada host sequencialmente. Quando um host quer transmitir, ele captura o token, transmite os dados durante um tempo limitado e depois encaminha o token até o próximo host no anel. O Token Ring é um ambiente sem colisões pois apenas um host é capaz de transmitir em qualquer dado momento.

Os protocolos MAC não-determinísticos usam uma abordagem primeiro a chegar, primeiro a usar. O CSMA/CD (Carrier Sense Multiple Access / Collision Detection) é um sistema bem simples. A placa de rede observa se há ausência de sinal nos meios físicos e começa a transmitir. Se dois nós transmitirem simultaneamente, ocorrerá uma colisão e nenhum dos nós poderá transmitir.

3 VLAN

3.1 Conceitos

Uma VLAN é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local.

As VLANs facilitam a administração de grupos lógicos de estações e servidores de modo que possam comunicar como se estivessem no mesmo segmento físico de uma rede local. Elas também facilitam a administração de mudanças, acréscimos e modificações nos membros desses grupos.

As VLANs segmentam logicamente as redes comutadas com base nas funções profissionais, departamentos ou equipes de projetos, independentemente da localização física dos usuários ou das conexões físicas da rede. Todas as estações de trabalho e servidores utilizados por um grupo de trabalho em particular compartilham a mesma VLAN, independentemente da sua conexão ou localização física.

A configuração ou reconfiguração de VLANs é realizada através de software. Portanto, a configuração de uma VLAN não requer o deslocamento ou conexão física dos equipamentos da rede.

A comunicação de uma estação de trabalho em um grupo VLAN é restrita aos servidores de arquivo no mesmo grupo VLAN. As VLANs segmentam a rede logicamente em diferentes domínios de broadcast de modo que os pacotes sejam comutados somente entre portas designadas à mesma VLAN. As VLANs consistem em hosts ou equipamento de rede interconectados por um só domínio de bridging. O domínio de bridging é suportado em diferentes equipamentos de rede. Os switches de rede local operam protocolos de bridging com um grupo de bridging separado para cada VLAN.

As VLANs são criadas para proporcionarem serviços de segmentação tradicionalmente proporcionados por roteadores físicos nas configurações de rede local. As VLANs tratam das questões de escalabilidade, segurança e gerenciamento da rede. Os switches não processam tráfego com bridges entre VLANs, porque isso viola a integridade dos domínios de broadcast das VLANs. O tráfego deve ser roteado entre as VLANs.

3.3 VLAN Trunk

Na indústria telefônica, o conceito de trunking é associado com o caminho ou canal de comunicação telefônica entre dois pontos. Um desses dois pontos é normalmente a Central Telefônica (CO). Troncos compartilhados também podem ser criados para oferecer redundância entre COs.

O conceito utilizado pelas indústrias telefônica e de rádio foi, então, adotado para a comunicação de dados. Um exemplo disso em uma rede de comunicações é um link de backbone entre um MDF e um IDF. Um backbone é composto de vários troncos.

Atualmente, o mesmo princípio de trunking é aplicado a tecnologias de comutação em redes. O nível de tráfego em certas VLANs talvez não justifique um link dedicado. Para isso, o trunking agrega vários links virtuais em um só link físico. Isso permite que o tráfego de várias VLANs transite sobre um único cabo entre os switches. (Figura 6)

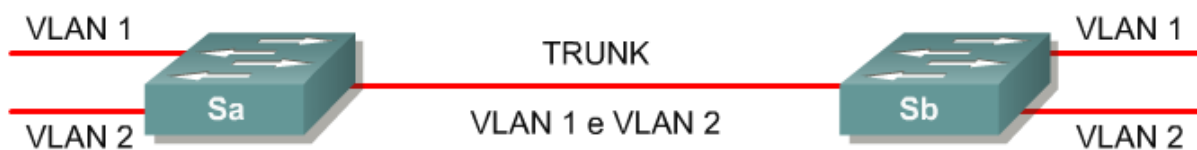


Figura 6 - VLAN Trunk

As tabelas de comutação em ambas as extremidades do tronco podem ser usadas para tomar decisões sobre encaminhamento baseado nos endereços MAC de destino dos quadros. À medida que vai aumentando o número de VLANs que transitam pelo tronco, as decisões de encaminhamento tornam-se mais lentas e mais difíceis de gerenciar. O processo de decisão torna-se mais lento porque as tabelas de comutação maiores demoram mais para serem processadas.

Os protocolos de trunking foram elaborados para gerenciar com mais eficácia a transferência de quadros de diferentes VLANs em uma única linha física. Os protocolos de trunking estabelecem um acordo para a distribuição de quadros para as portas associadas em ambas as extremidades do tronco.

Os dois tipos existentes de mecanismos de trunking são filtragem de quadros (frame filtering) e marcação de quadros (frame tagging). O frame tagging foi adotado como o mecanismo padrão de trunking pelo IEEE.

Os protocolos de trunking que utilizam frame tagging obtêm uma entrega

mais rápida de quadros e facilitam o gerenciamento.

O único link físico entre os dois switches consegue transportar tráfego para qualquer VLAN. Para conseguir isso, cada quadro enviado no link é marcado para identificar a VLAN à qual pertence. Existem diferentes esquemas de marcação.

3.3 VLAN Stacking

O VLAN stacking permite o encapsulamento de múltiplas VLANs utilizadas localmente sobre um único meio de rede..

O conceito de Stacking, em que os pacotes já marcados com um VLAN ID recebidos nas portas dos switches do operador não são verificados para conhecer a sua VLAN, mas são marcados com um segundo identificador, que será retirado quando o pacote for entregue ao equipamento do cliente, na localização de destino.

Ficamos assim com uma VLAN encapsulada dentro de outra, sendo que a VLAN cujo ID é adicionado na porta que faz Stacking é a Outer VLAN, ou VLAN exterior. A VLAN com a qual o pacote já estava marcado ao passar pela porta Stacking é a Inner VLAN ou VLAN interna (Figura 7). Esta idéia pode ser facilmente observada na Figura 6, onde é possível observar as portas Stacking, sendo que as portas restantes verificarão apenas a pertença (membership) dessa VLAN; nas extremidades da inner VLAN existirão as portas que farão tagging da VLAN interior.

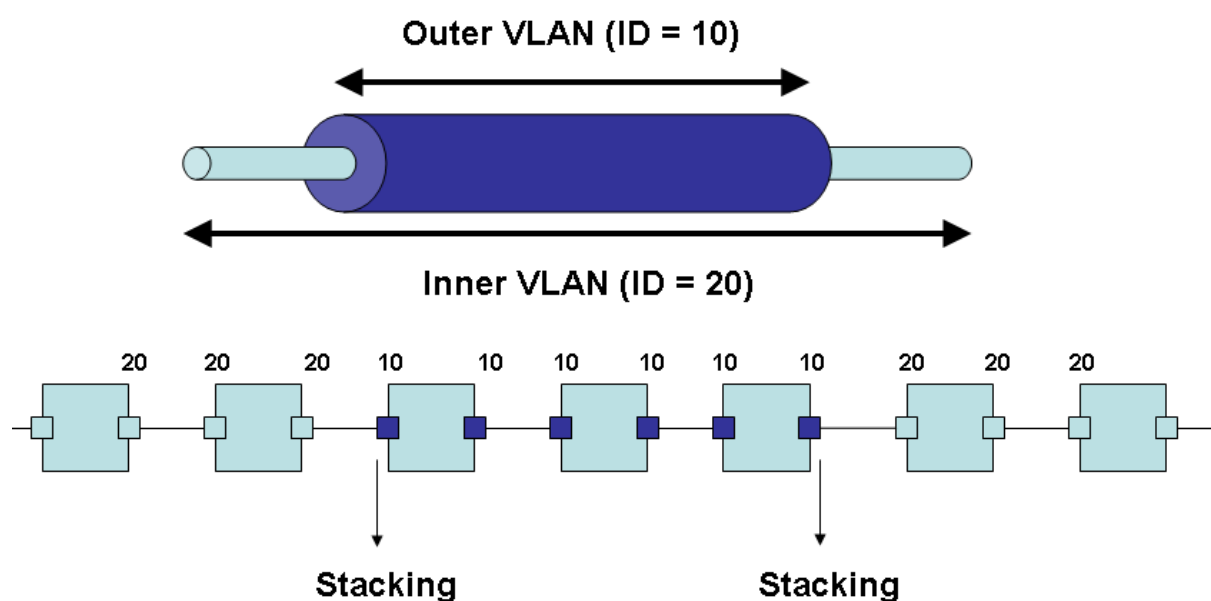


Figura 7 - VLAN Stacking.

Apenas as portas de entrada ou saída das Outer VLANs têm noção de que o pacote terá duas tags, os restantes consultarão apenas a primeira tag que encontrarem, desprezando se o pacote pertence ou não a Inner VLANs.

4 REDES METRO ETHERNET

4.1 Descrição de redes Metro Ethernet

Metro Ethernet é o conceito de utilizar redes Ethernet para áreas Metropolitanas e Geograficamente distribuídas.

Esse conceito surgiu pois, de acordo com projeções atuais, o tráfego de dados está superando o tráfego de voz nas redes Metropolitanas, portanto é mais interessante utilizar uma infraestrutura de transmissão de dados que uma estrutura de TDM (Time Domain Multiplexing).

E a Ethernet é a escolha lógica por causa do baixo custo, flexibilidade e facilidade de manutenção. Além de ser a tecnologia mais implementada e conhecida no transporte de dados.

Uma MEN (Metro Ethernet Network) é definida como uma rede que liga duas redes locais empresariais separadas geograficamente através de uma WAN, geralmente por fornecedores de serviços. As redes ethernet metropolitanas providenciam conectividade através da geografia metropolitana utilizando a Ethernet como protocolo nuclear e possibilitando aplicações de banda larga. Nas MAN (Metropolitan Area Networks), a Ethernet tem o potencial de aumentar economicamente a capacidade da rede e oferecer uma variada gama de serviços de uma forma escalável, simples e flexível. Uma rede metropolitana baseada em Ethernet é geralmente denominada por MEN. Nas redes empresariais, a Ethernet apresenta dois serviços que presentemente cativam mais atenção e que mais têm crescido: a ligação pública à Internet e interligação de redes locais de diferentes sítios da mesma empresa.

4.2 Arquitetura de Redes Metro Ethernet

O Metro Ethernet Fórum utiliza um modelo genérico para descrever os componentes internos e externos de uma rede Metro Ethernet. Esta estrutura descreve as interações entre a rede Metro através de interfaces bem definidas e seus pontos de referência. O modelo básico de referência de uma rede Metro Ethernet é mostrado na Figura 8.

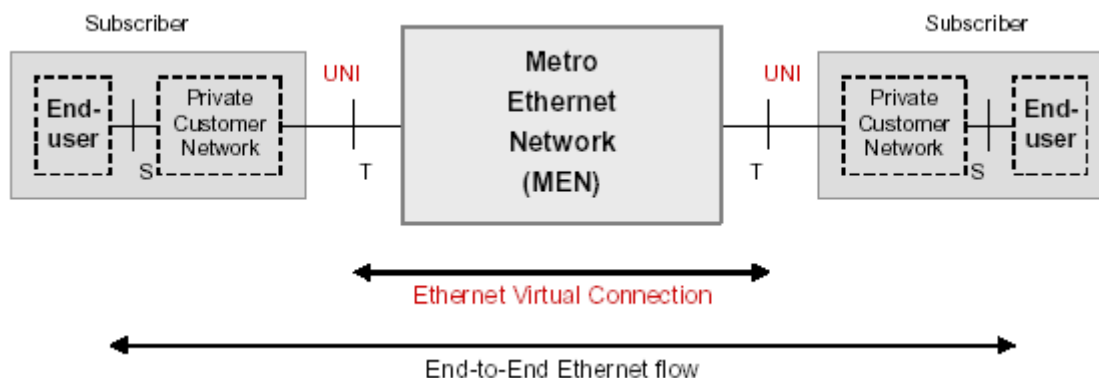


Figura 8 - Modelo básico de referência

O fluxo Ethernet (Ethernet flow) mostrado representa o tráfego de dados fim-a-fim entre dois equipamentos terminais, os quais originam e terminam os quadros Ethernet. A interface que interliga a rede de um cliente à rede de um provedor de serviços é denominada de UNI (User Network Interface). Do lado do cliente é chamada de UNI-C (User Network Interface Client) e do lado do provedor de serviços é denominada de UNI-N (User Network Interface Network).

4.3 Topologias de redes Metro Ethernet

Duas topologias principais são tipicamente contempladas em redes Metro Ethernet:

4.3.1 Anel

Segue a tradição das redes SDH implementadas nos anos de 1990, com base, principalmente, no racional dos modelos de tráfego da época (em que havia menor necessidade de conectividade entre sites locais e a maior parte do tráfego de acesso era direcionada para os POPs principais) e na redução dos custos associados com a rede de fibra óptica.

4.3.2 Mesh

Topologia hub & spoke, com conexão lógica entre todos os sites, é

atualmente a forma mais utilizada, embora implique altos custos devido à intensa utilização de fibra óptica. Quanto às arquiteturas, é possível vislumbrá-las sob duas formas principais:

4.3.2.1 Puras

Formadas estritamente por switches Ethernet (ou seja, usando uma referência do modelo OSI – Open System Interconnection para descrição lógica de redes, operando somente em nível 2-enlace). Interessante para redes pequenas, com reduzido número de clientes e sites.

4.3.2.2 Híbridas

Formadas por múltiplos domínios em nível 2-enlace (Ethernet puro) conectados por um núcleo nível 3-roteamento (IP/MPLS). Os quadros transportados de um domínio Ethernet para outro passam pelo núcleo, onde podem ser “tunelados” (envelopamento de informações visando otimizar controles na comunicação) via L2TP - Layer 2 Transport Protocol ou EoMPLS - Ethernet over Multi Protocol Label Switching. Para este último caso, o IETF – fórum de padronização de técnicas para o avanço das redes IP – está definindo uma especificação já conhecida no mercado como VPLS – Virtual Private LAN Service. A arquitetura híbrida é interessante para grandes redes Metro Ethernet.

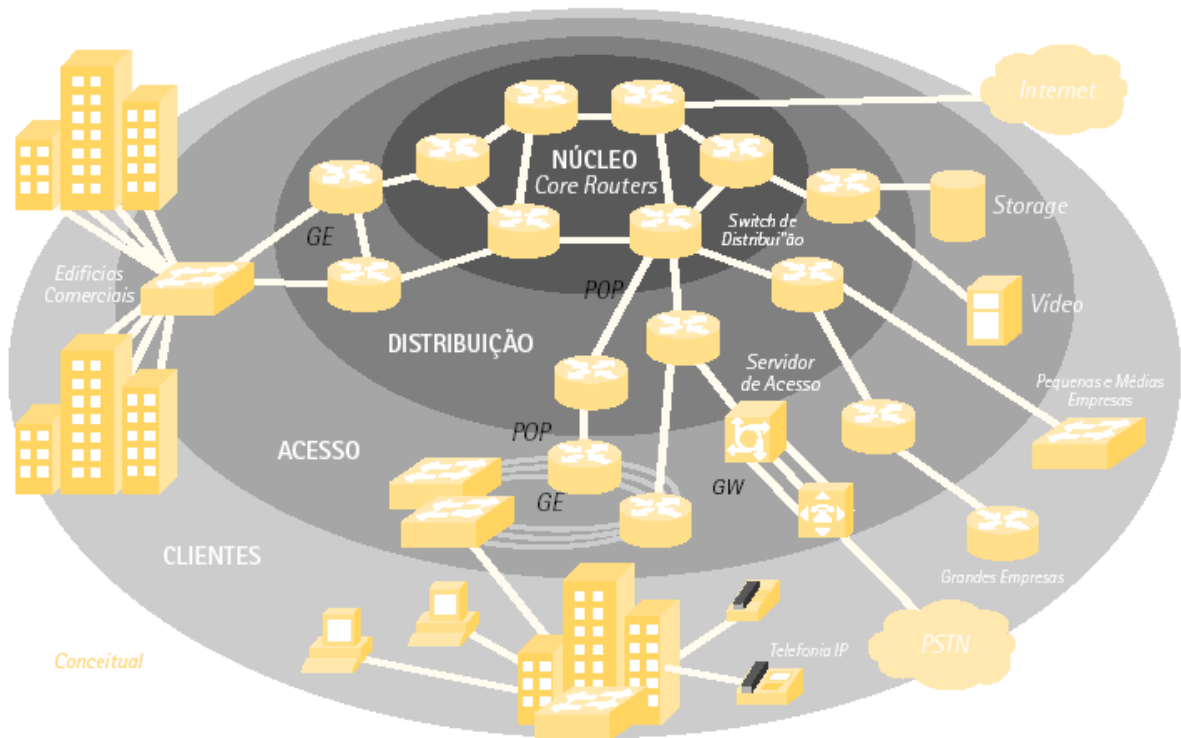


Figura 9 - Topologia típica de Metro Ethernet

5 SERVIÇOS METRO ETHERNET

5.1 Serviços

O serviço é assegurado pela operadora da MEN. O equipamento do cliente (CE) liga-se à rede através da interface de-rede (UNI), utilizando uma interface ethernet padrão. Os serviços são definidos da perspectiva do cliente final, e podem ser suportados sobre uma variedade de tecnologias e protocolos de transporte como SONET, DWDM, MPLS, etc. De qualquer forma, do lado do cliente a ligação no UNI é ethernet.

Um atributo chave de um serviço é a conexão virtual ethernet (EVC). Um EVC é definido como uma associação entre duas ou mais UNI, sendo UNI, como já referido, uma interface ethernet que demarca a fronteira entre o equipamento do cliente e a MEN do fornecedor de serviços. Uma EVC cumpre basicamente duas funções vitais: liga duas ou mais localizações do cliente, permitindo a troca de pacotes entre eles; e evita comunicações entre localizações que não façam parte da mesma EVC, o que possibilita a uma EVC providenciar segurança de dados e privacidade. A entrega de pacotes ethernet numa EVC é regida por duas regras básicas. Primeiro, um pacote de serviço nunca poderá ser entregue no mesmo UNI que a enviou, segundo, pacotes de serviços têm de ser entregues com os endereços ethernet e com o conteúdo inalterado. Isto contrasta com as redes encaminhadas típicas, onde os cabeçalhos ethernet são removidos e descartados. Com base nestas características, uma EVC pode ser usada para construir uma linha privada ou uma rede virtual privada de nível 2.

O MEF definiu dois tipos de EVCs, que suportarão os tipos de serviços correspondentes (Figura 10):

1. Ponto a Ponto
2. Multiponto a Multiponto

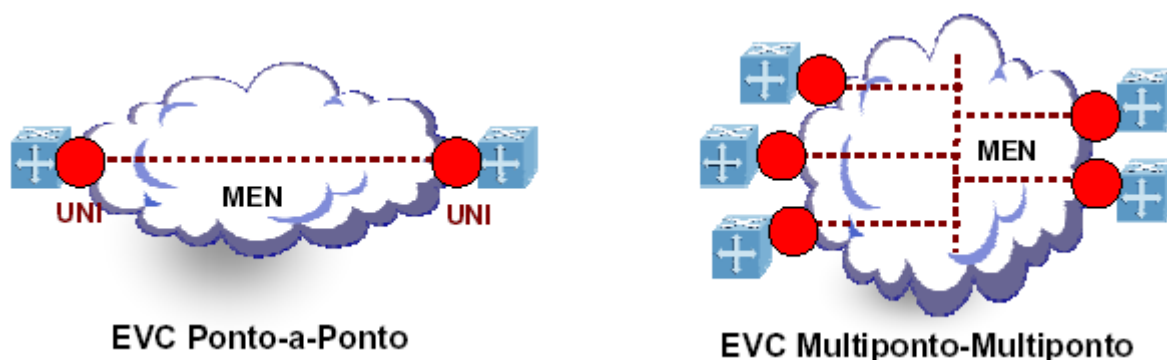


Figura 10 - Arquitetura Metro Ethernet ponto-a-ponto e multiponto-multiponto

De acordo com os tipos de EVCs existem também dois tipos de serviços, que são na realidade categorias, uma vez que serviços do mesmo tipo poderão ser bastante diferentes entre si dependendo dos atributos restantes que os caracterizam. Para definir completamente um serviço, um fornecedor terá que definir os UNIs e os atributos EVC associados ao serviço. Os dois tipos de serviço são a Ethernet Line e a Ethernet Lan.

O tipo de serviço Ethernet Line (E-Line) fornece uma ligação virtual ponto a ponto entre dois UNIs, tal como ilustrado na Figura 11.

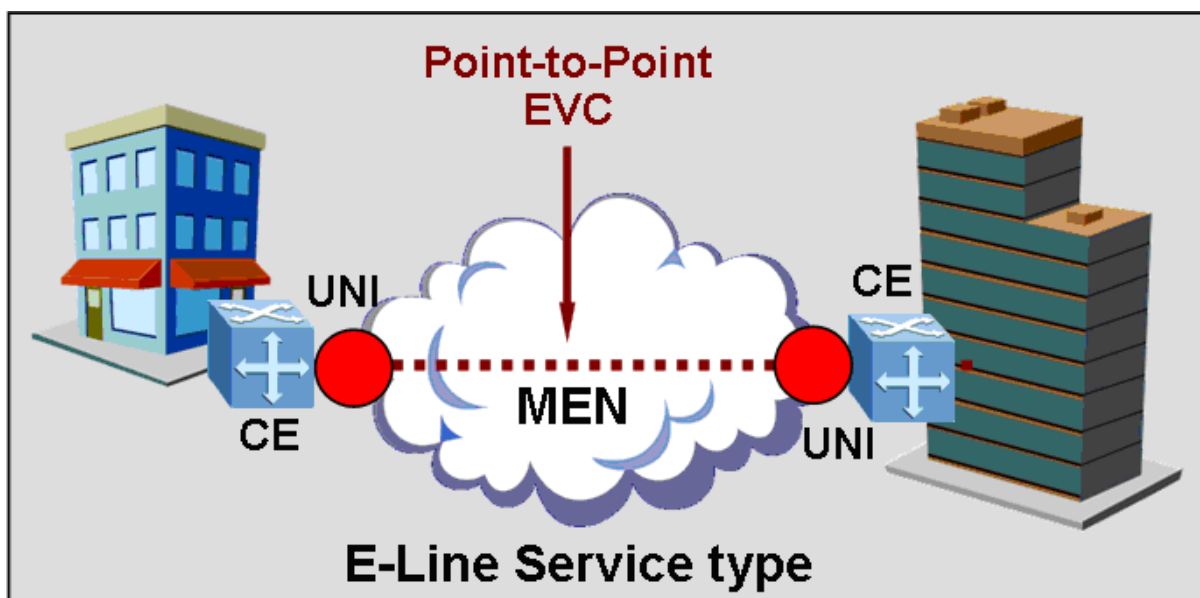


Figura 11 - Tipo de serviço E-Line

Na sua forma mais simples um serviço E-Line pode providenciar largura de banda simétrica para envio de dados em ambas as direções sem qualquer garantia de desempenho. Em formas mais sofisticadas, pode providenciar garantias de largura de banda, atraso de pacotes, taxas de envio de informação, etc. entre dois UNIs de diferentes

velocidades.

A multiplexação de serviços poderá também ser permitida num ou em ambos os UNIs de um serviço. Assim, por exemplo, mais de uma EVC ponto-a-ponto poderá ser fornecida no mesmo porto físico de um dos UNIs.

O tipo de serviço Ethernet LAN possibilita conectividade multiponto a multiponto e pode conectar dois ou mais UNIs, tal como ilustrado na Figura 12. Os dados enviados por um dos UNIs podem ser recebidos num ou mais dos restantes UNIs. Cada um dos UNIs das diferentes localizações de um cliente está ligado à mesma EVC multiponto, à qual serão também ligados novos UNIs que forem sendo adicionados, simplificando o fornecimento de serviços e sua ativação. Do ponto de vista de um cliente, um serviço E-LAN aparenta ser uma LAN.

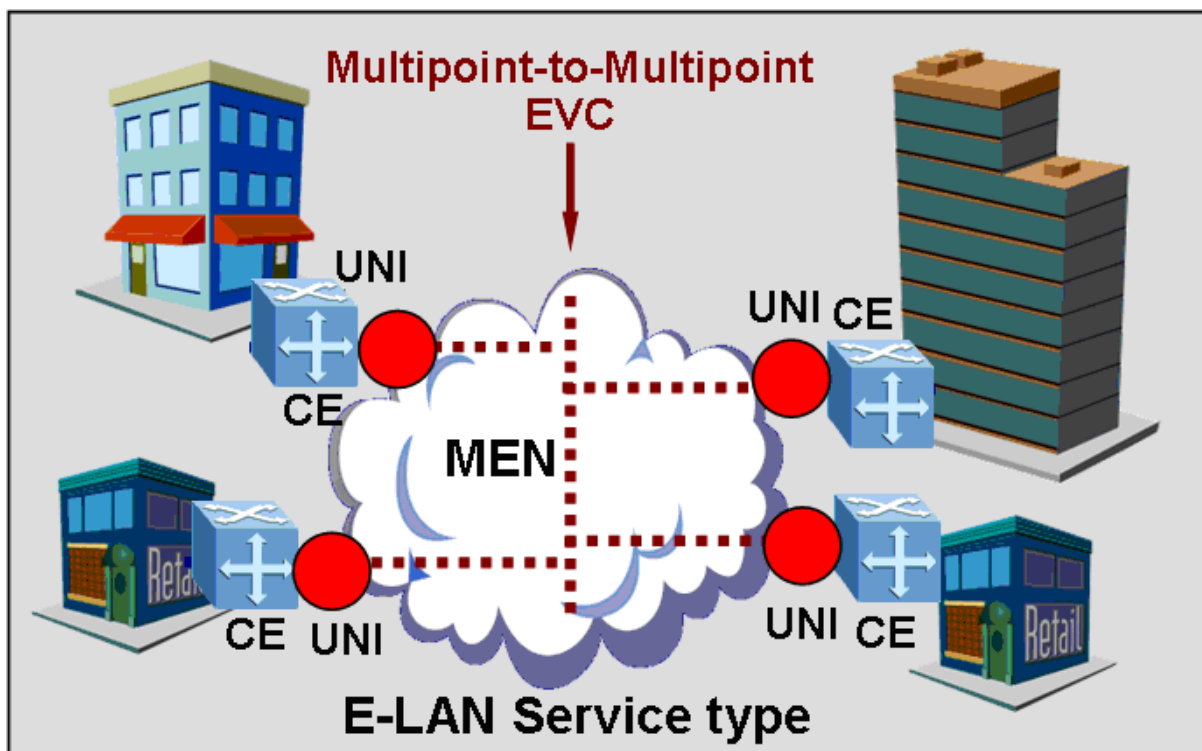


Figura 12 - Tipo de serviço E-Lan

Um serviço da categoria E-LAN pode ser utilizado, tal como um serviço E-Line, para criar uma quantidade diferente de serviços. Na sua forma mais simplificada, um ELAN fornece um serviço sem garantias de desempenho, enquanto que nas suas formas mais complexas pode apresentar as mais variadas garantias ao nível de largura de banda, atrasos, etc. Também nos serviços E-LAN é possível ter multiplexação, sendo possível oferecer no mesmo UNI, por exemplo, um serviço E-Line e simultaneamente um serviço E-LAN ou dois

serviços E-LAN. Enquanto poderá ser óbvio que poderemos conectar apenas dois UNIs com um E-LAN ficando o serviço muito semelhante a um E-Line, importa salientar as diferenças entre estes dois serviços. Ao adicionarmos um terceiro UNI a um E-Line, teremos que criar nova EVC que ligue o novo UNI a um dos UNIs já pertencentes ao E-Line.

Mas para obtermos conectividade total, teríamos que criar duas EVCs, e correspondentes E-Lines que ligassem o novo UNI a cada um dos dois UNIs existentes. No caso do E-LAN, isso não seria necessário, teria apenas que ser adicionado o novo UNI, sem ser necessária a criação de qualquer EVC ou serviço adicional para obter conectividade total. Um serviço E-LAN pode ligar um grande número de localizações com menor complexidade que ligações implementadas utilizando tecnologias de ponto-a-ponto, pois requer apenas uma EVC para obter uma conectividade multi-local. Uma E-LAN pode ainda ser usado para criar um amplo leque de serviços como as LANs privadas ou as LANs privadas Virtuais.

5.2 Interoperabilidade

Avanços recentes nas especificações do Ethernet caminham para viabilizar, por completo, a interoperabilidade (interworking), ou seja, a conexão funcional entre redes Metro Ethernet e outras redes WAN - Wide Area Network existentes. Através de um conjunto de técnicas de mapeamento e suporte a facilidades diversas, é possível interligar redes Metro Ethernet com sistemas ATM – Asynchronous Transfer Mode, Frame Relay e backbones IP/MPLS.

Esforços também vêm sendo conduzidos visando promover interoperabilidade entre os diferentes equipamentos produzidos por um grande conjunto de fornecedores de tecnologia voltada para redes Metro Ethernet. Recentemente, o Metro Ethernet Forum certificou o primeiro grupo de sistemas que atendem de forma completa todos os modelos de serviços Ethernet, como EPL - Ethernet Private Line, EVPL - Ethernet Virtual Private Line e E-LAN - Ethernet Multipoint-to-Multipoint.

5.3 Parâmetros de Tráfego

O Parâmetros de Tráfego (Bandwidth Profile) especifica o limite da taxa média de quadros de serviços Ethernet que podem entrar na rede do provedor de serviços através de uma UNI. O MEF tem definido três atributos de Bandwidth Profile, conforme mostrados na Figura 13 e a seguir descritos.

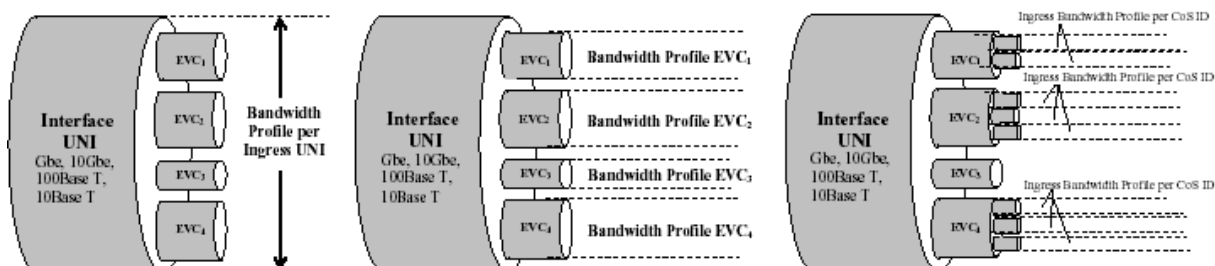


Figura 13 - Atributos de Bandwidth Profile

- **Perfil por UNI:** aplica-se para todos os quadros de serviço que entram na rede do provedor através da UNI.
- **Perfil por EVC:** aplica-se para todos os quadros de serviço que passam por um determinado EVC dentro da UNI.
- **Perfil pelo identificador CoS:** aplica-se a todos os quadros de serviço dentro de um EVC identificados pelos bits de prioridade da marcação (tag) de VLAN IEEE 802.1p do cliente.

Cada atributo de Bandwidth Profile definidos acima, consiste de quatro parâmetros de tráfego que definem a vazão (throughput) fornecida pelo serviço. Os parâmetros de tráfego são os seguintes:

- **CIR (Committed Information Rate):** taxa média garantida e de acordo com os objetivos de desempenho contratados (por exemplo: jitter, atraso, etc.) e especificados em um SLA (Service Level Agreement).
- **CBS (Committed Burst Size):** definido como o número máximo de bytes permitidos para os quadros de serviços que entram, sendo ainda contados dentro do CIR.
- **EIR (Excess Information Rate):** taxa média, excedente ao CIR, para a qual os quadros de serviços são entregues sem nenhuma garantia de desempenho.
- **EBS (Excess Burst Size):** definido como o número máximo de bytes permitidos para os quadros de serviços que entram, sendo ainda contados dentro do EIR.

Um meio prático de descrever ou marcar os quadros de serviços quando sua taxa média está conforme ou não ao perfil definido, é através do uso de cores (Figura 14). Os

quadros de serviço verdes são os que estão de acordo com o SLA contratado e geralmente não podem ser descartados. Os quadros de serviço amarelos são os que não estão de acordo com o SLA contratado, mas que tipicamente não são imediatamente descartados. Os quadros de serviços vermelhos também não estão de acordo com os objetivos de desempenho contratados e são imediatamente descartados.




| Conformance | Color | Service Frame Delivery |
|-------------------|--|---|
| CIR Conformant |  | Service Frames green and delivered per the performance objectives specified in the SLA/SLS. |
| EIR Conformant |  | Service Frames are yellow and may be delivered but with no performance assurances. |
| None |  | Service Frames are red and dropped. |

Figura 14 - Marcação dos quadros de serviço através de cores

A especificação do valor do CBS vai depender do tipo de aplicação ou tráfego que se deseja suportar. Por exemplo, para serviços destinados a suportar picos de transferência de dados TCP, o CBS deve ser muito maior que em aplicações VoIP, onde a taxa é mais constante.

5.4 Identificadores de Classes de Serviços (CoS)

As redes Metro Ethernet devem oferecer diferentes classes de serviço (CoS) para os clientes, identificados por meio de:

- **Porta Física:** nesse caso uma única classe de serviço pode ser fornecida.
- **CE-VLAN CoS (802.1p):** a classe de serviço é identificada pelos bits de prioridade do tag de VLAN do cliente. Nesse caso, o SLA deve especificar o Bandwidth Profile e os parâmetros de desempenho para cada classe de serviço.
- **DiffServ / IP TOS:** o segundo byte do cabeçalho IP pode ser usado

para definir classes de serviço. Para o caso do TOS, até 8 classes podem ser definidas. No caso do Diffserv, capacidades mais robustas de QoS podem ser fornecidas através do padronizados PHBs (Per-Hop Behaviors).

O provedor de serviços vai utilizar um desses identificadores para, por exemplo, separar um tráfego que estará sujeito a um determinado CIR. A Tabela 1 mostra um exemplo de SLA baseado em CoS para rede Metro Ethernet.

| Service Class | Service Characteristics | CoS ID | Bandwidth Profile per EVC per CoS ID | Service Performance |
|---------------|--|---------|--------------------------------------|--|
| Premium | Real-time IP telephony or IP video applications | 6, 7 | CIR > 0 EIR = 0 | Delay < 5ms Jitter < 1ms Loss < 0.001% |
| Silver | Bursty mission critical data applications requiring low loss and delay (e.g., Storage) | 4, 5 | CIR > 0 EIR ≤ UNI Speed | Delay < 5ms Jitter = N/S Loss < 0.01% |
| Bronze | Bursty data applications requiring bandwidth assurances | 3, 4 | CIR > 0 EIR ≤ UNI Speed | Delay < 15ms Jitter = N/S Loss < 0.1% |
| Standard | Best effort service | 0, 1, 2 | CIR=0 EIR=UNI speed | Delay < 30ms Jitter = N/S Loss < 0.5% |

Tabela 1 - Exemplo de SLA baseado em CoS

5.5 Desafios das Redes Metro Ethernet

As redes metro Ethernet, segundo alguns analistas, tem o potencial de aumentar a eficiência (em termos de custos) da capacidade de rede. De igual modo, podem disponibilizar um leque alargado de serviços de forma simples, escalável e flexível.

O mercado dos equipamentos metro Ethernet atingiu 1,7 mil milhões de dólares em 2004 e deverá crescer a um rácio anual composto de 26 por cento até 2009, segundo a IDC. Por outro lado, Sterling Perrin, especialista em redes ópticas na IDC, está convencido de que o mercado dos equipamentos metro Ethernet irá ultrapassar o mercado dos equipamentos Sonet e SDH (típicos das redes de telecomunicações públicas tradicionais) até 2009.

Com base nestas previsões, os fornecedores de equipamentos de telecomunicações terão que adaptar as infra-estruturas Sonet/SDH existentes para acomodarem o desafio Ethernet. A MSPP (Multi-Service Provisioning Platform) - que combina a funcionalidade de múltiplos elementos de rede - representa uma solução de rede mais flexível e com menores custos a curto prazo. No entanto, apesar da MSPP representar

uma boa solução intermédia, os grandes operadores terão que avançar da MSPP para redes Ethernet comutadas.

A IDC chegou ainda à conclusão que a região da Ásia/Pacífico será aquela que vai apresentar as maiores oportunidades aos subscritores metro Ethernet e aos fornecedores de equipamentos. Paralelamente, os routers e os comutadores de nível 2/3 dominam as oportunidades de receitas do mercado metro Ethernet.

6 EQUIPAMENTOS EMPREGADOS EM REDES METRO ETHERNET

O mercado tem investido cada vez mais em Ethernet e Metro Ethernet. Equipamentos dessa tecnologia têm registrado um crescimento explosivo devido a migração das redes de transporte de ATM para Ethernet. Nas redes de transporte, a migração ocorre do SDH e de Frame Relay para Metro Ethernet. O que impulsiona o segmento de equipamentos para rede física de transporte são as operadoras e seu tráfego cada vez mais crescente, com a oferta de banda larga pelas operadoras.

Para a implementação de uma Metro Ethernet são essencialmente necessários os equipamentos básicos para o transporte de dados (Routers e Switches), equipamentos para a segurança (servidores e gerência integrada, firewalls, IDPs e IDSs) e gerência. Mas apesar da aparente simplicidade, para garantir a escalabilidade e o desempenho da rede, estes equipamentos possuem uma gama enorme de protocolos e possíveis configurações.

Além dos já mencionados, também se pode empregar equipamentos que possibilitem o gerenciamento do tipo de tráfego que consomem os recursos da Metro Ethernet, acompanhados por outros que otimizam o tráfego “cacheando” os dados que vêm da Internet. Para executar estas funções foram desenvolvidos o Disciplinador de Tráfego e o Cache de Conteúdo HTTP, Estes podem ser chamados de Equipamentos para Otimização da Rede.

Para a inserção destes elementos na Rede Metro é necessário um profundo estudo sobre o perfil dos usuários que utilizam a Rede, pois as configurações nestes equipamentos, sem a devida atenção, pode causar insatisfação dos clientes ou piorar o desempenho da Metro Ethernet.

6.1 Equipamentos para transporte de dados

Basicamente, os elementos de transporte das Redes Metropolitanas estão divididos em três camadas: Core, Agregação (ou Concentração) e Acesso (Figura 15).

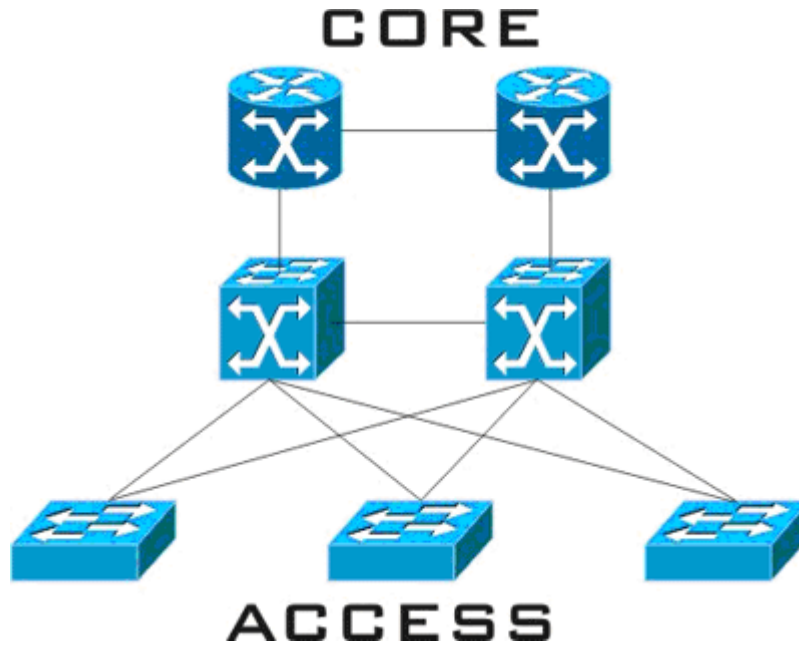


Figura 15 - Metro Ethernet - Topologia Básica

6.1.1 Core da Rede

O Core da Rede é composto por equipamentos nos quais passam todos os tráfegos de dados com destino fora da rede local. Para suportar todos esses tráfegos é necessária a utilização de roteadores de grande porte, de preferência com topologia redundante. As características principais de um roteador de core são:

- Alta capacidade de comutação de pacotes;
- Interfaces de conexão para altas velocidades;
- Memória para armazenamento de rotas com alto desempenho;
- Redundância nos módulos de controle, comutação, alimentação e ventiladores;
- Suportar os protocolos de roteamento utilizados na Internet, principalmente o BGP.

6.1.2 Switch de Agregação

O switch de agregação é projetado para superar uma ampla gama de aplicações, o que exige alto desempenho, escalabilidade e o mais alto nível de resiliência.

Ainda muito importante, precisa ser um equipamento projetado para atender às demandas futuras assim como as atuais. A extensibilidade é a chave para a construção de redes centrais inteligentes que possam se adaptar e responder a demandas que mudam com o tempo.

Entre as principais características deste switch estão:

- Concentração do tráfego vindo de outros switches;
- Provimento de conectividade entre os elementos de acesso, autenticação e gerenciamento;
- Escalonamento de portas;
- Redundância no acesso aos elementos da rede;
- Aplicação de QoS;
- Distribuição do tráfego com origem/destino nos usuários e servidores;
- Provimento de conectividade entre elementos de roteamento, servidores de autenticação, servidores de gerência, etc.

6.1.3 Switch de Acesso

Este elemento tem como finalidade a conexão com o cliente da rede. Neste switch podem ser conectados equipamentos que conectam o cliente diretamente (modems, conversores ópticos, switches, hubs, etc.) ou equipamentos Multiplexadores (DSLAMS).

Características principais:

- Devem permitir Switching em camada 2 e opcionalmente roteamento em Camada 3 com suporte a roteamento com rotas estáticas;
- Funcionalidades para limitação de banda, QoS, multicast;
- Suportar protocolos de roteamento e republicar rotas;
- Possuir portas de alta velocidade.

6.2 Equipamentos para segurança e gerência

6.2.1 Segurança - Firewall

Opcionalmente, pode-se implementar uma camada de segurança na rede, inserindo firewalls entre os equipamentos. Geralmente fica instalado entre o Roteador e a

camada Agregação (Figura 16).

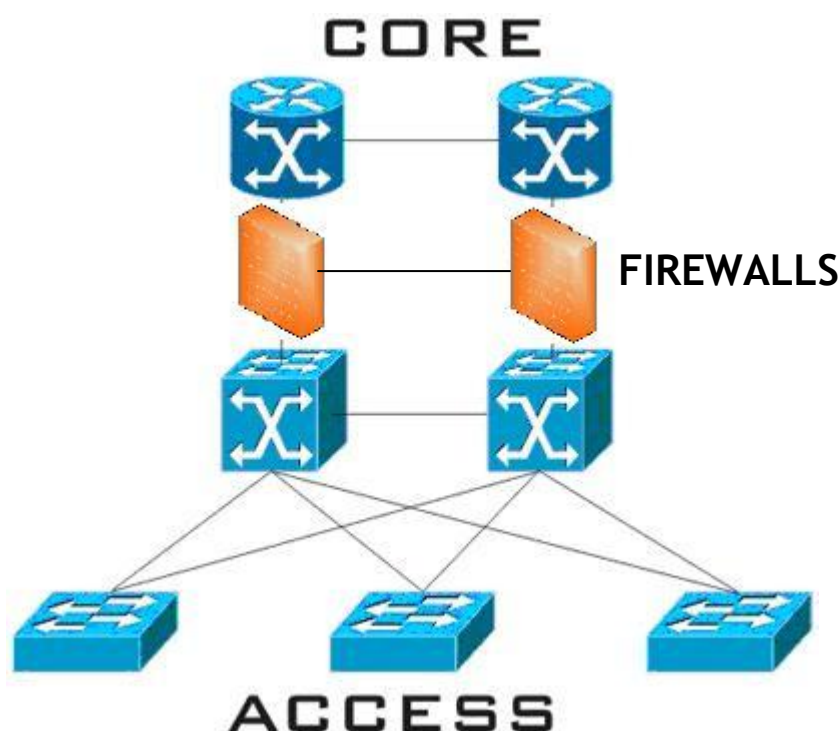


Figura 16 - Rede Metro com Firewall

Este equipamento tem por função, dentro da rede, de permitir a transmissão e recepção somente do tráfego autorizado via regras definidas na política de segurança. Pode ser projetado para efetuar o bloqueio de tráfego específico, e fazer o controle de banda (traffic management).

Por padrão o tráfego é todo bloqueado e as exceções são tratadas, mas no caso de Provedores de Internet e a posição na estrutura física da rede, o firewall pode liberar todo tráfego e tratar as exceções, com aplicações de políticas para controle de banda por serviço.

A limitação de banda principalmente para ICMP é uma prática comum, pois o aumento muito excessivo no tráfego de entrada pode indicar um de DoS (Denial of Service), uma vez definido o nível de tráfego o excedente é descartado. Para que exista a redundância na rede, dois equipamentos são ligados, utilizando protocolos de conexão.

6.2.2 Segurança – IDP (Intrusion Detection and Prevention)

De forma a garantir a segurança e disponibilidade dos serviços de AAA e

gerência, podem ser utilizados os IDP's. Estes appliances trabalham validando as conexões já permitidas aos servidores, verificando se o tráfego permitido é realmente íntegro.

Para tanto, se utiliza de 9 diferentes técnicas de detecção de intrusos:

- Stateful Signature Detection: Detecção através de padrões conhecidos, atualizados diariamente.
- Protocol Anomaly Detection: Detecta ataques desconhecidos ou permutados;
- Backdoor Detection: Detecta ataques oriundos da parte protegida (de dentro da rede);
- Traffic Anomaly Detection: Ataques que geram múltiplas sessões e conexões diferentes;
- IP Spoofing Detection: Detecta hosts que se fazem passar por outros hosts;
- Compound Signatures: Combina as assinaturas de ataques conhecidos com a detecção de anomalias de protocolo para detectar ataques de alta complexidade;
- DoS Detection: Barra ataques de Denial of Service conhecidos;
- Layer 2 Detection: Detecta ataques de camada 2 (ARP);
- Network Honeypot: Cria serviços que não existem, e esconde os serviços legítimos para confundir e comprovar a ação de hackers;

Caso o tráfego não esteja de acordo com as políticas (atualizadas diariamente por servidor NSM), ou pelas regras personalizadas, o IDP pode tomar a liberdade de bloquear ou apenas notificar a conexão indevida.

6.2.3 Gerência

Para executar a gerência de uma Rede Metropolitana é montada uma Rede de Servidores de Gerência. Os Servidores de gerência desempenham função de gerenciar, receber avisos, monitorar desempenho e utilização e configurar funções específicas de cada um dos equipamentos da Rede Metro. O ideal é que cada um dos servidores esteja conectado à porta de equipamentos gerenciados através de uma ambiente de rede separado logicamente do ambiente de produção da Sercomtel, o acesso à configuração dos equipamentos deverá ser feito unicamente através dos servidores.

A gerência da rede através dos servidores permite total controle dos elementos, executando-se operações que atribuem as mudanças de forma integrada a todos os elementos, possibilitando aos operadores efetuarem configurações com rapidez e precisão, reduzindo muito a ocorrência de falha humana nas operações.

Os softwares de gerência permitem muitas funções serem executadas através de interfaces amigáveis:

A gerência dos equipamentos é apresentada ao operador de forma com que ele tenha completa informação sobre a situação da Rede. Através desta da gerência é possível:

- Visualização do Status de cada equipamento, com geração de alarmes;
- Ter informação em Real Time das conexões entre os elementos;
- Inserção e retirada lógica de elementos na topologia;
- Visualização dos detalhes de configuração dos equipamentos através

de simples clic sobre os ícones.

- Criação e configuração de Vlan's na rede;
- Visualização do tráfego em qualquer ponto da Rede;
- Controle de permissão a operadores de gerência.

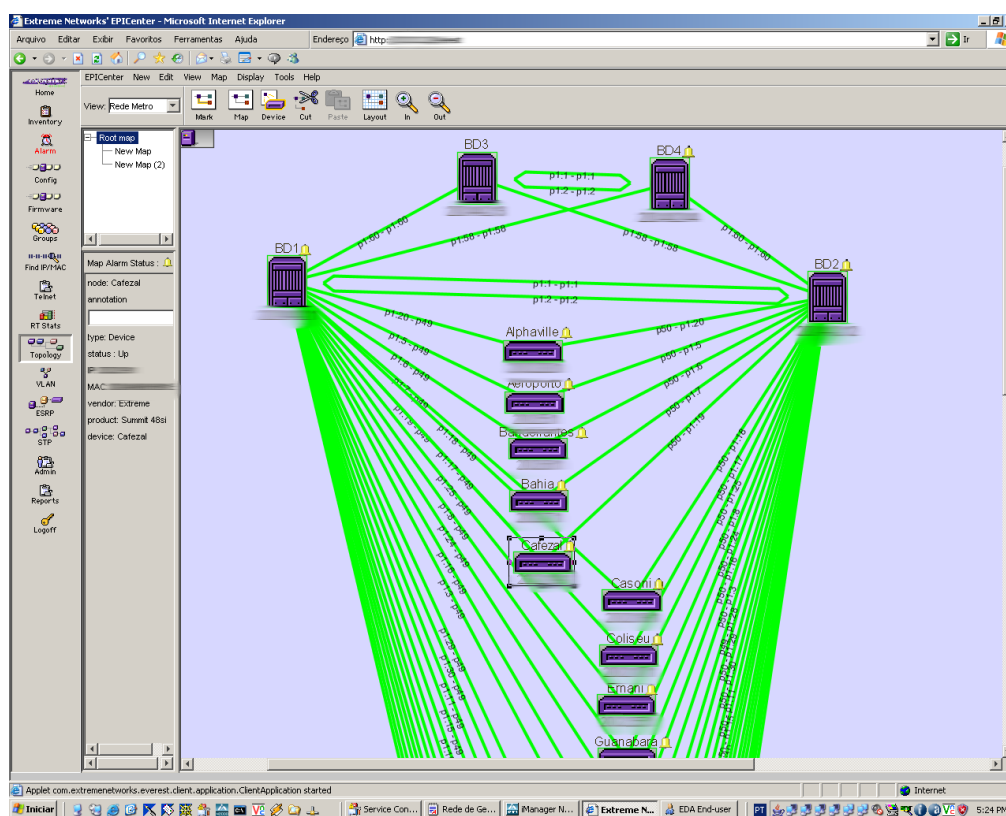


Figura 17 - Gerência da Rede Metro - Visualização completa dos elementos

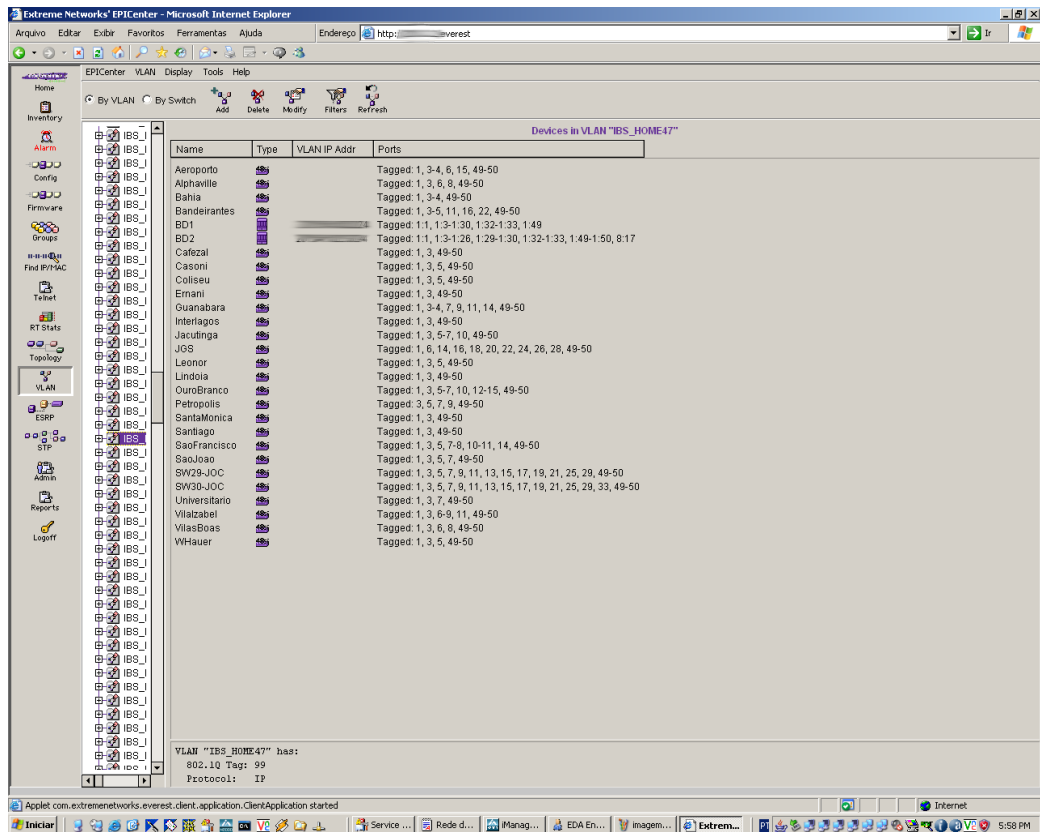


Figura 18 - Gerência da Rede Metro - Criação de VLANS

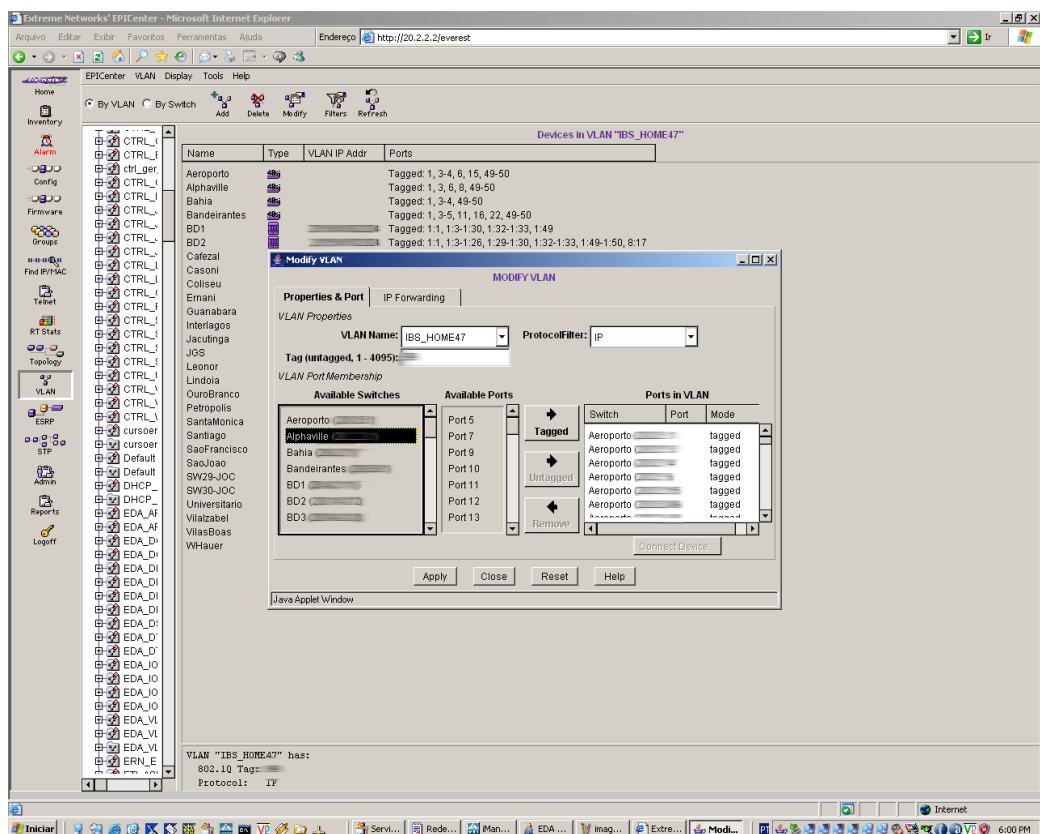


Figura 19 - Gerência da Rede Metro – Criação de VLANS

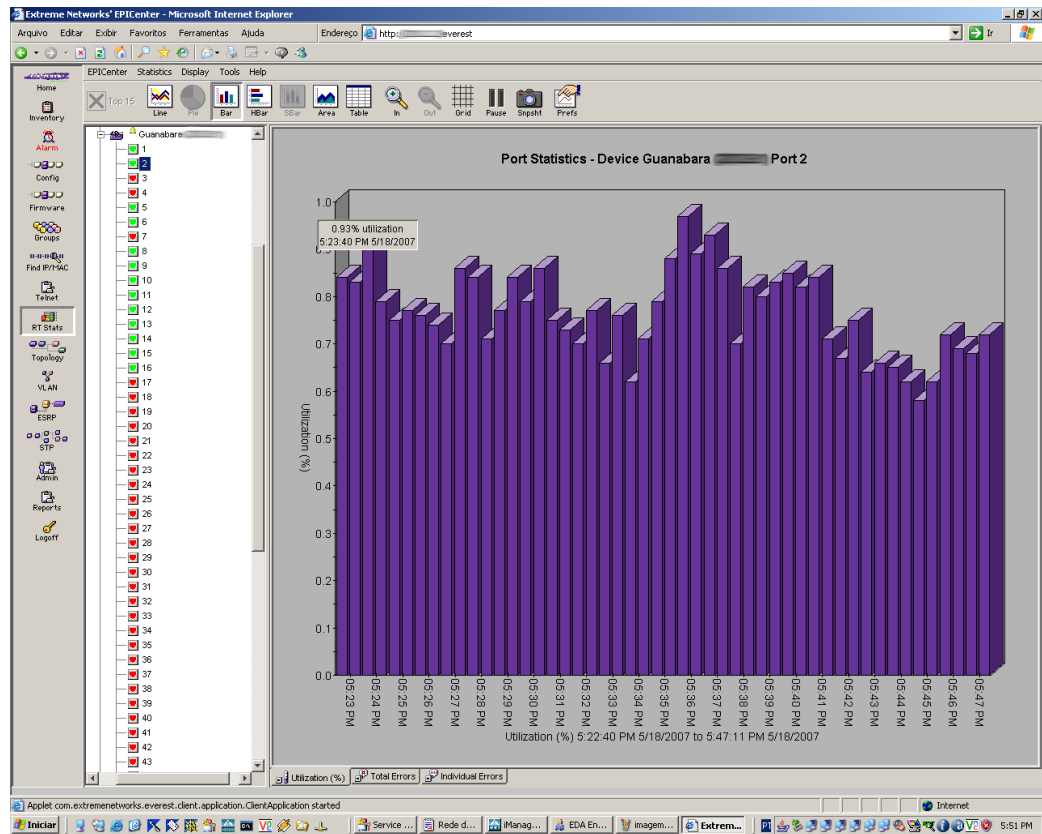


Figura 20 - Gerência da Rede Metro – Tráfego em Interfaces

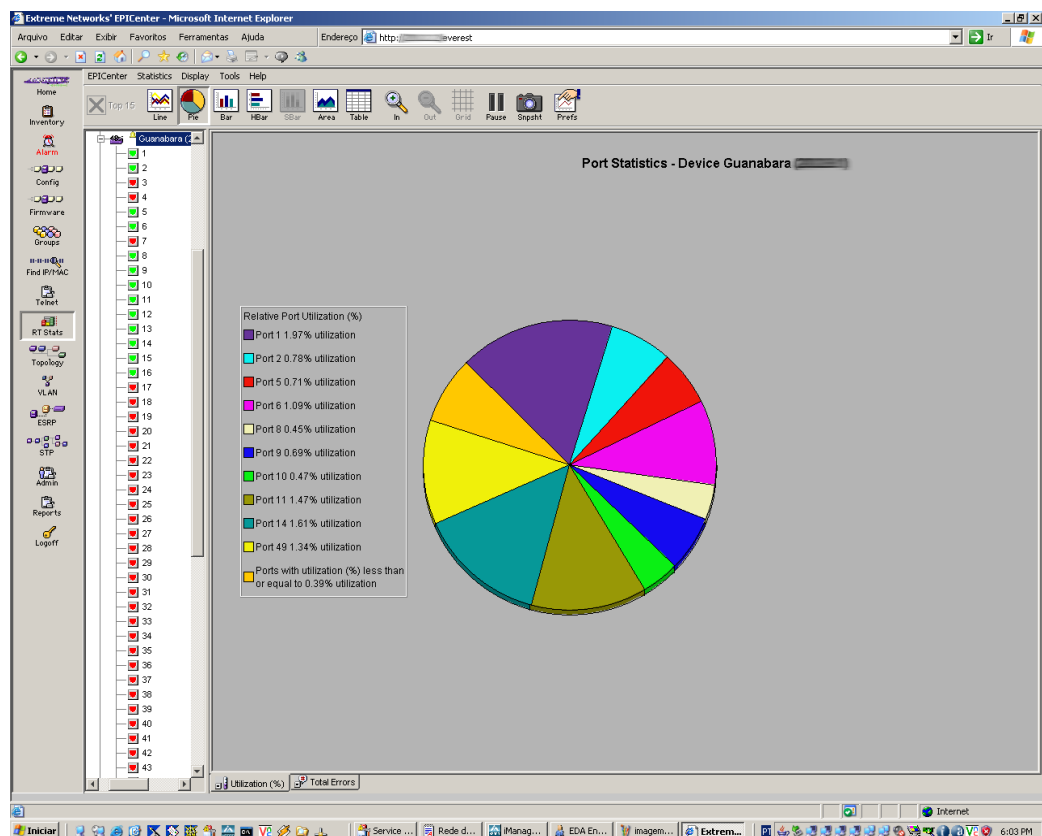


Figura 21 - Gerência da Rede Metro – Tráfego em Equipamentos

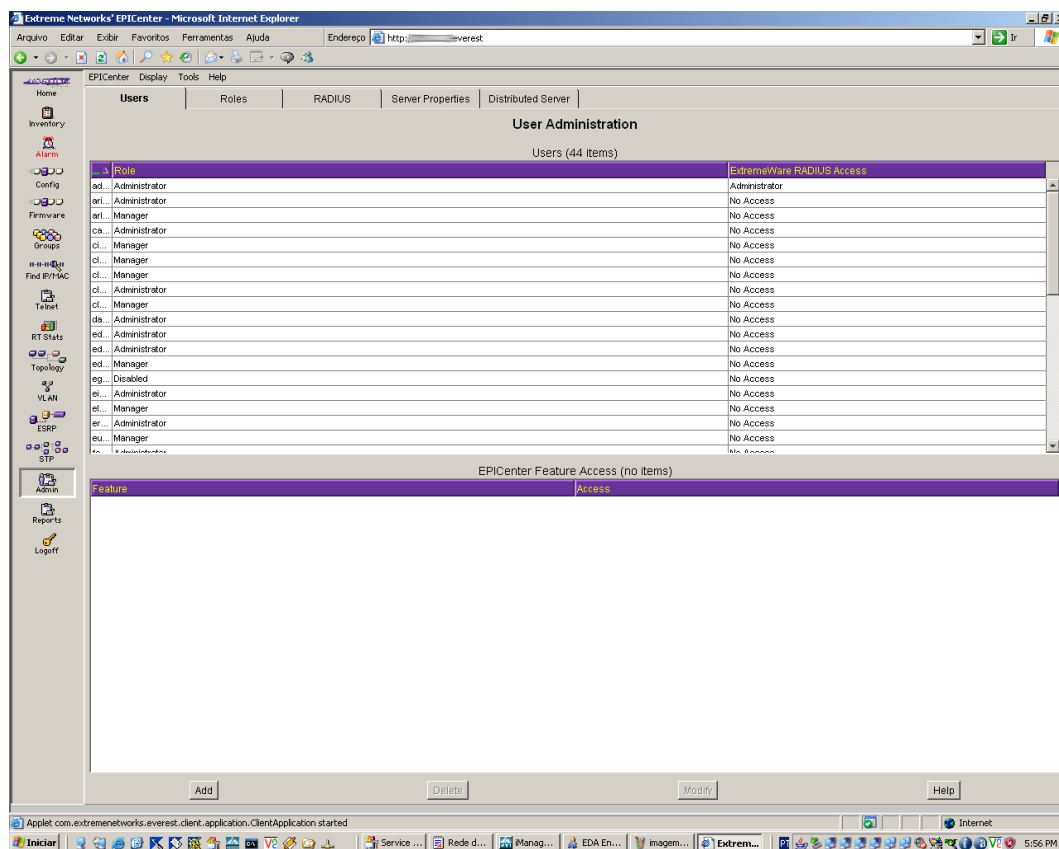


Figura 22 - Gerência da Rede Metro - Administração de Operadores

6.3 Equipamentos para Otimização da Rede

6.3.1 Disciplinador de Tráfego

Uma nova categoria de gerenciamento de Redes vem se tornando rapidamente uma necessidade, tanto em médias e grandes organizações, onde as mesmas estão buscando um melhor controle do que está trafegando em seu ambiente de rede, visando assegurar que as aplicações estratégicas sempre tenham recursos disponíveis, pois necessitam de uma ótima performance.

Diante disto, torna-se extremamente necessário um equipamento capaz de controlar o tráfego de rede, limitar a banda para certas aplicações, garantindo uma largura de banda mínima para outras, além de identificar o tráfego com alta ou baixa prioridade. Para tais funções torna-se necessário o “Gerenciamento do Tráfego” dentro de uma Rede.

Este tipo de equipamentos foi desenvolvido para o gerenciamento da banda de redes corporativas e links de Provedores de acesso à Internet, visando a aplicação dos

seguintes serviços:

- Monitoração/classificação de tráfego;
- Aplicação de QoS;
- Aplicação de políticas no tráfego;
- Segurança da Rede.

Com o Disciplinador de Tráfego é possível verificar todo o tráfego na Rede e aplicar regras para melhorar a performance geral dos clientes.

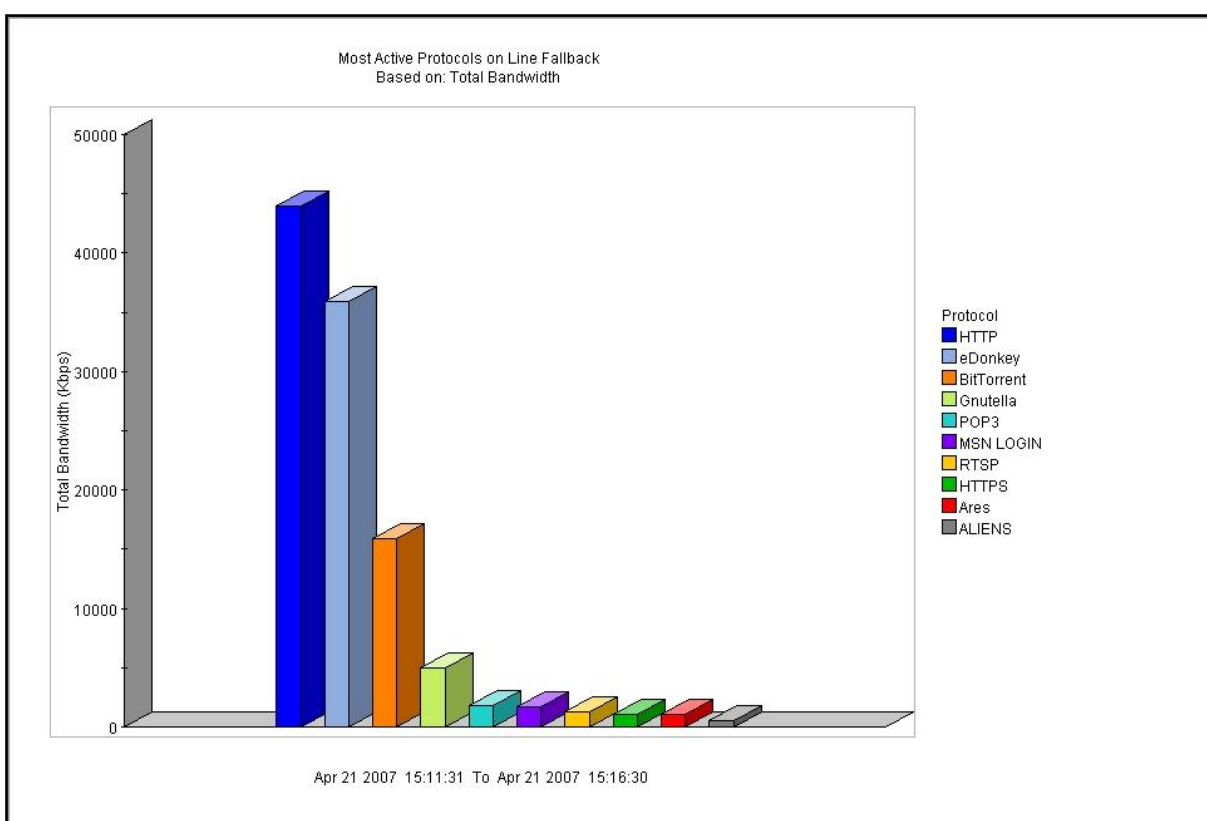


Figura 23 - Visualização instantânea dos protocolos que trafegam na Rede

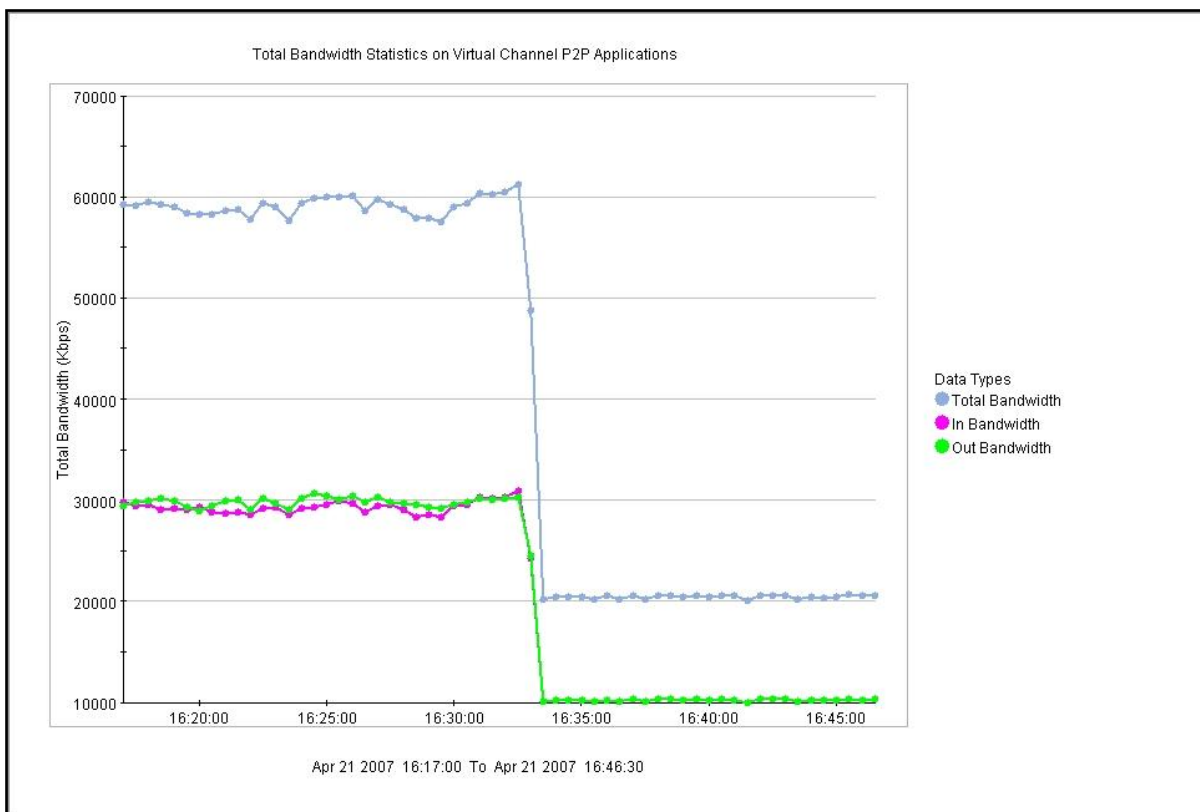


Figura 24 - Aplicação de regras para tráfegos prejudiciais à Rede

6.3.2 Cache de Conteúdo HTTP

O Cache é um equipamento que deve possuir alta performance e suportar os protocolos HTTP, FTP e Gopher.

De um modo simplificado, o Cache recebe os pedidos de usuários que desejam visualizar páginas externas à Metro e verifica se tem a página armazenada em seus discos. Se tiver a página em cache, verifica se ela ainda é válida e envia para o cliente. Se não tiver a página em cache, busca a página no servidor externo, armazena no cache e manda para o cliente. Assim, na próxima vez que alguém solicitar esta página a mesma será carregada muito mais rapidamente, pois estará em um cache local. Entre as principais vantagens de utilizar o Cache de Conteúdo HTTP estão:

- Aumento na segurança, pois todas as requisições para páginas externas irão passar através do proxy;
- Aumento da velocidade de navegação e/ou diminuição da utilização do link Internet, já que muitas páginas acessadas pelos usuários estarão em cache local;

7 CONCLUSÃO

As redes Metro Ethernet têm se mostrado um mercado crescente e promissor. A maioria dos provedores de serviço ou já implementam ou estão desenvolvendo/investigando o seu uso. Para atender às exigências de QoS e baixo custo exigidos pelo mercado, novos protocolos estão sendo padronizados ou propostos, atribuindo à rede Metro Ethernet QoS e segurança similares às redes de circuitos, com as vantagens de uma rede de pacotes.

8 REFERÊNCIAS

CISCO. **Cisco Systems**: Academy Connection - Training Resources. Disponível em: <<http://cisco.netacad.net/>>. Acesso em: 18 de Junho. 2008.

IEEE. IEEE Std 802.1Q-2005. **IEEE Standard for local and metropolitan area networks virtual bridged local area networks**. 2005.

IEEE. IEEE Std 802.1ad-2005. **IEEE Standard for Local and metropolitan area networks - virtual Bridged Local Area Networks**, Amendment 4: Provider Bridges. 2005.

KUROSE, James F; ROSE, Keith W. **Computer Networking**: A top down approach featuring the Internet. 3rd edition. Addison-Wesley, 2004.

SOUZA, Renier Edward. **Tendências em Redes Metropolitanas**. 2003.

LOPES, Rodrigo Azevedo. **Ethernet Network Manager**. Lisboa, 2006.

MEF. **Metro Ethernet Forum**. Disponível em: <<http://www.metroethernetforum.org>>. Acesso em: 09 de Julho. 2008.

Metro Ethernet Forum. **Ethernet in the Metro**. Disponível em: <<http://www.metroethernetforum.org/casestudyriverstonekoreatelecom012803.pdf>>. Acesso: 12 Julho. 2008.

SANTITORO, Ralph. **Bandwidth Profiles for Ethernet Services**. Metro Ethernet Forum, 2004.

TANENBAUM, Andrew S. **Computer Networks**. 3rd edition. Prentice Hall, 1996.

OUTROS TRABALHOS EM:

www.projetoederedes.com.br