RAFAEL DE MAGALHÃES DIAS FRINHANI

Projeto de re-estruturação do gerenciamento e otimização da rede computacional da Universidade Federal de Lavras

Monografia de Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel.

Orientador
Prof. Anderson Bernardo dos Santos

Co-Orientador
Prof. Dr. Rêmulo Maia Alves

Lavras
Minas Gerais - Brasil
2005

RAFAEL DE MAGALHÃES DIAS FRINHANI

Projeto de re-estruturação do gerenciamento e otimização da rede computacional da Universidade Federal de Lavras

Monografia de Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel.

Aprovada em *17 de Janeiro de 2005*

Prof. Anderson Bernardo dos Santos
(Orientador)

Prof. Dr. Rêmulo Maia Alves
(Co-Orientador)

Lavras
Minas Gerais - Brasil

Agradecimentos

Agradeço a Deus pela vida.

A meus pais e irmãs pelos conselhos e ombro amigo.

Aos amigos pelos momentos únicos.

Ao "Mestre dos Mares"e ao "Andersun Morcegão"pelas oportunidades e as minhas "meninas"que sempre choraram comigo nos momentos mais difíceis.

Dedico este projeto a todos que direta ou indiretamente me ajudaram a vencer mais esta batalha.

Resumo

Projeto de re-estruturação do gerenciamento e otimização da rede computacional da Universidade Federal de Lavras

O rápido crescimento da Internet e seus serviços, gerou nos últimos anos um grande impacto no fluxo de tráfego através das redes locais. Como resultado do uso das Intranets corporativas e principalmente da Internet, uma grande quantidade de tráfego e de informações estão sendo trocadas com recursos remotos. Por possuírem a característica de crescimento fácil, o impacto do fluxo de tráfego nas redes de campus é mais traumático e desta forma a sua infra-estrutura, em um curto período de tempo, não conseguirá suprir a demanda computacional de seus usuários.

A rede computacional da Universidade Federal de Lavras não é uma exceção a esta regra. Desde o seu surgimento a partir de 1990, sua estrutura de rede vem sofrendo um crescimento constante e acelerado o que, com o passar dos anos, vem contribuindo para uma queda gradativa no desempenho da rede.

É objetivo deste projeto, a realização de uma pesquisa e implantação de uma solução que através da reformulação da infra-estrutura lógica da rede UFLA, possa otimizar os recursos físicos já existentes e de certa forma, possa proporcionar melhorias no desempenho da rede UFLA bem como facilitar a aplicação das atividades de gerência.

Palavras-chave: redes de campus, segmentação, VLAN, otimização

Project of reorganization of the management and otimização of the computational net of the Federal University of Lavras

The fast growth da InterNet and its services, generated us last years a great impact on flow of traffic through of the local nets. As result of the use of the Intranets corporative and mainly of the InterNet, a great amount of traffic and information is being changed with remote resources. For possessing the characteristic of easy growth, the impact of the flow of traffic in the campus nets is more traumatic and of this form its infrastructure, in a short period of time, will not obtain to supply the computational demand of its users.

The computational net of the Federal University of Lavras is not an exception to this rule. Since its sprouting from 1990, its structure of net comes suffering a constant and speed up growth what, with passing of the years, it comes contributing for a gradual fall in the performance of the net.

Is objective of this project, the accomplishment of a research and implantation of a solution that through the reformularization of the logical infrastructure of net UFLA, can optimize existing the physical resources already and of certain form, it can provide improvements in the performance of net UFLA as well as and facilitates the application of the activities of management.

Keywords: Campus Networks, segmentation, VLAN, optimization

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

A computação distribuída baseada em rede de computadores agora é aceita sem questionamento levando todos os setores das pequenas às grandes corporações a sofrer um acelerado processo de informatização.

O rápido crescimento da Internet e seus serviços, gerou nos últimos anos um grande impacto no fluxo de tráfego através das redes locais. Como resultado do uso das Intranets corporativas e principalmente da Internet, uma grande quantidade de tráfego e de informações estão sendo trocadas com recursos remotos.

O impacto do fluxo de tráfego nas redes de campus é mais drástico. Por possuírem a característica de crescimento fácil, rápido e na maioria das vezes desordenado, a estrutura computacional das redes de campus, em um curto período de tempo, não conseguirá suprir a demanda computacional de seus usuários.

A transição das estruturas de rede tradicionais para um novo modelo de redes que consiga suprir esta demanda é inevitável. Os altos custos decorrentes dessa re-estruturação, abre espaço para técnicas de otimização que procuram adequar as estruturas de rede legadas aos novos padrões de conectividade.

As corporações estão cada vez mais dependentes dos serviços informatizados e devido a este fato, é cada vez mais preocupante a idéia de se assegurar integridade aos dados bem como a constante melhoria na qualidade dos serviços de rede.

A rede computacional da Universidade Federal de Lavras não é uma exceção a esta regra. Desde o seu surgimento a partir de 1990, sua estrutura de rede vem sofrendo um crescimento constante e acelerado o que, com o passar dos anos, vem contribuindo para uma queda gradativa no desempenho da rede.

É neste sentido que a necessidade de reformulação do gerenciamento e da infra-estrutura lógica da rede UFLA é cada vez mais preocupante. Com a intenção de otimizar os recursos físicos já existentes, o presente projeto apresenta os resultados da análise da atual infra-estrutura da rede UFLA e propõe uma solução que vise a melhora do seu desempenho e facilite a aplicação das atividades de gerência.

1.1 Hipótese

A segmentação da rede através de VLANs, é a técnica mais indicada para que se possa conter os altos níveis de tráfego de difusão e por consequência melhorar o desempenho da rede computacional da Universidade Federal de Lavras .

1.2 Objetivos

Ao constatar que a rede computacional da Universidade Federal de Lavras vem sofrendo com problemas relacionados ao crescimento rápido e desordenados típicos das redes de Campus, o Centro de Informática da UFLA vislumbrou a necessidade de se reestruturar a sua infra-estrutura e principalmente seus processos de gerência.

A Rede UFLA recentemente vem apresentando problemas relacionados principalmente à não otimização dos recursos atualmente disponíveis. A falta de uma formalização na infra-estrutura lógica da rede acaba por comprometer os processos de gerência o que de certa forma acaba por repercutir diretamente no seu desempenho.

O projeto em questão tem como principal objetivo, propor uma reestruturação na infra-estrutura lógica da rede UFLA que proporcione a otimização da infra-estrutura física já existente. O foco principal deste projeto é a apresentação de uma solução que possa segmentar a rede UFLA de forma a amenizar o alto fluxo de tráfego incoerente que está extrapolando os limites das redes locais (departamentos) e alcançando o backbone da rede.

1.3 Estrutura do Trabalho

O capítulo 2, faz uma abordagem sobre redes de computadores e seus conceitos básicos. Neste capítulo será mostrado as limitações dos modelos de redes de campus tradicionais e os benefícios incorporados aos novos modelos.

O capítulo 3, faz uma breve descrição das características do padrão Ethernet, que é o padrão utilizado na rede da UFLA. No capítulo 4, será apresentado os conceitos básicos da suíte de protocolos TCP/IP e a uma breve descrição de alguns protocolos de alto nível encontrados no ambiente computacional da rede em questão.

No capítulo 5, será descrito os principais equipamentos de interconexão utilizados em uma estrutura de rede. Será apontada as suas características, funcionalidades bem como suas limitações. O capítulo 6 mostrará os conceitos, e as vantagens de se segmentar uma rede.

O capítulo 7 introduzirá o conceito de VLANs, que é a tecnologia será utilizada na segmentação da rede UFLA. O capítulo 8 contém a metodologia de pesquisa

e implantação utilizada na segmentação e o capítulo 9 apresenta as conclusões do trabalho.

Capítulo 2

Redes de Computadores

Uma rede, na sua forma mais simples, é constituída por duas ou mais estações interligadas entre si através de uma mídia de compartilhamento. As principais razões para o surgimento das redes de computadores foram a redução de custos, a troca de informações e a descentralização dos recursos computacionais.

Existem dois tipos de tecnologia de transmissão sendo elas as redes de difusão e as redes ponto a ponto. As **redes de difusão** (*broadcasting*) têm apenas um canal de comunicação compartilhado por todas as máquinas. Os pacotes enviados por uma das estações são recebidos por todas as outras. Um campo dentro do pacote especifica o seu destinatário. Quando uma estação recebe um pacote, ela analisa o campo destinatário e se o pacote for endereçado para ela mesma ela o processará, ao passo que se for destinado a outra máquina ela o ignorará.

As **redes ponto a ponto** são tecnologias de transmissão de dados que utilizam uma mídia não compartilhada para conectar pares de computadores. Embora haja exceções, geralmente redes menores LAN's tendem a usar a tecnologia de difusão e as maiores MAN's e WAN's os sistemas ponto a ponto.

Existem diversas tecnologias de redes estando a Ethernet, FDDI, ATM e *Token Ring* dentre as mais populares. Cada tecnologia de Rede Local possui critérios distintos de projeto e desta forma várias topologias de rede estão atualmente em uso.

2.1 Topologias de Rede

Segundo [COELHO, 2003], existem dois tipos de topologia empregada nas redes locais. A **topologia física** refere-se à forma física de como interligar os computadores e a **topologia lógica**, também chamada de método de acesso, se refere ao aspecto de funcionamento das redes, determinando como as mensagens são transmitidas no meio físico de um dispositivo para outro.

As topologias físicas mais comuns são as topologias em Barramento, Estrela e Anel. Destas três topologias foram criadas topologias híbridas sendo as mais comuns a Malha, Árvore e a Estrela hierárquica [COELHO, 2003].

2.1.1 Topologia em Barramento

Uma rede que utiliza esta topologia, basicamente consiste de um cabo central onde as estações estão interligadas. Qualquer estação conectada ao barramento pode enviar sinais através do cabo e todas as estações recebem o sinal.

Segundo [MUELLER, 2003] um barramento possui também características de topologia lógica pois, do ponto de vista dos dispositivos, todas as outras estações se comunicam através do mesmo caminho compartilhado. Devido ao fato que esta é uma tecnologia de mídia compartilhada, mecanismos de arbitragem de tráfego precisam ser disponibilizados.

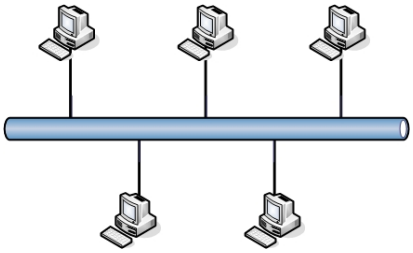

Figura 2.1: Topologia em Barramento

2.1.2 Topologia em Estrela

A topologia em estrela é uma estrutura onde cada nó da rede possui uma mídia de transmissão dedicada que é conectada a um ponto central [MUELLER, 2003].

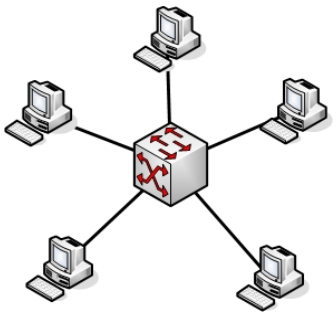

Figura 2.2: Topologia em Estrela

O formato em estrela lembra os raios de uma roda e devido a este fato o centro da rede com topologia em estrela é chamado Hub (centro). Um Hub típico consiste de um dispositivo eletrônico que recebe dados de uma estação transmissora e o entrega ao destino apropriado [COMER, 1999].

Cada dispositivo da rede utiliza uma conexão ponto-a-ponto ao Hub. Na prática, redes em estrela raramente possuem um formato simétrico na qual um Hub está localizado em uma distância igual a todas as estações.

As tecnologias de rede mais populares utilizam a topologia em estrela na sua implementação física devido a fatores que incluem facilidade de cabeamento, facilidade de remoção de uma estação problemática e a facilidade de configuração dos Hubs.

2.1.3 Topologia em Anel

Uma rede que utiliza uma topologia em anel dispõe as estações a serem conectadas em um loop fechado - um cabo conecta o primeiro computador no segundo computador, outro cabo conecta o segundo computador no terceiro, e assim por diante até que um cabo conecta o último computador de volta ao primeiro [COMER, 1999].

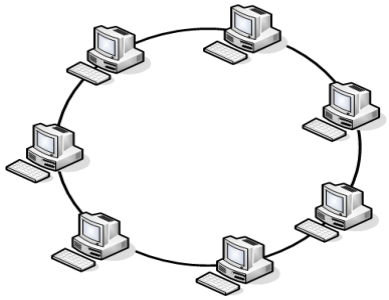

Figura 2.3: Topologia em Anel

Em uma topologia em anel, o acesso à rede é controlado através de uma token que é repassada de nó em nó como um mecanismo de arbitragem. Cada nó que tem o turno reivindica a token quando ela passa nas suas proximidades e este, quando de posse da token, tem a permissão de transmitir através do anel. Um pacote de dados é transferido de um nó para o próximo até que ele alcance o seu destino. Após o nó destino ter recebido o pacote, ele o modifica confirmando a sua recepção e o passa para frente.

Eventualmente o pacote percorre o círculo completamente e o nó transmissor recebe a confirmação de recebimento do pacote por parte do nó receptor. Quando o nó transmissor é finalizado, ele libera a token para seus vizinhos, e o processo se repete [MUELLER, 2003].

2.1.4 Topologias Híbridas

Cada topologia possui suas vantagens e desvantagens. As topologias híbridas foram desenvolvidas para resolverem necessidades específicas.

A **topologia em malha** é uma topologia onde múltiplas conexões são feitas entre os vários nós. Tipicamente a topologia em malha tem somente o propósito de garantir a redundância da rede. Exceto para redes pequenas, uma rede em malha completa não é muito utilizada devido ao seu alto custo pois cada nó da rede, possui uma conexão com cada outro nó pertencente a mesma rede.

A **topologia em árvore** é utilizada para estender os limites físicos da topologia em barramento. A **topologia em estrela hierárquica** é utilizada em sistemas de cabeamento estruturado. A idéia é um elemento que centraliza todo o gerenciamento de serviços, conexões e informações, mas mantém a independência em cada ponto [COELHO, 2003].

2.2 Redes Locais

[JACK, 2003], de uma forma geral, define uma Rede Local ou LAN *(Local Area Network)* como sendo qualquer rede, que conecta dois ou mais computadores ou dispositivos relacionados, localizados dentro de uma área geograficamente limitada (até uns poucos quilômetros).

As Redes Locais surgiram dos ambientes de institutos de pesquisa e universidades. O enfoque dos sistemas de computação que perduravam durante a década de 70, levava em direção à distribuição do poder computacional. Redes Locais surgiram para viabilizar a troca e o compartilhamento de informações e dispositivos periféricos (recursos de hardware e software), preservando a independência das várias estações de processamento e permitindo a integração em ambientes de trabalho cooperativo.

Pode-se caracterizar uma rede local com sendo uma rede que permite a interconexão de equipamentos de comunicação de dados numa pequena região que possuem distâncias entre 100m e 25km, embora as limitações associadas às técnicas utilizadas em redes locais não imponham limites a essas distâncias. Outras características típicas encontradas e comumente associadas às redes locais são as altas taxas de transmissão (de 0,1 a 100Mbps) e baixas taxas de erro (1 bit em cada 10^8 a 10^{11} bits transmitidos).

2.3 Redes de Campus

A definição de Rede de Campus nunca foi clara, mas uma bastante comum é a de um grupo de segmentos LAN localizados em um prédio ou grupo de prédios que estão interconectados de modo a formar uma rede. Estes segmentos LAN, tipicamente utilizam tecnologia Ethernet, Token Ring, FDDI ou ATM. O tamanho

de uma Rede de Campus não é definido, mas ela começa a tomar forma à medida que sai de um edifício e se difunde por um perímetro que engloba diversos outros edifícios como é o caso de um campus universitário [JACK, 2003].

Ainda segundo [JACK, 2003], o principal desafio do administrador de rede é fazer uma rede de campus funcionar eficientemente e efetivamente. Para alcançar este objetivo, é necessário conhecer a rede de campus tradicional, procurando entender as suas limitações, bem como aproveitar os benefícios das redes de campus emergentes.

2.3.1 Redes de Campus Tradicionais

Em 1990 as Redes de Campus Tradicionais surgiram como uma LAN que progrediu e cresceu de modo que foi necessária a sua segmentação apenas para mantê-la ativa e operando. Nesta época de rápida expansão, o tempo de resposta era uma preocupação secundária e era desejável apenas a garantia de que a rede estivesse funcionando.

Segundo [JACK, 2003], manter uma rede de campus típica funcionando em uma mídia 10BaseT é um desafio. Como resultado desta e outras limitações bem como o seu rápido crescimento, uma Rede de Campus possui um grande e único domínio de colisão - sem mencionar também um grande e único domínio de difusão. Fora essas limitações, a tecnologia Ethernet foi a mais utilizada por ser a mais escalável, eficaz e barata quando comparada a outras opções.

Como as Redes de Campus podem facilmente agregar vários edifícios, bridges são utilizadas para interconectá-los, isto de certa forma quebra os domínios de colisão, mas a rede continua possuindo um grande domínio de difusão. Com o passar do tempo, mais e mais usuários são anexados á rede o que rapidamente acarretará na queda do seu desempenho [JACK, 2003].

2.3.2 Problemas inerentes às Redes de Campus Tradicionais

[JACK, 2003] afirma que disponibilidade e performance são os maiores problemas encontrados nas Redes de Campus Tradicionais. Disponibilidade é afetada pelo número de usuários tentando acessar a rede ao mesmo tempo somada com a credibilidade da mesma. Os problemas mais comuns e que contribuem para a queda no desempenho das Redes de Campus Tradicionais incluem colisões, largura de banda, *broadcasts*.

1) Colisões

O efeito de dois nós enviando sinais de transmissão simultaneamente em um mesmo meio é chamado colisão. Quando estes sinais se encontram no meio (mídia de transmissão), os *quadros* de cada nó colidem e se danificam.

O **domínio de colisão** consiste na área onde todos os dispositivos que estão inseridos no mesmo perímetro, precisam competir pela mídia compartilhada e neste sentido, estão susceptíveis a colisões quando na transmissão de dados.

Uma Rede de Campus típica surgiu de um grande domínio de colisão. Desta forma todos os dispositivos podem se comunicar ao mesmo tempo e às vezes colisões podem ocorrer entre eles. Se um dispositivo passa a apresentar problemas (do tipo transmissão continua de quadros com erros), neste contexto, ele pode derrubar uma rede inteira.

Devido ao alto custo dos roteadores na década de 80, *bridges* foram utilizadas para separar os domínios de colisão em pequenos segmentos. De certa forma houve uma melhora para os problemas relacionados aos domínios de colisão, mas a rede continuaria a possuir um grande domínio de difusão e os mesmos problemas relacionados a ele.

2) Largura de Banda

Largura de banda é a faixa de freqüência que um circuito é capaz de transportar. É uma medida de capacidade de transmissão de um sistema que é influenciada pelas propriedades do material utilizado na mídia de transmissão. Quanto maior a taxa de transmissão, maior deverá ser a largura de banda [COELHO, 2003].

Quando o número de estações aumenta em um segmento, cada estação adquire uma pequena porção da banda disponível no seu segmento de rede. O congestionamento em um segmento acontece quando muitos dispositivos estão tentando utilizar a mesma banda.

A largura de banda é atualmente dividida pelo número de estações transmissoras. A simples conexão de uma estação não consome largura de banda até que o dispositivo inicie a sua transmissão. Quando uma estação transmite em uma rede e todas as outras estações apenas escutam, temos, neste caso, uma largura de banda dedicada a uma única estação, pois nenhum outro dispositivo pode transmitir. Por outro lado, se o transmissor nunca sofre com colisões e pode transmitir a qualquer momento, ele o faz a taxa total da mídia de comunicação [CLARK, *et.Al.*,1999].

A largura de banda de um segmento determina a quantidade de dados que podem ser transmitidos em uma mídia em um determinado instante. A capacidade máxima de transmissão da mídia de comunicação e a distância entre os dispositivos influenciam na largura de banda. O sinal digital precisa respeitar um valor e um fluxo de transmissão mínimo e constante o que do contrário prejudicaria o recebimento dos dados pelos elementos ativos da rede.

A largura de banda tem sido apontada como a principal variável que limita a quantidade e a velocidade da circulação da informação dentro e principalmente fora das redes corporativas (Internet).

3) Broadcasts

Um *Broadcast*[1] é um frame de dados (quadro) que é transmitido para todo nó no segmento de rede formado pelo seu domínio de difusão. O **domínio de difusão** ou domínio de *broadcast* consiste na área onde todos os dispositivos que estão inseridos em um mesmo perímetro, estão sujeitos ao recebimento de pacotes de difusão (pacotes de *broadcast*).

Praticamente todos os protocolos possuem a característica de *broadcast*, mas alguns protocolos podem realmente causar problemas se não estiverem configurados corretamente a citar, por exemplo, o *Internet Protocol* (IP), *Address Resolution Protocol* (ARP), *Network Basic Input Output System* (NetBIOS) e o *Routing Information Protocol* (RIP).

As estações enviam pacotes de *broadcast* por diversos motivos. Alguns protocolos de rede de alto nível usam quadros de *broadcast* como parte de seu processo de descoberta de endereço. *Broadcasts* também são usados para a atribuição dinâmica de endereço, o que normalmente acontece quando uma estação é ligada inicialmente e precisa encontrar um endereço de rede de alto nível para iniciar as comunicações (DHCP).

Multicasts podem ser usados por certos aplicativos de multimídia, que enviam dados de áudio e vídeo em quadros de *multicast* para serem recebidos por grupos de estações. Também podem ser usados por jogos multi-usuários como um meio de enviar dados para o grupo de jogadores. Portanto, uma rede típica sempre terá algum nível de quadros de *broadcast*.

Quando um host necessita se comunicar com a rede inteira, ele envia um *datagrama* para o endereço MAC 0xFFFFFFFF (*broadcast*), um endereço o qual a interface de rede de cada host precisa responder [BOYLES, *et.Al.*,1999].

A acumulação de tráfego *broadcast* oriundo de cada dispositivo na rede é chamado *broadcast storm* (tempestade de *broadcast*). Tempestades de quadros de difusão podem ser causadas não apenas por excesso de máquinas ou de tráfego de difusão em um domínio de difusão na rede, mas também, devido a problemas do tipo falha no protocolo de árvore de cobertura, curto tempo de envelhecimento da cache ARP em muitos equipamentos da rede, defeitos em equipamentos ou placas de rede ou mesmo aplicações com erro de programação [LOPES, *et.Al.*, 2000].

Ao ler um pacote, uma interface de rede precisa interromper a CPU para processar cada quadro de difusão, e desta forma uma *broadcast storm* não só contribui para o saturamento dos segmentos da rede como também afeta diretamente o desempenho dos *hosts*. Muito frequentemente o *host* não se beneficia com o processamento de *broadcast* - em outras palavras ou o *host* não é o destinatário procurado, ou ele não está envolvido com o serviço que requisitou a sua atenção ou realmente ele já está envolvido com o serviço em questão. Altos

[1] Existe uma outra forma de *broadcast* chamada *Multicast* destinado a um grupo específico de usuários

níveis de *broadcast* podem degradar a performance do *host* de forma considerável [BOYLES, *et.Al.*,1999], além de reduzir a quantidade de banda utilizável para o usuário final [ODOM, 2001].

As *broadcast storm* emanadas pelos elementos ativos da rede, mostra que é necessário limitar o número total de estações ligadas por eles através de um mesmo segmento para que a taxa de *broadcast* não fique tão alta a ponto de se tornar um problema [SPURGEON, 2000].

2.3.3 A Regra 80/20

As Redes de Campus Tradicionais alojam usuários e servidores no mesmo plano. Nesta concepção de rede, os usuários podem utilizar os serviços de rede e realizar o compartilhamento de recursos sem sair do âmbito local.

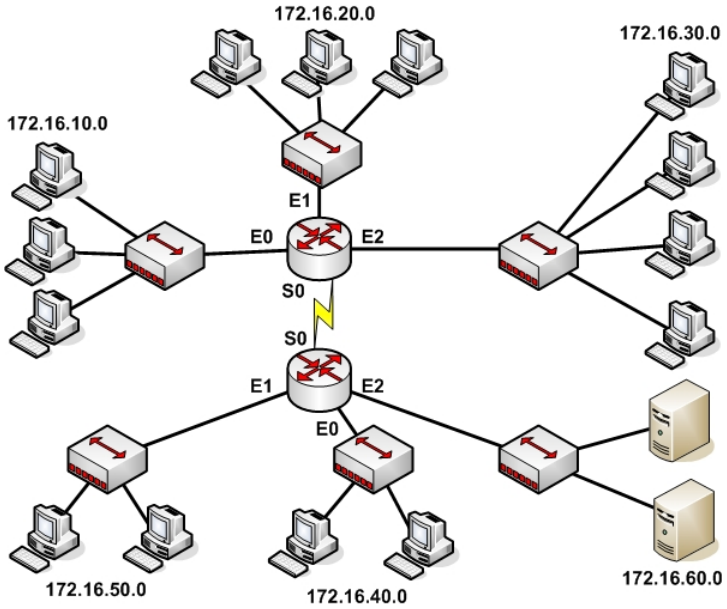

Figura 2.4: Rede de Campus Tradicional que segue a Regra 80/20

A regra a ser seguida para o estabelecimento deste tipo de rede é chamada de Regra 80/20 pelo fato de que 80% do tráfego dos usuários supostamente permanecem no segmento da Rede Local e supõe-se que somente 20% ou menos atravesse os roteadores ou bridges para alcançar os outros segmentos da rede [JACK, 2003].

Se mais de 20% do tráfego atravessa os dispositivos de segmentação os problemas de desempenho da rede aparecem. Ao seguir a Regra 80/20, o desempenho da rede é garantido se todos os recursos disponibilizados aos usuários (servidores,

impressoras, diretórios compartilhados e aplicações de rede), estiverem contidos no segmento das suas respectivas Redes Locais [JACK, 2003].

2.3.4 O Novo Modelo de Redes de Campus

As mudanças nos requerimentos das aplicações combinados com os problemas inerentes às Redes de Campus Tradicionais (colisões, largura de banda e *broadcasts*), levaram a estruturação de um novo projeto de Rede de Campus. A alta demanda dos usuários e aplicações cada vez mais complexas, obrigou os projetistas de rede a repensarem os padrões de tráfego ao invés de resolver problemas isolados em um departamento.

Segundo [JACK, 2003], não se deve apenas pensar na criação de sub-redes e na inserção de cada departamento em uma sub-rede. O ideal é possibilitar para os usuários a facilidade de se alcançar todos os serviços da rede. É desejável também atentar-se aos padrões de tráfego além de se buscar soluções para os problemas relacionados à largura de banda. Isto pode ser realizado com técnicas avançadas de roteamento e comutação através de switchs. O acesso aos serviços da rede ficaria definido da seguinte forma:

Serviços Locais

São os serviços de rede que estão localizados na mesma sub-rede ou rede que os usuários acessam. Os usuários não atravessam os dispositivos de nível 3 e estes serviços de rede estão localizados no mesmo domínio de difusão dos usuários. Este tipo de tráfego nunca deve cruzar o backbone.

Serviços Remotos

Estão perto dos usuários mas não estão localizados na mesma rede ou sub-rede. Os usuários precisam atravessar dispositivos de nível 3 para se comunicarem com os serviços da rede. Entretanto eles não devem atravessar o backbone.

Serviços Avançados

São definidos como serviços que são disponibilizados a todos os usuários da rede. Switches de nível 3 ou roteadores, são necessários neste cenário pelo fato de que um serviço avançado precisa estar restrito a camada central da rede. Exemplos destes tipos de serviço incluem acesso a Internet, e-mail e vídeo conferência. Quando servidores de serviços avançados são colocados próximo ao backbone, os dados dos usuários precisam cruzá-lo para que se possa ter acesso a estes serviços.

2.3.5 A Regra 20/80

Com as novas aplicações baseadas na web, uma estação cliente pode a qualquer instante ser um receptor ou transmissor de informações.

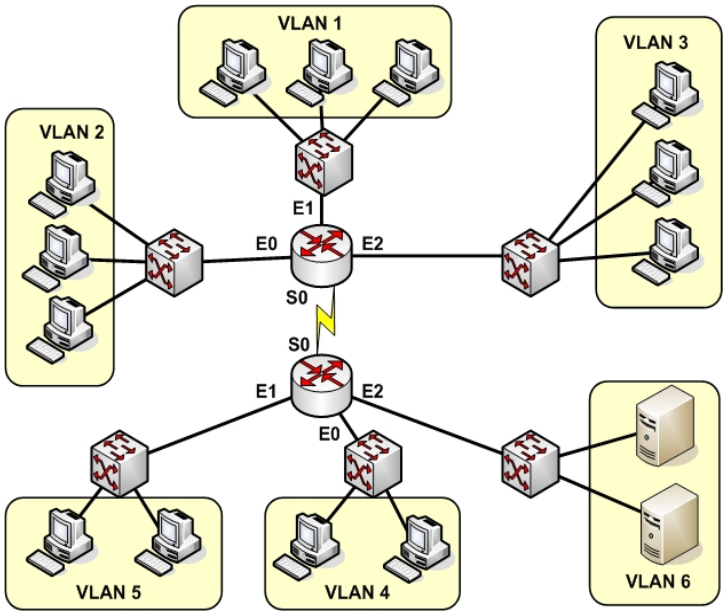

Figura 2.5: Uma Rede de Campus que segue a Regra 20/80

A utilização de servidores de aplicações remotas e a criação de *Server Farms*[2], mostram que a antiga Regra 80/20 está obsoleta e susceptível a falhar neste ambiente [JACK, 2003].

Praticamente todo o tráfego precisa cruzar o backbone do campus, e neste contexto podemos encontrar uma nova regra chamada Regra 20/80. De acordo com esta regra, 20% do que o usuário acessa na rede é local, enquanto que 80% dos acessos atravessam os pontos de segmentação da rede com a intenção de encontrar os demais serviços.

O problema da Regra 20/80 não está relacionado com o cabeamento e a topologia da rede e sim com os seus próprios equipamentos de interconexão que precisam estar hábeis a manipular uma grande quantidade de pacotes de forma rápida e eficiente.

[2]Ambientes que têm a intenção de centralizar os serviços e recursos da rede buscando-se segurança, redução de custos e melhoria nos processos administrativos

Capítulo 3

Padrão Ethernet

O padrão Ethernet é um dos mais populares protocolos e esquemas de cabeamento de rede utilizados atualmente. Sua arquitetura é baseada na mídia de comunicação compartilhada e seus elementos são provenientes dos estudos realizados em 1980 pelo consórcio de empresas Xerox, Intel e Digital Equipment Corporation que conceberam uma tecnologia de rede chamada DIX Ethernet. Em 1985 a IEEE[3] procurando desenvolver padrões de rede não proprietários, realizou algumas modificações no padrão DIX e criou o padrão 802.3 CSMA/CD mais conhecido como padrão Ethernet.

Na sua primeira versão (Ethernet 1.0 e 2.0) utilizava topologia em barramento onde os nós da rede eram conectados a um cabo coaxial grosso *Thick Ethernet* ou fino *Thin Ethernet*. A partir do padrão 802.3 esta tecnologia passou a utilizar além da topologia em barramento a topologia em estrela podendo utilizar o cabo par trançado ou a fibra óptica como mídia de comunicação.

A tecnologia Ethernet juntamente com suas variantes definidas no padrão IEEE 802.3, são atualmente as arquiteturas de redes locais mais utilizadas e suas vantagens incluem :

- Facilidade de instalação a um custo moderado;
- A tecnologia é muito bem conhecida e está disponível a partir de várias fontes;
- O padrão oferece grande diversidade de opções de cabeamento;
- Eficiente em redes que possuem altos níveis de tráfego que ocorrem em períodos não constantes.

Segundo [FEIBEL, 1996] uma rede Ethernet possui as seguintes características:

- Trabalha diretamente nas duas camadas mais baixas do modelo de referência TCP/IP: As camadas Enlace e Rede;

[3] *Institute of Electrical and Eletronics Engineers*

- Utiliza topologia em barramento (padrões Ethernet 1.0 e 2.0). O padrão 802.3 utiliza topologia em barramento ou estrela;
- Pode operar nas seguintes velocidades :
  - 10Mbps (10Base5, 10Base2, 10BaseT, 10BaseF);
  - 100Mbps (100BaseT, 100BaseTX, 100BaseFX, 100BaseT2);
  - 1000Mbps (1000BaseSX, 1000BaseLX, 1000BaseCX, 1000BaseT);
  - 10Gbps (Em fase de desenvolvimento).
- Utiliza o método de acesso ao meio CSMA/CD *Carrier Sense Multiple Access with Collision Detection* baseado na detecção de colisão (especificado como parte do documento do padrão IEEE 802.3);
- Transmissões *Broadcast*;
- É uma tecnologia de rede do tipo banda base (indicada para transmissões a distâncias curtas) embora suas variantes suportarem redes de banda larga.

3.1 O Quadro Ethernet

O núcleo do sistema Ethernet é o seu quadro. Os bits no quadro Ethernet são distribuídos em campos especificados conforme é mostrado na figura 3.1 abaixo :

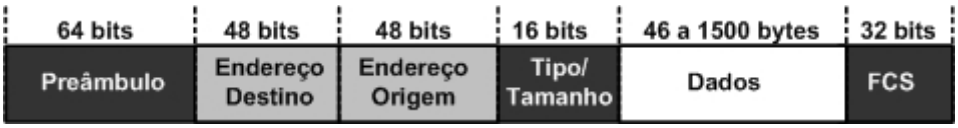

Figura 3.1: O quadro ethernet

O primeiro campo do quadro, **Preâmbulo**, dá a todo dispositivo de um sistema Ethernet de 10Mbps, um tempo de partida de sinal. Este tempo é útil pois permite que o dispositivo possa reconhecer que um quadro está sendo transmitido, e desta forma se prepare para o recebimento dos dados. Os sistemas Ethernet mais recentes, rodando a 100 e 1000Mbps, utilizam sinalização constante, que evita a necessidade de um preâmbulo. No entanto, o preâmbulo ainda é transmitido nesses sistemas, para evitar mudanças na estrutura do quadro [SPURGEON, 2000].

Após o preâmbulo estão os **Endereços de Destino** e **Origem** utilizados para armazenar os endereços MAC das interfaces de comunicação origem e destino respectivamente. A atribuição destes endereços é controlada pela IEEE *Standarts Association*(IEEE-SA). Ao atribuir blocos de endereço para serem usados pelos fabricantes de rede, a IEEE-SA oferece um código OUI (*Organization Unique Indentifier*) de 24-bits que é exclusivo a cada organização que fabrica interfaces

de rede. Isto favorece a construção de NICs (*Network Interface Cards*) com endereços de hardware exclusivos para cada interface montada. Este processo evita o problema de que duas ou mais interfaces Ethernet em uma rede tenham o mesmo endereço.

Um fabricante de interfaces cria um endereço Ethernet exclusivo de 48-bits para cada interface usando o seu OUI para os 24-bits iniciais do endereço e mais 24-bits atribuídos pelo próprio fabricante. O endereço de 48-bits resultante normalmente é chamado de endereço de *hardware* (ou endereço físico) ou mais comumente endereço MAC (*Media Access Control*), pois o sistema de controle de acesso à mídia Ethernet inclui o quadro e seu endereçamento [SPURGEON, 2000].

O campo de **Tipo** ou **Tamanho** possui 16-bits e normalmente são utilizados para identificar qual tipo de protocolo de rede de alto nível está sendo transportado no campo de dados (por exemplo TCP/IP) ou informações de tamanho (em número de octetos) do campo dados.

Após o campo de tipo, pode aparecer de 46 a 1500 bytes de dados. O campo de **Dados** precisa ter pelo menos 46 bytes o que garante que os sinais do quadro permanecerão na rede por tempo suficiente para que cada estação do segmento possa escutar o quadro dentro dos limites de tempo corretos. É neste campo, que são transportados os dados da aplicação e as informações oriundas dos protocolos de alto nível.

O último campo do quadro **FCS** (*Frame Check Sequence*), contém um CRC (*Cyclic Redundancy Checksum*), que fornece uma verificação da integridade dos dados no quadro inteiro.

Capítulo 4

TCP/IP

O conjunto de protocolos TCP/IP permite que computadores de todos os tamanhos, dos mais diferentes fabricantes, rodando sistemas operacionais totalmente diferentes, possam se comunicar entre si. Do que iniciou no final da década de 60 como um projeto de pesquisa financiado pelo governo para redes de comutação, foi na década de 90, transformado no protocolo de redes mais utilizado na comunicação entre computadores. O protocolo TCP/IP é essencialmente um sistema aberto na sua definição de conjunto de protocolos e muitas das suas implementações estão publicamente disponíveis [STEVENS, 1993].

Protocolos de rede são normalmente desenvolvidos em camadas, onde cada camada é responsável por facetas diferentes na comunicação. Uma suíte de protocolos ou um conjunto de protocolos, como o TCP/IP, é uma combinação de protocolos diferentes em cada camada. TCP/IP é normalmente considerado como um sistema de 4 camadas definidos como na figura 4.1 abaixo:

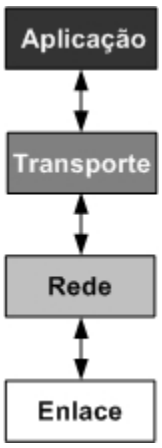

Figura 4.1: As quatro camadas da suíte de protocolos TCP/IP.

Cada camada possui uma responsabilidade diferente [STEVENS, 1993]:

1. A camada de **Enlace**, as vezes chamada Link de Dados (*Data Link*) ou simplesmente *Link*, normalmente inclui o *driver* de dispositivo no sistema operacional e a sua interface de rede correspondente no computador. Juntos eles tratam todos os detalhes de hardware, e a comunicação física com a mídia de transmissão utilizada;

2. A camada de **Rede** (ás vezes chamada de camada internet ou Inter-rede) trata do movimento dos pacotes (ou *datagramas*) na rede. O roteamento de pacotes ocorre nesta camada. IP (*Internet Protocol*), ICMP (*Internet Control Message Protocol*), e IGMP (*Internet Group Management Protocol*) fazem parte da camada de rede no suíte de protocolos TCP/IP;

3. A camada de **Transporte** determina o fluxo de dados entre os hosts, para a camada de aplicação localizada acima. Na suíte de protocolos TCP/IP existe dois protocolos de transporte diferentes: TCP (*Transmission Control Protocol*) e UDP (*User Datagram Protocol*).

   - **TCP** cuida do fluxo de dados confiável entre dois hosts. Ele se preocupa com tarefas do tipo, repartir os dados que passam por ele vindos da camada de aplicação em pedaços de tamanho apropriado para a camada de rede, reconhecer pacotes recebidos ajustando *timeouts* para garantir o reconhecimento de pacotes que enviou, etc. Devido a este fluxo de dados confiável proporcionado pela camada de transporte, a camada de aplicação pode ignorar estes detalhes.
   - **UDP**, por outro lado, fornece um serviço mais simples para a camada de aplicação. Ele apenas envia pacotes de dados de um host para outro, mas ele não garante que estes pacotes alcançarão o seu destino. Qualquer recurso de confiabilidade que seja desejado, precisa ser adicionado à camada de aplicação.

4. A camada de **Aplicação**, cuida dos detalhes de uma aplicação em particular. Existem várias aplicações TCP/IP algumas delas estão listadas abaixo:

   - Telnet, para conexão remota;
   - FTP (*File Transfer Protocol*), protocolo de transferência de arquivo;
   - SMTP (*Simple Mail Tranfer Protocol*), para correio eletrônico;
   - SNMP (*Simple Network Management Protocol*), para gerenciamento de redes;

Cada camada possui um ou mais protocolos para comunicação com seu par, localizados na mesma camada no *host* origem e no *host* destino. Um protocolo, por

exemplo, permite que duas camadas TCP possam se comunicar, e outro protocolo permite que duas camadas IP possam se comunicar.

Normalmente a camada de Aplicação é um processo do usuário enquanto as outras três camadas são usualmente implementadas no *kernel* (o sistema operacional). Outra diferença entre a camada de Aplicação e as outras três camadas é que esta se preocupa com os detalhes da aplicação e não com o movimento dos dados através da rede. As outras três camadas não sabem nada a respeito da aplicação, mas cuidam de todos os detalhes de comunicação.

A figura 4.2 mostra um exemplo de quatro protocolos diferentes cada um em sua camada específica. FTP é um protocolo da camada de Aplicação, TCP é um protocolo da camada de Transporte, IP é um protocolo da camada de Rede e o protocolo Ethernet opera na camada de Enlace [STEVENS, 1993].

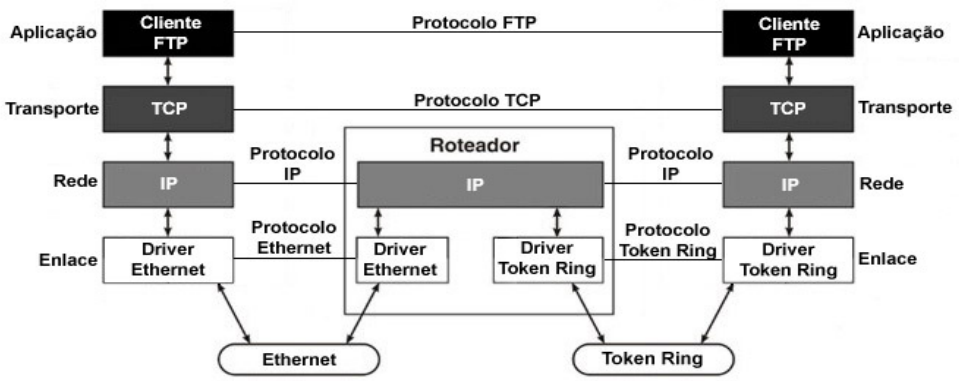

Figura 4.2: Os protocolos em sua camada específica.

O propósito da camada de Rede e da camada de Aplicação são óbvios - o primeiro cuida dos detalhes da mídia de comunicação enquanto o segundo trata uma aplicação específica do usuário (FTP, Telnet, etc.). O roteador é o equipamento utilizado para conectar uma rede a internet. Os roteadores podem proporcionar conexões dos mais diferentes tipos de rede.

4.1 Endereços IP

Cada interface na internet precisa ter um endereço único chamado endereço IP. Os IPs são endereços de 32-bits. Em vez de utilizar endereços planos, o endereço IP utiliza um sistema hierárquico de endereços. A figura abaixo mostra cinco classes diferentes de endereços IP:

Estes endereços de 32-bits são normalmente escritos em quatro números decimais, um para cada byte do endereço. Para sabermos em que classe um endereço

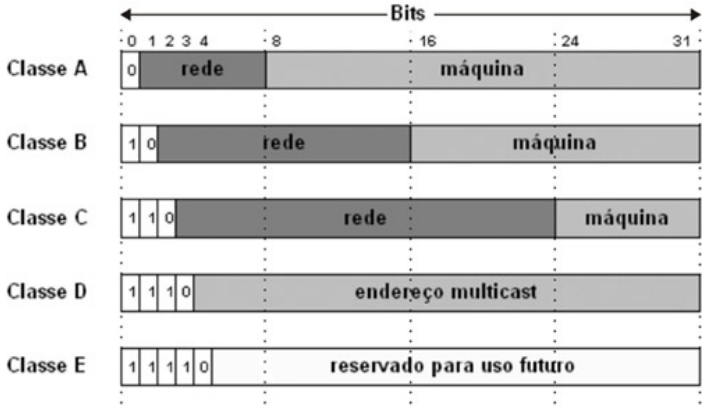

Figura 4.3: As cinco classes de endereços IP.

IP está localizado, devemos olhar o primeiro campo do endereço. A figura 4.3 abaixo mostra as diferentes classes, com o primeiro número em negrito.

Classe	Limite
A	**0**.0.0.0 à **127**.255.255.255
B	**128**.0.0.0 à **191**.255.255.255
C	**192**.0.0.0 à **223**.255.255.255
D	**224**.0.0.0 à **239**.255.255.255
E	**240**.0.0.0 à **247**.255.255.255

Figura 4.4: Faixa de endereços IP por classe.

Endereços privados são definidos na RFC1918 "*Address Allocation for Private Internets*", que compreende um conjunto de endereços IP que não são globalmente alocados e podem ser utilizados internamente por qualquer organização. Os endereços privados surgiram como uma alternativa à suprir a escassez de endereços IP.

Classe	Limite
A	10.0.0.0 à 10.255.255.255
B	172.16.0.0 à 172.31.255.255
C	192.168.0.0 à 192.168.255.255

Figura 4.5: Endereços IP privados.

Os pacotes que possuem este endereço nunca devem ter a permissão para sair diretamente da rede de uma corporação e trafegar pela Internet. Para permitir

aos *hosts* que utilizam estes endereços privados a comunicação com a internet, o roteador da rede corporativa executa um recurso chamado **NAT** (*Network Address Translation*).

O NAT, intercepta pacotes com endereços privados e re-escreve os endereços da fonte utilizando um endereço IP real e às vezes um número de porta de origem diferente. O NAT mantém uma tabela dos mapeamentos que fez entre os pares endereço/porta origem interno e externo de modo que a tradução possa ser realizada em sentido contrário quando os pacotes de resposta chegam da Internet. A utilização do NAT permite que várias comunicações sejam multiplexadas em um único endereço IP real, de modo que este possa ser compartilhado com vários clientes [NEMETH, *et.Al.*, 2001].

4.1.1 Máscara de sub-rede

Em adição ao endereço IP, um *host* também precisa saber quantos bits estão sendo utilizados para a ID da sub-rede e quantos bits são destinados à ID do *host*. A máscara de sub-rede é o endereço que determina estes limites. Esta máscara possui uma faixa de 32 bits contendo bits 1 para a ID da rede e da sub-rede, e bits 0 para a ID do *host*.

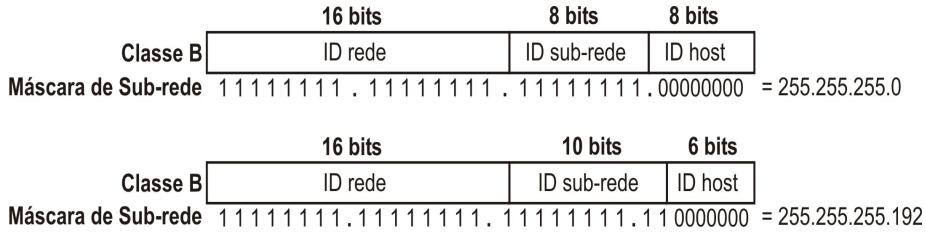

Figura 4.6: Exemplo de uma máscara de sub-rede com duas disposições de classe B diferentes

Embora estes endereços IP sejam normalmente escritos em notação ponto-decimal, as máscaras de sub-rede são frequentemente escritas em hexadecimal, especialmente se seus limites não são limites de byte, e por esta razão a máscara de sub-rede é uma máscara bit.

Um *host*, dado seu IP e sua máscara de sub-rede, pode determinar se um datagrama IP é destinado para (1) um *host* na sua própria sub-rede, (2) um *host* em uma sub-rede diferente localizado na sua própria rede ou (3) um *host* em uma rede diferente. Ao interpretarmos o endereço IP, temos a indicação da sua classe de endereçamento que mostra os limites entre a ID da rede e a ID da sub-rede. A máscara de sub-rede indica os limites entre a ID da sub-rede e a ID do *host*.

4.2 Encapsulamento

Quando uma aplicação transmite um conjunto de dados usando o protocolo TCP, o mesmo é enviado de cima para baixo na pilha de protocolos, passando por cada uma das camadas, antes de enviar um fluxo de bits através da rede. Cada camada acrescenta no começo dos dados que recebeu um cabeçalho (às vezes também adiciona informações ao final). A figura 4.6 mostra este processo.

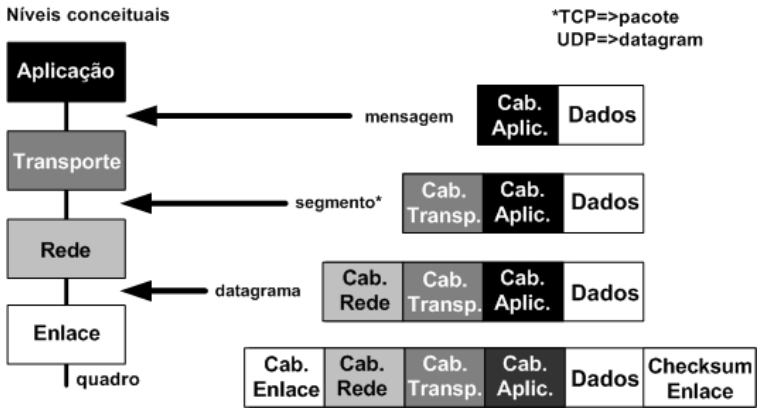

Figura 4.7: Processo de encapsulamento.

A unidade de dados que o protocolo TCP envia para o protocolo IP é chamado de **segmento TCP**. A unidade de dados que o protocolo IP envia para a interface de rede é chamada **datagrama IP**. O fluxo de bits que flui pela mídia de comunicação é chamado **quadro** (*frame*) [STEVENS, 1993].

Quando um datagrama IP é encapsulado em um *frame*, o mesmo é colocado na sua área de dados. O transmissor e o receptor devem combinar o valor utilizado no campo tipo do frame e desta forma, o receptor saberá que a área de dados contém um datagrama IP. Ao adicionar o datagrama na área de dados, o processo de encapsulamento requer que o transmissor forneça o endereço MAC do próximo computador para o qual o datagrama precisa ser enviado. Este procedimento é realizado pelo protocolo *ARP* que tem a função de traduzir o endereço IP do próximo *hop* em um endereço MAC equivalente que é utilizado como endereço destino no cabeçalho do frame [COMER, 1999].

Ao alcançar o *host* destino o frame sofre o desencapsulamento que é o processo onde o frame sobe da camada de Enlace, passando pelas camadas intermediárias até alcançar a camada de Aplicação. Cada camada lê e retira o conteúdo do seu cabeçalho, até que a mensagem possa ser entregue para a aplicação correspondente.

4.3 ARP (*Address Resolution Protocol*)

Quando dois dispositivos baseados em IP localizados no mesmo segmento de rede desejam se comunicar, eles o fazem utilizando protocolos de baixo nível e mecanismos específicos de endereçamento definidos pela tecnologia utilizada.

O padrão Ethernet, por exemplo, é formado por endereços de 48-bits. Para que sistemas IP possam se comunicar entre si, eles primeiramente precisam ser capazes de identificar os endereços MAC dos outros dispositivos localizados no mesmo segmento de rede. Neste caso, é necessário um protocolo que possa associar um endereço proprietário de uma interface, ao seu endereço IP correspondente (que possui tamanho de 32-bits). Este serviço é realizado pelo protocolo de resolução de endereços ou ARP (*Address Resolution Protocol*) [HALL, 2000].

A RFC826 "*An Ethernet Address Resolution Protocol*"introduziu os conceitos do protocolo ARP como um caminho útil para que os dispositivos possam localizar o endereço MAC Ethernet de outro *host* IP localizado na mesma rede local. ARP também é útil para vários tipos de tecnologias de rede - não apenas Ethernet - e vem sendo incorporado em muitas outras tecnologias.

Todas as mídias LAN - e muitas mídias WAN - agora utilizam ARP para localizar os endereços de hardware de outros dispositivos IP dentro da rede local. Quando um dispositivo precisa enviar um pacote IP para outro dispositivo na rede local, o programa IP primeiro verifica se o dispositivo conhece o endereço MAC associado com o endereço IP destino. Neste caso, o transmissor apenas transmite os dados para o destinatário, utilizando os protocolos e endereços apropriados para a mídia de comunicação utilizada pelos dois dispositivos [HALL, 2000].

Entretanto, se o endereço MAC do destinatário não for conhecido, o programa IP precisa localizá-lo antes que qualquer dado possa ser enviado. Neste ponto, o protocolo IP faz uma chamada para o protocolo ARP objetivando localizar o endereço MAC do destinatário.

ARP realiza esta tarefa produzindo um *broadcast* de baixo nível na rede, requisitando que o sistema que utiliza o endereço IP solicitado responda com o seu endereço MAC. O destinatário, caso esteja ativo na rede, responde diretamente ao transmissor à requisição. Pacotes ARP trabalham na camada de Rede, a mesma dos pacotes IP [HALL, 2000].

4.4 RIP (*Routing Information Protocol*)

O RIP é um protocolo de roteamento, definido na RFC1058 "*Routing Information Protocol*". É um antigo protocolo da Xerox que foi adaptado para redes IP. O RIP, é um protocolo de vetor de distância que utiliza contagens de *hops* como métrica de custo [NEMETH, *et.Al.*, 2001].

Em um protocolo de vetor de distância, para cada segmento da rede é atribuído um peso e a distância até um determinado destinatário é definida como sendo a

soma dos pesos através do caminho até ele. Um *hop* envia de tempos em tempos um pacote de comunicação através da rede para seus vizinhos. Cada pacote, contém pares de (endereço destino, distância). Quando um pacote chega a um determinado vizinho, ele o examina e muda a sua tabela de roteamento caso o pacote possua algum caminho mais curto que o valor correspondente contido na sua tabela atual [COMER, 1999].

Para garantir que um roteamento não emperre durante um período de tempo muito longo, o tempo de reenvio deve ser curto exigindo aos *hops* que utilizam este protocolo o envio de *broadcasts* com todas as informações de roteamento em intervalos de 30 segundos.

Na época em que foi criado as redes eram relativamente pequenas e devido a este fato o protocolo RIP considera inacessível qualquer *host* que esteja a 15 ou mais *hops* de distância, não sendo indicado para redes locais que têm mais de 15 roteadores ao longo de um único caminho [NEMETH, *et.Al.*, 2001].

RIP é um protocolo que não carrega informações de máscara de rede em suas atualizações de roteamento e por isso ele é incapaz de suportar "Mascaramento de sub-rede de tamanho variável"ou VLSM (*Variable Length Subnet Masking*) e redes descontínuas.

O RIP-2 definido na RFC2453 "*RIP Version 2*"é uma pequena revisão do RIP e acrescenta suporte a autenticação, habilidade de um roteador anunciar rotas procurando beneficiar outro roteador e a alteração mais importante que é a capacidade de distribuir máscara de rede junto com endereços de próximo *hop* fornecendo assim um melhor suporte para sub-redes.

4.5 NetBEUI (*NetBIOS Enhanced User Interface*)

NetBEUI é um *driver* de dispositivo de rede para a camada de transporte fornecido pelo sistema operacional Windows e suas variantes. *NetBEUI* se comunica com a interface de rede através do driver de dispositivo NDIS (*Network Driver Interface Specification*).

O NetBIOS é uma API (*Application Programming Interface*) de programação do protocolo *NetBEUI* que tem a função de fazer o interfaceamento entre as aplicações e o protocolo *NetBEUI*. O *NetBIOS* pode também ser utilizado em conjunto com outros protocolos permitindo que as aplicações utilizem uma "liguagem"comum para acessarem a rede.

NetBIOS foi projetado para utilização em grupos de computadores, que dividem uma mídia de difusão. Serviços orientados e não orientados à conexão, bem como *broadcasts* e *multicasts* são suportados. Os participantes são identificados por nome sendo estes distribuídos dinamicamente.

Aplicações *NetBIOS* empregam mecanismos *NetBIOS* na localização de recursos, estabelecimento de conexões, envio e recebimento de dados com outro par aplicação e término de conexões.

A Resolução de nome *NetBIOS*, refere-se ao mapeamento do nome *NetBIOS* em um endereço IP. O endereço IP, está diretamente relacionado à localização da interface de rede de um *host* destino.

Um dos métodos de resolução de nomes através do *NetBIOS* é através de *Broadcast* Local. Neste método um pacote UDP é enviado através de *broadcast*, por uma máquina *NetBIOS*, para cada computador localizado no seu segmento de rede, anunciando seu nome. Pelo fato de cada computador no segmento analisar e responder o seu nome ao *host* transmissor, *broadcasts* de *NetBIOS* poderão consumir uma quantidade significativa de largura de banda, especialmente se este for o único método de resolução de nomes em uso [SHINDER, *et.Al.*, 2003].

Ao contrário do protocolo TCP/IP, o *NetBIOS* foi concebido para ser usado em redes de pequeno porte. Devido ao método simples de endereçamento, o *NetBIOS* por ser utilizado em redes com no máximo 255 estações além do fato de que não possui o recurso de enumeração de redes ou seja, para o *NetBIOS*, todas as estações estão ligadas na mesma rede.

Capítulo 5

Equipamentos de Interconexão

Uma rede de computadores é constituída de hospedeiros (estações de trabalho e servidores) e os equipamentos de interconexão que tem a função de favorecer a comunicação entre os hospedeiros.

Segundo [COELHO, 2003], qualquer ambiente de comunicação tem limitações definidas por características próprias de sua tecnologia: distância, número de dispositivos permitidos em um segmento de rede, tráfego, excesso de tráfego e conexão com dispositivos em ambientes remotos são alguns exemplos destes limites.

Existem basicamente três tipos de equipamentos de interconexão:

- Repetidor (também chamado Concentrador, *Hub* ou *Hub* Repetidor);
- Comutador (também chamado *Switch* ou *Hub* Comutador);
- Roteador;

As diferenças entre os tipos de equipamentos ocorrem em várias dimensões:

- Na **escalabilidade**, isto é, no tamanho da sub-rede de comunicação que pode ser concebida com o equipamento: repetidores são usados para montar redes pequenas, comutadores para fazer redes maiores e roteadores para redes ainda maiores;
- No **alcance geográfico** atingível: repetidores e comutadores são usados para redes de campus e roteadores são utilizados tanto em redes de campus quanto em redes de longo alcance;
- Na **camada de protocolo** onde atuam: repetidores atuam na camada de Enlace (nível 1), comutadores na camada de Rede (nível 2) e roteadores na camada de Transporte (nível 3);
- No **preço**: repetidores são tipicamente mais baratos do que comutadores que são tipicamente mais baratos do que roteadores;

- Na sofisticação dos **serviços oferecidos**: geralmente, os serviços vão crescendo em sofisticação à medida que se passa de repetidor para comutador, e deste para roteador.

Os equipamentos de interconexão também possuem características relacionadas à forma como gerenciam o acesso ao meio e a forma como propagam pacotes do tipo *broadcast*. Em uma rede com topologia plana, o domínio de colisão e difusão é formado por todas as interfaces inseridas no mesmo segmento ou sub-rede. Se não existem dispositivos para dividir a rede, teremos somente um domínio de colisão e difusão.

5.1 Repetidores

Desde o aparecimento da tecnologia *Fast Ethernet* (100 Mbps) e do barateamento de comutadores, repetidores têm sido usado cada vez menos. Porém, eles foram largamente utilizados no passado e ainda são ubíquos em redes de campus, principalmente na camada de acesso do modelo de projeto hierárquico (conectados diretamente a estações de trabalho).

O repetidor é simplesmente um amplificador de sinais: o que é recebido numa porta é amplificado e re-transmitido instantaneamente em todas as outras portas. É uma evolução do segmento Ethernet, que usava cabos coaxiais (tecnologias 10BASE-5 e 10BASE-2) para uma solução em que o segmento (o cabo) está logicamente presente dentro do repetidor e cada hospedeiro se conecta individualmente ao segmento com seu próprio cabo, tipicamente usando cabos de pares trançados ou fibras óticas [LOPES, *et.Al.*, 2000].

Ainda segundo [LOPES, *et.Al.*, 2000], devido à operação do repetidor, pode-se afirmar que:

- Apenas um hospedeiro poderá estar transmitindo de cada vez (a operação é half-duplex);
- Todas as portas deverão operar usando a mesma tecnologia Ethernet (tipicamente 10BASE-T ou 100BASE-TX);
- Regenera o sinal em cada porta, em vez de apenas amplificá-lo;
- Faz "imposição de colisão"para ter certeza de que uma colisão é detectada sem ambigüidade por todos os hospedeiros envolvidos;
- Devido à operação do repetidor na camada de Enlace, qualquer falha presente numa das portas do repetidor afetará todos os hospedeiros conectados ao mesmo. Um cabo partido, um conector defeituoso, uma placa de rede

defeituosa podem causar falhas tais como tempo excessivo de colisão, interferência no sinal, etc. Nos repetidores que possuem o recurso de auto-particionamento uma porta que apresente problemas é automaticamente desativada após a ocorrência de um número pré-determinado de quadros com erro e restaurada após o recebimento de um único quadro sem erro;

- Um repetidor é transparente. Os hospedeiros não sabem de sua existência, no sentido que nunca o endereçam por não possuir nem endereço MAC e nem endereço IP.

Os repetidores podem ser cascateados, ou dependendo do modelo empilhados, de forma a suprirem o aumento do número de hospedeiros. A tecnologia empregada (10BASE-T, 100BASE-TX etc) estabelece um limite tanto no número de "saltos de repetidor"que podem existir entre dois hospedeiros quaisquer como também impõe um limite no comprimento dos cabos. Os detalhes variam com a tecnologia empregada.

Repetidores estão caindo em desuso, devido principalmente ao barateamento de comutadores, mais vantajosos em termos de desempenho. Atualmente repetidores raramente são empregados em novas redes de campus, a não ser em redes muito pequenas com baixo tráfego agregado. Há, por outro lado, uma quantidade enorme de repetidores em uso em redes mais antigas.

5.2 Comutadores

Os comutadores surgiram da necessidade de resolver os problemas relacionados aos repetidores. Com o aumento do número de hospedeiros bem como dos recursos necessários aos serviços de rede da atualidade, surgiu a necessidade de um equipamento que pudesse obedecer aos seguintes requisitos básicos:

- Pudesse oferecer banda passante dedicada em cada porta com o objetivo de evitar a saturação dos enlaces;

- Tal como o repetidor, o comutador deve ser transparente: os hospedeiros não sabem de sua existência, no sentido que nunca o endereçam;

Os comutadores são derivados das *bridges*. Seu princípio básico de operação é impedir que um sinal recebido numa porta seja imediatamente retransmitido. O comutador recebe o sinal numa porta, reconhece o quadro, armazena-o internamente, escolhe a porta de destino do quadro e o re-encaminha para esta porta. Uma vez que nem todos os pacotes são encaminhados entre redes, cada segmento de cabo é menos saturado com tráfego do que seria se todas as máquinas estivessem no mesmo cabo. Pelo fato da maior parte da comunicação tende a

ser localizada, o aumento aparente na largura de banda pode ser impressionante [NEMETH, *et.Al.*, 2001].

Seu desempenho é normalmente medido tanto pela taxa de varredura de pacotes como pela taxa de encaminhamento de pacotes. Os comutadores estão se tornando mais inteligentes à medida que mais funcionalidades estão sendo construídas em seu *firmware* [NEMETH, *et.Al.*, 2001].

O re-envio do quadro recebido na porta de saída ocorrerá em momento distinto da recepção do quadro na porta original. Este procedimento classifica o comutador como um equipamento do tipo armazenamento-e-reenvio *(store-and-forward)*. Neste tipo de equipamento, há três atividades distintas ocorrendo: recepção, escolha do destino e reenvio. Essas atividades ocorrem em momentos distintos e para ser efetuada é necessária a utilização de outra camada de protocolos (camada 2 - Rede), além da camada de Enlace. No processo de escolha do destino (comutação) foi necessária a análise do quadro para descobrir o endereço de destino.

Ao receber um quadro, o comutador o armazena e analisa o endereço MAC do *host* destino. O comutador possui uma tabela de endereços em memória chamada SAT *(Source Address Table)* que armazena o endereço MAC e a porta associada a cada *host*. Quando um quadro é recebido e o endereço de destino não está cadastrado na SAT, o comutador utiliza uma técnica chamada *flooding* que envia um *broadcast* para as máquinas localizadas no seu domínio de difusão, com a intenção de encontrar o *host* destino. Se o *host* é encontrado, o endereço MAC e a porta associada são adicionados na tabela.

[LOPES, *et.Al.*, 2000] aponta algumas conseqüências da utilização dos comutadores:

- **Comunicação paralela:** O fato de o comutador ser um equipamento do tipo *store-and-foward* significa que várias comunicações paralelas poderão estar ocorrendo simultaneamente nas várias portas do equipamento;
- **Comunicação *full-duplex*:** Pelo fato de não haver dispositivos concorrentes, o comutador e a estação de trabalho podem transmitir e receber dados simultaneamente;
- **Portas com velocidades e tecnologias diferentes:** Já que a re-transmissão de uma porta para outra não é imediata, as portas de um comutador não precisam necessariamente operar na mesma velocidade. A probabilidade de ocorrerem "gargalos"em um repetidor é maior pois, todas as portas devem necessariamente operar na mesma velocidade;

5.3 Roteadores

[LOPES, *et.Al.*, 2000] cita alguns motivos que impedem que uma rede de grande porte seja construída apenas por comutadores:

1. **Falta de escala:** Os comutadores Ethernet utilizam dois mecanismos que não possuem escala:

   - O primeiro mecanismo é o uso de inundações *(flooding)* para encaminhar quadros. Uma inundação alcança todos os hospedeiros que estejam localizados no mesmo domínio de difusão. A técnica de *flooding* é eficiente para transmissão de quadros a *hosts* que estejam localizados a poucos segmentos de distância. Em se tratando de transmissões mais longas, os canais de comunicação ficariam completamente saturados devido ao excesso de tráfego.
   - O segundo mecanismo que não se adapta bem ao crescimento da rede é o tratamento de quadros de difusão. Por encaminhar tais quadros em todas as portas, temos um mecanismo com pouca escalabilidade: é impossível fazer difusão para todos os hospedeiros de uma rede de grande porte. Neste sentido temos a necessidade de um mecanismo que impeça que os quadros de difusão possam chegar a *hosts* que não estejam participando do processo de comunicação.

   Dos dois mecanismos mencionados, a difusão é a mais traumática já que ela entregará um quadro a cada um dos hospedeiros da rede. A inundação faz com que o quadro seja visto por todas as placas de rede dos hospedeiros, mas ele só será aceito pela placa de rede endereçada.

2. **Falta de interfaces:** Normalmente os comutadores não possuem interfaces para tecnologias de longo alcance, tais como T1/E1, E3/T3, OC-12/ATM, OC-3/ATM etc.

3. **Falta de controle:** O comutador não permite estabelecer controle administrativo sobre qual tráfego pode ser encaminhado para onde. Nas empresas, é importante ter controle sobre o encaminhamento da informação, tanto para dizer qual tráfego vai onde, como para dizer qual tráfego deve simplesmente ser rejeitado.

Os roteadores são equipamentos de interconexão concebidos com a intenção de sanar os problemas mencionados acima e que permitam a concepção de redes de grande porte. Tais equipamentos deverão obedecer aos seguintes requisitos básicos:

- O equipamento não pode usar a técnica de inundação ou outra técnica que não possua escala quando na transmissão de quadros;
- O equipamento não deve propagar quadros de difusão de camada de Rede, isto é, quadros enviados para o endereço MAC de difusão (FF-FF-FF-FF-FF-FF);

- O equipamento deve disponibilizar interfaces que permitam montar redes de longo alcance;

- O equipamento poderá prover serviços que permitam estabelecer controle administrativo sobre o encaminhamento de tráfego;

Em dois aspectos fundamentais, o roteador é semelhante ao comutador: ele é um equipamento do tipo *store-and-foward*, possui uma tabela de encaminhamento (tabela de roteamento). As grandes diferenças se baseiam no que o roteador faz quando não acha o destino na tabela e como esta tabela é preenchida.

Para poder eliminar os defeitos de escala dos comutadores, o roteador faz a informação "subir"mais uma camada: a camada de Transporte. É na camada de Transporte que se localiza a tabela de roteamento e onde ocorre a decisão de encaminhamento tomada pelo roteador. A existência dessa camada faz com que o roteador possa delimitar as inundações e os quadros de difusão que causaram problemas de escala nos comutadores.

Um segundo ponto importante a ser destacado é que, diferente do repetidor e do comutador, o roteador não é um equipamento transparente. Um *host* origem deverá encaminhar uma informação a um roteador que esteja localizado entre ele e o *host* de destino. O roteador por sua vez, poderá encaminhar a informação diretamente para o *host* destino (se for o último roteador até ele) ou para outro roteador que esteja entre ele e o *host* destino. Este processo se repete até a informação poder ser encaminhada corretamente até o *host* destino correto. O roteador não é um equipamento transparente, pois o *host* origem sabe da sua existência e uma das conseqüências da não transparência do roteador é que este deve ser endereçado pelos hospedeiros (na realidade, todos os hospedeiros e roteadores devem ser endereçados) [LOPES, *et.Al.*, 2000].

O endereçamento por MAC é uma possibilidade, mas não pode ser empregada por dois motivos:

- Nem toda tecnologia empregada na camada de Rede possui endereçamento. Endereços MAC existem para tecnologia Ethernet, por exemplo, mas não para enlaces E1;

- Os endereços MAC formam um espaço de endereçamento que chamamos de plano, o que significa que não há hierarquia útil nos endereços. Porém, para fazer roteamento baseado em endereços, é extremamente útil ter um esquema de endereçamento hierárquico.

O protocolo TCP/IP determina um sistema de endereçamento hierárquico e por esta razão pode ser utilizado para fins de roteamento. Na camada de rede, cada *host* e cada roteador possui uma tabela de roteamento que indica o próximo endereço no caminho para cada destino possível. Se um *host* origem deseja enviar

um pacote para um *host* destino, ele consulta sua tabela de roteamento e localiza o endereço do *host* destino ou pelo menos a região onde ele possa estar localizado. A tabela de roteamento do *host* origem indicará o endereço do roteador ao qual se deve encaminhar o pacote. O *host* origem deve necessariamente poder enviar um quadro para o roteador usando apenas a camada de Rede, ou seja, *host* origem e roteador devem pertencer à mesma rede física.

Ao receber o quadro, o roteador faz "subir"seu conteúdo para a camada de Transporte onde a decisão de roteamento (como alcançar o *host* destino) é tomada. Como resultado, o pacote seguirá, de roteador em roteador, até chegar ao endereço destino.

Roteadores são equipamentos extremamente variáveis se considerarmos a funcionalidade adicional que pode ser agregada ao equipamento. [LOPES, *et.Al.*, 2000] menciona algumas dessas funcionalidades :

- Roteadores possuem freqüentemente uma grande variedade de interfaces LAN (rede local) e WAN (para longo alcance);
- Roteadores, normalmente, dão suporte a uma variedade de protocolos de roteamento, tais como *Border Gateway Protocol* (BGP), *Intermediate System-to-Intermediate System* (IS-IS), *Open shortest Path First* (OSPF) etc.;
- Roteadores, normalmente, dão suporte a diversos protocolos de *multicast*, tais como PIM, IGMP, CGMP, DVMRP etc.;
- Roteadores são freqüentemente multi-protocolo (conseguem rotear tráfego de vários protocolos de rede, tais como IP, IPX etc.);
- Roteadores freqüentemente incluem um filtro de pacotes (ou até um *firewall* completo), permitindo estabelecer regras de segurança sobre que tipo de tráfego pode ser roteado pelo equipamento;
- Devido a sua criticalidade, roteadores freqüentemente possuem recursos especiais para aumentar a disponibilidade da rede ou melhorar a manutenibilidade. Exemplos de tais recursos incluem suporte ao *Hot Standby Routing Protocol* (HSRP), módulos redundante (módulos de processamento, fontes de alimentação, ventiladores etc.) e *hot swappable*;
- Roteadores podem ter recursos especiais para priorizar o tráfego roteado ou, de forma geral, dividir os recursos disponíveis, principalmente a banda passante dos enlaces, entre várias classes de tráfego (QoS). Esses recursos incluem *Weighted Fair Queuing* (WFQ) e roteamento baseado em políticas administrativas (*Policy Based Routing*);
- Suporte a uma vasta gama de recursos e protocolos adicionais tais como: MPLS, VPN, tunelamento GRE e gerência via protocolo SNMP.

A principal característica que permite que roteadores tenham escala podendo ser utilizados para montar redes muito grandes, é a não transparência. Os recursos dos roteadores são utilizados em redes onde:

- Há necessidade de acessar um local remoto usando um enlace de longa distância;
- Há necessidade de conter quadros de difusão; isso ocorre normalmente na camada distribuição de uma rede de campus;
- Há necessidade de policiar tráfego, tipicamente na camada de distribuição de uma rede de campus ou no ponto em que a rede corporativa se conecta a redes externas.

Capítulo 6

Segmentação

Projetistas de rede frequentemente se defrontam com a necessidade de estender o perímetro da rede, o número de usuários no sistema, ou a largura de banda disponível para os usuários.

Mudar a infra-estrutura da rede para que estas necessidades possam ser atendidas, não implica somente na substituição das interfaces de rede, mas principalmente na substituição dos equipamentos de interconexão. Embora eficiente, uma atualização na rede pode resultar em custos proibitivos.

A segmentação é uma técnica que procura disponibilizar aos usuários largura de banda adicional sem a necessidade de se substituir todos os seus equipamentos. Através da segmentação, pode-se quebrar uma rede em porções menores e conectar estar porções com o equipamento de interconexão apropriado [CLARK, *et.Al.*,1999].

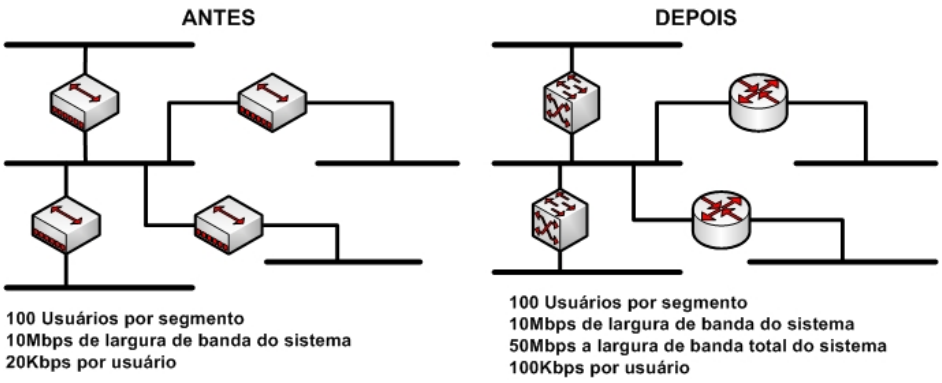

Figura 6.1: Ilustração de uma situação antes e depois da segmentação de rede

No exemplo acima, antes da segmentação, todos os 500 usuários dividiam a banda de 10Mbps pelo fato dos segmentos estarem interconectados com repetidores. Após a substituição dos repetidores por comutadores e roteadores, os segmentos foram isolados e mais largura de banda pôde ser disponibilizado para os

usuários. Comutadores e roteadores aumentam a largura de banda pois criam novos domínios de colisão e difusão. Com a redução do número de usuários por segmento, mais largura de banda está disponível para cada um. O caso extremo, dedica um usuário para cada segmento disponibilizando a total largura de banda da mídia de comunicação para cada usuário [CLARK, *et.Al.*,1999].

Conforme descrito no capítulo 5, repetidores não realizam a segmentação da rede e não criam mais largura de banda. Eles simplesmente permitem o aumento do diâmetro da rede. Comutadores e roteadores são os equipamentos mais adequados para a segmentação.

São diversos os motivos que levam a segmentação dos dispositivos em uma rede. Segundo [MUELLER, 2003] estes podem incluir:

- **Limitações topológicas:** Quando se deseja incluir mais nós em uma rede, mas a expansão é impedida devido a limitações de distância ou o número máximo de nós por segmento já foi atingido.
- **Limitações no protocolo de rede:** Quando o espaço de endereçamento é dividido e tem se a necessidade de conectar segmentos que possuem endereços de rede diferentes.
- **Limitações na largura de banda da rede:** Quando servidores de alto desempenho ou estações de trabalho consomem grande parte da banda do segmento.
- **Razões de segurança:** Quando se deseja limitar os acessos externos à rede interna (políticas de segurança) e acessos internos à rede externa (políticas de uso).
- **Conexões geograficamente distantes:** Quando se deseja assegurar que um tráfego desnecessário não alcance uma conexão remota o que de certa forma consumiria largura de banda.

6.1 Segmentando LAN's com Repetidores

Sistemas Ethernet legados como 10Base5, 10Base2 e 10BaseT possuem limitações de distância para segmentos. Entretanto tais equipamentos são úteis quando se deseja estender a distância de um segmento. Por serem equipamentos não-inteligentes eles não têm conhecimento dos dados que estão manipulando, repassando os sinais de um segmento para todos os segmentos [CLARK, *et.Al.*,1999].

Se um quadro contém erros, o repetidor o repassa. Se um quadro viola o comprimento mínimo ou máximo de tamanho especificado pelo padrão, o repetidor o repassa. Se uma colisão ocorre em um segmento ela ocorrerá em todos os outros segmentos ligados a ele. Repetidores são verdadeiramente uma extensão do cabo.

Todas as estações ligadas ao repetidor enxergam todo o tráfego sendo ele bom ou ruim. Existem limitações em um repetidor provenientes de diversas causas e estas precisam ser consideradas quando se estende uma rede com repetidores. As limitações incluem os seguintes:

- Colisões poderão ocorrer no segmento;
- Toda a rede assim formada consiste de um único segmento compartilhado. Portanto, a banda passante disponível não é aumentada e deve ser compartilhada entre mais hospedeiros, o que aumenta as chances de saturação do segmento;
- Ainda como conseqüência do segmento único, a rede inteira assim formada consiste de um único domínio de colisão e difusão. Qualquer hospedeiro, localizado em qualquer um dos repetidores, poderá ter sua transmissão colidindo com a transmissão de qualquer outro hospedeiro. O incremento de hospedeiros causará, portanto, um incremento na taxa de colisões e no número de transmissões *broadcast*.

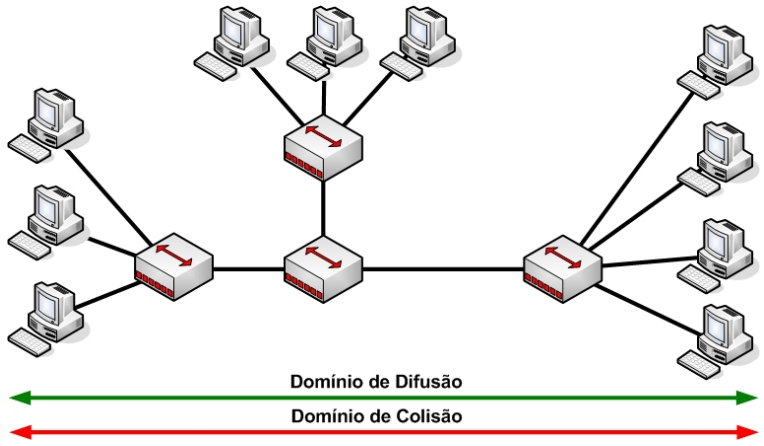

Figura 6.2: Abrangência do Domínio de Colisão e Difusão proporcionado pelos repetidores.

- Limitação no número de estações por segmento;

Banda Compartilhada

Um repetidor estende não apenas a distância do segmento, mas também estende o domínio de colisão. Colisões em um segmento afetam estações e qualquer outro repetidor conectado a ele. Colisões se estendem através de um repetidor e consomem largura de banda em todos os segmentos interconectados. Outro lado do

efeito dos domínios de colisão é a propagação de quadros pela rede *(broadcast)*. Se a rede utiliza uma tecnologia de mídia compartilhada, todas as estações no repetidor base dividem a mesma largura de banda.

Adicionando-se mais estações ao repetidor potencialmente dividimos mais a largura de banda. Sistemas Ethernet legados trabalham sobre a mídia compartilhada. As estações fazem turnos para utilizarem a largura de banda e quando o número de estações de trabalho aumenta, a quantidade de banda disponível diminui.

6.2 Segmentando LAN's com Comutadores

Quando utilizamos comutadores na interconexão de redes, surgem diferenças significantes comparadas à interconexão por repetidores. Ao contrário do que acontece com os repetidores, os comutadores utilizam um processo de filtragem para determinar se um quadro deve, ou não ser repassado para outras interfaces. O processo de filtro diferencia-se dos métodos de acesso utilizado na tecnologia Ethernet e *Token Ring*.

No padrão Ethernet, por exemplo, um processo chamado *Transparent bridging* examina o endereço MAC do *host* destino e determina se um quadro deve ser repassado, filtrado ou inundado.

Por trabalharem na camada de Rede, os comutadores possuem a capacidade de examinar os cabeçalhos MAC dos quadros de transmissão e desta forma, podem tomar decisões de encaminhamento baseados nestas informações.

Considerando os requisitos desejados em uma segmentação, duas características podem ser observadas nos comutadores:

- **Domínios de colisão:** Devido à operação de *store-and-forward*, cada porta de um comutador é um domínio de colisão independente. No caso de um repetidor, existiria um único domínio de colisão envolvendo todos os equipamentos inseridos no segmento.

- **Domínio de difusão único:** Os quadros de difusão são sempre encaminhados por inundação por um comutador. Como conseqüência, uma rede formada com um ou mais comutadores e repetidores forma um único domínio de difusão. Um quadro de difusão será entregue para todos os equipamentos que possam ser alcançados, passando por repetidores e comutadores.

Conforme mostrado na figura 6.3, a largura de banda está sendo dividida em cada um dos segmentos circulados, entretanto cada segmento pertence a um domínio de colisão diferente.

A melhora significante na largura de banda demonstra os benefícios advindos com a segmentação refletidos aos usuários. Para uma mesma quantidade de

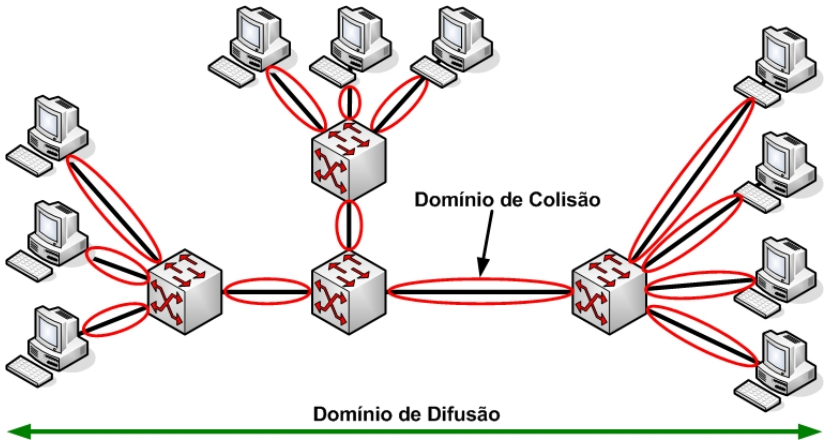

Figura 6.3: Abrangência do Domínio de Colisão e Difusão proporcionado pelos comutadores.

usuários em uma rede que utiliza comutadores, temos uma quantidade maior de largura de banda quando comparada com uma rede que utiliza repetidores. Cada usuário possui toda a largura de banda local para si, somente uma estação e a sua respectiva porta no comutador residem no mesmo domínio de colisão.

Se por um lado, comutadores filtram o tráfego quando o *host* origem e o *host* destino residem no mesmo meio, os quadros de difusão são a exceção pois um comutador repassa mensagens de *broadcast* para todas as interfaces. Uma requisição ARP ou mesmo uma vídeo conferência podem saturar rapidamente o segmento.

Em muitas redes, os quadros de difusão não são a maioria. Alguns protocolos geram mais quadros de difusão que outros, mas a largura de banda consumida por estes é relativamente uma pequena porcentagem da banda utilizada [CLARK, *et.Al.*,1999].

Quando um *host* origem e destino se encontram no mesmo meio , um comutador filtra os quadros e não os repassa para outro meio (salvo os quadros de difusão). Se *host* origem e destino estão em meios diferentes, o comutador repassa o quadro para a interface apropriada para que se possa alcançar o destinatário.

O processo de filtragem e repasse seletivo preserva a banda dos outros segmentos. Esta é uma vantagem significativa dos comutadores sobre os repetidores. Assim como em um repetidor, um comutador repassa um quadro sem modificá-lo (apenas regenera o seu sinal antes de enviá-lo). Endereços MAC não são modificados por repetidores e comutadores, mas são modificados por roteadores.

Para os comutadores, a regra 80/20 garante que estes são mais eficientes quando 80% do tráfego do segmento é local e somente 20% atravessa o comutador para alcançar outro segmento. Nesta regra, os clientes não frequentemente necessitam acessar dispositivos do outro lado do comutador. Enquanto este tipo de tráfego balanceado é mantido, cada segmento na rede, mostra-se com a quantidade total de

banda. Se, entretanto, o balanceamento do fluxo muda (uma quantidade maior de tráfego está sendo repassado pelo comutador), a rede comporta-se como se todos os segmentos operassem na mesma mídia compartilhada [CLARK, *et.Al.*,1999].

6.3 Segmentando LAN's com Roteadores

Por operarem na camada de transporte, os roteadores possuem mais funcionalidades que os comutadores. Roteadores assim como os comutadores, possuem a capacidade de estender o diâmetro da rede e de segmentar os domínios de colisão, mas em contrapartida possuem a capacidade de segmentar os domínios de difusão. Roteadores impedem que os quadros de difusão se propaguem através da rede.

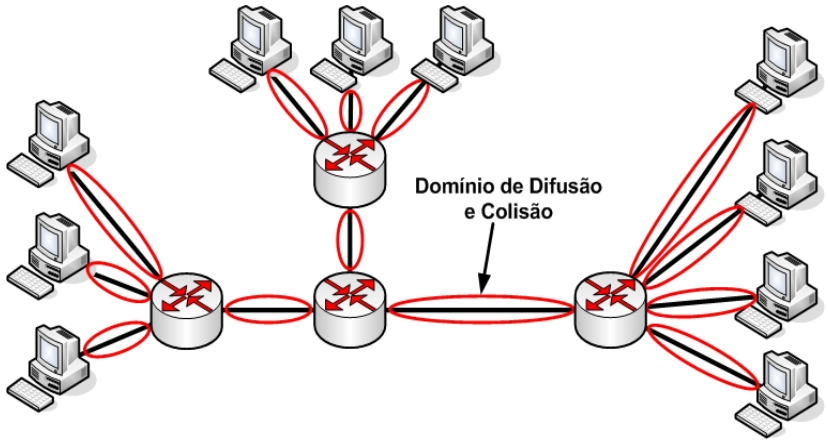

Figura 6.4: Abrangência do Domínio de Colisão e Difusão proporcionado pelos roteadores.

Em um repetidor ou comutador, todas as estações pertencem a mesma sub-rede pelo fato de estarem todos pertencentes ao mesmo domínio de difusão. Entretanto, em uma rede baseada em roteador, são criados múltiplos domínios de difusão, e desta forma cada segmento pertence a uma sub-rede diferente [CLARK, *et.Al.*,1999].

Em uma rede baseada em repetidores e comutadores, uma estação de trabalho realiza uma transmissão se o *host* origem e destino estiverem no mesmo domínio de difusão. Entretanto quando tais *hosts* estão localizados em domínios de difusão diferentes, ambos precisam estar cientes da presença do roteador e precisam endereçar o seu tráfego para o rotedor.

No exemplo da figura 6.5, quando a estação do segmento A deseja se comunicar com a estação do segmento B, a estação A observa pela comparação do endereço lógico do destinatário, que ele está localizado em uma rede diferente da sua. Neste caso A sabe que precisa utilizar o roteador para alcançar o *host* B.

O roteador é definido como rota padrão (ou *gateway*) na estação A. Para comunicar com roteador, o *host* A utiliza o endereço MAC (camada 2). O *host* origem primeiro envia uma requisição ARP para o roteador (seta 1) e após o recebimento da requisição (seta 2) cria um quadro com o endereço MAC do roteador, como endereço físico destino, e com o endereço IP da estação do segmento B, como endereço destino lógico (seta 3). Quando o quadro entra no roteador, o mesmo determina como chegar ao endereço destino.

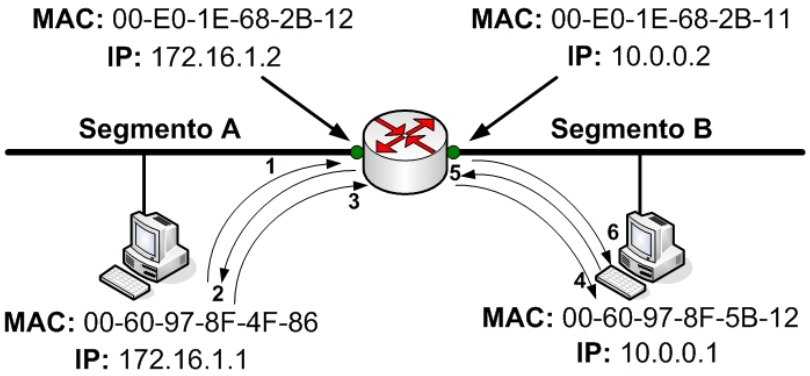

Figura 6.5: Manipulação de pacotes realizadas pelo roteador.

	Cabeçalho da camada de Rede (Modificado)		Cabeçalho da camada de Transporte (Não-modificado)	
Quadro	MAC Destino	MAC Origem	IP Origem	IP Destino
1*	FF-FF-FF-FF-FF-FF	00-60-97-8F-4F-86	172.16.1.1	172.16.1.2
2**	00-60-97-8F-4F-86	00-E0-1E-68-2B-12	172.16.1.2	172.16.1.1
3***	00-E0-1E-68-2B-12	00-60-97-8F-4F-86	172.16.1.1	10.0.0.1
4*	FF-FF-FF-FF-FF-FF	00-E0-1E-68-2B-11	10.0.0.2	10.0.0.1
5**	00-E0-1E-68-2B-11	00-E0-1E-68-2B-12	10.0.0.1	10.0.0.2
6***	00-E0-1E-68-2B-12	00-E0-1E-68-2B-11	172.16.1.1	10.0.0.1
*Requisição ARP **Resposta ARP ***Quadro de dados do usuário				

Figura 6.6: Troca de quadros em uma rede que utiliza roteadores.

O roteador realiza uma requisição ARP para a estação do segmento B (seta 4) com a intenção de descobrir o seu endereço MAC. Após o recebimento da requisição (seta 5), ele cria um quadro que tem como endereço físico destino, o endereço MAC da estação B (seta 6) e como endereço físico origem o endereço MAC da interface do roteador ligada ao segmento B.

O roteador utiliza endereços da camada 3 para as estações A e B. Para que a comunicação possa ser estabelecida, o roteador insere como endereços lógicos o

endereço IP do *host* do segmento A como endereço origem e o endereço IP do *host* do segmento B como endereço destino.

A camada de rede modifica o quadro movendo-o através do roteador, enquanto o cabeçalho da camada de transporte continua o mesmo. Assim como nos comutadores, o roteador previne que quadros defeituosos possam entrar na rede destino [CLARK, *et.Al.*,1999].

Capítulo 7

VLAN *(Virtual Local Area Network)*

Uma VLAN *(Virtual Local Area Network)* é a união de dispositivos de uma rede local em um agrupamento lógico que tem a intenção de segmentar a rede em pequenos domínios de difusão.

As VLANS representam uma solução alternativa ao uso dos roteadores para a contenção de quadros de difusão, permitindo aos comutadores a capacidade de contenção deste tipo de tráfego. São definidas pelo IEEE conforme o padrão 802.1Q *(Virtual Bridged Local Area Networks)*.

Ao se estabelecer uma VLAN em uma porta de um comutador, é como se usássemos um roteador para conter os *broadcasts* em um segmento. Cada VLAN se transforma em um domínio de difusão individual. Quando um nó da rede envia um *broadcast* para os outros nós do seu segmento, somente os nós determinados pela VLAN possuem a capacidade de recebê-lo, ou seja, quadros de *broadcast* são transmitidos somente para as portas de um comutador localizadas na mesma VLAN [ODOM, 2001].

As VLANs não possuem limitações físicas e podem ser organizadas por localização de *hosts*, função, departamento, aplicações ou protocolos, sem se preocupar com a localização de recursos ou usuários.

7.1 Características das VLANs

As VLANs resolvem alguns dos problemas de escalabilidade das grandes redes de topologia plana ao quebrar um único domínio de difusão em partes menores. Cada parte é atribuída a uma LAN virtual. Um ponto a ser considerado, é que cada LAN virtual possui as características de escalabilidade de uma LAN comum e desta forma, uma VLAN por si só não é suficiente na resolução dos problemas com quadros de *broadcast* herdados de uma rede que possui topologia plana. As

VLANs sem roteadores não possuirão escala nas grandes redes de campus. O roteamento neste ambiente é necessário para que se possa obter VLANs escaláveis sendo esta a única forma de se impor hierarquia em uma rede comutada que possua VLANs [MCGREGOR, 1998]. As VLANs possuem os seguintes benefícios:

1. **Controle de *Broadcast*:** Da mesma maneira que os comutadores isolam domínios de colisão e repassam o tráfego para a porta apropriada, VLANs refinam este conceito provendo um isolamento completo entre as VLANs. Uma VLAN é um único domínio de difusão e todo o tráfego *broadcast* ou *multicast* é contido por ela. Diferente de um sistema que utiliza mídia compartilhada, onde somente uma estação poderá transmitir por vez, uma rede comutada permite que várias transmissões concorrentes possam acontecer sem afetar diretamente outras estações que estejam dentro ou fora do seu domínio de difusão.

2. **Segurança:** A habilidade das VLANs para servirem de *firewalls* pode também satisfazer os requisitos mais severos de segurança e desta forma substituir muitas das funcionalidades dos roteadores nesta área. As VLANs podem garantir a segurança de duas formas:

   - Usuários especiais, mesmo estando localizados em diferentes meios físicos, podem ser agrupados em uma VLAN e nenhum usuário fora da VLAN poderá se comunicar com este grupo.
   - Pelo fato das VLANs serem grupos lógicos que se comportam como entidades fisicamente separadas, a comunicação entre VLANs é executada por um roteador. Quando a comunicação entre VLANs ocorre através de um roteador, todas as funcionalidades de segurança e filtragem que os roteadores tradicionalmente fornecem podem se utilizados. No caso de protocolos não-roteáveis, toda a comunicação precisa ocorrer na mesma VLAN.

3. **Desempenho:** Quando usuários estão conectados no mesmo segmento, eles dividem a largura de banda total da mídia e desta forma, quanto mais usuários estão conectados no mesmo segmento menor será a quantidade de banda para cada um. Se o compartilhamento se torna muito grande há uma perda de desempenho nas aplicações compartilhadas. VLANs são geralmente criadas em equipamentos de comutação o que de certa forma garante mais largura de banda para cada usuário [CLARK, *et.Al.*,1999].

4. **Gerenciamento da Rede:** O agrupamento lógico de usuários independente da sua localização física ou geográfica permite um gerenciamento de rede mais fácil. Neste contexto, não é mais necessário manusear cabos para que

se possa mover um usuário de uma rede para outra. A realização de mudanças é possível através de uma simples inserção de uma porta do comutador na VLAN apropriada. Os altos custos com reestruturação do cabeamento que tem a intenção de estender o ambiente comutado, não são mais necessários pois o gerenciamento da rede pode ser realizado através de atribuições lógicas de usuários [CLARK, *et.Al.*,1999].

5. **Alto desempenho e redução da latência de rede:** Quando a rede se expande, mais e mais roteadores são necessários para dividir a rede em domínios de difusão. Quando o número de roteadores aumenta, a latência começa a degradar o desempenho da rede. Um alto grau de latência na rede é um problema para muitas aplicações legadas, mas isto é particularmente preocupante para aplicações novas com características de tempo real. Comutadores podem utilizar VLANs para realizar a divisão da rede em domínios de difusão, e de certa forma possuem tempos de latência muito menores quando comparados aos roteadores [PASSMORE, 1996].

6. **Custo:** A interface de um roteador é mais cara que as de um comutador. Além disso, a utilização de comutadores e a implantação de VLANs permite que uma rede seja segmentada a um custo mais baixo se comparado a segmentação da rede através de roteadores [PASSMORE, 1996].

7.2 Classificação das VLANs

As VLANs podem ser classificadas quanto a sua forma de agrupamento de elementos. Existem várias formas de agrupamento podendo estas ser classificadas dentro de quatro principais tipos [PASSMORE, 1996]:

- Agrupamento por portas;
- Agrupamento por endereços MAC;
- Agrupamento por protocolo;
- Agrupamento por IP *multicast*;

7.2.1 Agrupamento por portas

Como o próprio nome sugere, uma VLAN por agrupamento de portas representa uma LAN virtual criada pelo agrupamento de portas de um comutador para formar um domínio de difusão [HELD, 2003]. As implementações iniciais definiam o agrupamento de portas em somente um único comutador. A segunda geração de VLANs baseada em agrupamento de portas permitiu a configuração de portas de múltiplos comutadores na formação de uma VLAN.

As vantagens associadas com esta técnica incluem a habilidade de se usar as capacidades de comutação do equipamento de interconexão e a habilidade de suportar múltiplas estações por porta (cascateamento).

A principal desvantagem associada a esta técnica é que geralmente só pode ser atribuída uma VLAN por porta. O administrador precisará re-configurar o agrupamento caso necessite mover um usuário (ou grupo de usuários) de uma porta à outra.

Todo o tráfego dentro da VLAN é comutado e o tráfego entre VLANs deverá ser roteado. Este tipo de VLAN é também conhecido como VLAN baseada em segmento [PASSMORE, 1996].

7.2.2 Agrupamento por endereços MAC

VLANS baseadas em endereços MAC, permitem aos administradores da rede a movimentação de uma estação de trabalho em diferentes localizações físicas na rede, sendo que a estação é automaticamente reagrupada à sua VLAN original.

Fora a vantagem da mobilidade, uma das desvantagens desta técnica é a necessidade de todos os usuários inicialmente estarem configurados em pelo menos uma VLAN. Após a configuração manual, o remanejamento automático de usuários é possível. Entretanto a desvantagem da configuração inicial pode se tornar clara em redes muito grandes onde centenas de usuários precisam ser explicitamente atribuídos a uma VLAN.

As VLANs baseadas em endereçamento que são implementadas em mídias compartilhadas, sofrerão com a perda de desempenho, quando membros de VLANs diferentes coexistirem na mesma porta do comutador bem como em implementações que envolvam muitos usuários.

7.2.3 Agrupamento por protocolo

As VLANs que utilizam esta técnica, levam em conta o tipo do protocolo (se múltiplos protocolos são suportados) ou endereços de rede (endereços de sub-rede para redes TCP/IP) na determinação dos membros da VLAN. O fato destas VLANs serem baseadas em endereçamento de alto nível, não constitui necessariamente em roteamento de pacotes. Mesmo que o comutador examine o endereço IP do pacote para determinar a sua VLAN, não existe cálculo de rotas e nem protocolos de roteamento que realizam o transporte dos quadros. O roteamento entre as VLANs que utilizam esta técnica ainda se faz necessário.

O particionamento por protocolo e a mobilidade física das estações de trabalho sem a necessidade de re-configuração de endereços IP, estão dentre as vantagens de se utilizar este tipo de VLAN. Uma das desvantagens deste tipo de VLAN sobre os dois tipos anteriores está relacionado ao desempenho. E necessário mais tempo para se inspecionar endereços IP em pacotes de transmissão do que endereços

MAC em quadros. Além deste fato, as VLANs por agrupamento de protocolo possuem dificuldades ligadas aos protocolos não-roteáveis como NetBIOS.

7.2.4 Agrupamento por IP *multicast*

Grupos de endereço IP multicast representam uma abordagem diferente na definição de VLAN, embora os conceitos fundamentais de VLAN, como domínios de difusão, continua sendo aplicado. Quando um pacote IP é enviado por *multicast*, ele é enviado a um endereço que serve de procurador para um grupo de endereços IP explicitamente definidos e que são estabelecidos dinamicamente. A cada estação de trabalho, é dada a oportunidade de entrar em um grupo de IP *multicast* quando esta confirma uma notificação *broadcast* que declara a existência do grupo.

Todas as estações de trabalho que adentram em um grupo de IP *multicast* podem se tornar membros da mesma LAN virtual. Entretanto elas são somente membros de um grupo *multicast* durante certo período de tempo. Desta forma, a natureza dinâmica das VLANs definidas por este agrupamento permite um alto grau de flexibilidade. Além disso, VLANs deste tipo estão hábeis a transpor roteadores e desta forma estabelecer conexões WAN.

7.3 Formas de Configuração de VLANs

Outra classificação utilizada na concepção de VLANs está relacionada ao seu grau de configuração automatizado. Existem três níveis de automação utilizados na configuração de uma VLAN [PASSMORE, 1996]:

- **Manual:** Com uma configuração puramente manual, os ajustes iniciais e todos os movimentos e mudanças subseqüentes na rede são controlados pelo administrador. Uma configuração manual permite um alto grau de controle. Entretanto, em redes de grande porte, este tipo de configuração não é prático. Fora este fato, a configuração manual não concede um dos principais benefícios das VLANs que é a eliminação do tempo gasto pelo administrador na implantação de mudanças e movimentação de usuários na rede.

- **Semi-automática:** A configuração semi-automática refere-se à opção de automatização das configurações iniciais, e re-configurações subseqüentes (movimentações/mudanças). A configuração inicial automatizada é normalmente efetuada com um conjunto de ferramentas que mapeiam as VLANS em sub-redes existentes ou outro critério qualquer. A configuração semi-automática pode também se referir a situações onde VLANs são configuradas inicialmente de forma manual e todos os movimentos subseqüentes são rastreados automaticamente.

- **Totalmente automática:** Um sistema que automatiza totalmente as configurações de VLAN, implica na agregação das estações de trabalho automaticamente e dinâmicamente, dependendo da aplicação, ID do usuário, política ou outro critério definido pelo administrador.

7.4 Comunicação entre membros de uma VLAN

Os comutadores devem possuir uma forma de reconhecer os membros de cada VLAN quando o tráfego da rede chega até ele oriundo de outros comutadores ou, de outra forma, as VLANs podem estar limitadas a um único comutador. Geralmente VLANs baseadas na camada de rede (definidas por porta ou endereço MAC), devem se comunicar de forma implícita (*implicity tagging* - marcação implícita), enquanto membros de VLAN baseados em IP (protocolo ou *multicast*) comunicam-se explicitamente (*explicity tagging* - marcação explícita).

A **marcação implícita** é aquela onde a decisão é baseada nos dados que realmente já estão presentes no formato do quadro existente e o comutador precisa apenas examinar os dados no cabeçalho do quadro e implicitamente decidir qual VLAN ele pertence. Quando este tipo de marcação é utilizado, nenhuma espécie de informação adicional precisa ser adicionada ao quadro pela estação transmissora, e desta forma, os dispositivos da rede não tem consciência da existência da VLAN [MUELLER, 2003].

A **marcação explicita** requer a adição de um campo dentro do cabeçalho do quadro ou pacote para que se possa especificar a VLAN associada [HELD, 2003]. Geralmente é utilizada em aplicações de alto nível e em WANs de grande porte. Para este método a estação precisa saber da existência da VLAN. O comutador precisa entender o método e saber onde localizar a informação de marcação no quadro de dados e desta forma, determinar qual VLAN o quadro pertence.

7.5 Roteamento entre VLANs

VLANs podem ser utilizadas para definir domínios de difusão de uma rede da mesma forma que roteadores, mas elas não possuem a capacidade de repassar o tráfego de uma VLAN a outra. O roteamento ainda se faz necessário para o estabelecimento de tráfego entre VLANs.

São três as opções de roteamento [JACK, 2003]:

- Roteamento através de Múltiplos Enlaces;
- Roteamento por *Trunking* em um Enlace Único;
- Roteamento por Processador de Rotas Interno;

7.5.1 Roteamento através de Múltiplos Enlaces

Este modelo é também chamado "Roteamento por Roteador Externo". Neste tipo de roteamento, cada interface do roteador está ligada a uma porta do comutador que faz parte de uma VLAN. Cada estação de trabalho em uma VLAN, deve possuir um endereço *gateway* padrão que geralmente é o endereço IP da interface do roteador, ligada a sua VLAN correspondente.

Esta é uma solução prática para redes pequenas, mas não possui escala em ambientes com muitas VLANs. A principal desvantagem deste tipo de técnica é o desperdício de portas do comutador e interfaces no roteador. Quanto maior o número de interfaces ativas no roteador, maior deve ser a sua capacidade de processamento o que do contrário fatalmente geraria um gargalo.

Neste tipo de roteamento, a utilização de roteadores de grande porte (que geralmente possuem um custo proibitivo) se faz necessário.

7.5.2 Roteamento por *Trunking* em um Enlace Único

É o modelo mais prático e econômico utilizado na comunicação entre duas ou mais VLANs, em um ou mais comutadores. A tecnologia para que este processo seja possível é conhecido como *Trunking*. Nesta tecnologia, a determinação do tráfego de cada VLAN é realizada através da análise das *tags* contidas nos pacotes de dados. As *tags* indicam a VLAN a qual o pacote em questão está relacionado.

Para que este processo possa ser realizado, uma das portas do comutador deve ser configurada com um protocolo de *trunking* e, desta forma, todo tráfego oriundo das múltiplas VLANs será encaminhado para esta porta. A mesma configuração deverá ser efetuada na interface do roteador onde será criada uma sub-interface para cada VLAN e será atribuído o número de cada VLAN para as sub-interfaces correspondentes.

Toda vez que uma estação de trabalho conectada em uma das VLANs desejar se comunicar com outra estação conectada em outra VLAN, o pacote percorrerá o *trunk* entre o comutador e o roteador. Ao chegar ao roteador, o pacote é modificado e encaminhando para a VLAN correspondente.

Este é provavelmente o esquema mais simples para que se possa realizar a comunicação entre VLANs, além de não consumir muitos componentes.

7.5.3 Roteamento por Processador Interno de Rotas

Modelo também chamado "Roteamento com auxílio de comutador de nível 3". Neste cenário temos um *multilayer switch* que é um equipamento de comutação capaz de manipular dados da terceira camada (transporte) e desta forma possui as mesmas características de um roteador externo com as vantagens de um roteamento interno (tabelas de roteamento em memória cache, sistemas operacionais específicos etc).

O tráfego entre as VLANs não é realizado por agentes externos sendo o próprio comutador responsável pelo roteamento. Este modelo de roteamento entre VLANs é considerado o mais eficiente, embora os custos iniciais desta solução sejam bastante elevados.

Capítulo 8

Metodologia

8.1 Método de Pesquisa

Quanto ao objetivo geral da pesquisa, ela será classificada como **pesquisa exploratória**. Pesquisa exploratória tem como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses. Pode-se dizer que esse tipo de pesquisa tem como objetivo principal o aprimoramento de idéias ou a descoberta de intuições [GIL, 1991].

Quanto aos procedimentos técnicos utilizados, a pesquisa utilizará **pesquisa bibliográfica** e **pesquisa documental**. A pesquisa bibliográfica é desenvolvida a partir do material já elaborado, constituído principalmente de livros e artigos científicos [GIL, 1991].

A pesquisa documental assemelha-se muito à pesquisa bibliográfica. A diferença essencial entre ambas está na natureza das fontes, já que a pesquisa documental vale-se de materiais que não receberam ainda um tratamento analítico, ou que ainda podem ser re-elaborados de acordo com os objetivos da pesquisa.

8.2 Procedimento Metodológico

O projeto em questão, surgiu da necessidade de se otimizar a estrutura e principalmente o desempenho da rede da Universidade Federal de Lavras. Repercutindo todos os problemas típicos de uma rede de campus, a rede UFLA dentre outros agravantes, vem sofrendo com os altos níveis de *broadcast*.

Oriundo dos protocolos de comunicação ou mesmo dos serviços de rede, os pacotes de difusão são a principal causa da sobrecarga dos equipamentos de interconexão. Esta elevada taxa de tráfego de certa forma vem contribuindo para o saturamento dos equipamentos e na perda da qualidade dos serviços de rede utilizados pelos usuários finais.

Este projeto trouxe o desafio de encontrar uma solução que fosse viável a uma instituição pública com orçamento tecnológico deficiente, corpo técnico reduzido e que de certa forma se adaptasse a atual estrutura da rede.

Para definir a melhor solução a ser adotada, foi realizada uma série de etapas para a pesquisa, análise, teste e implantação da solução. Essas etapas podem ser vistas no fluxograma abaixo:

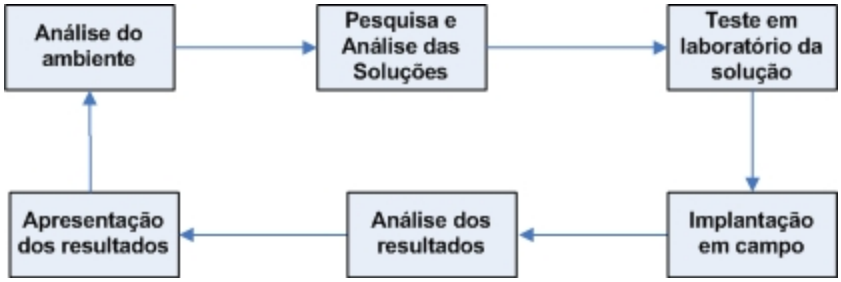

Figura 8.1: Fluxograma das etapas executadas durante a metodologia.

8.3 Análise do Ambiente

Na primeira etapa do projeto foi realizada uma análise da rede com o intuito de conhecer o ambiente. Nesta etapa foi analisado o campus da UFLA, sua topologia e hierarquia de rede, equipamentos, serviços disponibilizados, sistemas operacionais, processo de gerencia, suporte e corpo técnico.

Esta análise contribuiu para mapeamento dos principais problemas, equipamentos existentes, limitações e recursos disponíveis. A observação do ambiente (salas de equipamentos, usuários) e principalmente reuniões com membros do corpo técnico foram os principais instrumentos de análise utilizados.

O Campus da Universidade Federal de Lavras possui uma área física de 600ha com uma área construída de 158.359m^2. Atualmente dispõem de 16 departamentos didático científicos além de laboratórios e prédios administrativos. O Campus da UFLA está dividido em Campus Histórico e Novo Campus. O Campus Histórico abrange:

- Centro Assistencial, Odontológico e Serviço Social;
- Museu "Bi Moreira";
- Creche;
- Hotel Alvorada;
- FAEPE (Fundação de Apoio ao Ensino Pesquisa e Extensão);
- Gráfica e Editora UFLA;
- UFLATEC (Centro de Tecnologia em Informática);

- Cooperativa de Consumo;
- Rádio FM Universitária e TV Universitária;
- Laboratório de Idiomas;
- Alojamentos;

Já o Campus Novo é constituído por:

- Reitoria;
- Depto. de Administração e Economia (DAE);
- Depto. de Agricultura (DAG);
- Depto. de Biologia (DBI);
- Depto. de Ciência da Computação (DCC);
- Depto. de Ciência dos Alimentos (DCA);
- Depto. de Ciências Exatas (DEX);
- Depto. de Ciências Florestais (DCF);
- Depto. de Ciência do Solo (DCS);
- Depto. de Educação (DED);
- Depto. de Educação Física (DEF);
- Depto. de Engenharia (DEG);
- Depto. de Entomologia (DEN);
- Depto. de Fitopatologia (DFP);
- Depto. de Medicina Veterinária (DMV);
- Depto. de Química (DQI);
- Depto. de Zootecnia (DZO);
- Biblioteca;
- Prefeitura do Campus, Almoxarifado;
- Lanchonetes;
- Postos Bancários, Central de Fotocópias, Agência de Correio, Livraria, Restaurante;

Cada departamento possui um ou mais prédios sendo o prédio administrativo do departamento geralmente é considerado o seu prédio principal.

8.3.1 Estrutura da Rede UFLA

A rede da Universidade Federal de Lavras e gerenciada pelo Centro de Informática da UFLA (CIN-UFLA) que dentre outras funções é responsável pelo recepção e distribuição do link internet, gerência de serviços de rede (email, http, servidor de arquivos, etc), suporte a usuários etc.

Uma das principais atribuições do CIN-UFLA é controlar toda a infra-estrutura de rede da UFLA. Esta infra-estrutura deve abranger todos os órgãos e departa-

mentos inseridos na UFLA de forma a possibilitar o acesso destes órgãos e departamentos aos serviços de rede.

O CIN-UFLA está localizado no prédio da Reitoria. Um esboço do campus da UFLA pode ser observado abaixo:

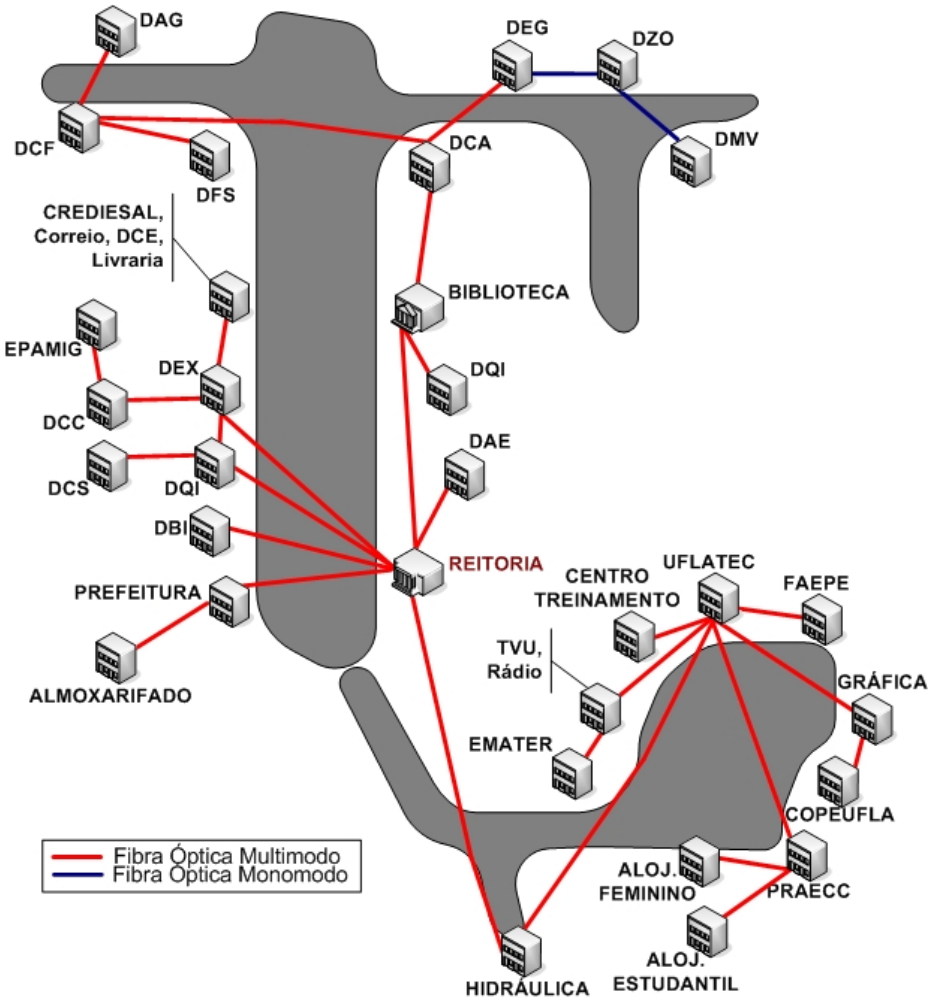

Figura 8.2: Disposição dos departamentos e links de fibra.

Atualmente o CIN-UFLA conta com um corpo técnico ligado diretamente a gerência da rede, o qual é constituído por 5 membros sendo 1 Chefe de Setor, 1 Gerente de Rede, 2 Administradores, 1 Cabista. O CIN-UFLA também conta com o auxílio de estudantes que exercem a função de monitoria de rede e suporte técnico. Estes monitores atuam nos departamentos e órgãos da UFLA.

Topologicamente, a rede UFLA apresenta características de uma rede em estrela hierárquica, sendo o CIN-UFLA, o seu centro de convergência. Um esboço da topologia lógica da rede UFLA pode ser observado abaixo:

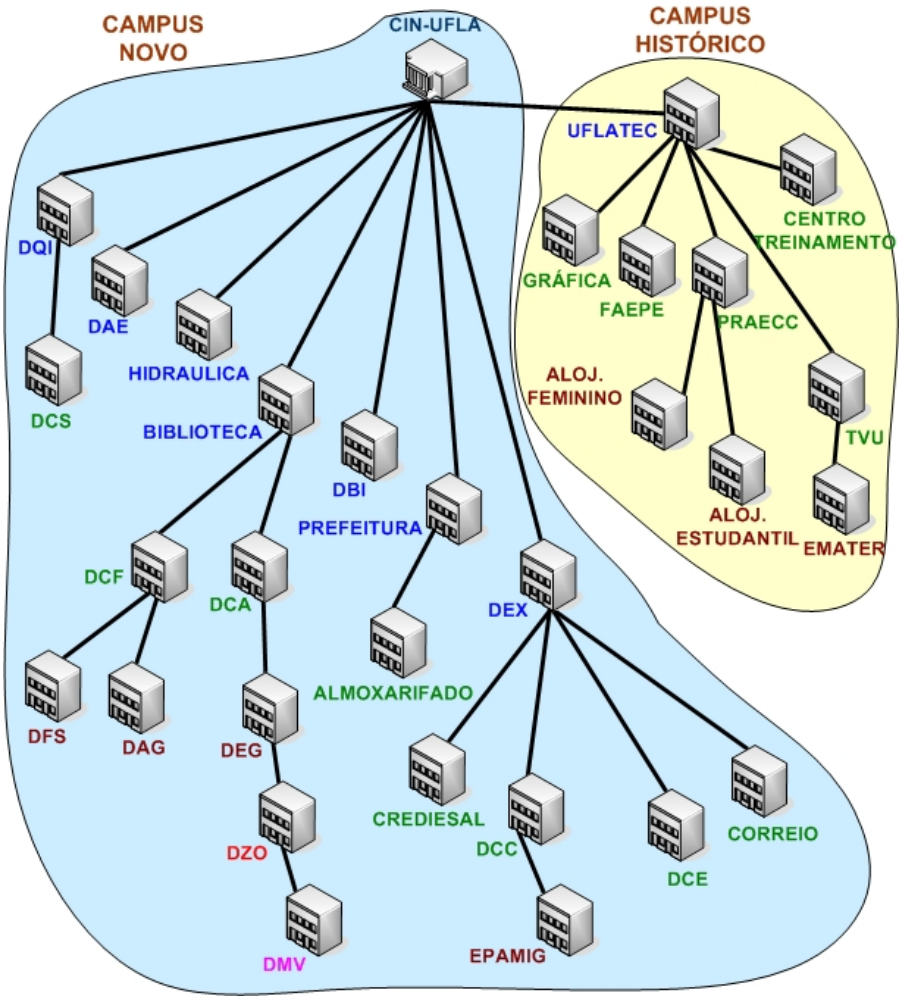

Figura 8.3: Topologia lógica da rede UFLA.

O padrão de rede utilizado na UFLA é o Ethernet. No CIN-UFLA estão localizados os equipamentos que servem de convergência para os links departamentais. Estes links utilizam um canal de fibra óptica multimodo com a exceção do departamento de Medicina veterinária que utiliza fibras monomodo. Um switch gerenciável da marca Planet modelo WGSW-1602 é utilizado como equipamento de convergência dos links departamentais. Este switch está localizado debaixo da escada no prédio da reitoria.

Um roteador Cisco modelo 3600 é utilizado para o roteamento dos links de internet da Embratel (link comercial, classe 200.251.242.128 máscara 255.255.255.128) e POP-MG (link acadêmico, 200.131.250, 200.131.251 e 200.131.253, máscara 255.255.255.0). Esses IPs estão distribuídos entre servidores e equipamentos de interconexão gerenciáveis.

Nos principais departamentos da UFLA existe um switch gerenciável (Planet modelo WGSW-1602) que tem a função de receber o link da Rede UFLA e distribuir para os demais equipamentos de interconexão localizados nos outros prédios do próprio departamento. A interligação destes equipamentos de interconexão com o switch gerenciável é feita através de fibra óptica. Os equipamentos de interconexão utilizados nos prédios de cada departamento estão divididos entre hubs e switchs.

Basicamente, cada departamento possui o seguinte conjunto de equipamentos:

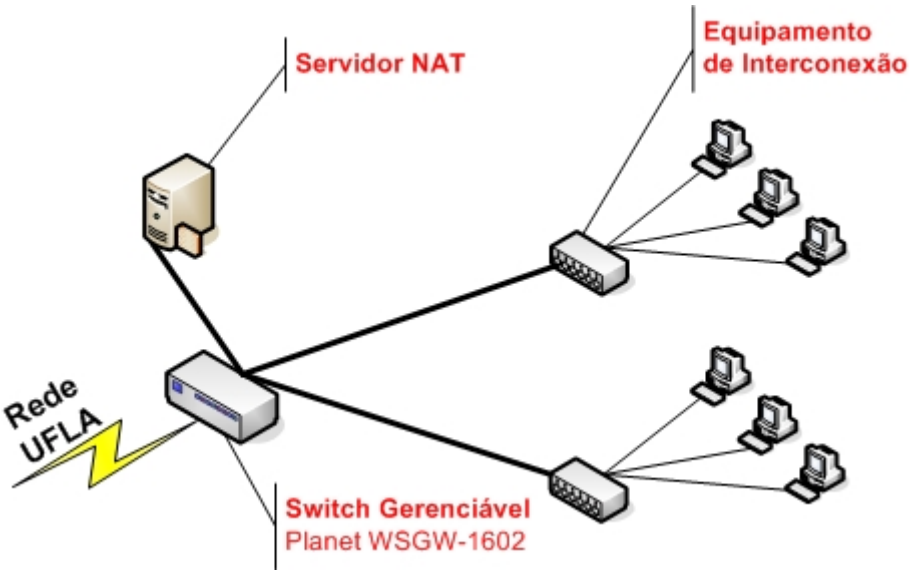

Figura 8.4: Equipamentos e Topologia básica nos departamentos da UFLA.

Um conversor de mídia recebe o sinal óptico da fibra e converte para sinal elétrico que é transmitido para o cabeamento metálico que é inserido no switch. A maioria dos conversores é de 10/100Mbps embora muitos conversores de 10Mbps ainda existam em alguns departamentos.

Uma outra função dos switchs gerenciáveis é a repetição de sinais para os equipamentos de outros departamentos (cascateamento). Cada departamento possui um micro computador (K6-II 550Mhz, 64Mb RAM) que tem a função de traduzir um IP válido em uma faixa de IPs inválidos que são utilizados pelas suas estações de trabalho (NAT).

O sistema operacional mais utilizado nas estações de trabalho dos departamentos da UFLA é o Windows 98, seguido pelo Windows XP.

8.3.2 Principais problemas encontrados

Após a realização do processo de análise, os principais problemas encontrados na rede UFLA são os seguintes:

- **Documentação:** A Rede UFLA é extremamente carente de documentação. Detalhes de infra-estrutura, equipamentos de interconexão, especificação dos armários de telecomunicação, rotas de cabos, configurações de equipamentos e demais itens não estão presentes na documentação do Centro de Informática. A falta deste tipo de documentação acaba por comprometer a agilidade na resolução de problemas de rede, o bom funcionamento das demais atividades de gerência e principalmente dificulta a implantação de melhorias.

- **Infra-Estrutura:** Os equipamentos de rede utilizados pelos departamentos da UFLA na sua grande maioria estão instalados em locais inadequados (salas de professores, secretarias, almoxarifados) sujeitos a poeira, umidade e acesso de pessoal não autorizado. O acesso dos técnicos do CIN-UFLA aos equipamentos é restrito e dificultado principalmente onde os equipamentos estão em salas de docentes e laboratórios. Os *racks* estão na sua maioria desorganizados o que dificulta a resolução de problemas. Os servidores de NAT estão depreciados e a falta de manutenção preventiva está comprometendo o funcionamento dos equipamentos.

- **Desempenho:** Com o crescimento rápido e desordenado típico de uma rede de campus, a Rede UFLA sofre com a excessividade de cascateamentos entre os switchs departamentais. Existem camadas hierárquicas bem mais extensas que as permitidas (EIA/TIA 568B) o que resulta em uma árvore de comunicação muito grande e sujeita e a longos períodos de *delay*. Por não estar segmentada o desempenho da rede sofre com os altos fluxos de pacotes de difusão. Os *loops* de encaminhamento de pacotes também são uma ameaça ao desempenho da rede. Este tráfego incoerente acaba por sobrecarregar os equipamentos de rede bem como as estações de trabalho. A perda de desempenho da rede UFLA também está relacionada com o excesso de gargalos. Existem departamentos que ainda possuem Hubs e conversores de 10Mbps.

- **Redundância:** A rede UFLA não possui rotas alternativas entre os departamentos e nem links de redundância. O excesso de cascateamentos entre os switchs dos departamentos compromete o tempo de parada da rede. Se um departamento que cascateia outros departamentos pára, os departamentos

subseqüentes também param. A falta de redundância inviabiliza a inclusão de rotas alternativas que de certa forma diminuiriam a sobrecarga em enlaces com muito tráfego.

- **Corpo Técnico:** O corpo técnico especializado do CIN-UFLA é bastante enxuto. Os monitores de rede mesmo recebendo todo o amparo do CIN-UFLA, não recebem treinamento e se destinam exclusivamente a solucionar problemas de suporte técnico.

8.4 Pesquisa e análise das soluções

A etapa de pesquisa teve a intenção de proporcionar uma maior familiaridade com o problema proposto e favorecer o conhecimento das soluções disponíveis. Esta fase possibilitou o mapeamento da rede não está segmentada. A infra-estrutura atualmente disponível na Rede UFLA pode ser observado na figura abaixo:

É também nesta etapa que o referencial teórico do projeto começou a tomar forma. Durante a fase de pesquisa pôde ser observado que as redes de campus possuem problemas pré-definidos e que estão totalmente relacionados com a sua natureza (crescimento rápido e desordenado).

O problema de desempenho das redes de campus são bastante claros e dentre outros fatores, refletem a falta de segmentação da rede. Com a falta de segmentação, um pacote de difusão lançado em uma rede local dentro de um dos departamentos da rede, pode percorrer todo o seu perímetro, mesmo já tendo encontrado o seu destino.

Dentre as formas de segmentação pesquisadas (Capítulo 6 - Segmentação e Capítulo 7 - VLAN) a segmentação por VLAN foi considerada a mais apropriada para rede UFLA pelos seguintes motivos:

- **Equipamentos de Interconexão:** Os switchs departamentais (Planet modelo WGSW-1602) são gerenciáveis e possuem capacidade de implementação de VLANs.

- **Hierarquia e Infra-estrutura:** A rede UFLA possui uma árvore hierárquica muito extensa (até a 7ª camada) e os switchs departamentais na maioria dos enlaces estão cascateados entre si. A VLAN permitiria a implementação de um "túnel"lógico que separaria o tráfego do departamento do tráfego da rede UFLA. No "túnel"da rede UFLA trafegaria somente os pacotes com destino ao CIN-UFLA. Pacotes de difusão estariam restritos aos departamentos. Com a diminuição de tráfego o tempo de *delay* para o encaminhamento de pacotes também seria reduzido.

- **Flexibilidade e Facilidade:** A implantação de VLAN é um processo mais flexível e amigável de ser implantado do que a configuração de um roteador.

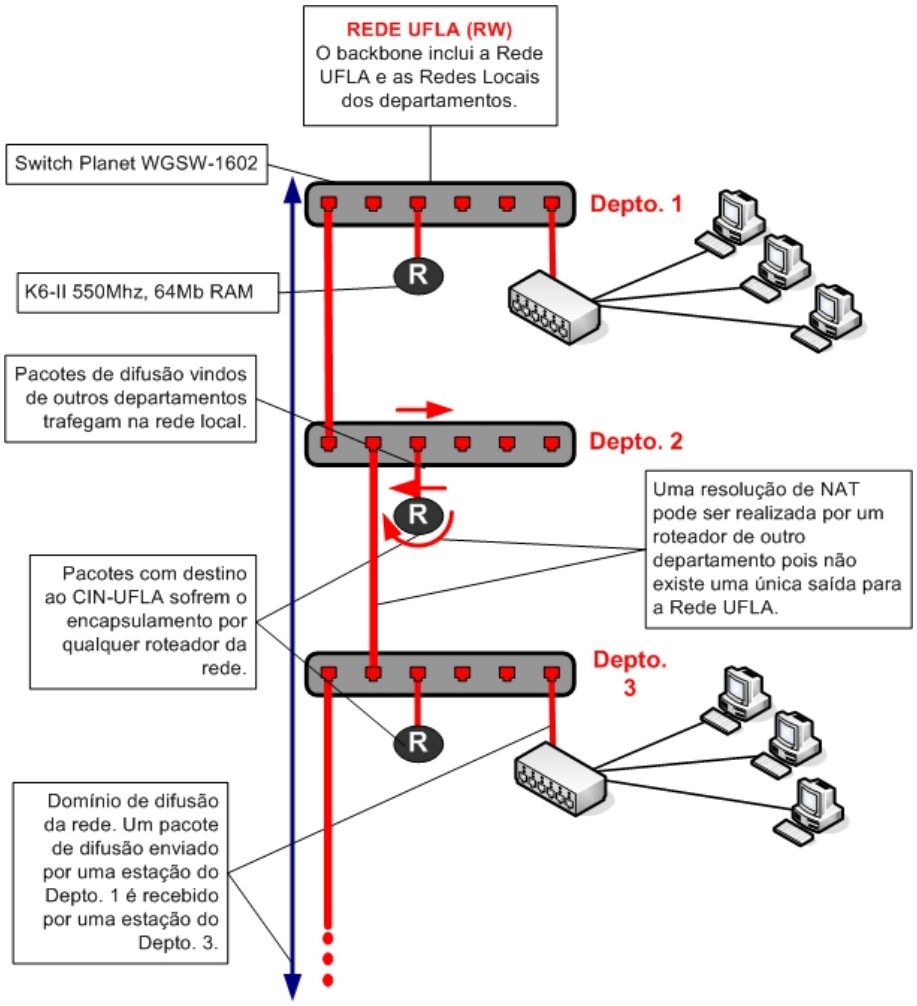

Figura 8.5: Infra-estrutura atual da Rede UFLA (Rede Não Segmentada).

A interface Web presente nos switchs gerenciáveis agiliza a definição das portas e o seu relacionamento com cada VLAN.

- **Gerência:** Por serem gerenciáveis estes equipamentos podem ser administrados via Web evitando o deslocamento de um técnico do CIN-UFLA ao departamento. A inclusão ou retirada de uma porta membro de uma VLAN, e as punições de departamentos por transgressão de políticas de uso podem ser realizadas remotamente. Estes equipamentos também possuem dados estatísticos por porta contribuindo para o enriquecimento de diagnósticos de rede.

- **Custo:** O custo de adequação da infra-estrutura é praticamente nulo pois os equipamentos já estão disponíveis. A readequação dos enlaces se faz necessária, mas poderia ser realizada aos poucos. As VLANs seriam uma medida emergencial e de baixo custo.

Com a segmentação da Rede UFLA a nova estrutura da rede ficaria da seguinte forma:

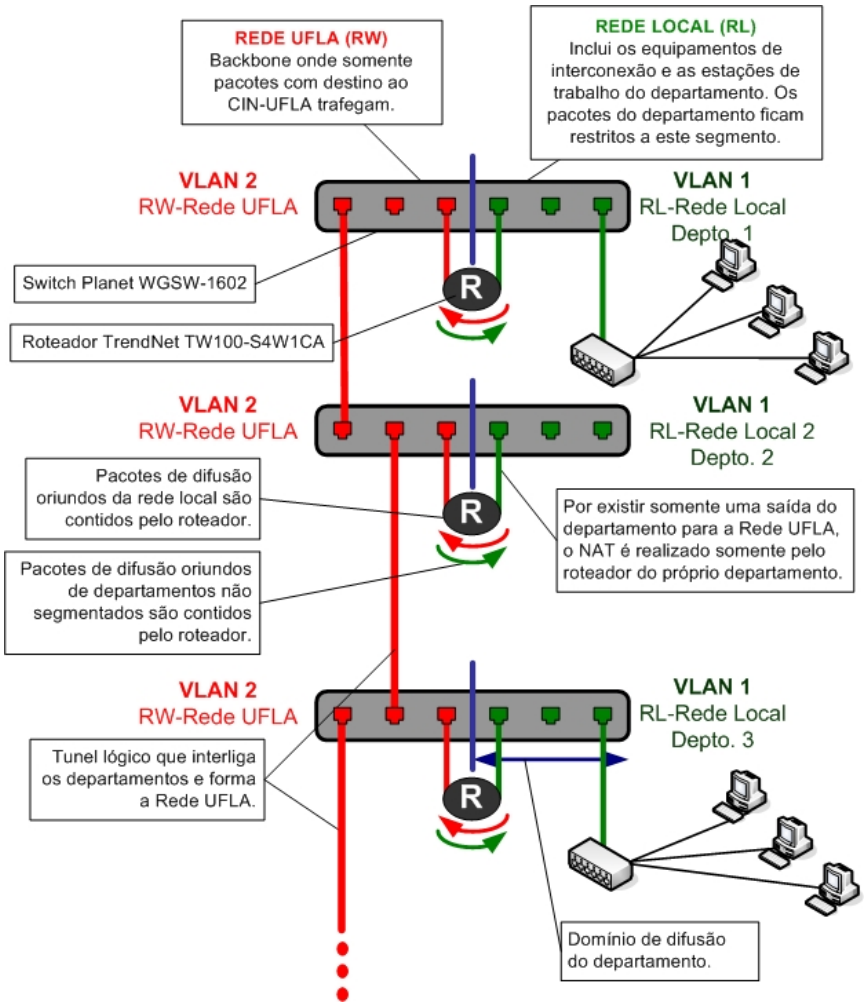

Figura 8.6: Nova proposta de infra-estrutura para Rede UFLA (Rede Segmentada).

8.5 Teste em laboratório da solução

Para que a implantação em campo fosse menos traumática, previamente foi realizada a fase de configuração e testes. Nesta fase a eficácia da VLAN também foi testada.

O CIN-UFLA foi utilizado como laboratório de teste da solução proposta. Um switch gerenciável de 24 portas marca XB Systems modelo XB 30400, foi utilizado no teste da VLAN. Para a configuração da VLAN foi utilizado um notebook Toshiba (Pentium IV 2.8Ghz, 512Mb RAM, Windows XP). Inicialmente o switch foi acessado por interface terminal e seu endereço IP foi configurado como 200.131.250.115. Após configurado o switch foi acessado via http. A forma de configuração da VLAN foi a manual (Capítulo 7 - VLAN pág45). Este tipo de configuração foi escolhida pois a inserção de novos membros em cada VLAN é estática.

As VLANs devem ser criadas antes da atribuição das portas. Um número (PID) e um nome é atribuído para a VLAN. A VLAN 1 é a VLAN padrão do equipamento. Foi criada a VLAN 2 (**PVID=2**) cujo nome foi definido como **redelocal**, e a VLAN 3 (**PVID=3**), cujo nome foi definido como **redewan**. A VLAN 2 abrange todos os equipamentos de interconexão e estações de trabalho do departamento. Todo tráfego local incluindo os pacotes de difusão fica restrito a esta rede. Na VLAN 3 temos a rede UFLA que trafega os pacotes de dados com destino ao CIN-UFLA.

Para determinar os membros de cada VLAN foi utilizado o agrupamento por portas (Capítulo 7 - VLAN pág43). Este tipo de VLAN foi escolhido pois atende bem ao propósito da segmentação além do fato de que todos os membros da VLAN estão localizados no mesmo equipamento. A facilidade de gerenciamento deste tipo de VLAN também foi considerada pois de certa forma agilizaria a resolução de problemas.

Após a criação das VLANs as portas foram atribuídas. As portas 10 a 14 foram configuradas na VLAN 2 e foram atribuídas para a Rede Wan (Rede UFLA). As portas 15 a 20 foram configuradas na VLAN 3 e foram utilizadas pela Rede Local.

Todas as portas utilizaram o padrão de comunicação implícito (Capítulo 7 - VLAN pág46). A marcação explícita não se fez necessária pelo fato de que todos membros da VLAN estão localizados no mesmo equipamento. Para receber a característica de marcação implícita, as portas foram marcadas como U (*Untagged*). Neste tipo de marcação os pacotes se relacionam com cada VLAN através do seu número PVID (*Port VLAN Identification*).

O tipo de comunicação utilizado para o estabelecimento de tráfego entre as VLANs foi roteamento externo (Capítulo 7 - VLAN pág47 "7.5.1 - Roteamento através de múltiplos enlaces"). Foi utilizado um roteador de Banda Larga Planet modelo XRT-401D para realizar o roteamento entre as VLANs. O baixo custo deste equipamento foi considerado na sua escolha. Este roteador também tem o

propósito de substituir os servidores NAT dos departamentos, os quais conforme citado anteriormente, estão depreciados. As vantagens da utilização deste tipo de roteador residem na fácil configuração, a possibilidade de gerência remota via web, firewall integrado e o baixo consumo de energia.

O roteador XRT-401D possui 5 portas sendo 1 porta WAN e 4 portas LAN. A porta WAN foi configurada estaticamente com um IP válido 200.131.250.118. O endereço da interface local do roteador foi definido como 192.168.199.1. Com este IP o roteador também realiza a função de gateway e realiza o NAT utilizando a faixa de IPs 192.168.199. A opção de DHCP foi desabilitada com a intenção de retirar a sobrecarga do roteador.

Após a configuração do roteador, a porta Wan foi conectada a porta 14 do switch e a porta 1 do roteador foi conectada a porta 15 do switch. Na porta 10 foi ligado o link com a Rede UFLA. Um notebook Compaq modelo Armada 1500c (Celeron 350Mhz, 64Mb RAM, Windows XP), foi configurado como estação de trabalho na rede local com o endereço IP 192.168.199.2 e foi inserido na porta 16 do switch. O notebook Toshiba foi conectado na porta 17 do switch com o endereço IP 192.168.199.11.

Antes de ativar as VLANs foi utilizado um analisador de protocolos (Sniffer Pro 4.7) com a intenção de analisar os pacotes e os protocolos que estavam trafegando na rede. Neste teste antes da segmentação foi constatada uma grande quantidade de pacotes de difusão de departamentos do campus histórico e principalmente de departamentos do novo campus.

Após a execução deste teste, a VLAN 1 foi desativada e as VLANs 2 e 3 foram ativadas. Um esboço das conexões realizadas pode ser observado abaixo:

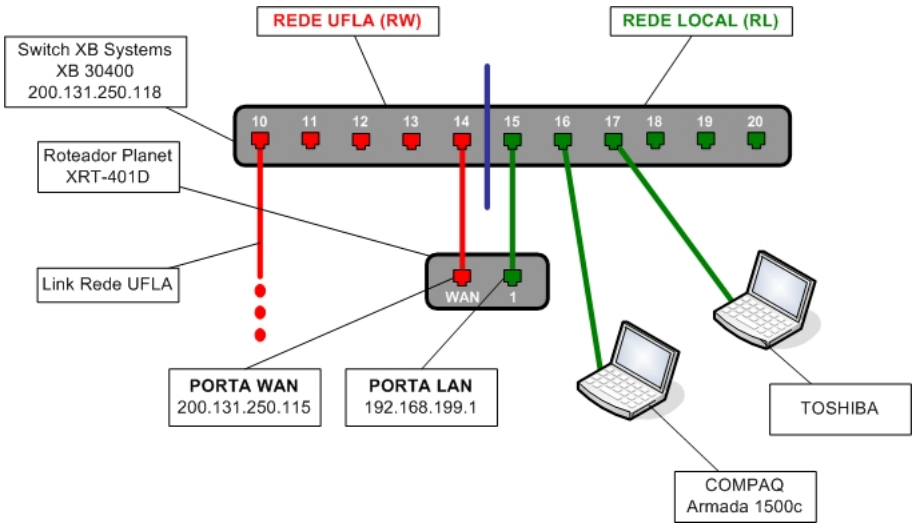

Figura 8.7: Escopo das conexões utilizadas durante a fase de testes.

Após a ativação das VLANs 2 e 3 a rede local de teste estava segmentada. Inicialmente foi feito um teste de busca e navegação, utilizando os notebooks, em sites da internet. Neste teste tanto a busca quanto a navegação se comportaram normalmente.

Foi executado um ping dos notebooks ao endereço 200.131.250.1 (servidor de DNS) e este procedeu corretamente com perdas mínimas de pacote (menos de 3%). Após este teste o Compaq foi colocado diretamente na rede UFLA. Um ping foi executado novamente ao endereço 200.131.250.1, mas ao contrário do que acontecia na rede não segmentada o ping não pode ser estabelecido. Esta falha ocorreu pois o micro Compaq não pode encontrar o seu servidor de NAT e desta forma não pode sofrer o encapsulamento necessário para que um pacote trafegue de uma rede de IPs inválidos para uma rede de IPs válidos.

O notebook Compaq foi novamente inserido na rede Local mas teve o seu endereço IP trocado para 192.168.70.15. Uma nova execução de ping foi realizada ao servidor DNS mas igual ao teste anterior ele não recebeu resposta. Este teste provou que uma máquina fora de sua rede local, quando na rede segmentada, não consegue encontrar o seu servidor de NAT pois é "barrado"pelo roteador.

Um novo teste com o analisador de protocolos foi realizado onde foi constatado que somente pacotes com endereço 192.168.199 trafegavam na rede local. Após este teste a eficiência da segmentação estava comprovada.

8.6 Implantação em Campo

A implantação do projeto foi realizada no Campus da Universidade Federal de Lavras mais precisamente no Departamento de Medicina Veterinária da UFLA. Um esboço da rede do departamento de medicina veterinária pode ser observado abaixo:

O departamento de veterinária foi escolhido por estar situado na última camada da hierarquia da rede UFLA, sendo uns dos departamentos que mais sofre com a quantidade excessiva de cascateamentos.

O departamento de Veterinária é um complexo composto de 6 prédios (Morfologia, Farmacologia, Patologia, Medicina Veterinária Preventiva, Hospital Veterinário e Bloco Cirúrgico). No prédio da Patologia está localizado o switch principal (WSGW-1602). Um conversor de 10Mbps converte o sinal da fibra monomodo, que tem origem no departamento de zootecnia, para o cabeamento metálico.

O rack da Patologia é o principal do departamento. Nele estão localizados o switch gerenciável e os conversores de mídia utilizados pelos outros prédios do departamento bem como o conversor utilizado no link com o departamento de zootecnia. Os principais problemas encontrados foram o sub-dimensionamento

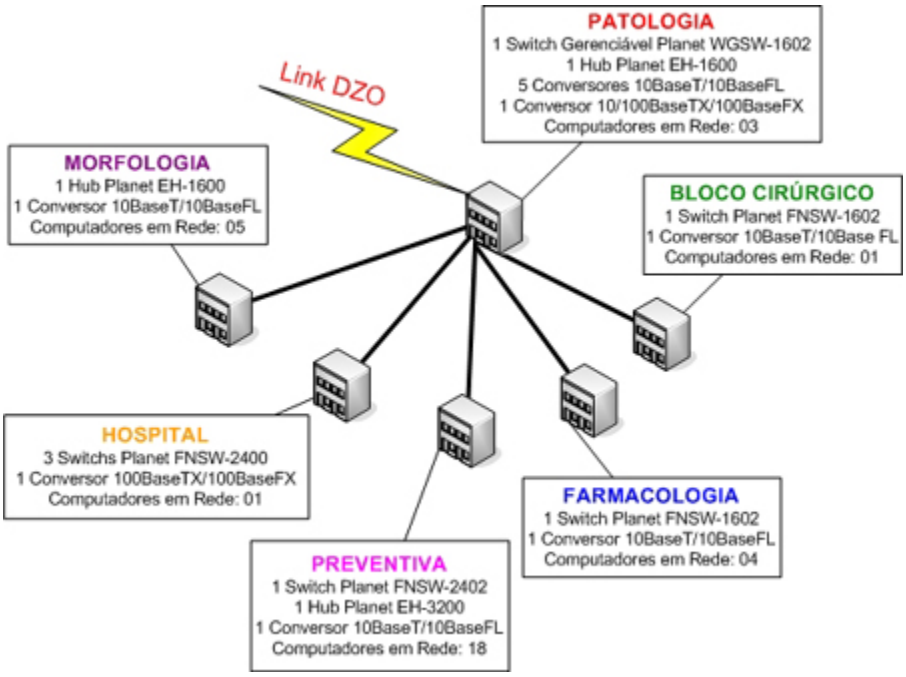

Figura 8.8: Topologia de Rede do Departamento de Medicina Veterinária.

do rack, que dificultou a sua organização e os conversores dos outros prédios do departamento que não estavam identificados.

Inicialmente o switch foi acessado via terminal e seu endereço IP (200.131.250.119) foi configurado. A partir desta configuração todos os ajustes foram realizados através da interface web.

É uma premissa para a instalação das VLANs que o rack que comporta o switch principal da rede do departamento seja organizado e os links para cada prédio estejam identificados. Somente desta forma, uma separação das portas a serem utilizadas em cada VLAN poderá ser realizada corretamente.

Na porta 8 do switch foi conectado o link da rede local que por sua vez foi inserido na porta LAN número 1 do roteador. Na porta 12 do switch foi conectado o link da rede UFLA que por sua vez foi inserido na porta WAN do roteador.

A organização das portas do switch ficou estabelecida conforme a figura abaixo:

Após a organização dos cabos os conversores foram conectados ao switch principal em seqüência das portas 1 a 6. Na porta 16 foi conectado o conversor do link que vem da zootecnia e devido a este conversor esta porta foi configurada para uma velocidade de transmissão de 10Mbps Half Duplex. O conversor passou a funcionar corretamente no switch somente após a definição desta velocidade de comunicação.

Figura 8.9: Configuração geral do switch.

Figura 8.10: Configuração dos IPs.

Como equipamento alternativo aos atuais servidores de NAT, foi utilizado um roteador TrendNet TW100-S4W1CA. O roteador foi configurado estaticamente com o IP válido 200.131.250.118, gateway 200.131.250.129. A faixa de endereços utilizada foi a 192.168.110 sendo o endereço 192.168.110.1 atribuído ao roteador.

Conforme citado anteriormente, as vantagens da utilização destes equipamentos residem na fácil configuração, no baixo consumo de energia, no firewall integrado a na possibilidade de configuração remota via http. Uma outra vantagem deste tipo de equipamento é que ele é dedicado ao seu propósito enquanto que as estações atualmente utilizadas são moldadas para se tornarem um servidor de NAT. Por possuir uma arquitetura mais simples que um PC, a possibilidade de ocorrer falhas no equipamento também são muito menores.

Após configuração do roteador, as VLANs foram configuradas conforme pode ser observado na figura abaixo:

Foram criadas duas VLANs sendo a VLAN 1 determinada para a rede local (PVID=1, RL-DMV) e a VLAN 2 determinada para a rede UFLA (PVID=2, RW-REDEUFLA). As portas 1 a 9 foram ajustadas para a VLAN 1 e as portas 10 a 16 para a VLAN 2.

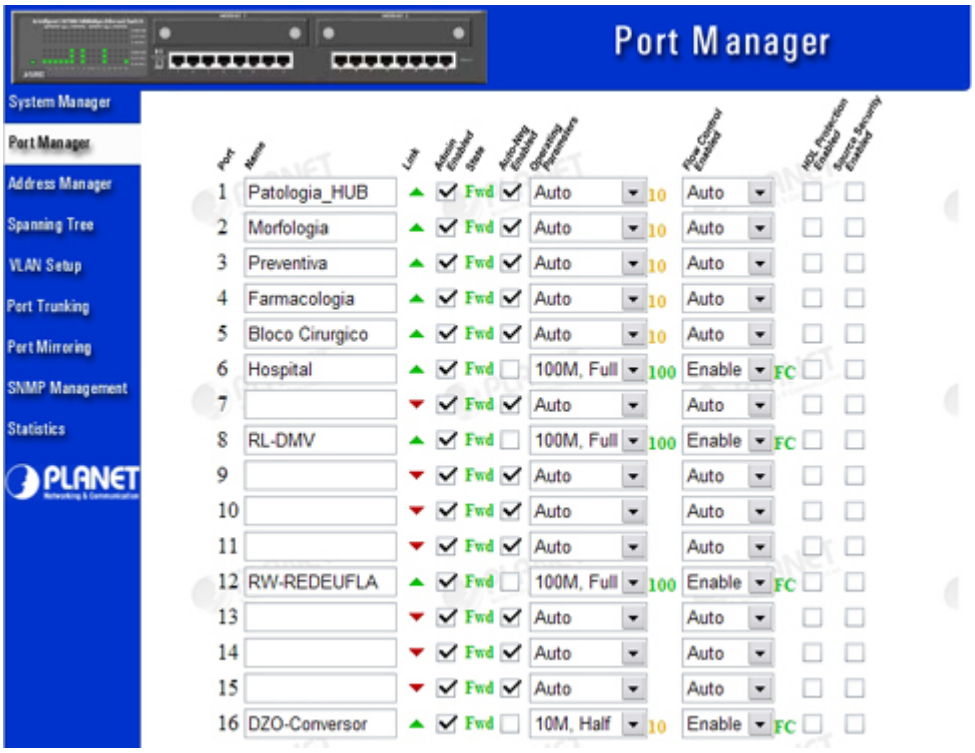

Figura 8.11: Gerência das portas do switch.

Para que um pacote possa ser encaminhado corretamente para sua VLAN, cada porta do switch deve ser atribuída com um PVID da sua VLAN correspondente.

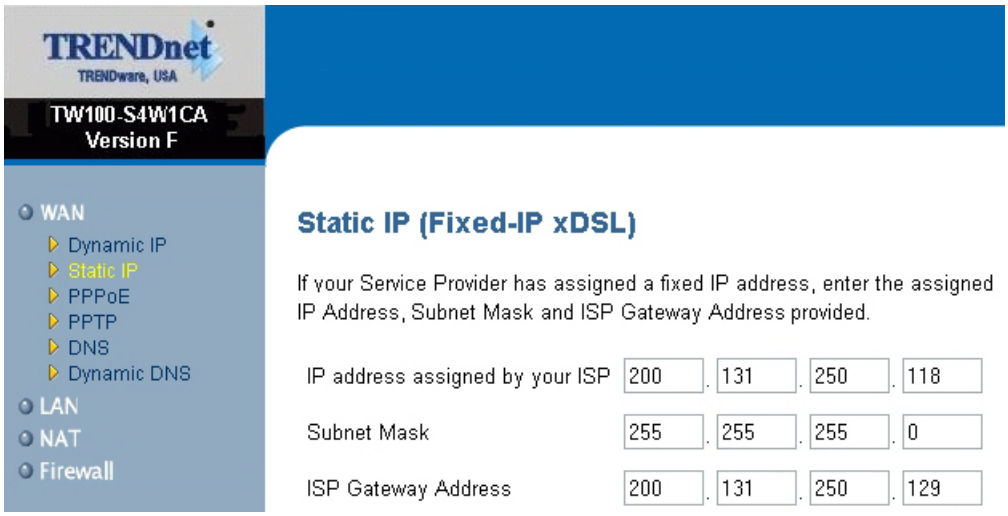

Figura 8.12: Configuração dos IPs do roteador.

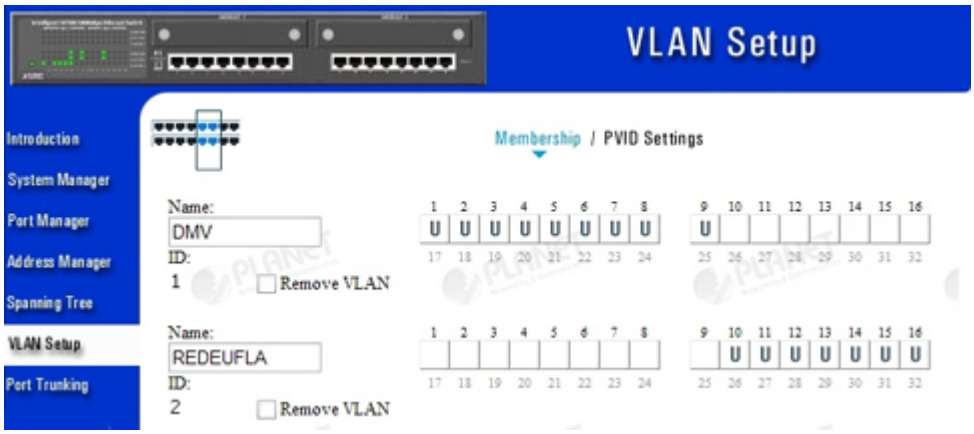

Figura 8.13: Determinação do conjunto de portas para cada VLAN.

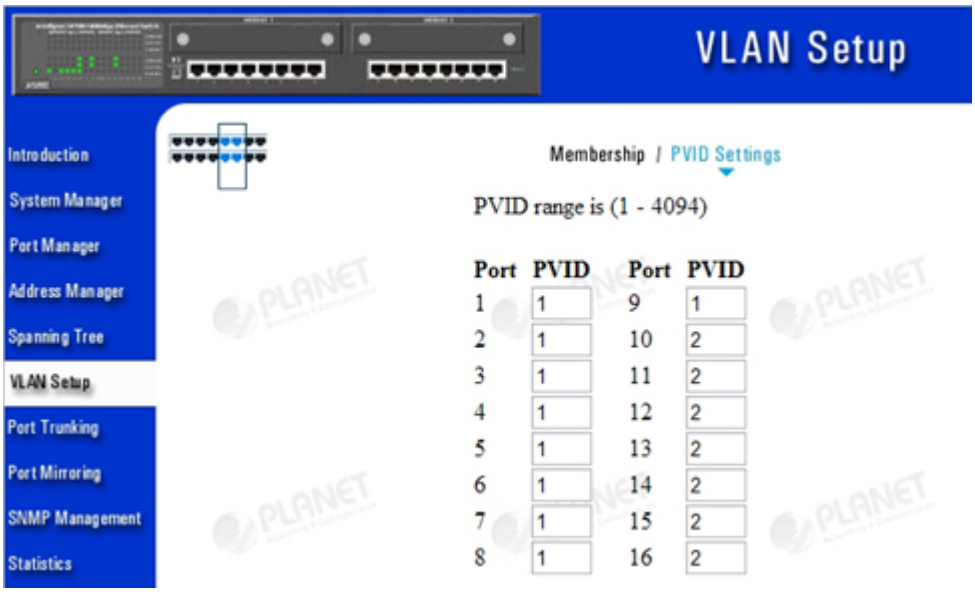

Figura 8.14: Determinação dos PVIDs de cada porta da VLAN.

Capítulo 9

Apresentação dos resultados

Um notebook HP Pavilhon ZE4300 (Pentium IV 2.2Ghz, 512Mb de RAM), foi utilizado como estação de teste sendo conectado a porta 10 que sofreu um espelhamento da porta 16 do switch. Este procedimento, também é chamado de SPAN (*Switched Port Analyzer*).

9.1 Teste da Tabela de *Hosts*

O primeiro teste realizado foi a análise da tabela de hosts inseridos na rede do DMV e pode ser observado na figura abaixo:

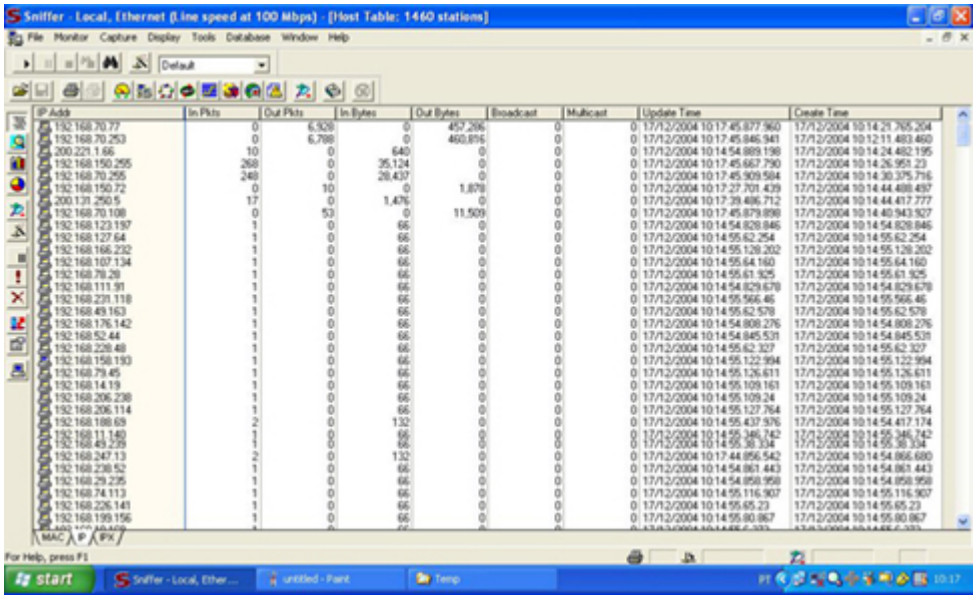

Figura 9.1: Análise dos hosts presentes na rede do DMV antes da segmentação.

Este teste além de detalhar todos os equipamentos inseridos na rede realiza uma contagem dos pacotes que ela enviou e recebeu. Antes da segmentação ter sido realizada, o analisador de protocolos constatou a presença de *hosts* de praticamente todas as redes válidas e inválidas disponíveis na rede UFLA. Este teste comprova que sem a segmentação a rede UFLA se comporta como uma grande e única rede. Durante este teste foi detectada a presença de 1460 estações.

O teste também serviu para mostrar que além de pacotes de difusão, pacotes *unicast* advindos de outras redes também entram no departamento. A presença deste tipo de pacote constatada pois os switchs (quando não segmentados) realizam a função de roteamento, e por trabalharem na segunda camada, não realizam tal procedimento de forma eficaz.

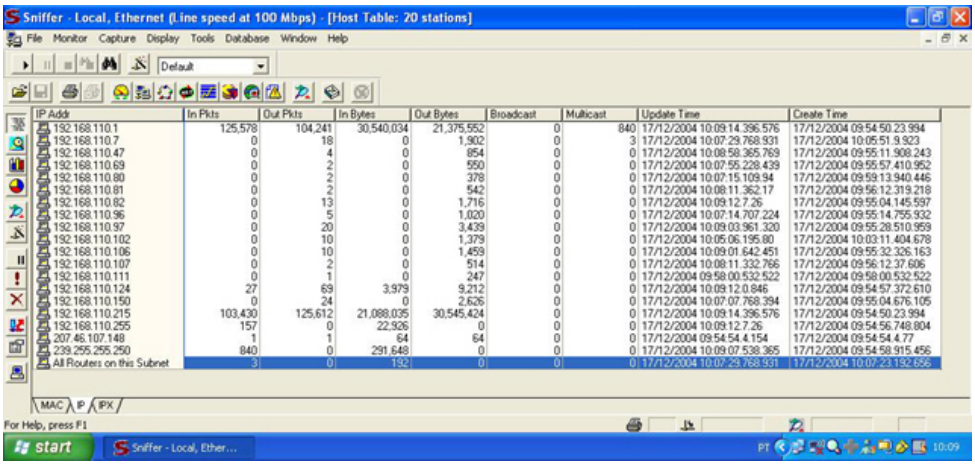

Figura 9.2: Análise dos pacotes que trafegam no DMV após a segmentação.

O mesmo teste foi realizado após a segmentação do departamento. O notebook foi conectado na porta 9 do switch que foi atribuída a VLAN 1. A porta 8 do switch, que é a porta que sai do roteador e serve de interface para a rede local, foi espelhada na porta 9 e desta forma todo o tráfego que entra na rede local passa pelo analisador.

Observando a figura acima podemos constatar somente a presença de estações da rede 192.168.110 que é justamente a rede do departamento de veterinária. Alguns IPs válidos também estão presentes no tráfego da rede mas estes são a minoria.

9.2 Teste da Distribuição de Protocolos

O segundo teste realizado foi a distribuição de protocolos de comunicação utilizados na rede UFLA.

Conforme pode ser observado na figura 9.3, uma grande variedade de protocolos estão sendo disponibilizados no departamento. O protocolo http, utilizado na navegação web, está entre os protocolos mais utilizados seguido pelo POP, utilizado pelo serviço de e-mail. A grande utilização destes protocolos reforça a necessidade de se estruturar a rede UFLA conforme a regra 20/80 já que quase a totalidade do tráfego disponibilizado pelas estações locais, possui a *Server Farm* (CIN-UFLA) como *site* destino.

Após a segmentação uma quantidade significativa de protocolos deixaram de ser distribuídos na rede local. Este teste serviu para mostrar o poder de otimização da VLAN já que somente os protocolos realmente utilizados pelas estações do departamento estão disponibilizados.

9.3 Teste da Matrix de Conectividade

O terceiro teste realizado foi a matriz de conectividade. A matriz de conectividade obtida antes da segmentação pode ser observada na figura 9.4.

Neste teste todas as interligações de comunicabilidade entre as estações de trabalho são apresentadas. Após a segmentação a matriz sofre uma redução de conexões considerável. Somente as estações do próprio departamento podem estabelecer uma conexão direta pois estão na mesma rede. Os pacotes de difusão ficam restritos as estações de trabalho do próprio departamento não alcançando a rede UFLA.

Um número reduzido de estações de trabalho passa a disputar o meio de comunicação. De uma rede com aproximadamente 2000 estações de trabalho obtemos uma rede com apenas 20 estações.

Esta redução de equipamentos favorece a obtenção de uma maior largura de banda para as máquinas do departamento. Um reflexo direto da segmentação é a redução no tráfego dentro do segmento local. Com um tráfego reduzido tanto os equipamentos de interconexão quanto as estações de trabalho diminuem o processamento de pacotes.

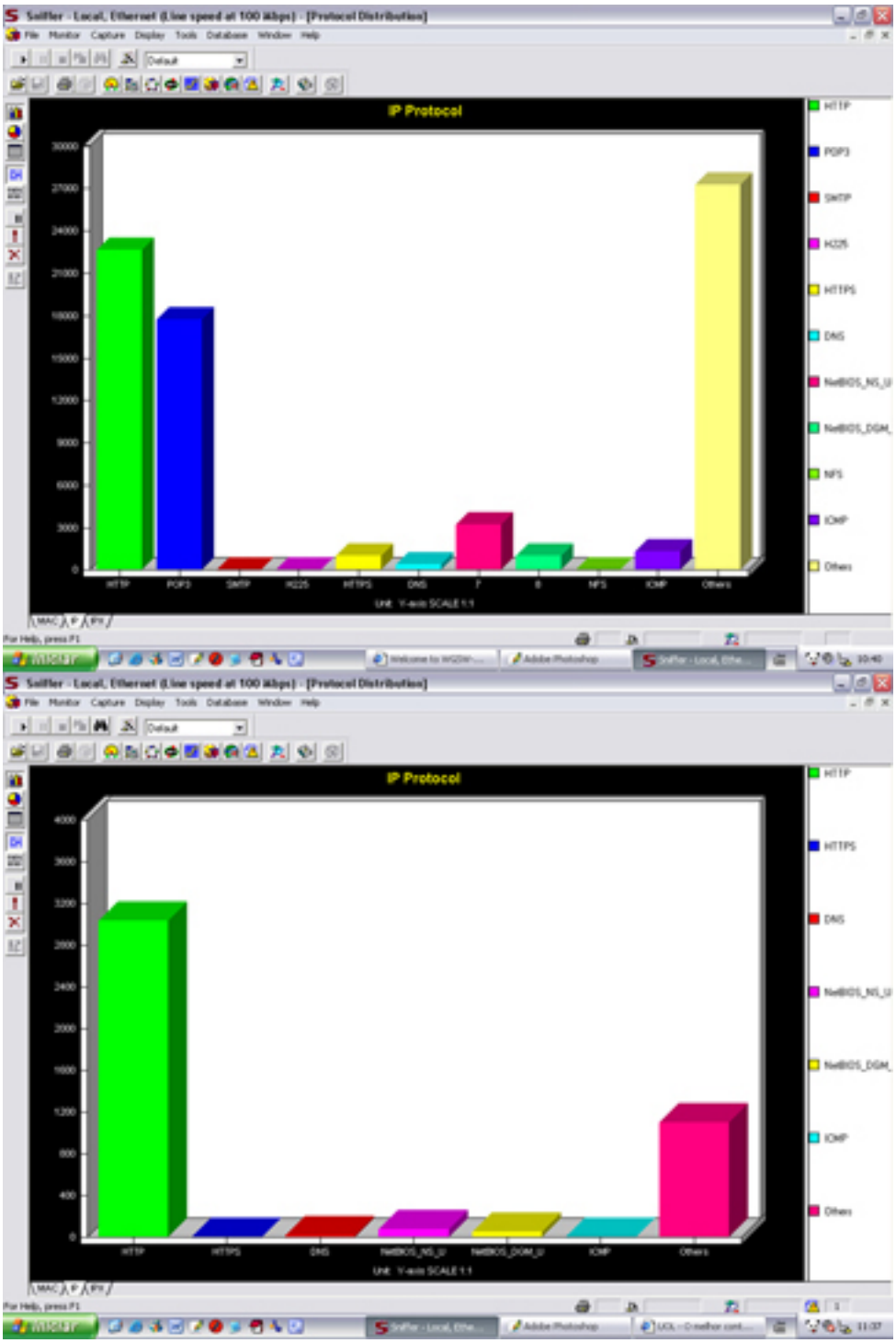

Figura 9.3: Análise dos protocolos que trafegam no DMV antes e depois da segmentação.

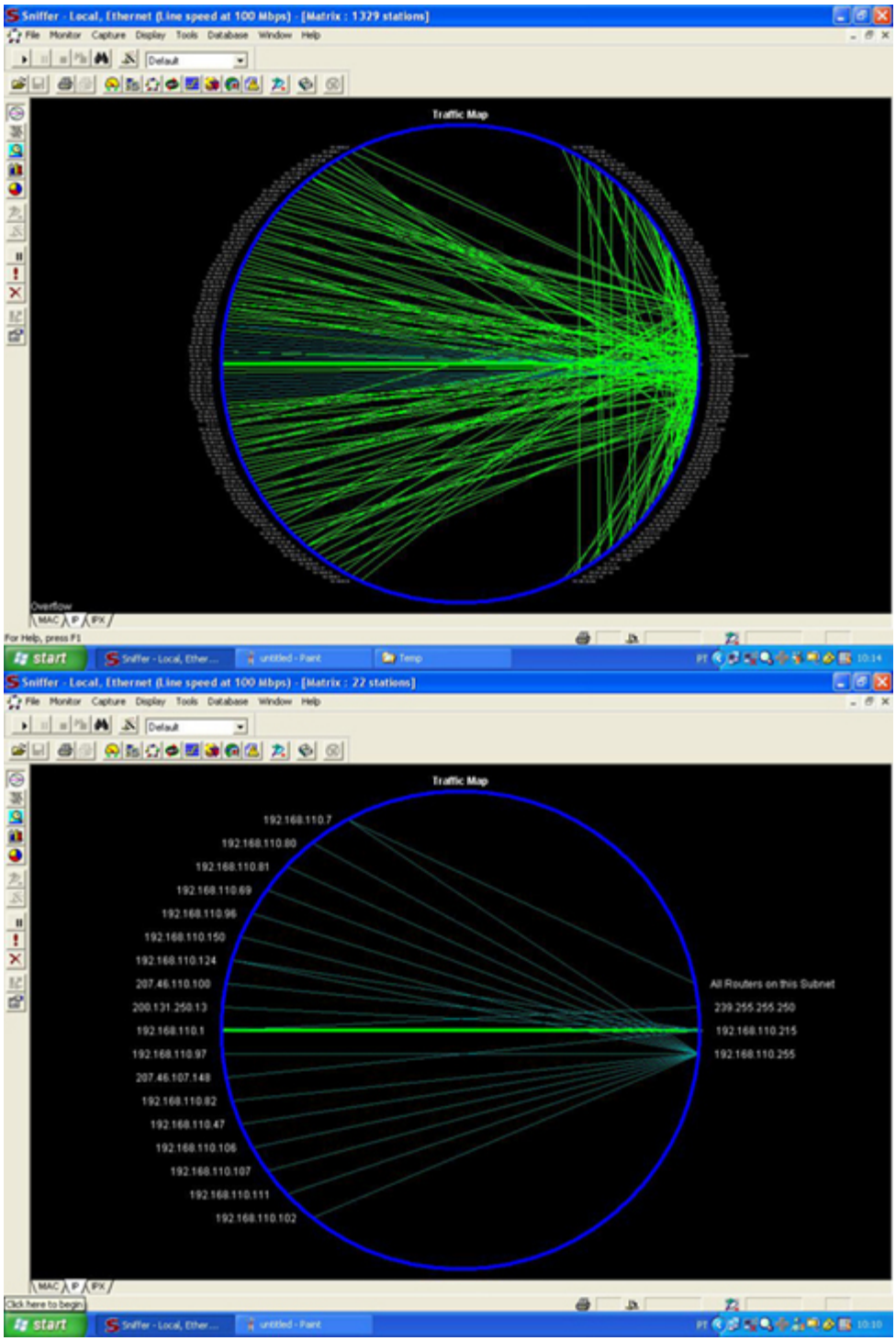

Figura 9.4: Matriz de conectividade da rede do DMV antes e depois da segmentação.

Capítulo 10

Conclusão

Após a implantação e testes da VLAN, foi possível constatar na prática a eficiência da segmentação como técnica de otimização do tráfego da rede UFLA. A hipótese de que a VLAN seria a melhor técnica a ser utilizada foi comprovada por ser a mais amigável, a de menor custo e a que se adaptou mais facilmente a atual infra-estrutura física da rede.

É interessante observar que a otimização dos recursos já existentes ainda é considerada a forma mais coerente para a resolução dos problemas enfrentados pela rede UFLA. A configuração dos equipamentos já disponíveis contribuiu para que os objetivos fossem alcançados a um custo praticamente zero.

Vale ressaltar também, que a utilização destes recursos favorece a gerência remota, atividade indispensável a uma equipe técnica enxuta como é o caso do CIN-UFLA. Os processos de resolução de problemas de rede, a aplicação de punições por transgressões de políticas de uso, os diagnósticos de estado da rede bem como outras atividades são facilitadas com a implantação da gerência remota.

Como trabalho futuro, além da segmentação de todos os departamentos da UFLA uma identificação e documentação de toda a sua infra-estrutura, bem como a implantação de DHCP[4] nos departamentos poderiam ser realizados. Isso resultaria em uma maior otimização dos recursos disponíveis e agilizaria os processos de gerência e resolução de problemas da rede.

[4](*Dynamic Host Configuration Protocol*). Protocolo de configuração dinâmica de host. O IP da estação é determinado automaticamente quando ela é inserida na rede

Referências Bibliográficas

[BOYLES, *et.Al.*,1999] BOYLES, Tim; DOWNES, Kevin; ***Cisco Lan Switch Configuration Exam Certification Guide*** - Copyright© 1999 by Cisco Press.

[CLARK, *et.Al.*,1999] CLARK, Kennedy; HAMILTON, Kevin; ***CCIE Professional Development: Cisco LAN Switching*** - 1st Edition Copyright© 1999 by Cisco Press.

[COELHO, 2003] COELHO, Paulo E.; ***Projeto de Redes Locais com Cabeamento Estruturado*** - 1ª Edição Editora Instituto On Line, 2003.

[COMER, 1999] COMER, Douglas; ***Computer Networks and Internets*** - 2nd Editon Copyright© 1999 by Prentice Hall Inc.

[FEIBEL, 1996] FEIBEL, Werner; ***Encyclopedia of Networking*** - 2nd Edition Copyright © 1996 by SYBEX Inc.

[GIL, 1991] GIL, Antônio Carlos; ***Como Elaborar Projetos de Pesquisa*** - 3ª Edição Atlas, 1991.

[HALL, 2000] HALL, Eric A.; ***Internet Core Protocols: The definitive guide*** - 1st Edition Copyright© 2000 by O'Reilly.

[HELD, 2003] HELD, Gilbert; ***Ethernet Networks: Design, Implementation, Operation, Management*** - 4th Edition Copyright© 2003 by John Wiley & Sons Ltda.

[JACK, 2003] JACK, Terry; ***CCNP: Building Cisco Multilayer Switched Networks*** Copyright© 2003 SYBEX Inc.

[LOPES, *et.Al.*, 2000] LOPES, Raquel V.; SAUVÉ, Jacques P.; NICOLLETTI, Pedro S.; ***Melhores Práticas para Gerência de Redes de Computadores*** - Copyright© 2003 Editora Campus.

[MCGREGOR, 1998] MCGREGOR, Mark; ***Cisco CCIE Fundamentals: Network Design & Case Studies*** - 2nd Edition Copyright© 1998 by Macmillan Technical Pub.

[MUELLER, 2003] MUELLER´s, Scott; ***Upgrading and Reparing Networks*** - 4th Edition Copyright© 2003 by Que® Publishing.

[NEMETH, *et.Al.*, 2001] NEMETH, Evi; SNYDER, Garth; SEEBASS, Scott; HEIN, Trend R.; ***Manual de Administração do Sistema UNIX*** - 3ª Edição Copyright© 2001 Editora Bookman.

[ODOM, 2001] ODOM, Sean; NOTTINGHAN, Hanson ***Cisco Switching Black Book*** - Copyright© 2001 by Coriolis Group.

[PASSMORE, 1996] PASSMORE, David; ***The virtual LAN technology report*** Copyright© 1996 by Decisys.

[SHINDER, *et.Al.*, 2003] SHINDER, Debra Littlejohn; SHINDER, Thomas W.; **MCSA/MCSE:** ***Implementing, Managing, and Maintaining a Windows Server 2003 - Network Infrastructure Guide*** - Copyright© 2003 by Syngress.

[SPURGEON, 2000] SPURGEON, Charles E.; ***Ethernet: O guia definitivo*** - Copyright© 2000 O'Reilly, Tradução autorizada à Editora Campus Ltda.

[STEVENS, 1993] STEVENS, W. Richard; ***TCP/IP Illustrated Vol.1 - Protocols*** - Copyright© 1993 by Addison-Wesley.