UTFPR - UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

RODRIGO DURAN GONZALEZ

PROPOSTA DE IMPLEMENTAÇÃO DE UMA ESTRUTURA DE REDE DE DADOS PARA UMA COMISSÃO REGIONAL DE OBRAS

Curitiba

2015

RODRIGO DURAN GONZALEZ

PROPOSTA DE IMPLEMENTAÇÃO DE UMA ESTRUTURA DE REDE DE DADOS PARA UMA COMISSÃO REGIONAL DE OBRAS

Monografia apresentada à Universidade Tecnológica Federal do Paraná para conclusão do curso de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes.

Orientador: Prof. Kleber Kendy Horikawa Nabas

Curitiba

2015

RODRIGO DURAN GONZALEZ

PROPOSTA DE IMPLEMENTAÇÃO DE UMA ESTRUTURA DE REDE DE DADOS PARA UMA COMISSÃO REGIONAL DE OBRAS

Monografia apresentada à Universidade Tecnológica Federal do Paraná para conclusão do curso de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes.

Orientador: Prof. Kleber Kendy Horikawa Nabas

Aprovação em: _____/_____/_____

Banca Examinadora:

_____

Prof. _____

_____

Prof. _____

_____

Prof. _____

RESUMO

Esta monografia tem como objetivo geral criar uma proposta de implementação de uma estrutura de rede de dados para uma comissão regional de obras. Os objetivos específicos são analisar a estrutura de rede atual da comissão, e realizar um estudo teórico sobre tecnologia de redes, ressaltando seu histórico, modos de transmissão, topologias e classificação de redes; compreender as tecnologias de redes, em especial as redes ethernet; estudar os equipamentos de rede, como switchs, roteadores e outros; além de teorizar sobre as ferramentas de rede, como VPNS, VLANS e outras. A metodologia é a revisão de literatura. Este trabalho procurou mostrar alguns aspectos importantes a serem considerados em projetos relacionados à redes de computadores. Diante das novas tecnologias disponíveis no mercado, a queda de custos de equipamentos e serviços, aliados ao aumento da velocidade e capacidade dos meios comunicação e processamento de informações disponíveis no mercado, permitem atender a uma demanda de novos serviços e melhorar o desempenho dos existentes, criando novas demandas nas empresas.

Palavras-chave: Redes de Dados. Implementação. Estrutura.

ABSTRACT

This paper has as main objective to create a proposal to implement a data network structure for a regional commission works. The specific objectives are to analyze the structure of local networks, highlighting its history, modes of transmission, and network topologies classification; understand the technology networks, especially Ethernet networks; study the network equipment such as switches, routers and other; in addition to theorize about the networking tools, as VPNS, VLANs and more. The methodology is the literature review. This paper sought to show some important aspects to be considered in projects related to computer networks. Given the new technologies available in the market, the fall of equipment and services costs, combined with increased speed and capacity of the media communication and processing information available on the market let meet a demand for new services and improve the performance of existing, creating new demands on companies.

Keywords: Data Networks. Implementation. Structure.

SUMÁRIO

INTRODUÇÃO

A evolução do ambiente de informática, como sempre, acontece de forma muito rápida e com as redes de computadores a situação não é diferente. Nos últimos anos assiste-se a um aumento na velocidade dos meios de comunicação e a novas alternativas para estabelecer uma rede.

Descartou-se a utilização de cabos coaxiais que interligavam algumas estações conectadas em um barramento, passando para redes com muitas estações que utilizam cabos de par trançado de alto desempenho, ou ainda, conexões de redes sem fio que utilizam de rádio frequência e até raio infravermelho para interligar equipamentos.

Além das novas facilidades para interligar as estações, a abrangência das redes foram estendidas, possibilitando a interligação de novos equipamentos sob uma mesma infraestrutura física e protocolos de comunicação, como é o caso das câmaras de vídeo IP, sensores de presença, dispositivos de segurança, controladores de acesso e uma série de outros dispositivos.

Tudo isto junto com a maior velocidade das estações de trabalho, novos softwares, maior facilidade e rapidez para interligar ambientes distantes, levam a uma maior oferta de tipos diferentes de serviços aos usuários. Toda esta evolução tem levado as empresas a demandar novos recursos de informática no seu ambiente interno e por isto precisam que a sua rede interna esteja adequada à recepção e utilização dos novos recursos que estão sendo disponibilizados no mercado.

A maioria das propostas de metodologia de projetos de redes apresenta foco na implantação de uma nova rede de computadores e dá pouca ou nenhuma atenção ao processo de expansão ou modernização. A grande maioria das

empresas já possui algum tipo de infra-estrutura de rede interligando alguns computadores e, normalmente, desejam fazer uma adequação e atualização dos recursos da infra-estrutura de rede existente, para atender à nova demanda de serviços e/ou às novas tecnologias, principalmente no que tange à convergência e aplicações multimídia interativas.

Avanços recentes têm ocorrido de maneira muito rápida, tornando as metodologias existentes, obsoletas ou defasadas. O processo de atualização e renovação de infra-estrutura de redes não é um processo simples, pois implica em obter várias informações detalhadas a respeito da rede existente, quanto à situação e características técnico/operacionais da infra-estrutura física existente, como: tubulação para passagem de cabos de rede e eletricidade, os materiais utilizados na infraestrutura de cabeamento, a categoria dos componentes, idade e tipo de equipamentos utilizados e também do ambiente de trabalho dos usuários.

Além disto, é preciso conhecer também outros aspectos importantes como: topologia de comunicação, aplicativos utilizados, a cultura interna de informática e de muitas outras informações relevantes para que o projetista possa avaliar e propor as mudanças necessárias.

Outro aspecto a ser considerado é que o processo de atualização normalmente oferece um custo de implantação menor do que o processo de construção de uma nova rede. A atualização, dependendo da necessidade da empresa, poderá ser dividida em etapas de implantação, o que possibilita em um parcelamento do investimento necessário, o fracionamento das atividades de implantação, o reaproveitamento parcial ou total dos equipamentos e recursos existentes, menor tempo de paralisação ou interrupção das atividades dos setores envolvidos nas mudanças.

Desta forma, este trabalho tem como objetivo geral criar uma proposta de implementação de uma estrutura de rede de dados para uma comissão regional de obras. Os objetivos específicos são analisar a estrutura de redes locais, ressaltando seu histórico, modos de transmissão, topologias e classificação de redes; compreender as tecnologias de redes, em especial as redes *ethernet*; estudar os equipamentos de rede, como *switchs*, roteadores e outros; além de teorizar sobre as ferramentas de rede, como VPNS, VLANS e outras. A metodologia é a revisão de literatura.

CAPÍTULO 1

ESTRUTURAS DE REDES LOCAIS

Neste item será apresentada uma visão geral sobre as tecnologias de redes mais recentes, os principais equipamentos e algumas novas funcionalidades. Estas tecnologias são as que prestam suporte às novas demandas geradas pelas empresas, oferecendo maior largura de banda, recursos de segurança e gerenciamento, enfim, inserindo mais facilidades e funcionalidades de interconexão, nas redes e nos equipamentos.

Para atender a este objetivo, este capítulo foi dividido em alguns tópicos básicos que segmentam as informações com a intenção de tornar a exploração do assunto mais didática, pretendendo explorar os aspectos gerais sobre técnicas de comutação, modos de transmissão de informação, topologias físicas, classificação e topologias de redes.

Nos últimos anos, com a evolução dos recursos técnicos e facilidades de rede, ocorreu um direcionamento das empresas do mercado para a adoção de redes que utilizem tecnologia *Ethernet*. Apesar da grande variedade de propostas que existiam anteriormente, ocorreu uma polarização do mercado para a utilização deste tipo de rede nos ambientes locais.

Com o aumento da oferta de banda promovida pelas empresas fornecedoras de equipamentos, redução do custo do *hardware* e novas soluções de infra-estrutura, a tecnologia *Ethernet* está sendo utilizada até na criação de *backbone* para redes MAN e WAN. Assim, as redes *Ethernet* praticamente tornaram-se o padrão de mercado.

A tecnologia de redes locais apresenta uma evolução acelerada e contínua desde o surgimento das primeiras redes *Ethernet* no final dos anos 70. Essa evolução é sustentada pelo interesse de atender a novas aplicações com uma tecnologia de baixo custo e alta capacidade de transmissão. (TANENBAUM.; ZUCCHI, 2006)

A taxa de transmissão sempre foi o ponto forte das redes locais. Nas primeiras redes *Ethernet*, a capacidade de transmitir dados a 10 Mbit/s possibilitou a implantação de ambientes onde a comunicação entre máquinas da mesma rede era transparente para o usuário, representando um significativo avanço em relação às tecnologias de transmissão de dados disponíveis na época. Hoje a tecnologia de redes locais já está operando em taxas de 10 Gbit/s, devendo se tornar em breve o padrão para *backbones* e também para as redes de armazenamento de dados. (SANs - *Storage Área Networks*). (FARREL, 2005)

As redes locais também evoluíram muito no que diz respeito aos meios físicos. Inicialmente utilizava cabos coaxiais, grossos, pesados, caros e de difícil manutenção. Alguns anos depois, as redes locais passaram a utilizar cabos de par trançado e também os cabos de 5 fibras ópticas e, mais recentemente, já utilizam as ondas de rádio em aplicações de curtíssimas, curtas e médias distâncias.

Novos tipos de cabos UTP de alta tecnologia foram criados para suportar as instalações de redes locais, podendo transmitir taxas de 10 Gbit/s. Estes novos meios físicos possibilitaram um grande aumento da área de cobertura das redes locais e assim, é possível encontrar atualmente enlaces de rede local de 100 Mbit/s ou de l Gbit/s com distâncias superiores a 50 km sem o uso de nenhum repetidor. Essas características possibilitaram o aparecimento de redes metropolitanas que

podem ser construídas totalmente com tecnologia de redes locais. (KUROSE; ROSS, 2006)

A redução de custos é um terceiro aspecto onde as redes locais superaram as estimativas mais otimistas. Esta redução é devida à economia de escala na produção dos produtos e também ao significativo avanço do grau de integração de componentes que permitem construir equipamentos com muitos recursos utilizando poucos componentes.

1.1 HISTÓRICO

As redes locais (LANs) usam tecnologias digitais para conectar estações de trabalho e dispositivos de armazenamento ao longo de múltiplos locais. A tecnologia LAN progrediu rapidamente desde a sua introdução nos anos 80, desenvolvendo novas interfaces e técnicas de comutação, que possibilitaram aos sistemas acompanhar o crescente uso da multimídia e aplicações distribuídas pelos grupos de trabalho. (BLAKE et al., 1998)

Nos anos 80, a clássica topologia de barramento das redes *Ethernet* de 10Mbps (IEEE 802.3 – 1982) lideravam, seguidas mais tarde pelas topologias em anel das redes *Token Ring* de 4 ou 16Mbps (IEEE 802.5 – 1985). Nos anos 90, mais de 90% das LANs ainda utilizavam estas tecnologias. (CASNER; JACOBSON, 1999)

À medida que os processadores tornaram-se cada vez mais rápidos, abrindo as portas para o uso crescente de multimídia e aplicações distribuídas, o número de estações por rede tinha de ser reduzido, pois nos anos 90 não era incomum encontrar redes com mais de 300 estações interligadas por uma rede *Ethernet* 802.3 de 10Mbps.

No final dos anos 80, foi desenvolvida uma nova especificação LAN chamada FDDI - *Fiber Distributed Digital Interface*, que é uma topologia em anel de fibra óptica, com capacidade de 100Mbps. Esta tecnologia possibilitou a instalação das primeiras estruturas de Backbone de alto desempenho, mas a aceitação do mercado foi relativa, devido ao alto custo dos componentes de *hardware* exigidos, como os lasers nas placas de rede e a infra-estrutura de cabos ópticos. (BERNERS-LEE et al., 1998)

Logo se verificou que esta largura de banda (100Mbps), quando compartilhada, entre os nós da rede, não seria suficiente para as aplicações multimídia emergentes. Devido à falta de melhor alternativa, vários *backbones* foram reestruturados para utilizar a tecnologia FDDI, até que na metade da década de 90, este cenário foi modificado com o surgimento da técnica de comutação nas LAN, a *Ethernet* de 100Mbps, 1000Mbps, e também do ATM. (SOARES et al., 1995)

1.2 MODOS DE TRANSMISSÃO

A transmissão de informações em uma rede pode empregar diversos tipos de meios de comunicação, ou seja, podem ser utilizados cabos metálicos, fibras ópticas, rádio frequência e raios infravermelhos, para transmitir informações entre dois pontos. As fibras ópticas são utilizadas como meio de transmissão de ondas eletromagnéticas, como a luz. (TANENBAUM, 2003)

Devido a suas características, a transmissão de dados não sofre interferências de origem externa, permitindo o trafego de grandes volumes de informações na velocidade da luz. Permitem também atingir maiores distâncias, podendo interligar pontos distantes alguns quilômetros.

Possui algumas desvantagens como o custo de materiais que ainda é alto e devido a sua fragilidade, exige cuidados especiais na instalação e montagem. Os cabos metálicos de pares trançados foram inicialmente concebidos para sinais analógicos de baixa amplitude e frequência.

Atualmente é o sistema de transmissão mais utilizado nas redes locais devido ao seu custo, ao custo dos seus acessórios, facilidade de instalação e montagem, e também, a sua grande capacidade de transmissão de informações. Possui algumas desvantagens como, o limite máximo de 100 metros para os segmentos e a possibilidade de sofrer interferências eletromagnéticas externas, sendo necessários cuidados na sua instalação. (TANENBAUM, 2003)

1.3 TOPOLOGIAS DE REDE

A topologia refere-se ao "*layout* físico" e ao meio de conexão dos dispositivos na rede, ou seja, como estes estão conectados. Os pontos no meio onde são conectados recebem a denominação de “nós" e estão sempre associados a um endereço para que possam ser reconhecidos pela rede. Devido ao crescimento das redes e ao aumento do volume de estações de trabalho conectadas, o Modelo Hierárquico está sendo cada vez mais utilizado. Este modelo ajuda a definir uma rede em blocos onde cada um possui um objetivo diferente.

Este modelo é estruturado em três níveis conforme segue (GONCALVES, 2000):

a) Camada *Core* ou Núcleo – onde estão instalados os roteadores e *switchs* de alto desempenho e alta disponibilidade, *layer 3.*

b) Camada de Distribuição – onde estão instalados os *switchs* e roteadores que executam as políticas de distribuição, *layer 2*.

c) Camada de acesso – onde estão instalados *switchs* e *hubs* utilizados para conectar os usuários à rede.

A utilização de um modelo hierárquico torna-se interessante, pois, ainda segundo Gonçalves (2000):

a) Oferece maior escalabilidade do que uma rede de apenas um nível (rede de camada 2), que é limitada devido ao *broadcast*.

b) Os equipamentos de cada camada são especializados em uma determinada função, facilitando a administração, testes e manutenção.

c) Facilita as mudanças, pois as interconexões são mais simples.

d) Oferece maior disponibilidade, pois permite definir caminhos redundantes entre os equipamentos da camada de distribuição entre si e com a camada de núcleo (*Core*).

e) Pode oferecer um atraso mais baixo.

f) Permite utilizar protocolos de roteamento com “sumarização de rotas”.

g) Permite utilizar caminhos redundantes entre os *switchs* de uma hierarquia oferecendo maior escalabilidade, disponibilidade, atraso mais baixo e rota alternativa em caso de falha em um dos enlaces.

h) Pode minimizar os custos por utilizar equipamentos de dimensão apropriada para cada grupo de usuários e camada hierárquica.

i) Facilita a manutenção e resolução de problemas.

Em uma rede LAN, utilizando uma estrutura hierárquica, equipamentos apropriados deverão ser utilizados em posições específicas, ou seja, roteadores ou *switch* de camada 3 são utilizados para delimitar domínios de *broadcasts*. *Switchs* de alto desempenho são utilizados para maximizar a banda passante, *switchs* mais simples são usados em locais que poderão ter acessos de menor prioridade.

Segundo Spurgeon (2000), a maioria das empresas de menor porte utiliza uma topologia de conexão do tipo plana, que possui uma configuração mais simples. Nestas redes todas as estações de trabalho e servidores estão conectadas a um ou mais *hubs* ou *switchs* em uma topologia plana. Um problema sério das redes *Ethernet* de um único segmento são os *broadcasts*, que dependendo do volume de estações interligadas, começam a ocupar uma parcela importante da banda de tráfego disponível, reduzindo consideravelmente o desempenho da rede.

As topologias de Malha Total e Malha Parcial oferecem alternativas de conexão de baixo atraso e boa disponibilidade. Na Malha Total, todos os roteadores e/ou *switchs* estão conectados com todos os outros *switchs*/roteadores, oferecendo alto desempenho e disponibilidade, mas com um custo muito alto devido à redundância das conexões.

Na topologia de Malha Parcial, as conexões redundantes são limitadas às conexões mais importantes e algumas rotas alternativas são definidas com o objetivo de oferecer maior disponibilidade. Esta é uma alternativa mais barata, mas têm escalabilidade limitada aos equipamentos roteadores e/ou *switchs* adjacentes. (BASET; SCHULZRINNE, 2004)

As topologias de redes em malha apresentam alta confiabilidade, mas possuem algumas desvantagens se não forem projetadas com cuidado, pois podem ser dispendiosas na distribuição e manutenção. Estas redes também podem ser

difíceis de manter, solucionar problemas e atualizar, a não ser que sejam projetadas com o uso de um modelo hierárquico simples, como mostra Birkner (2003):

1) Modelo Hierárquico - Este modelo é mais escalável para grandes redes corporativas e permite a agregação do tráfego em três níveis diferentes, onde cada nível tem um papel específico, ou seja:

a) A “Camada de Núcleo” provê o transporte rápido entre as localidades definindo um *backbone* de alta velocidade. Deve-se utilizar dispositivos de alta vazão para minimizar o atraso, possuir componentes redundantes para atender ao seu aspecto crítico nas conexões. Nesta camada deverão ser suprimidas as configurações que possam comprometer a vazão, como, por exemplo, filtro de pacotes. O seu diâmetro ou número de conexão com segmentos de rede deverá ser pequeno para ter baixo atraso, desempenho previsível e facilidade na solução de problemas. A conexão a outras redes e acessos a Internet são feitos nesta camada. Esta camada deve ser altamente confiável e se adaptar rapidamente a mudanças.

b) A “Camada de Distribuição” conecta os equipamentos de acesso ao Núcleo. Implanta as políticas de segurança como o controle de acesso aos recursos. Controla o tráfego que cruza o núcleo central (*Core*), administrando e promovendo desempenho. Delimita os domínios de *broadcasts* e pode promover o roteamento entre as VLANs. Pode fazer tradução de endereços se a camada de acesso utilizar endereçamento privativo.

c) A “Camada de Acesso” em uma rede LAN provê o acesso aos usuários finais nos segmentos locais. Nesta camada estão localizados os *switchs* por onde os equipamentos tais como estações de trabalho, câmeras de vídeo, sensores, e vários outros fazem o acesso à rede. (BIRKNER, 2003)

Alguns cuidados a serem tomados na elaboração de um projeto hierárquico como controlar o diâmetro da topologia inteira da rede para minimizar o atraso, manter controle rígido sobre a camada de acesso. É neste nível que departamentos com alguma independência implantam suas próprias redes, podendo causar transtornos e dificultar a operação na rede inteira.

Um conselho importante para facilitar o planejamento de capacidade é iniciar o projeto pela camada de Acesso, em seguida trabalhar a camada de Distribuição e finalmente a camada de Núcleo da Rede (*Core*).

2) Topologias redundantes – permite oferecer maior disponibilidade na rede. Os recursos que poderão ser duplicados são os circuitos de comunicação, roteadores importantes, *switchs*, fontes de alimentação, portas de comunicação cabos de conexão e outros componentes. O grande problema da implantação da redundância é o custo da solução, necessário para duplicar os componentes. (BIRKNER, 2003)

A utilização de Topologias Redundantes em um projeto de rede deverá ser aplicada dependendo da necessidade do cliente em possuir caminhos alternativos para os enlaces. Deverão ser utilizados equipamentos apropriados para administrar a utilização de circuitos duplos, que permitam controlar o tempo de reconfiguração dos caminhos, o congestionamento, à divisão do tráfego e outras questões envolvidas.

Outro aspecto importante é definir uma rotina de testes periódicos para verificar se os caminhos alternativos estão realmente funcionando ou utilizar equipamentos que permitam montar um esquema de balanceamento de carga entre

caminhos paralelos. Em uma LAN é possível estabelecer enlaces redundantes entre *switchs* com o objetivo de aumentar a disponibilidade. (BIRKNER, 2003)

Segundo Comer (2006), com a utilização do protocolo *spanning tree* (IEEE802.1d) é possível estabelecer a redundância do enlace e também evitar a criação de laços (*looping*). Este protocolo administra os enlaces redundantes, ativando e desativando quando necessário, mas não disponibiliza balanceamento de carga entre os enlaces. Redundância de Servidores é necessário para alguns serviços com DHCP, DNS, *Proxy*, aplicativos especiais e outros.

A ausência destes serviços na rede poderão causar sérios transtornos para a continuidade da operação da rede e por conseqüência influenciar nos negócios, por esta razão é interessante avaliar a viabilidade de duplicação. Dependendo da característica da empresa e necessidades específicas do negócio, poderá ser necessário utilizar alguns recursos técnicos como os segmentos redundantes para a rede WAN, conexões múltiplas à Internet e a utilização de VPN (Redes Privadas Virtuais).

O uso de segmentos redundantes aumenta a disponibilidade e poderão ser utilizados em uma topologia de malha parcial, onde os cuidados com as rotas e acessos físicos deverão ser considerados, pois, por exemplo, o rompimento de um cabo poderá interromper o funcionamento de todos os enlaces. (COMER, 2006)

A utilização de balanceamento de carga entre circuitos permite que, além do aumento da disponibilidade com a utilização de um caminho redundante, melhorar as características de desempenho entre dois pontos de uma rede. Apesar da maioria dos equipamentos e protocolos de comunicação permitir esta utilização, este recurso deverá ser bem planejado.

Na elaboração de um projeto de rede de campus, alguns pontos especiais deverão ser considerados como: manter domínios de *broadcasts* pequenos, incluir segmentos redundantes na camada de distribuição, implantar esquemas de redundância nos servidores e serviços importantes e também incluir formas alternativas de uma estação achar um roteador para se comunicar fora da rede de camada 2. (BIZER et al, 2009)

No projeto de uma topologia de rede deverá ser considerada a utilização de redes virtuais conhecidas como VLANs. As redes virtuais ou VLANs nada mais é do que um “domínio de *broadcast*” configurável, criados em um ou mais *switchs*, para agrupar usuários e/ou serviços em uma comunidade que possuam características, afinidades e objetivos comuns.

Os usuários de uma comunidade poderão ser agrupados independentes do cabeamento físico, ou seja, podem ser agrupados mesmo que estejam em segmentos físicos distintos. Esta facilidade é importante, pois devido ao crescimento rápido das empresas não é possível garantir que funcionários que participem de um mesmo projeto estejam localizados juntos. (DOYLE; CARROLL, 2010)

Nos *switchs* de camadas 2 mais recentes é possível configurar as portas para pertencer a uma determinada VLAN ou criar portas tronco para o transporte de informações de mais de uma VLAN simultaneamente. Os *switchs* de camada 3, possuem capacidade de roteamento e permitem que algumas informações sejam migradas de uma VLAN para outra, isolando o domínio de *broadcast* de cada uma.

No caso de empresa que baseiam seus negócios na Internet, o uso de conexões múltiplas a provedores poderá ser fundamental para manter a disponibilidade dos sistemas. Desta forma, dependendo da estrutura e distribuição geográfica da empresa, a utilização de provedores diferentes e/ou localizados em

cidades diferentes, e/ou com enlaces de acesso (a partir da empresa) partindo de unidades diferentes da empresa, poderá constituir de uma estratégia operacional importante.

Algumas das vantagens e desvantagens que deverão ser consideradas, segundo Zucchi (2011), são: custo, facilidade de uso, substituição e redundância de equipamentos de acesso, enlaces redundantes, redundância de ISP (Provedor Internet), complexidade de configurações e regras operacionais. Na Topologia de Rede, aspectos de segurança também deverão ser observados. Verificar a localização dos equipamentos e políticas de controle de acesso não autorizado, roubo físico, vandalismo, e outros.

Para Zucchi e Amancio (2013), um recurso de segurança importante na rede é a utilização de um *firewall*, que é um sistema que estabelece um limite entre duas ou mais redes como, por exemplo, separar a rede corporativa da Internet. Ele pode ser implementado de diversas formas, desde um modelo simplificado que utilize apenas um roteador, com filtro de pacotes para utilização em empresas com políticas de segurança muito simples, até sistemas mais complexos que utiliza um software especializado rodando em *hardware* de alta disponibilidade e confiabilidade.

O *firewall* executa a verificação de cada pacote que tenta passar por ele confrontando com uma tabela de critérios de filtragem, se não houver nenhuma restrição ele permite a passagem, caso contrário, descarta o pacote.

Outros processos poderão ser incorporados na rede para aumentar a segurança para os acessos como o uso de endereçamento privativo na rede corporativa, implantando o NAT – *Network Address Translation* e/ou *Proxy* para determinados serviços. Para empresas que precisam publicar informações na

Internet, pode-se ter alguns servidores em uma local de acesso diferenciado para a Internet, numa área chamada de DMZ – *Demilitarized Zone*.

Nesta área poderão ser colocados alguns servidores, separados dos servidores da rede corporativa, que poderão ser acessados por usuários via Internet. O objetivo básico é proteger a rede corporativa e disponibilizar informações para a Internet. (ZUCCHI; AMÂNCIO, 2013)

1.4 CLASSIFICAÇÃO DAS REDES

As redes também podem ser classificadas conforme a sua abrangência, ou seja, a área geográfica e a taxa de transmissão das redes. Usualmente são consideradas quatro classes de redes (TANENBAUM; ZUCCHI, 2006):

a) Redes Pessoais ou PAN (*Personal Area Network*) – são redes de curta distância, utilizadas para interligar dispositivos em uma área limita a poucos metros de raio. Por exemplo, poderíamos citar a interligação de Palmtops, impressora, estação de trabalho e notebook dentro de um ambiente de escritório utilizando freqüências de rádio como o “Bluetooth” ou raios infravermelhos para efetuar a troca de informações entre eles.

b) Redes Locais ou LAN (*Local Area Network*) – normalmente utilizadas para interligar computadores pessoais ou estações de trabalho dentro de uma área geográfica pequena, podendo ser uma sala, um andar de um prédio, um prédio ou até a um conjunto de prédios dentro de uma área limitada (por exemplo, um campus ou planta fabril). Normalmente as redes locais atendem as necessidades de comunicação de uma única organização.

c) Redes Metropolitanas ou MAN (*Metropolitan Area Network*) – correspondem a uma classe de redes que normalmente operam dentro do limite de diversos blocos de prédios até uma cidade inteira. Normalmente possui circuitos de moderada a alta capacidade de tráfego, para a interconexão de redes locais ou computadores. É administrada por uma única organização e atende as necessidades de um grupo de usuários ou organizações.

d) Redes de Longa Distância ou WAN (*Wide Area Network*) – são normalmente utilizadas para interconectar computadores, redes locais ou redes metropolitanas distantes geograficamente, podendo envolver cidades, estados, paises ou até continentes. Podem utilizar desde canais de velocidade relativamente baixa a até canais de grande capacidade de tráfego.

Outras classificações como GAN – *Global Area Network*, HSLN – *High Speed Local Network*, SAN – *Storage Area Network*, RAN – *Residential Area Network*, não serão abordadas por este trabalho, mas várias publicações fazem referencias a elas. Atualmente é comum vermos na mídia a utilização dos termos, Internet, Intranet e Extranet. (TANENBAUM; ZUCCHI, 2006)

Na verdade são nomes parecidos para o uso diferenciado de uma mesma tecnologia e infraestrutura. A Internet é a rede de informática em escala global que utiliza padrões abertos com acesso a milhões de servidores em todo o mundo. As Intranets são redes privativas, corporativas que utilizam as mesmas tecnologias da Internet.

São utilizadas na comunicação interna da própria empresa e/ou comunicação com outras empresas associadas. Estão diretamente relacionadas à Internet, pois compartilham os mesmos softwares e equipamentos de rede, falando a mesma

linguagem. Podem ser ligadas à Internet, com segurança, utilizando "*Firewall*s" que restringe o uso e acesso aos dados privados da empresa.

Este recurso auxilia no processo de descentralização das informações, na distribuição de dados e no desenvolvimento de aplicações, além de permitir maior participação do usuário final na criação de aplicações. A Extranet é uma combinação de uso da Internet com Intranet, com acesso temporário e restrito de dentro para fora e fora para dentro da rede da empresa. (OPPENHEIMER, 1999)

CAPÍTULO 2

TECNOLOGIAS DE REDES LOCAIS

As redes locais geralmente utilizam canais de comunicação com alta taxa de transmissão, pequenos atrasos e baixa taxa de erros. Estas características gradualmente estão sendo repassadas também para as redes metropolitanas, devido à extensão e aplicação das características das redes *Ethernet* para cobertura destas áreas.

Assim, os principais fatores que diferenciam uma rede local de uma rede metropolitana, estão relacionados com a sua área geográfica e propriedade. Um dos fatores que diferenciam as tecnologias de rede é o método de acesso empregado, por exemplo, as redes *Ethernet* utilizam o CSMA/CD enquanto que nas redes *Token Ring*, *Token Bus* e FDDI usam o método de passagem de *token*. (ABERER et al, 2007)

Estas tecnologias se baseiam no principio do *broadcast*, onde cada pacote de dados transmitido é recebido por todas as estações da rede. Cada estação deve analisar as informações do endereço de destino para determinar se deve aceitar ou ignorar o pacote. Quanto mais nós existirem numa dada rede, maior é a carga e maior o tempo gasto para avaliar os endereços dos pacotes destinados aos outros nós.

Nos primeiros anos, isto não era visto como problema devido a grande largura de banda disponível quando comparada com a capacidade de transmissão isolada de cada estação e a quantidade de estações das redes. Com os avanços e o aumento da utilização das redes, logo surgiram gargalos e por isto as redes foram

divididas em segmentos, os quais se interconectam por dispositivos de seleção como *switchs* e roteadores. (BERNERS-LEE et al., 2001)

Com essa tecnologia, os dados locais permanecem no segmento local e os segmentos vizinhos não ficam sobrecarregados com o tráfego que não lhe pertence. Várias foram às tecnologias de redes desenvolvidas, mas poucas conseguiram uma base de usuários significativa e foram sendo substituídas por outras que apresentavam outras vantagens operacionais, técnicas e financeiras. A maioria das especificações para as tecnologias de redes locais (LAN) é definida pelo IEEE e vários fóruns industriais.

Pode-se citar que destas tecnologias, as mais utilizadas são a *Ethernet*, *Token Ring* FDDI e ATM, que apresentam as seguintes características (SPURGEON, 2000):

1) *Ethernet* – É a tecnologia de LAN mais utilizada pelas empresas devido a sua simplicidade operacional e baixo custo. Nos últimos anos apresentou uma grande evolução na sua capacidade de transmissão, passando dos originais 10Mbps para 100Mbps (*Fast Ethernet*) e posteriormente para 1000Mbps (*Gigabit Ethernet*).. Atualmente está sendo difundida a *10Gigabit Ethernet*.

2) *Token Ring* – Originalmente desenvolvida pela IBM, esta tecnologia transmite *tokens* por uma topologia em forma de anel a 4 ou 16Mbps. Esta tecnologia perdeu espaço em muitas instalações, devido ao custo dos equipamentos, baixa velocidade e dificuldades de suporte técnico.

3) FDDI – Oferece uma tecnologia estável, bem conhecida, que opera a 100Mbps com redundância. Esta tecnologia em geral opera sobre fibra óptica, mas existiram algumas instalações que utilizaram cabos de cobre. O FDDI foi utilizado

em muitas redes, mas acabou perdendo espaço para a *Fast Ethernet*, devido ao custo dos equipamentos, a grande base de redes *Ethernet* e dificuldades de suporte técnico.

4) ATM - É uma arquitetura de *hardware* e software que troca pequenas unidades de dados de tamanho fixo, denominado células. É uma tecnologia de multiplexação e comutação, orientada por conexão, projetada para flexibilidade e desempenho. Pode ser executada em velocidades baixas de 154Mbps, até instalações que utilizavam OC- 48 trabalhando a 2,4Gbps.

O ATM tem uma grande base instalada, oferece capacidade de tráfego garantida, largura de banda escalável, tempo de retardo de transmissão constante, flexibilidade e eficiência em tráfego intermitente, aceita opções de Qualidade de Serviços (QoS).

Devido a estas características é uma tecnologia que suporta muito bem o tráfego de voz, dados e imagens. Devido ao custo dos equipamentos, falta de pessoal técnico especializado tem perdido espaço para as tecnologias *Gigabit* e *10Gigabit Ethernet*. (BIRKNER, 2003)

2.1 REDES *ETHERNET*

Segundo Zucchi e Amancio (2014), a *Ethernet* é a tecnologia LAN mais utilizada atualmente devido à simplicidade e baixo custo. Sua principal desvantagem é que ela se baseia probabilisticamente em CSMA/CD (*Carrier Sense Multiple Access* / *Collision Detection*), que é um esquema de barramento arbitrado, que define o mecanismo pelo qual uma estação deseja transmitir dados pelo fio (barramento).

O CSMA/CD também está associado à criação de um domínio de colisão (*collision domain*), que é um conceito exclusivo do ambiente *Ethernet*. Embora estes eventos sejam normais neste ambiente, um número excessivo deles poderá diminuir drasticamente a largura de banda disponível.

Essa redução da largura de banda pode ser remediada pela segmentação da rede por meio de *bridges*, comutadores ou roteadores. Segmentação é o processo de divisão de um domínio de colisão em dois ou mais domínios de colisão. Pode ser executada com o uso de um *switch* de Camada 2 (*Layer 2*) para a criação de domínios de colisão separados. (ZUCCHI; AMÂNCIO, 2014)

A implantação de segmentos na rede resulta em maior largura de banda disponível para as estações conectadas a estes segmentos. Apesar da segmentação do domínio de colisão, as estações ainda estarão no mesmo domínio de *broadcasts*. Os domínios de *broadcasts* poderão ser quebrados com o uso equipamentos como roteadores e *switch* de Camada 3 (layer 3) e definição de VLANs.

Um comutador *Ethernet*, como é o caso dos *switchs*, dedica total largura de banda (10,100 ou 1000Mbps) a cada uma de suas portas, pois o seu backplane tem largura de banda, no mínimo, idêntica à largura de banda agregada a todas as suas portas. Isso é chamado de comutação sem blocagem (*non-blocking switch*). (ZUCCHI; AMÂNCIO, 2014)

Alguns comutadores foram projetados para acomodar um único dispositivo (host) por porta, outros assumem que uma porta de comutação onde será atribuído a um segmento inteiro de LAN. Essa técnica é chamada de comutação de segmento (segment *switch*ing).

O *Fast Ethernet* é uma rede *Ethernet* atualizada para trabalhar a 100Mbps. Utiliza a topologia de barramento lógico orientado a *broadcast* da *Ethernet* padrão, em conjunto com o método CSMA/CD para controle de acesso.

O padrão *Gigabit Ethernet* (802.3z), trabalha a 1000Mbps e também se baseia na tecnologia CSMA/CD. Utiliza o esquema de codificação de sinal denominada 8B/10B, que fazia parte originalmente da tecnologia *Fiber Channel ANSI*. Esta tecnologia, em essência, foi anexada à camada MAC do *Fast Ethernet*, acelerando em 10 vezes, e assim conseguindo o *Gigabit Ethernet*. (BIRKNER, 2003)

A norma *10Gigabit Ethernet* (802.3ae) surgiu em meados de 2002, e foi concebida para a construção de *backbone* de alto tráfego sobre fibra óptica (monomodo e multimodo) no centro das redes empresariais. O grupo de trabalho IEEE 802.3an trabalha na definição da norma *Ethernet 10Gigabit* sobre cobre, conhecida sob a designação *10GBaseT.*

O objetivo é atingir este alto volume de tráfego a uma distância de 100 metros, respeitando ao mesmo tempo as normas existentes de instalação e utilização de cabeamento de par entrançado (UTP ou STP) e um conector RJ45.

Isto apresenta um desafio que consiste em transmitir 10Gbit/s num cabo de quatro pares, ou seja, 2,5Gbit/s por par. O desafio é ultrapassar os problemas inerentes de diafonia, que ocorre quando estão instalados em grandes feixes, pois para atingir 10Gbit/s, é necessário transmitir freqüências muito altas (próximas a 900MHz) num cabo UTP grosso, em que os pares entrançados (desprovidos de blindagem) estão muito próximos uns dos outros. (ZUCCHI, 2011)

CAPÍTULO 3

EQUIPAMENTOS DE REDE

3.1 *SWITCHS*

Segundo Tanembaum (2007), o desenvolvimento de microprocessadores e *chipsets* econômicos e de alto desempenho no início dos anos 90, abriu caminho para que complexas tecnologias de comutação e multiplexação fossem utilizadas na comunicação de dados nas redes. Desde então, o uso de equipamentos de comutação nas redes tem crescido continuamente.

O componente central das redes LANs comutadas é o *switch*, cuja tarefa é encaminhar os pacotes que chegam para a porta de saída apropriada o mais rápido possível e com o mínimo de colisões. A comutação de segmento é uma implementação especial do principio de comutação e é usada para ligar as topologias LAN tradicionais (*Ethernet* de 10/100/1.000/10.000 Mbps, *Token Ring* e FDDI) numa rede de alto desempenho.

Como esclarece Stallings (2005), os segmentos da LAN são conectados por *switchs* que encaminham pacotes entrantes a seu segmento de destino. Como as *bridges*, os *switchs* LAN impedem que os pacotes sejam enviados a outros segmentos conectados, diferentes do seu segmento de destino, permitindo assim, conexões de comunicação múltiplas e simultâneas entre segmentos.

Esta capacidade de processar comunicação em paralelo é a principal vantagem da comutação na LAN, pois, desta forma, pode multiplicar a largura de banda disponível. Por exemplo, um *switch* LAN de 6 portas, pode criar até 3 vias de

comunicação paralelas simultâneas e se a velocidade de cada conexão for 10Mbps, teremos uma largura de banda total de 30Mbps.

Os pacotes de dados são transferidos dentro dos sistemas de comutação a velocidades extremamente altas, pois são armazenados apenas até que o endereço de destino completo seja recebido. Uma vez completo, o endereço é analisado e o pacote é imediatamente encaminhado para a porta de destino. Isso reduz a latência de cada pacote para cerca de 40μs.

Por definição, segundo Comer (2006), todos os três tipos tradicionais de LAN (*Ethernet*, *Token Ring* e FDDI), são tecnologias *half duplex*. Isto significa que uma dada estação pode receber ou transmitir dados de forma não simultânea. Muitos sistemas de comutação oferecem os modos *half* e *full duplex*. O modo *full* duplex permite a transmissão e recepção simultânea de dados, o que, efetivamente, dobra a largura de banda disponível do enlace, permitindo uma maior capacidade de vazão (*throughput*) nas suas portas.

As técnicas *full duplex* podem apenas ser utilizadas em topologias ponto a ponto, nas quais o acesso ao meio já não precisem ser reguladas por CSMA/CD (na *Ethernet*) ou “entrega do bastão” (*Token Ring* e FDDI). Isto significa que onde são usados componentes *full duplex*, a rede não é mais conectada através de *hubs* ou concentradores passivos, mas apenas por meio de *switchs full duplex*. Este modo de operação aumenta a largura de banda teórica, passando, por exemplo, de 100Mbps para 200Mbps nas redes *Fast Ethernet*.

Os *switchs* normalmente se conectam como redes, mas também é possível conectar redes distintas, usando *switchs* de tradução ou encapsulamento. Cada porta de um *switch* define um domínio de colisão, diferente do funcionamento dos

hubs, que na ocorrência de uma colisão em qualquer porta, esta não é ecoada para todas as outras portas e equipamentos conectados ao *switch*.

Esta característica dos *switchs* demonstra uma arquitetura de comutação e não de compartilhamento como nos *Hubs*. Isso permite que, como uma "*bridge*", aprenda os endereços físicos de rede, montando um mapa de endereços em uma tabela interna denominada "*MAC Address Table*". (COMER, 2005)

Estes endereços fazem com que o tráfego seja direcionado para a porta correspondente. Este processo de aprendizagem, que consiste no *switch* armazenar por um período de tempo "X" denominado de "*Aging Time*". Geralmente este tempo é configurado por padrão em 300 segundos e após este tempo, os nós de rede que não se comunicarem são retirados da tabela.

Dentre vários recursos e mecanismos empregados pelo *switch*, existe o método de encaminhamento de quadros, ou *frames*. Existem dois métodos mais usados de encaminhamento, que é o *Store-and-Forward*, o mais usado e o *Cut-Through*, também conhecido como "*Fast-forwarding*". Basicamente, conforme Zucchi (2011), eles funcionam da seguinte forma:

1) *Store-and-Forward* - O menor tamanho de um quadro *Ethernet* é de 64 octetos. Se um quadro é recebido com tamanho inferior a 64 octetos, este é encarado como colisão e é descartado. Se um quadro recebido é maior que 64 octetos, o *switch* o armazena ("*Store*") até seu tamanho total que geralmente é no máximo 1508 octetos. Após a recepção deste quadro, é calculado o CRC para validar a integridade do quadro e então este quadro é encaminhado (*Forwarded*), e assim sucessivamente.

2) *Cut-Through* - Neste modo, o *switch* opera com um pouco mais de desempenho comparado ao modo "*Store-and-Forward*", pois o *switch* não aguarda o total recebimento do quadro para armazenar e encaminhar. Se o quadro recebido for maior que 64 octetos, ao passo que os dados vão chegando, eles são enviados, não sendo calculado o CRC do quadro total.

Existem alguns fabricantes de *switchs* que operam em modo "*Cut-Through*" e também operam em modo "*Store-and-Forward*". Quando o *switch* apresenta falhas por mais de cinco vezes no envio de quadros com problemas ou corrompidos, o *switch* automaticamente inicia a operação em modo "*Store-and-Forward*", dando uma maior garantia de integridade aos dados, portanto baixando seu desempenho.

Para Farrel (2005), além do emprego de *switchs* em uma arquitetura de rede moderna, são necessários bons cálculos de tráfego para evitar gargalos em alguns nós da rede que prejudicariam o seu desempenho. Os *switchs* não eliminam totalmente os *broadcasts*, mas os equipamentos mais modernos empregam mecanismos de *multicasting*, filtros de *broadcasts* e também o descarte de *broadcasts* em excesso (função configurável), mas não totalmente.

Esta função é normalmente feita pelos roteadores que faz o tratamento dos pacotes de dados na Camada 3 do modelo OSI. Normalmente o roteamento é mais caro que a comutação, mas possibilita a separação lógica da rede em domínios de *broadcasts* (*broadcast domains*).

Os *switchs* normalmente possuem um recurso denominado de VLAN (*Virtual LAN*) que separa as portas físicas conectadas ao mesmo *switch* formando domínios de *broadcasts* distintos. O problema é quando um conjunto de informações precisa migrar de uma VLAN para outra VLAN seria necessário o uso de um roteador. Decisões de camada 3 não podem ser tomadas por um equipamento que trabalha

na camada 2, como é o caso dos *switchs* convencionais, a menos que neste equipamento seja implementada a tecnologia de comutação multicamada ou *Multi Layer Switching* – MLS.

Com o MLS é possível combinar o roteamento e comutação em um único equipamento procurando fornecer o melhor de ambas tecnologias. No MLS um cachê especial mantém informações de fluxo de todos os fluxos ativos e, ao invés de solicitar ao processador rotas para cada pacote no fluxo, os pacotes subseqüentes são comutados, gerando um alto taxa de saída (*throughput*), do que se cada pacote fosse roteado individualmente. Estes equipamentos são os *switchs layer 3*, que acumulam as funções de comutação e roteamento. (BIRKNER, 2003)

Existem os seguintes protocolos de switching (TANENBAUM; ZUCCHI, 2006):

1) Spanning tree – É um mecanismo que permite detectar a existência de caminhos redundantes dentro de uma rede, controlando para que apenas um deles seja ativado, colocando os demais em modo de espera (*standby*) para serem ativados em caso de falha. Deve-se levar em conta que a existência de múltiplos caminhos não aumenta a taxa de transmissão, pois este protocolo irá deixar somente um caminho ativo, desativando todos os demais.

O protocolo *spanning tree* desobriga o administrador da rede de todo tipo de configuração manual durante a operação da rede. Novos equipamentos podem ser inseridos, assim como outros removidos mesmo com a rede em funcionamento, que o protocolo irá reconfigurar a rede de modo a garantir a unicidade de caminhos entre a origem e o destino. (TANENBAUM; ZUCCHI, 2006)

Também é possível que um *switch* se interligue diretamente a outro através de um enlace ponto-a-ponto, que também é considerado uma sub-rede. O primeiro

passo na operação do protocolo é escolher o *switch* que irá atuar como raiz da árvore. A árvore que irá corresponder à topologia ativa da rede irá consistir de raios que partem do *switch* raiz e atingirão todas os demais *switchs* e sub-redes do ambiente.

Cada *switch* também recebe um número de prioridade seguido pelo endereço do *switch*, é chamado de identificador do *switch*. A raiz da árvore é sempre o *switch* com o menor identificador de *switch*. Como as prioridades são analisadas primeiro, o *switch* com a menor prioridade será a raiz.

Se houver um empate, a segunda parte do identificador, formada por um endereço MAC, é usada como critério de desempate (note que os endereços MAC são sempre distintos). Os *switchs* descobrem os identificadores um dos outros trocando mensagens que contêm essa informação. (TANENBAUM; ZUCCHI, 2006)

Essas mensagens são denominadas BPDU - *Bridge Protocol Data Unit* e constituem propriamente o protocolo *spanning tree*. O processo de escolha do *switch* raiz é denominado "eleição". A partir do *switch* raiz os demais *switchs* vão ativando suas portas a partir de comandos recebidos da raiz. Essa escolhe sempre as portas disponíveis de menor custo para chegar a um certo destino.

O custo de cada porta também é um parâmetro que pode ser configurado pelo administrador de rede, embora existam valores *default*. A escolha do *switch* raiz pode ser, portanto, determinada pelo administrador. Alguns critérios devem ser considerados para essa escolha (TANENBAUM; ZUCCHI, 2006):

a) Deve ter uma posição central no ambiente. O protocolo *spanning tree* gera mensagens de atualização periódicas e uma escolha central irá minimizar a quantidade de mensagens de controle transmitidas;

b) Deve ser um equipamento de alta confiabilidade. Se ela cair, um outro *switch* poderá ser escolhido como raiz, mas durante o processo de escolha o tráfego na rede local fica desabilitado. Numa rede de grande porte essa interrupção de operação pode ser da ordem de minutos;

c) Deve ser um equipamento rápido e conectado a enlaces com altas taxas de transmissão, uma vez que durante a operação normal da rede muitas mensagens irão atravessá-la;

d) Deve ser localizada numa área que tenha facilidade de acesso e prontos recursos de manutenção.

Segundo Comer (2006), a escolha do custo das portas de cada *switch* também deve receber atenção. A regra geral consiste em atribuir menores custos aos canais com maior taxa de transmissão. Dessa forma, se houver uma rota de 10 Mbit/s e outra de 100 Mbit/s para a mesma sub-LAN, a rota com taxa mais rápida sempre será a escolhida. Os valores default recomendados para os custos já levam em conta esse fator, de modo que em muitos casos a configuração desse parâmetro é desnecessária.

Observa-se que o algoritmo *spanning tree* não escolhe simplesmente a porta de menor custo de um dado *switch*, mas considera a soma dos custos para chegar a um determinado *switch* como o critério de escolha do caminho a ser ativado.

2) *Link Aggregation* – O *Link Aggregation* ou Agregação de Enlaces permite que os enlaces redundantes sejam utilizados o tempo todo, ou seja, permite estabelecer múltiplos enlaces paralelos entre os equipamentos de uma rede funcionando simultaneamente. A utilização deste recurso, multiplica a capacidade de

tráfego entre dois equipamentos, permitindo a transferência de grandes volumes de dados e também maior disponibilidade devido a redundância de enlaces em operação.

Esse recurso é tão útil que muitos fabricantes se adiantaram ao padrão e definiram seus próprios mecanismos de agregação de enlaces no passado. Uma vez que a operação desse recurso depende de mensagens trocadas entre os equipamentos, uma solução proprietária implica que os equipamentos que o utilizam precisam prover de um mesmo fornecedor. (COMER, 2006)

Em 1988, o IEEE deu início ao grupo de trabalho 802.3ad, que produziu uma versão padronizada do serviço em março de 2000. A característica mais significativa da solução é que o protocolo que a implementa pode ser desenvolvido num *device driver*, permitindo o aproveitamento das placas de rede já desenvolvidas.

É prática comum utilizar enlaces *full-duplex* para a constituição de enlace agregado. Todos os enlaces que compõem um enlace agregado devem operar com a mesma taxa de transmissão.

Como mostram Kurose e Ross (2006), um enlace virtual deve se comportar da mesma maneira que um enlace real. Isto implica que um enlace virtual que serve um sistema final (como um servidor, por exemplo) deve possuir seu próprio endereço MAC. Os quadros que o servidor envia trazem no campo de endereço origem o endereço do enlace virtual e não o endereço de cada placa de rede em particular. Os quadros que são enviados para o servidor transportam o endereço do enlace virtual no campo do endereço de destino.

A agregação de enlaces acrescenta uma nova subcamada na já poluída arquitetura de redes locais. A subcamada de agregação de enlace é responsável por controlar o processo de agregação, definindo quais enlaces reais deve-se tentar

agregar com base nas informações de configuração do equipamento. Após o estabelecimento de um enlace agregado, são trocadas mensagens de controle periodicamente para monitorar o estado do enlace.

O protocolo de controle de agregação exige que cada equipamento seja identificado por um endereço MAC único. Além disso, cada porta física precisa receber um número de porta e uma prioridade. Esse esquema é semelhante ao utilizado pelo protocolo *spanning tree*. (KUROSE; ROSS, 2006)

3.2 ROTEADORES

Segundo Birkner (2003), os roteadores possuem várias opções de conexão com LAN’s e WAN's. Para LAN, pode-se ter portas UTP, FDDI ou AUI. As interfaces WANs servem para estabelecer a conexão com dispositivos de transmissão remota (modens), seguindo os padrões de protocolos V-35, RS- 449, RS-232 entre outros.

Os roteadores atuam nas camadas 1, 2 e 3 do modelo ISO/OSI e devido às suas habilidades sofisticadas de gerenciamento de redes, podem ser utilizados para conectar redes que utilizam protocolos diferentes (de *Ethernet* para ATM, por exemplo).

Os roteadores são capazes de interpretar informações complexas de endereçamento e tomar decisões sobre como encaminhar os dados através dos diversos Links que interligam as redes. Podem selecionar caminhos alternativos entre segmentos de rede local (desde que disponíveis) e podem interligar redes locais usando esquemas de composição de pacotes e de acesso a meios físicos completamente diferentes.

Os protocolos de roteamento podem ser baseados em classes e sem classes. As vantagens do roteamento sem classes é que há mais sumarização de rotas com prefixos menores (*super netting*), tem suporte a sub-redes não contíguas e tem suporte a *Variable-Length Subnet Masking*, incluindo suporte a equipamentos (hosts) móveis. (BIRKNER, 2003)

3.3 OUTROS EQUIPAMENTOS

As *bridges* diferem dos repetidores pois manipulam pacotes ao invés de sinais elétricos, com a vantagem de não retransmitir ruídos ou erros e por isso não retransmitem *frames* mal formados. Um frame deve estar completamente validado para ser retransmitido por uma *bridge*. (DOYLE; CARROLL, 2010)

As *bridges* também compatibilizam segmentos que trabalham em velocidades diferentes, por exemplo, de 10Mbps para 100Mbps e vice-versa. Funcionalmente, um *Switch Layer 2* é uma *bridge*, mas atualmente são mais rápidos, tem mais portas, tratam um volume maior de informações, tem mais opções de segurança e suportam VLANs.

O uso de muitos *hubs* em um segmento de rede pode trazer problemas de desempenho, pois sendo ele um elemento repetidor, repetirá tudo o que receber em uma determinada porta para todas as demais portas conectadas. Todos os pacotes de comunicação são encaminhados a todas as portas ativas.

Aumentando o número de estações conectadas no segmento, aumenta-se também a quantidade de pacotes de dados e também de *broadcasts* na rede, prejudicando sensivelmente seu desempenho e elevando o número de colisões. (DOYLE; CARROLL, 2010)

CAPÍTULO 4

FERRAMENTAS DE REDE

Para Gonçalves (2000), os equipamentos como os *switch*, roteadores e *gateways* podem disponibilizar algumas funcionalidades para as redes como: VPN, VLAN, MPLS, *Firewall*, VRRP, NAT, DHCP e outros. Estes auxiliam na incorporação de maior nível de segurança para rede, funcionalidades de administração e gerencia dos recursos, melhoraria da utilização dos links de comunicação e equipamentos.

A preocupação com segurança é uma das questões cruciais na implantação de qualquer rede. Várias ações devem ser tomadas no sentido de implantar mecanismos de proteção as informações. Cabe ao especialista orientar o cliente, dependendo da sua estrutura, na busca de suporte técnico especializado e também na aquisição de equipamentos e recursos para auxiliar nesta tarefa.

Não é objetivo deste trabalho aprofundar-se no quesito de segurança nesta rede, mas por tratar de um assunto de extrema importância, cabe fazer menção a alguns produtos e serviços, mas principalmente lembrar que a preocupação com segurança não pode ser deixada de lado.

4.1 REDES PRIVADAS VIRTUAIS - VPNS

Uma rede privada virtual (VPN) pode ser definida como uma rede na qual a conectividade entre as diversas localidades do cliente ocorre sobre uma infra-estrutura compartilhada, com as mesmas políticas de segurança e de acesso de uma rede privada. Assim, partes da rede, separadas fisicamente, podem operar

como em uma rede única, utilizando um meio de comunicação não dedicado. (FARREL, 2005)

VPNs podem ser implementadas de diversas formas e sobre uma variedade de infra-estruturas de redes diferentes. Opcionalmente, os dados podem trafegar criptografados no meio compartilhado como, por exemplo, utilizando-se IPSec sobre pacotes IP. A infra-estrutura mais encontrada nas VPNs atualmente está sobre redes Frame Relay ou ATM, interligando as localidades de clientes por circuitos virtuais (VC).

A crescente demanda por conectividade no perfil "*any-to-any*" aumenta a complexidade e número de VCs necessários e, por conseqüência, a demanda por soluções de VPN escaláveis. A topologia de uma VPN pode ser classificada como: *overlay* e *peer-to peer*.

Para o provedor de serviço, o modelo *overlay* torna-se difícil de gerenciar e provisionar quando cresce o número de localidades e, consequentemente, o número de circuitos. Por outro lado, o modelo *peer-to-peer* não permite o isolamento de tráfego entre clientes distintos como no modelo *overlay*. (DOYLE; CARROLL, 2010)

Uma das mais interessantes aplicações da VPN é o suporte para usuários que utilizam dispositivos móveis como *notebooks*, que estão trabalhando fora da empresa e precisam estabelecer comunicação com a Intranet da empresa para coletar ou atualizar informações nas bases de dados, ou ainda fazer consultas a uma conta bancaria utilizando a Internet.

O meio mais comum de fazer esta comunicação é estabelecer um acesso a Internet e fechar um *Link* de comunicação com o destino desejado. Quando os dados estão sendo enviados ou recebidos pelo computador via Internet, passam

através de diversos roteadores até chegar ao seu destino final e estão sujeitos a ataques de diversas maneiras.

Para aumentar a segurança, o uso de uma VPN entre a origem e o destino permite criar um túnel particular dentro de uma rede publica como a Internet. Este túnel criado é uma conexão segura pelo uso de criptografia dos dados e técnicas de autenticação dos dados entre duas redes. Segundo Birkner (2003), existem duas maneiras básicas de estabelecer uma conexão VPN como segue:

a) Entre roteadores – Os roteadores de origem e destino estão configurados estabelecer comunicações utilizando VPN. Quando os roteadores estabelecem a comunicação, criam a VPN, criptografando e decriptografando os dados que são transmitidos e recebidos.

b) Computador para roteador – O computador deverá utilizar um software VPN *client* que suporte IPSec e deverá estar configurado com os padrões estabelecidos pela empresa. Desta forma o computador poderá estabelecer a VPN com o roteador do destino e habilitar a comunicação segura.

4.2 VLANS

Para Tanembaum (2003), é um agrupamento lógico de dois ou mais dispositivos de rede e pode se estender através de muitos *switchs*. Os agrupamentos de dispositivos são baseados em um conjunto de fatores dependentes das características funcionais e da configuração da rede. Estes dispositivos podem ser estações de trabalho, impressoras de rede, controladores de

acesso (catracas), relógios de ponto, telefone IP, câmeras de vídeo ou qualquer outro equipamento conectado fisicamente a rede.

As razões envolvidas na criação e definição das VLANs podem ser de diversas categorias como: controle de *broadcasts*, segurança, gerenciamento de endereçamento de nível 3 (*layer* 3) e consolidação dos recursos de rede.

1) Controle de *broadcasts* – Depende da quantidade de dispositivos dentro do mesmo domínio de *broadcast*, ou seja, quanto maior a quantidade de dispositivos dentro do mesmo domínio, maior será a quantidade de *broadcasts* gerado por estes dispositivos circulando dentro do domínio.

Para cada *broadcast* recebido pelo dispositivo de rede, a sua CPU deverá executar uma interrupção dos processos para avaliar o conteúdo do frame recebido. Estas interrupções tomam tempo de processamento dos dispositivos e também ocupam espaço nas transmissões da rede.

Um aspecto importante das VLANs neste caso é que os *broadcasts* transmitidos dentro de uma VLAN não se propaga para as demais VLANs, fechando assim um domínio de *broadcasts*. Pela limitação da quantidade de dispositivos dentro de uma VLAN, o volume de *broadcast* dentro do segmento também poderá ser limitado. A Fluke recomenda uma taxa média de 30 *broadcasts*/segundo, ou menos, para obter-se um bom desempenho de funcionamento no segmento de rede. (ZUCCHI; AMÂNCIO, 2013)

2) Segurança – Se todos os dispositivos estão dentro do mesmo domínio de rede, fica difícil controlar e limitar os acessos. Colocando os dispositivos da rede

dentro de domínios de *broadcasts*, torna-se possível limitar os acessos com a utilização de filtros de endereços e listas de acessos.

Para o tráfego de uma VLAN passar para outro, é necessário utilizar um dispositivo que execute roteamento dos *frames*, com o uso de roteadores ou *switchs Layer* 3. Assim é possível especificar quais dispositivos de um segmento podem acessar outros dispositivos de outro segmento. Com o uso deste controle de acesso, é possível administrar e monitorar os acessos a dispositivos restritos como, por exemplo, alguns servidores ou serviços específicos. (ZUCCHI; AMÂNCIO, 2013)

3) Administração de endereçamento de *Layer 3* – A definição de sub-redes baseada no tipo de dispositivos é uma pratica comum dentro das redes, ou seja, as impressoras de rede podem ser definidas dentro de uma sub-rede como também algumas estações de trabalho e/ou servidores pertencentes a um grupo podem ser definidos dentro de outra sub-rede. Esta distribuição lógica pode ser impraticável dentro de uma grande rede, sem a utilização de VLANs. (ZUCCHI; AMÂNCIO, 2013)

4) Consolidação de recursos – O uso de VLANs permite o compartilhamento de equipamentos e da infra-estrutura física de uma rede para a utilização de diversos serviços diferentes. Por exemplo, com a definição de VLANs torna-se possível compartilhar a utilização de um *switch* de rede, de modo simultâneo, para atender a rede de câmeras de vigilância, a rede de impressoras, de controladores de acessos, e outras redes dentro da estrutura da entidade. (ZUCCHI; AMÂNCIO, 2013)

Quando um projeto rede com VLANs é definido, as razoes acima listadas devem ser cuidadosamente exploradas e levadas em consideração na definição da estruturação geral da rede. Por exemplo, se a instituição pretende utilizar serviços de VoIP na rede, a definição de uma VLAN para comportar este tráfego, separado do tráfego de dados, permitindo oferecer um serviço de melhor qualidade para reduzir os índices de atraso e perda de pacotes no tráfego de voz.

Para Kurose e Ross (2006), existem três tipos de VLANs, as baseadas em portas, em protocolos e em MAC Address, que possuem as seguintes características:

1) Portas - Cada porta dos *switchs* devem ser configuradas para pertencer a uma especifica VLAN. Qualquer dispositivo conectado a esta porta, estará automaticamente vinculado ao mesmo domínio de *broadcast* das outras portas configuradas com o mesmo número de VLAN.

2) Protocolos - Utilizam o endereçamento de nível 3 (*Layer 3*) transportado pelos *frames*, para determinar os seus membros. Isto pode ser interessante para trabalhar em ambientes multiprotocolo, no caso de redes baseadas predominantemente em IP, este método não é prático.

3) MAC - O endereço MAC dos dispositivos da rede é utilizado para identificar os seus membros. Infelizmente, a correlação de endereços MAC com VLANs, consome um grande volume de tempo e por isto raramente é usado.

Os *frames* transportados entre os *switchs* de uma rede que utiliza VLANs, possuem um campo de endereçamento em seu cabeçalho, chamado de TAG. Este

tag é usado para diferenciar os *frames* pertencentes a cada VLAN e permanece no frame durante todo o tempo em que estiver sendo transportado dentro da rede.

Os *tags* são inseridos no frame no momento em este entra pela porta do *switch*, recebendo a marca da VLAN vinculada, sendo retirado na porta do *switch* de destino no momento de ser entregue para o dispositivo. O formato destas *tags* é definido pelo padrão IEEE 802.1Q que é utilizada pela grande maioria dos fabricantes de *switchs*. (KUROSE; ROSS, 2006)

A documentação e manutenção é o grande desafio da utilização de VLANs dentro das redes. Não é fácil saber qual VLAN está definida para uma porta de *switch*, ou quais portas estão definidas para serem utilizadas como porta "*trunk*". Sem a disponibilidade de uma documentação atualizada, a única maneira de descobrir a configuração de uma porta é acessar as configurações internas do equipamento.

Este processo requer a disponibilidade de senha de acesso ao *switch* como também conhecimento dos comandos de configuração do equipamento. Assim, a adição, movimentação e troca de dispositivos dentro de uma rede deve ser acompanhada de um criterioso procedimento de registro e documentação, como também é importante definir uma verificação periódica das configurações dos dispositivos de rede. (KUROSE; ROSS, 2006)

1) *Trunk Ports* – Nas redes que possuem mais de um *switch*, é necessário definir uma das portas para habilitar a comunicação entre os *switchs* para também poder enviar os *frames* com o VLAN *tag* no cabeçalho. A diferença entre as portas de acesso e as portas trunk é que nesta última, o VLAN *tag* dos *frames* não é retirado na ocasião da passagem pela porta. Com o VLAN *tag* dos *frames*

preservados, o *switch* que recebe o frame consegue identificar para quais portas de destino as informações poderão ser encaminhadas. (KUROSE; ROSS, 2006)

4.3 OUTRAS FERRAMENTAS

Tanembaum e Zucchi (2006) listam uma série de outras ferramentas são utilizadas nas redes prestando diversos tipos de serviços de segurança, suporte a administração e controle como:

1) NAT (*Network Address Translator*) - Usada nos roteadores conectados à Internet para converter um único endereço exclusivo da Internet em vários endereços de rede privada. Ou seja, vários dispositivos podem compartilhar um único endereço de Internet e, como os endereços privados não podem ser acessados diretamente a partir de outro usuário da Internet, isso se torna uma medida de segurança. Ela pode estar disponível em roteadores de pequenas empresas conectadas via Internet e também em locais maiores para o roteador de limite.

2) DHCP (*Dynamic Host Configuration Protocol*) - Usado para emitir automaticamente endereços IP para computadores, assim não é necessário configurar seus endereços manualmente. Isso simplifica a configuração dos computadores, pois eles podem ser configurados para usar o DHCP e selecionarão um endereço quando forem ligados e conectados à rede.

Ele também é útil para *laptops* usados em locais diferentes, pois eles receberão automaticamente um endereço IP adequado a cada local. Em locais

centrais, um serviço DHCP será executado em um servidor, mas em pequenas empresas talvez não haja um servidor, portanto, pode ser necessário que o roteador emita os endereços DHCP.

3) *Firewall* - Os roteadores podem oferecer um recurso de *firewall* e ele é útil em qualquer roteador conectado à Internet, como o roteador de uma filial ou o roteador de limite em empresas maiores. Embora um roteador completo seja aconselhável em empresas maiores, o roteador de limite está do lado de fora do *firewall* e precisa proteger-se.

CONCLUSÃO

Este trabalho procurou mostrar alguns aspectos importantes a serem considerados em projetos relacionados à redes de computadores. Diante das novas tecnologias disponíveis no mercado, a queda de custos de equipamentos e serviços, aliados ao aumento da velocidade e capacidade dos meios comunicação e processamento de informações disponíveis no mercado, permitem atender a uma demanda de novos serviços e melhorar o desempenho dos existentes, criando novas demandas nas empresas.

Estes novos equipamentos, materiais e serviços, aliados às novas demandas das empresas, passaram a exigir condições especiais de funcionamento e consequentemente tem elevado o aumento da complexidade das redes das redes de comunicação.

Para atender esta maior complexidade é necessário que para o desenvolvimento de um projeto de redes de comunicação, uma maior quantidade de variáveis sejam levantadas e avaliadas. As empresas estão mais conscientes quanto a importância em fazer um investimento adequado em obras de infra-estrutura de rede, utilizando empreiteiras responsáveis, exigindo a aplicação das normas técnicas pertinentes e a utilização de produtos como: cabos, conectores, *patch pannel*, e outros passivos de rede de boa procedência e qualidade comprovada.

Recomenda-se ainda que sejam aplicados profissionais especializados para tratamento de cada evento do projeto. Deve-se considerar também, em projetos de cabeamento, uma especificação tecnológica que contemple no mínimo dez anos sem sofrer alterações em infra-estrutura. No mercado já está mais do que provado técnico e economicamente que a infra-estrutura de redes (cabeamento) é o menor peso do investimento e em contra partida é o maior funil de defeitos de uma rede de Telecomunicações.

Uma característica importante a ser considerado no projeto físico é que o sistema deverá ter flexibilidade suficiente para que sejam instalados ou remanejados pontos dentro do ambiente sem que haja necessidade de passagem de cabos adicionais; porém em alguns casos poderão ser necessárias readequações de cabos dentro dos ambientes corporativos.

Na falta de definição da utilização de cada ponto de uma rede, deve-se assumir que todos os pontos são passíveis de trafegar dados na rede com uma capacidade de transmissão mínima de 1 Gbit/s. Assim, todos os recursos da infra-estrutura deverá ser compatível com esta característica.

REFERÊNCIAS

ABERER, K. et al. **The Semantic Web: Lecture Notes in Computer Science**. [S.l.] Springer Berlin / Heidelberg, 2007.

BERNERS-LEE, T.; HENDLER, J.; LASSILA, O. The Semantic Web. **Scientific American**, v. 284, n. 5, p. 34–43, maio. 2001.

BIRKNER, M. H. **Projeto de Interconexão de Redes**. São Paulo: Editora Makron Books, 2003.

BIZER, C. et al. DBpedia - A crystallization point for the Web of Data. **Web Semantics**, v. 7, n. 3, p. 154-165, set. 2009.

BLAKE, S.; BLACK, D.; CARLSON, M.; DAVIES, E.; WANG, Z.; WEISS, W. **An Architecture for Differentiated Services: RFC 2475.** [S.l.]: Internet Engineering Task Force, Network Working Group, 1998.

CASNER, S.; JACOBSON, V. **Compressing IP/UDP/RTP Headers for Low-Speed Serial Links: RFC 2508**. [S.l.]: Internet Engineering Task Force, Network Working Group, 1999.

COMER, D. E. **Interligação de Rede Com TCP/IP: Princípios, Protocolos e Arquitetura**. Rio de Janeiro: Elsevier, 2006.

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados**. Rio de Janeiro: Elsevier, 2005.

DOYLE, J.; CARROLL, D. **Routing TCP/IP**. Volume II. Indianapolis: Cisco Press, 2010.

FARREL, A. **A Internet e Seus Protocolos: Uma Análise Comparativa**. Rio de Janeiro: Elsevier, 2005.

GONCALVES, A. R. **Método para Planejamento de Capacidade de Redes ATM baseado em Simulação**. 2000. Dissertação (Mestrado em Ciência da Computação). Programa de Pós-Graduação em Computação, Universidade Federal do Rio Grande do Sul. Porto Alegre, 2000.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet: uma abordagem top-down**. 3. ed. São Paulo: Pearson Addison-Wesley, 2006.

OPPENHEIMER, Priscilla. **Projeto de redes Top-down: um enfoque de análise de sistemas para projeto de redes empresariais**. Rio de Janeiro: Campus, 1999.

SOARES, L. F. G.; LEMOS, G.; COLCHER, S. **Redes de Computadores - Das LANs, MANs e WANs às Redes ATM.** Rio de Janeiro: Elsevier, 1995.

SPURGEON, C. E. **Ethernet - O Guia Definitivo**. Rio de Janeiro: Elsevier, 2000.

TANENBAUM, A. S. **Redes de Computadores**. 4.ed. Rio de Janeiro: Elsevier, 2003.

TANENBAUM, A. S. **Sistemas Operacionais Modernos**. 2. ed. São Paulo: Ed. Prentice Hall, 2007.

TANENBAUM, A.; ZUCCHI, W. L. **Organização Estruturada de Computadores**. 3. ed. São Paulo: Pearson, 2006.

ZUCCHI, W. L. ; AMÂNCIO, A. B. Automação Industrial e o Protocolo Ethernet. **RTI Redes, Telecom e Instalações**, v. 165, p. 84-87, 2014.

ZUCCHI, W. L. ; AMÂNCIO, A. B. Construindo um Data Center. **Revista USP**, v. 3, n. 7, p. 43-58, 2013.

ZUCCHI, W. L.. A Evolução das Redes de Transporte. **RTI Redes, Telecom e Instalações**, v. 135, p. 84-87, 2011.