UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

GERALDO FERNANDES BARBOSA

IMPLEMENTAÇÃO DE UMA ESTRUTURA DE REDE USANDO O MODELO HIERÁRQUICO

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2012

GERALDO FERNANDES BARBOSA

IMPLEMENTAÇÃO DE UMA ESTRUTURA DE REDE USANDO O MODELO HIERÁRQUICO

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná Orientador: Prof. Fabiano Scriptore de Carvalho

CURITIBA
2012

RESUMO

BARBOSA, Geraldo F. **IMPLEMENTAÇÃO DE UMA ESTRUTURA DE REDE USANDO O MODELO HIERÁRQUICO.** 2012. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

Este trabalho tem o foco na implementação de uma rede de computadores utilizando a estrutura hierárquica de camadas visando a segurança e o desempenho. O trabalho aborda também os problemas decorrentes de redes mal projetadas e as tecnologias disponíveis atualmente para que administradores de redes possam projetar e implementar as redes de computadores provendo maior segurança e disponibilidade a essas redes. Além de todo o embasamento teórico que é estudado, o trabalho apresenta, no último capítulo, uma implementação prática contemplando Redundância, que faz com que a rede se mantenha disponível mesmo havendo ruptura em um dos caminhos, Segurança de Porta, que faz com que cada porta do switch seja configurada para determinado host.

Palavras chave: Modelo Hierárquico, estrutura de rede, caminho redundante

ABSTRACT

BARBOSA, Geraldo F. **Estrutura de Rede Usando o Modelo Hierárquico.** 2012. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

This work has focused on implementing a computer network using the hierarchical structure of layers for the security and performance. The work also addresses the problems arising from poorly designed networks and technologies available today to network administrators can design and implement computer networks providing increased security and availability to these networks. Besides all the theoretical foundation that is studied, the study shows, in the last chapter, a practical implementation contemplating redundancy, which makes the network remains available even if there is a rupture of the paths, Port Security, which makes each switch port is configured for a specific host.

Key Words: Hierarchical model, network structure, redundante path.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

DoD	Department of Defense
DoS	Denial of Service
EIGRP	Enhanced Interior Gateway Routing Protocol
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
NLANR	National Laboratory for Applied Network
OSPF	Open Shortest Path First
POP3	Post Office Protocol
RIP	Routing Information Protocol
SMTP	Simple Mail Transfer Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol

ÍNDICE

1 Introdução

Neste capítulo será tratado o tema, delimitação da pesquisa, problemas e premissas, o objetivo geral, os objetivos específicos, justificativa, procedimentos metodológicos, embasamento teórico e a estrutura deste trabalho.

1.1 Tema

Com o objetivo de atender às necessidades da população, a cada dia novos empreendimentos são inaugurados. Boa parte desses empreendimentos começam a operar sem utilizar recursos computacionais, mas depois de certo tempo, quando o empreendimento passa a produzir resultados mais expressivos, se torna indispensável a utilização de softwares que provêem avançados sistemas de armazenamento e pesquisa para facilitar e agilizar o acesso às informações melhorando a competitividade do empreendimento. Inicia-se a utilização dos recursos computacionais com poucos computadores e, por falta de foco em planejamento computacional, operando de forma individual.

O velho modelo de um único computador atendendo a todas as necessidades da organização foi substituido por outro em que os trabalhos são realizados por um grande número de computadores separados, porém interconectados. Esses sistemas são chamados redes de computadores (Tanembaum, 2011)

Passamos a depender da conexão com a Internet até mesmo para as tarefas mais básicas e a armazenar cada vez mais informações em servidores remotos (Morimoto, 2010).

Para atender as demandas de infraestrutura, as redes de computadores são implementadas muitas vezes de maneira inadequada, por profissionais desprovidos de conhecimento necessário. Infelizmente as redes que são montadas sem um planejamento podem trazer uma série de problemas. Entre os principais

problemas pode-se citar a indisponibilidade e o acesso não autorizado às informações.

O objetivo deste estudo é analisar as tecnologias atualmente disponíveis para a implementação de um projeto de rede profissional que garanta confidencialidade, integridade e disponibilidade às informações de um empreendimento.

1.1.1 Delimitação de Pesquisa

Para um bom entendimento dessa pesquisa, será mostrado primeiramente como as redes de computadores são improvisadas nos pequenos empreendimentos e quais são os principais problemas que surgem em virtude da falta de profissionalismo. Depois serão mostradas as tecnologias necessárias para a implementação de um projeto de rede profissional.

1.2 Problema e Premissas

Muitas empresas têm um número significativo de computadores. Por exemplo, uma empresa pode ter um computador para cada trabalhador e os usa para projetar produtos, escrever documentos e elaborar a folha de pagamento. Inicialmente, alguns desses computadores podem funcionar isoladamente dos outros, mas, em determinado momento, a gerência pode decidir conectá-los para extrair e correlacionar informações sobre a empresa inteira (Tanembaum, 2011).

Na dinâmica do dia a dia, em alguns casos, os computadores são conectados de maneira mal planejada, porém ao ver que foi possível estabelecer conexão entre um computador e outro, acomodam-se e dão o problema como resolvido. Problemas consequêntes disso aparecem tempos depois, quando a rede começa a ficar instável e também ficar claro que a segurança da informação está ameaçada.

1.3 Objetivos

1.3.1 Objetivo Geral

Implementar uma estrutura de rede hierárquica levando em consideração os aspectos de disponibilidade, segurança e integridade da informação

1.3.2 Objetivos Específicos

- Identificar os equipamentos que serão implementados nos cenários;
- Identificar os protocolos que serão configurados;
- Agrupar os diversos setores em domínios de colisão separados;
- Implementar políticas de segurança e QoS nos equipamentos;
- Implementar agregação de enlaces para melhorar o desempenho da rede;
- Fazer um mapeamento da rede implementada.

1.4 Justificativa

Visto que, a cada ano, as redes de computador estão se tornando mais comuns até mesmo em pequenos empreendimentos, a demanda por profissionais qualificados para prestar mão-de-obra técnica sobre essas redes aumenta.

Conhecer os problemas decorrentes de uma rede mal implementada, as técnicas utilizadas pelos invasores e os equipamentos e tecnologias disponíveis, bem como sua perfeita configuração, é habilidade essencial de um bom profissional de redes.

Este estudo está sendo feito com o objetivo de efetivar os conhecimentos necessários para a implementação de uma rede profissional em uma empresa, considerando os aspectos de segurança, disponibilidade e integridade da informação.

1.5 Procedimentos Metodológicos

Este estudo será elaborado com base em livros, materiais didáticos da internet e o conteúdo do curso CCNA.

1.6 Embasamento Teórico

Entre o material estudado para estabelecer o embasamento teórico sobre Redes de Computadores, destaca-se o trabalho bibliográfico de Tanembaum (2011), William Stallings (2011), Wendell Odom (2008), Wendell Odom (2011), André Sato Filho (2009), Carlos Eduardo Morimoto (2008) e artigos e monografias publicadas na Internet.

1.7 Estrutura

O trabalho está organizado em três capítulos.

O capítulo 1 deste trabalho apresenta a Introdução, falando do tema, delimitação da pesquisa, problemas e premissas, objetivos, justificativa, procedimentos metodológicos, embasamento teórico e a estrutura descrita aqui.

O capítulo 2 traz todo o referencial teórico pesquisado.

O capítulo 3 apresenta implementação prática onde é apresentando a rede em tempestade de broadcast devida à redundância, depois é mostrada a configuração do protocolo STP para solucionar a tempestade de broadcast.

2 Referenciais Teóricos

Neste capítulo será descrito o referencial teórico do trabalho, que contém os seguintes assuntos: Redes de Computadores, Criptografia e Seguraça de Redes, CCENT/CCNA ICND1, CCNA ICND2.

2.1 Redes de Computadores

Segundo (Tanembaum, 2011) uma organização cria redes de computadores para deixar todos os programas, equipamentos e, especialmente dados ao alcance de todas as pessoas na rede, indemente da localização física do recurso ou do usuário. Um exemplo óbvio e bastante disseminado é um grupo de funcionários de um escritório que compartilham uma impressora comum. Nenhum dos indivíduos realmente necessita de uma impressora privativa, e uma impressora de grande capacidade conectada em rede muitas vezes é mais econômica, mais rápida e de manutenção mais fácil que um grande conjunto de impressoras individuais.

Porém, talvez mais importante que compartilhar recursos físicos, como impressoras e unidades de fita, seja compartilhar informações. Toda empresa, grande ou pequena, tem uma dependência vital de informações computadoizadas. A maioria das empresas tem registros de clientes, informações de produtos, estoques, extratos financeiros, informações sobre impostos e muitas outras informações on-line. Hoje, até mesmo uma pequena agência de viagens ou uma empresa jurídica com três pessoas depende instantaneamente de redes de computadores para permitir a seus funcionários acessar informações e documentos relevantes de forma quase instantânea.

2.2 Arquiteturas de Redes

No início das redes de computador cada fabricante criava seus próprios protocolos de forma fechada, isto é, os detalhes não eram disponibilizados ao público. Isso fazia com que os protocolos de cada fabricante tivessem suporte somente aos computadores do próprio fabricante.

Segundo Odom (2011), com o passar do tempo, os fabricantes passaram a formalizar e publicar os seus protocolos de rede, o que permitiu que outros

fabricantes criassem produtos que pudessem se comunicar com os computadores dos primeiros.

Atualmente há duas importantes arquiteturas de rede: os modelos de referência OSI e TCP/IP. O modelo OSI é mais antigo e seus protocolos raramente são usados nos dias atuais. Contudo o modelo em si ainda é bastante válido e as características de cada camada ainda são essencialmente importantes. Na arquitetura TCP/IP ocorre o oposto, pois o modelo propriamente dito não é muito utilizado enquanto que seus protocolos são.

2.2.1 Modelo de Referência OSI

Diante do problema referente a cada fabricante criar seus próprios protocolos fazendo com que tecnologias de fabricantes diferentes não se comunicassem, a *International Organization for Standardization* (ISO) teve a iniciativa de estabelecer uma arquitetura padrão e aberta, para que diferentes fabricantes produzissem seus protocolos observando o padrão estabelecido e, assim, os produtos de diferentes fabricantes pudessem se cumunicar.

A arquitetura OSI está projetada em sete camadas de maneira que, cada camada, possui uma lista própria de protocolos e serviços e, também, descreve a maneira como cada camada intererage com a camada imediatamente superior e inferior.

Segundo Filho (2009)

> Cada camada é independente e poderá se comunicar com a mesma camada em outro host

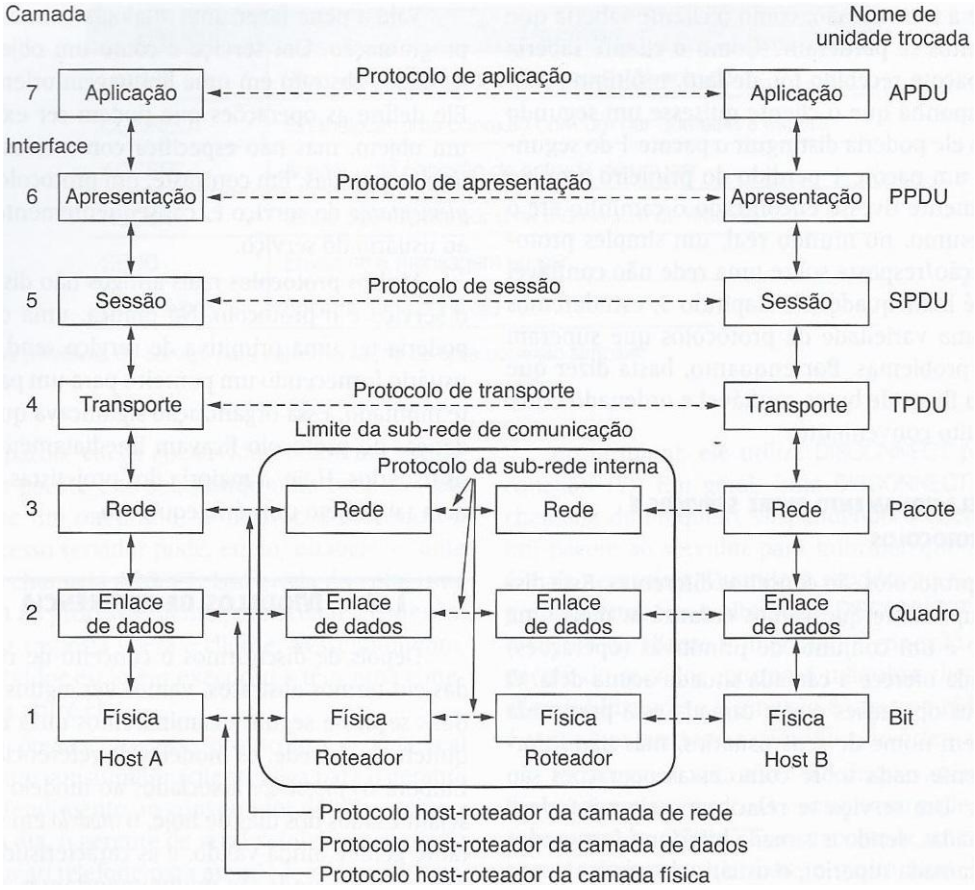

Figura 1 - O modelo de referência OSI

Fonte: Tanembaum (2011)

Tabela 1 - Resumo funcional do Modelo OSI

	Camada	**Descrição Funcional**
7	Aplicação	Faz interface entre a rede e softwares aplicativos. Inclui também serviços de autenticação
6	Apresentação	Define o formato e a organização dos dados. Inclui criptografia
5	Sessão	Estabelece e mantém fluxos bidirecionais de um terminal a outro. Inclui o gerenciamento de fluxos de transação
4	Transporte	Fornece uma variedade de serviços entre os dois computadores hosts, incluindo o estabelecimento e a finalização da conexão, controle de fluxo, recuperação de erros e segmentação de grandes blocos de dados em partes menores para transmissão
3	Rede	Endereçamento lógico, roteamento e determinação de caminhos
2	Enlace	Formata dados em frames apropriados para transmissão

		através de alguma mídia física. Define regras para quando a mídia pode ou não ser usada. Define meios pelos quais se pode reconhecer erros de transmissão
1	Física	Define os detalhes elétricos, óticos, de cabeamento, de conectores e de procedimentos requeridos para se transmitirem os bits, representados como alguma forma de energia e se movendo através de um meio físico

Fonte: Odom (2011)

2.2.2 Modelo de Referência TCP/IP

No início, havia a ARPANET, que era uma rede de pesquisa patrocinada pelo Departamento de Defesa dos Estados Unidos (DoD). Tanembaum (2011, p. 28) afirma que

> Pouco a pouco, centenas de universidades e repartições públicas foram conectadas, usando linhas telefônicas dedicadas. Mais tarde, quando foram criadas as redes de rádio e satélite, os protocolos existentes começaram a ter problemas de interligação com elas, o que forçou a criação de uma nova arquitetura de referência. Deste modo, quase desde o início, a capacidade para conectar várias redes de maneira uniforme foi um dos principais objetivos do projeto.

Tanembaum (2011, p. 28) afirma, ainda, que - "Essa arquitetura posteriormente ficou conhecida como **modelo de referência TCP/IP**, graças a seus principais protocolos".

O modelo de referência TCP/IP foi definido pela primeira vez em 1974, depois melhorado e estabelecido como um padrão na comunidade da Internet. Este modelo foi projetado para se manter funcionando, mesmo no caso de parte dos hosts pararem de funcionar. Por exemplo, se um grupo de hosts parar de funcionar, o restante dos hosts devem continuar funcionando mesmo sem aqueles que deixaram de funcionar.

Segundo Torres (2007)

> O TCP/IP não é na verdade um procolo, mas sim um conjunto de protocolos - uma pilha de protocolos, como ele é mais chamado. Seu nome, por exemplo, já faz referência a dois protocolos diferentes, o TCP (Transmission Control Protocol, Protocolo de Controle de Transmissão) e o IP (Internet Protocol, Protocolo de Internet)

De forma análoga ao modelo de referência OSI, o modelo de referência TCP/IP também está estruturado em camadas, como mostra a tabela abaixo

Tabela 2 - Modelo Arquitetônico TCP/IP e Exemplos de Protocolos

	Camada	**Exemplos de Protocolos**
4	Aplicação	HTTP, POP3, SMTP
3	Transporte	TCP, UDP
2	Internet	IP
1	Acesso	Ethernet, Frame Relay

Fonte: Odom (2011, p. 16)

2.3 Equipamentos de Rede

Diversos equipamentos são necessários em uma rede de computadores. Hubs, switches e roteadores, por serem mais complexos, são apresentados abaixo.

2.3.1 HUB

HUBs são dispositivos repetidores com múltiplas portas físicas. Um hub recebe um sinal através de uma das portas, o regenera e o reenvia através de todas as outras portas. As portas de um HUB trabalham com largura de banda compartilhada e, frequentemente, reduzem o desempenho da rede em razão de colisões e recuperações.

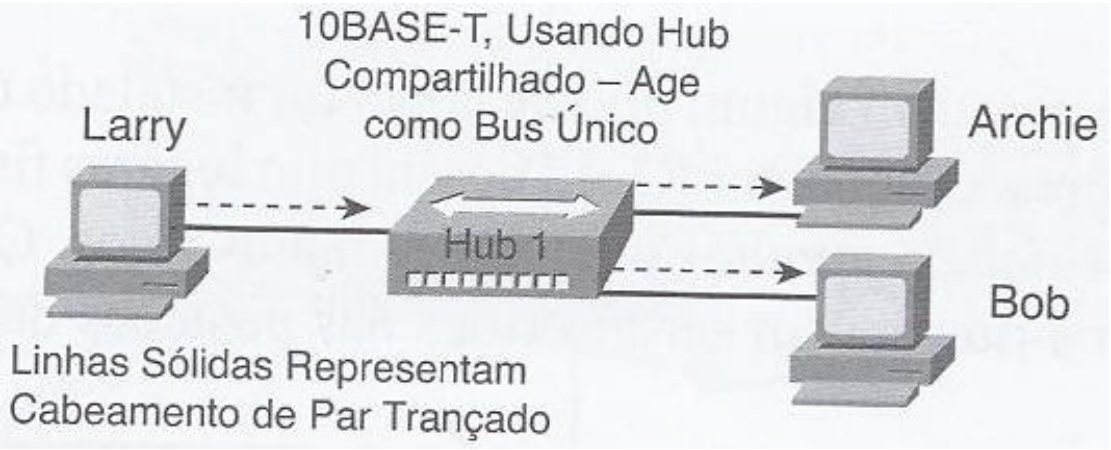

Figura 2 - Pequena rede usando HUB

Fonte: Odom(2011, p. 37)

2.3.2 Switch de Camada 2

Operando na Camada 2 do modelo OSI, um Switch de Camada 2 é um dispositivo de rede, intermediário, que interconecta outros dispositivos. O switch difere do hub pelo fato de interpretar os bits em cada frame recebido e enviar o frame para apenas a porta requerida, em vez de enviar a todas as portas, diminuido ou eliminando, assim, a quantidade de colisões na rede.

Segundo Tanembaum (2011, p. 12) "A função do switch é repassar os pacotes entre os computadores que estão conectados, usando o endereço em cada pacote para determinar para qual computador enviá-lo".

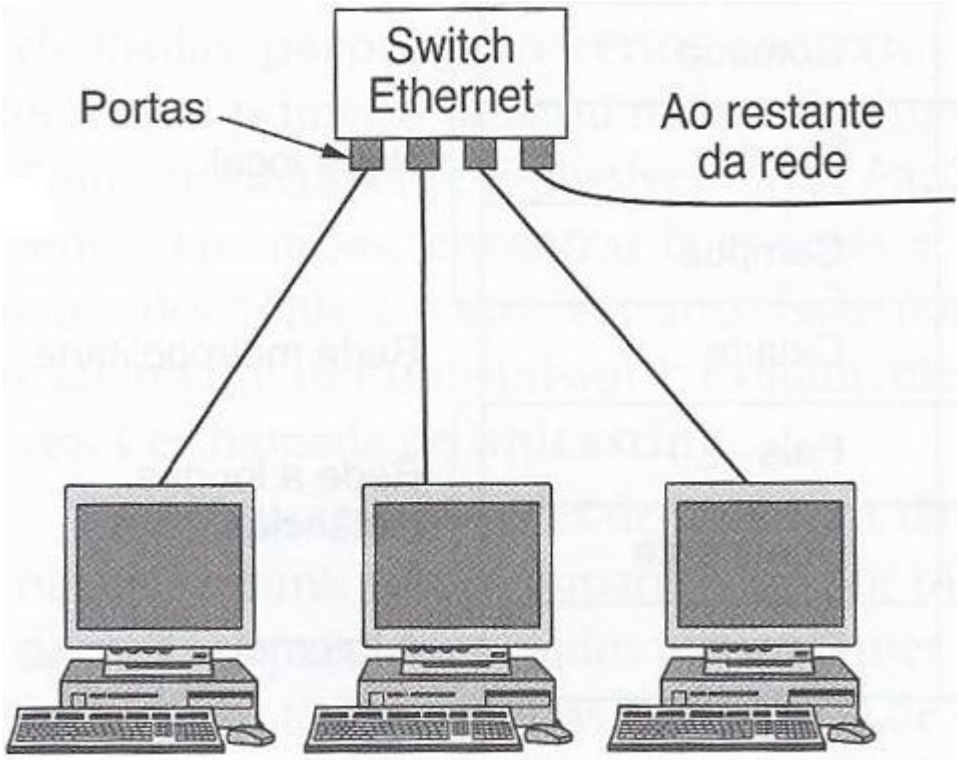

Figura 3 - Pequena rede usando Switch

Fonte: Tanembaum (2011, p. 12)

2.3.3 Switch de Camada 3

Operando na Camada 3 do modelo OSI, um Switch de Camada 3 é um dispositivo de rede, intermediário, que interconecta outros dispositivos. O Switch de

Camada 3 faz todas as funções do Switch de Camada 2. Além disso, tem a capacidade de aprender sobre endereços IP detectando quais endereços IP estão associados a suas interfaces e ainda fazer o serviço de roteamento deixando desnecessária a utilização de roteadores em uma rede local.

2.3.4 Roteadores

Roteadores são dispositivos de rede primários que são usados para conectar uma rede a outra. Os switches conectam dispositivos dentro de uma mesma rede. Os roteadores conectam as redes propriamente ditas. Cada porta do roteador faz conexão com uma rede diferente e o roteador roteia os pacotes entre as redes.

Routers, ou roteadores, realizam a compatibilização das redes ao nível da camada de rede do modelo OSI (Oliveira, 2002)

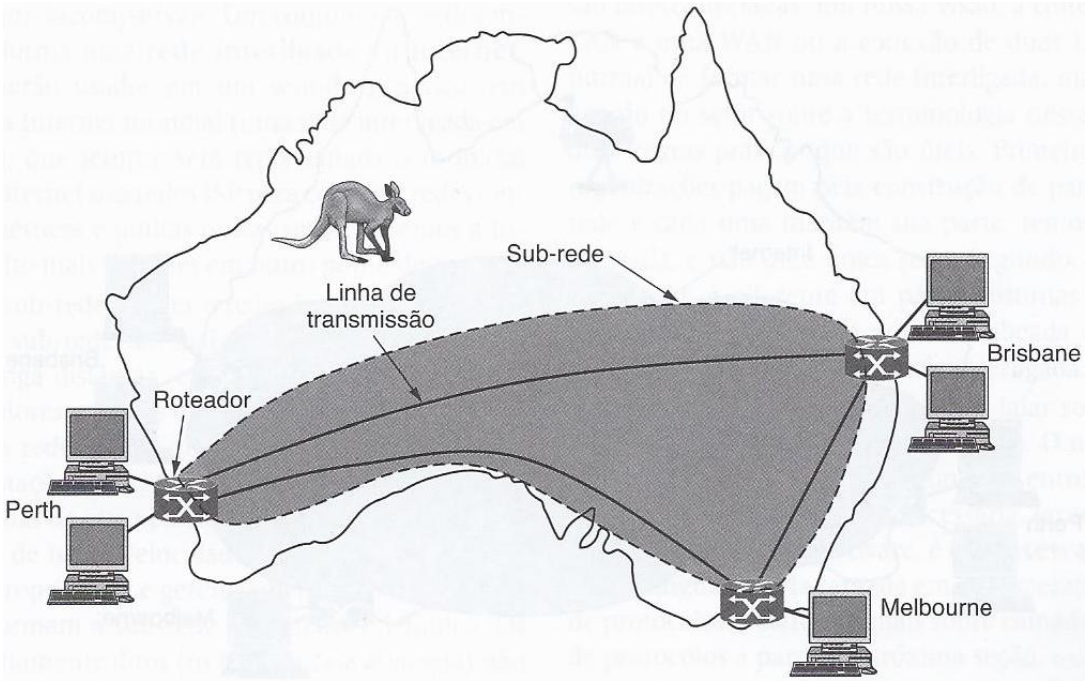

Figura 4 - Roteador conectando redes diferentes

Fonte: Tanembaum (2011, p. 15)

2.4 Tópicos Relacionados a Redes Hierárquicas

Rede Hierárquica é uma rede desenhada de maneira que os switches são projetados em camadas lógicas com a finalidade de facilitar o gerenciamento e a implementação de técnicas essenciais como redundância, por exemplo. As camadas de uma Rede Hierárquica são três, descritas abaixo.

- **Camada de Acesso** - nesta camada são alocados roteadores, switches, bridges, hubs e pontos de acesso wireless. Esses dispositivos fazem interface com dispositivos finais para que estes obtenham acesso ao restante da rede.
- **Camada de Distribuição** - esta camada controla o fluxo de tráfego de rede e determina domínios de broadcast, realizando funções de roteamento entre redes locais (VLANs) definidas na camada de acesso.
- **Camada de Núcleo** - esta camada é o backbone de alta velocidade da das redes interconectadas. Esta camada deve ser capaz de encaminhar grandes quantidades de dados rapidamente e deve ser altamente disponível.

2.4.1 Redundância

Para garantir melhor disponibilidade é importante implementar o conceito de redundância que consiste, por exemplo, em duplicar as conexões de rede entre dispositivos ou duplicar os próprios dispositivos. Desta maneira, havendo falha em um dos dispositivos, o outro passa a operar no lugar do dispositivo falho. Segundo Odom (2011, p. 43)

> Os switches podem falhar, e os cabos podem estar cortados ou desligados, mas, se switches e cabos redundantes forem instalados, o serviço de rede pode, ainda assim, permanecer disponível para a maioria dos usuários.

2.4.1.1 STP - Spanning Tree Protocol

Ao implementar redundância em uma rede cria-se mais de um caminho por onde os frames Ethernet podem trafegar. O objetivo dessa técnica é, caso um dos caminhos deixe de operar, outro possa continuar operando garantindo a disponibilidade da rede. O efeito colateral disso, segundo Odom (2011, p. 43) é que

> LANs com links redundantes oferecem a possibilidade de os frames fazerem um loop em torno da rede indefinidamente. Esses frames em looping causariam problemas de desempenho na rede.

O padrão IEEE 802.1d especifica o protocolo STP, que permite que links redundantes sejam utilizados na rede sem que os frames entrem em loop. Odom (2011, p. 45) afirma que

> Com o STP ativado, alguns switches bloqueiam as portas de forma que essas portas não encaminham frames. O STP escolhe quais portas bloquear para que exista somete uma passagem ativa entre qualquer par de segmentos da LAN (domínio de broadcast). Em consequência disso, os frames podem ser entregues a cada dispositivo, sem causar os problemas criados quando os frames fazem loop através da rede.

2.4.2 VLAN

O conceito LAN Virtual (VLAN) foi padronizado pelo comitê IEEE 802 com o intuito de permitir que em um mesmo switch se possa configurar mais de um domínio de broadcast, como se cada domínio de broadcast fosse um switch separado. Essa estratégia melhora o desempenho da rede. Tanembaum (2011, p. 215) afirma que - "algumas LANs são utilizadas mais intensamente que outras, e pode ser interessante separá-las".

Souza (2009) afirma que

> O switch segmenta uma rede em blocos, ou seja, LANs Virtuais, segmentos logicamente separados. Trata-se de um domínio de broadcast criado por um ou mais switches. Em virtude disso, em vez de todas as portas formarem um único dmínio de broadcast, o switch as separa em várias, de acordo com a configuração.

Sem utilizar VLANs, a separação das LANs implicaria em utilizar um switch para cada LAN. Utilizando VLANs um mesmo switch pode ser configurado para criar várias VLANs de forma lógica, o que gera economia, facilidade de administração e aumenta a segurança da rede.

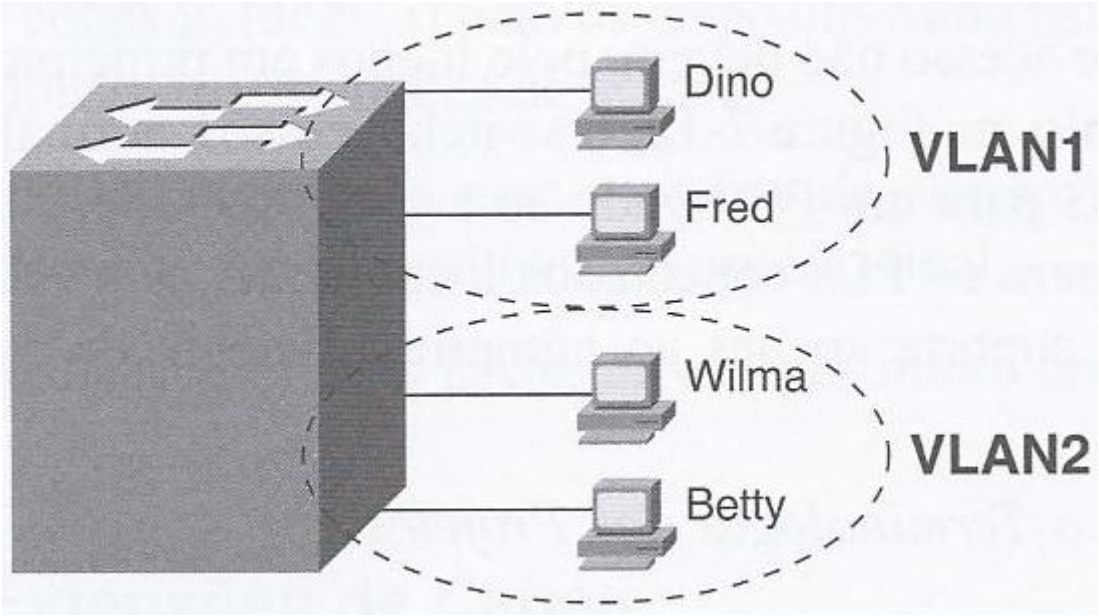

Figura 5 - Duas VLANs usando em um Switch

Fonte:Odom (2008, p. 137)

2.4.2.1 Trunk

Quando são utilizadas VLANs entre switches interconectados, ao enviar e receber os frames os switches precisam saber a qual VLAN cada frame pertence. O padrão IEEE 802.1Q especifica o *Trunking de VLAN*. Odom (2008, p. 9) afirma que

> O Trunking de VLAN faz com que os switches utilizem um processo chamado *VLAN tagging*, através do qual o switch de envio acrescenta outro cabeçalho ao frame antes de enviá-lo pelo trunk. Este cabeçalho de VLAN adicional possui um campo *VLAN identifier* (*identificador de VLAN*) (VLAN ID) de forma que o switch de envio possa listar o VLAN ID e o switch de recebimento possa saber a qual VLAN pertence cada frame.

Desta forma o switch de recebimento, ao enviar o frame para o próximo salto, o enviará para a porta configurada com mesmo VLAN ID determinado no cabeçalho do frame recebido.

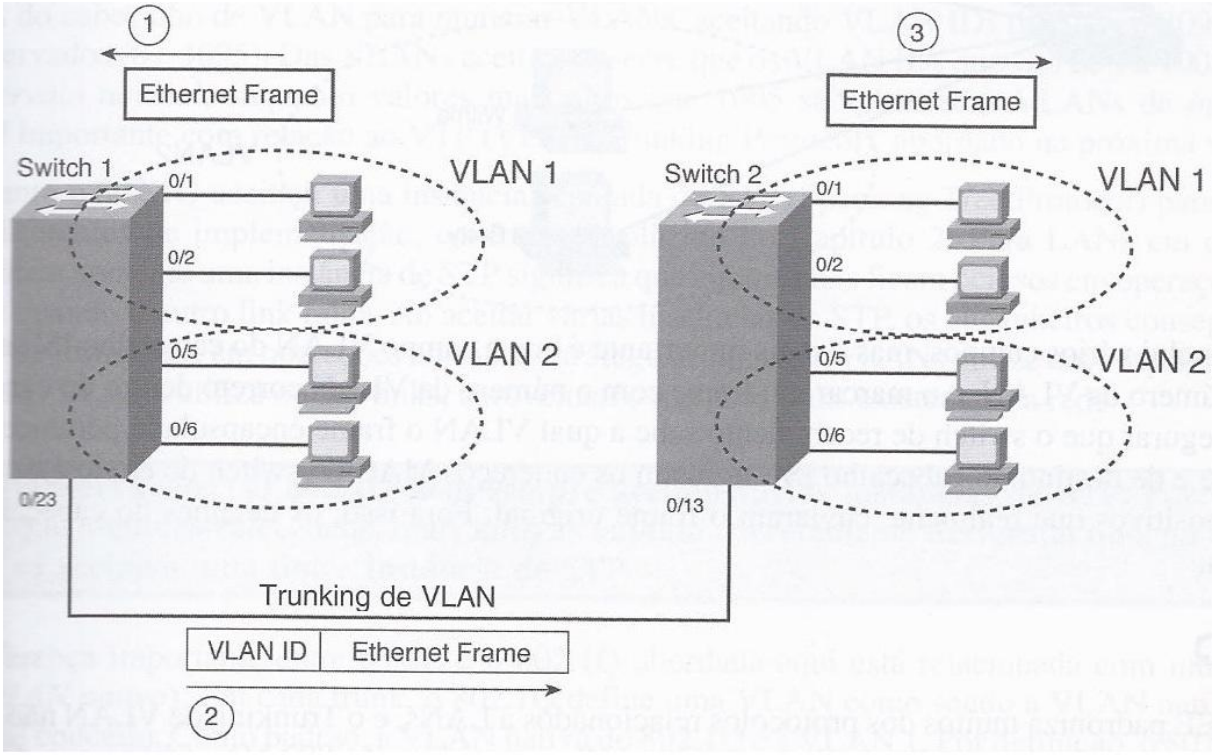

Figura 6 - Trunking de VLAN entre dois Switches

Fonte: Odom (2008, p. 9)

2.4.2.2 Protocolos de Roteamento

Diversos protocolos de roteamento IP foram desenvolvidos com o objetivo de fazer com que os roteadores se mantivessem com uma tabela sempre atualizada provendo as melhores rotas disponíveis na rede. Odom (2008, p. 327) afirma que

> Protocolos de roteamento ajudam os roteadores a aprender rotas fazendo cada roteador anuncie as rotas que conhece. Cada roteador começa conhecendo apenas as rotas diretamente conectadas. Depois, cada roteador envia mensagens, definidas pelo protocolo de roteamento, que listam as rotas. Quando um roteador ouve uma mensagem de atualização de roteamento de outro roteador, o roteador que esta ouvindo a atualização aprende a respeito das sub-redes e adiciona rotas em sua tabela de roteamento.

Nesta pesquisa serão abordados os protocolos RIP-2, OSPF e EIGRP.

Protocolo RIP-2

RIP-2 é um protocolo de roteamento que faz com que cada roteador anuncie uma pequena quantidade de informações sobre suas sub-redes aos roteadores vizinhos. Os roteadores vizinhos, por sua vez, anunciam para seus vizinhos, e assim por diante até que todos os roteadores conheçam todas as sub-redes.

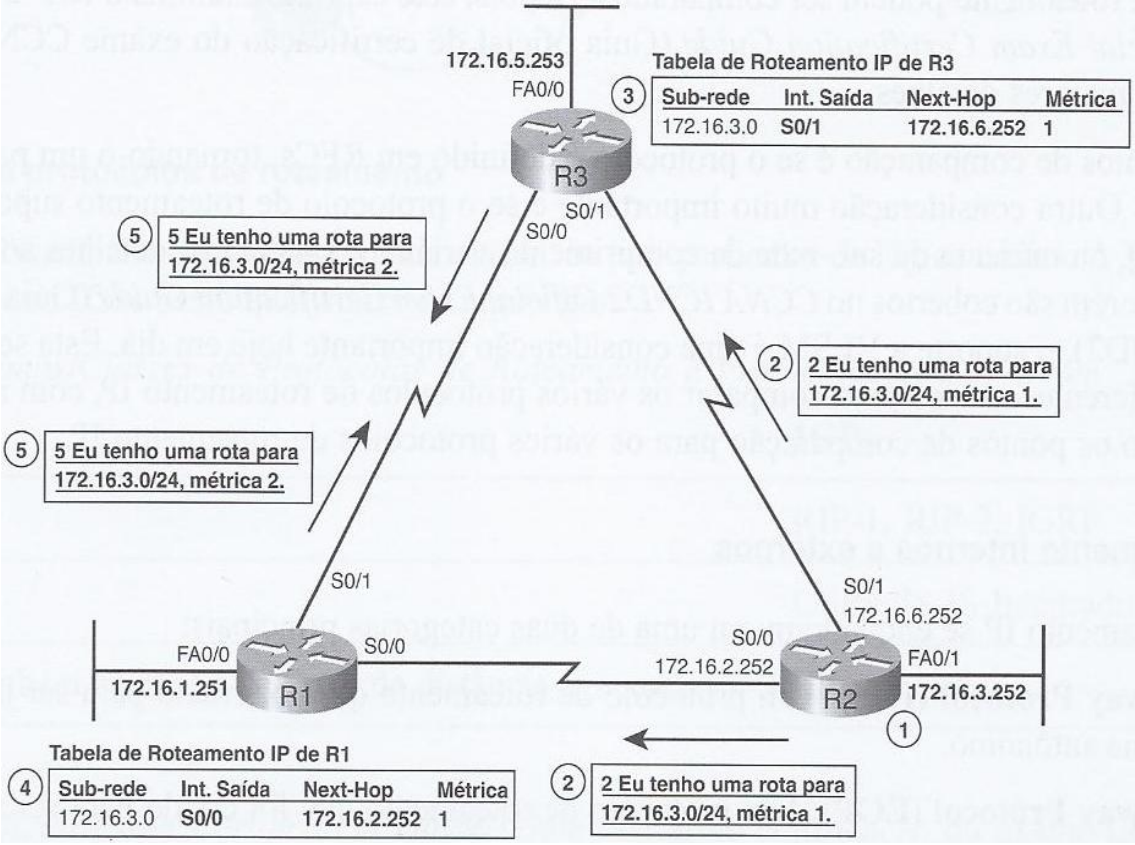

Figura 7 - RIP-2 Anunciando Rotas

Fonte: Odom (2008, p. 327)

Protocolo OSPF

OSPF (*Open Shortest Path First*) é o protocolo de roteamento *link-state* mais comumente utilizado nos dias atuais. Odom (2008, p. 251) afirma que

> Para ajudar no processo de aprendizado, os recursos OSPF podem ser divididos em três categorias principais: vizinhos, troca de banco de dados e cálculo de rotas. Primeiramente os roteadores OSPF formam uma relação de vizinhos que fornece a base para toda a comunicação contínua do OSPF. Depois que os roteadores se tornam vizinhos, eles trocam o conteúdo dos seus respectivos LSDBs através de um processo chamado troca de banco de dados. Finalmente assim que um roteador tem as informações de topologia em seu LSDB (link-state data base), ele utiliza o algorítmo Dijkstra SPF para calcular as melhores rotas atuais e acrescentá-las à tabela de roteamento IP.

Protocolo EIGRP

EIGRP (*Enhanced Interior Gateway Routing Protocol*) é um protocolo de roteamento, proprietário da Cisco, que disponibiliza um vasto conjunto de recursos destinados ao aprendizado das rotas. Odom (2008, p. 251) afirma que

> O EIGRP não se enquadra perfeitamente nas categorias gerias de protocolos de roteamento vetor distância e link-state. Às vezes a Cisco se refere ao EIGRP simplesmente como um protocolo vetor distância avançado, mas em outrsa ocasiões, a Cisco se refere ao EIGRP como sendo um tipo novo: um protocolo balanced hybrid. Não importa a categoria, os conceitos fundamentais e os processos usados pelo EIGRP podem ter algumas semelhanças com outros protocolos de roteamento, mas o EIGRP possui mais diferenças, tornando-o um protocolo de roteamento único, por si mesmo.

2.4.4 Segurança

Um bom projeto de rede de computadores precisa contemplar, também, a questão da segurança da informação. É necessário manter a informação disponível, porém de forma segura, isto é, a informação deve estar disponível somente para os usuários que tiverem direito de acesso a elas. O invasor, em muitos casos, são pessoas de dentro da própria organização. Tanembaum (2011, p. 479) afirma que, em sua forma mais simples, a segurança da informação

> Preocupa-se em impedir que pessoas mal-intencionadas leiam, ou pior ainda, modifiquem secretamente mensagens enviadas a outros destinatários. Outra preocupação da segurança são as pessoas que tentam ter acessoa a serviços remotos que não estão autorizadas a usar.

Para (Milanez, 2007)

> Nos dias de hoje, a segurança da informação é uma das maiores preocupações e, sem dúvida, uma das tarefas mais importantes dos profissionais de TI.

A Tabela 2, abaixo, apresenta alguns dos invasores mais comuns, juntamente com seus objetivos de invasão.

Tabela 2 - Adversários da segurança com seus objetivos

Adversário	**Objetivo**
Estudante	Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas
Cracker	Testar o sistema de segurança de alguém; roubar dados
Representante de Vendas	Tentar representar toda a Europa e não apenas Andorra
Executivo	Descobrir a estratégia de marketing do concorrente
Ex-funcionário	Vingar-se por ter sido demitido
Contador	Desviar dinheiro de uma empresa
Corretor de Valores	Negar uma promessa feita a um cliente por meio de uma mensagem de correio eletrônino
Vigarista	Roubar números de cartão de crédito e vendê-los
Espião	Descobrir segredos militares ou industriais de um inimigo
Terrorista	Roubar segredos de armas bacteriológicas

Fonte: Tanembaum (2011, p. 479)

2.4.4.1 Segurança de Porta

Uma importante estratégia de segurança é definir precisamente os dispositivos que devem ser conectados a cada interface do switch e configurar a Segurança de Porta (Port Security) para restringir cada interface do switch de modo que apenas os dispositivos configurados possam utilizá-la. Odom (2011, p. 183) afirma que

> Isso reduz a exposição a alguns tipos de ataques, nos quais o hacker conecta um laptop a uma tomada que esteja também conectada a uma porta de um switch configurado para usar a segurança das portas. Quando esse dispositivo não-autorizado tenta enviar frames para a interface do switch, o switch pode emitir mensagens informativas, descartar os frames vindos desse dispositivo ou até mesmo descartatr frames vindos de todos os dispositivos, efetivamente desligando a interface.

2.4.4.2 Ataque de DDoS (Distributed Denial of Service)

Um tipo comum de ataque a uma rede é o Ataque de DoS (Denial of Service). Este tipo de ataque consiste no envio massivo de pacotes inúteis a um provedor de serviços de maneira que os recursos do provedor são esgotados e o serviço pára de responder. Com isso se impede que um usuário legítimo tenha acesse ao serviço. Quando provém de uma única origem este ataque é chamado, simplesmente, de Ataque de DoS. Stallings (2011, p 438) afirma que

> Uma ameaça mais séria é imposta por um ataque de DDoS. Em um ataque de DDoS, um atacante é capaz de recrutar diversos hosts pela Internet para desferirem simultaneamente, ou de maneira coordenada, um ataque ao alvo.

2.5 Voz sobre IP (VoIP)

Além da transferência de dados, atualmente, com a melhora na largura de banda, se tornou possível transferir também áudio e vídeo. Com a utilização da tecnologia VoIP (Voice over IP) é possível realizar chamadas telefônicas que trafegam nas redes de dados. Odom (2008, p. 107) firma que

> A maioria das empresas hoje em dia ou já começou ou planeja migrar para o uso de telefones IP, os quais passam o tráfego de voz através da rede de dados, dentro de pacotes IP e usando protocolos de aplicativos conhecidos genericamente como voz-sobre-IP (VoIP)Uma ameaça mais séria é imposta por um ataque de DDoS. Em um ataque de DDoS, um atacante é capaz de recrutar diversos hosts pela Internet para desferirem simultaneamente, ou de maneira coordenada, um ataque ao alvo.

A Figura 8, abaixo, mostra alguns dos detalhes de como o VoIP funciona a partir de uma conexão de alta velocidade à Internet, com um adaptador de voz genérico (VA) convertendo o sinal de voz analógico do telefone normal em um pacote IP.

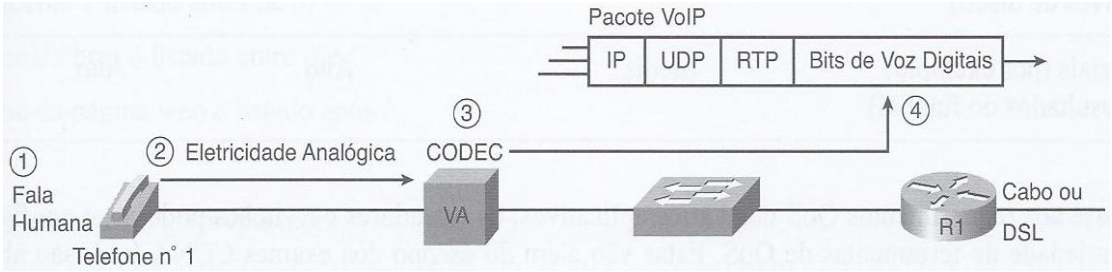

Figura 8 - Voz sobre IP

Fonte: Odom (2008, p. 107)

Segundo Odom (2008, p. 107)

> Uma única chamada VoIP que atravesse uma WAN geralmente usa menos de 30 kbps de largura de banda, o que não é muito se comparado com muitos aplicativos de dados de hoje em dia. Na realidade, a maioria dos aplicativos de dados consome tanta largura de banda quanto conseguir ocupar. Entretanto, o tráfego VoIP tem diversos outros requerimentos de QoS sobre a rede que ainda complicam o uso dessa tecnologia.

Entre os requerimentos de QoS necessários ao tráfego de voz estão:

- **Baixo delay**: requer, normalmente, menos de 200 milisegundos(0,2 segundos). Muito menos do que o requerido por aplicativos comuns
- **Baixo jitter**: Jitter é uma variação do deley. Para pacotes VoIP consegutivos não pode ultrapassar 30 milisegundos (0,3 segundos)
- **Perda**: por causa das questões do delay e do jitter não há necessidade de se tentar recuperar pacotes perdidos - um pacote perdido seria inútil se fosse recuperado.

A Tabela 3, abaixo, resume algumas questões sobre as necessidades de vários tipos de aplicativos para os quatro principais requerimentos de QoS.

Tabela 3 - Comparação das necessidades mínimas dos aplicativos

Tipo de Aplicativo	Largura de Banda	Delay	Jittter	Perda
VoIP	Baixa	Baixo	Baixo	Baixa
Vídeo sobre IP de duas vias(vídeoconferência)	Média/Alta	Baixo	Baixo	Baixa
Vídeo sobre IP de uma via(câmera de vigilância)	Média	Médio	Médio	Baixa
Dados interativos críticos(folha de pagamento)	Média	Médio	Alto	Alta
Dados empresariais interativos(chat online)	Baixa/Média	Médio	Alto	Alta
Transferência de arquivos(backup)	Alta	Baixo	Alto	Alta
Não-empresariais(resultados do futubel)	Média	Baixo	Alto	Alta

Fonte: Odom (2008, p. 108)

2.6 Ferramentas de Rede

Para analisar uma rede de computadores alguns aplicativos são importantes. Neste trabalho utilizamos o iPerf e o Wireshark, que servem para gerar tráfego na rede e possibilitar análise detalhada dos dados que trafegam, simultaneamente.

2.6.1 iPerf

O iPerf é um software do tipo cliente/servidor desenvolvido pelo *National Laboratory for Applied Network Research* (NLANR). A finalidade deste software é gerar tráfego de rede enviando pacotes TCP ou UDP para testar a largura de banda de uma rede de computadores.

No ambiente Linux, em distribuições derivadas do Debian, o iPerf pode ser instalado com o comando ***apt-get install iperf***.

Para verificar a largura de banda entre dois computadores, um dos computadores deve ser definido como servidor, para receber o tráfego, e o outro como cliente, para gerar o tráfego.

No servidor, o iPerf deve ser executado com o comando ***iperf -s***. Desta maneira o iPerf ficará aguardando conexão do cliente.

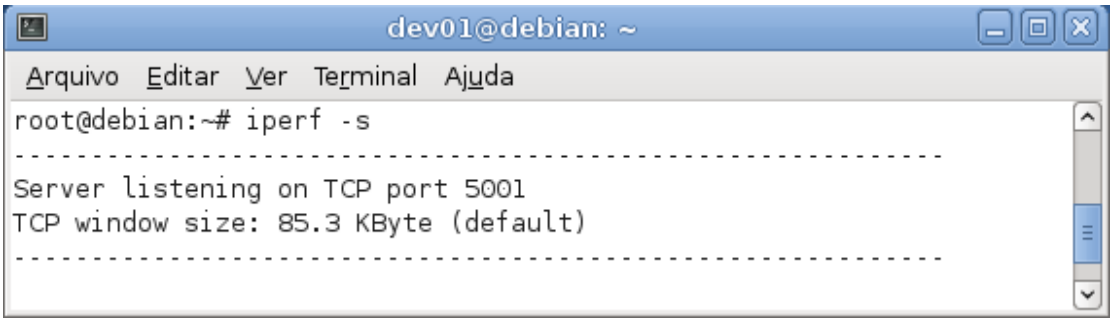

Figura 9 - iPerf Server

Fonte: autoria própria

No outro computador o iPerf deve ser executado com o comando ***iperf -c IP***, onde IP é o endereço IP do servidor. Desta maneira o iPerf será o cliente. Na Figura, abaixo, o iPerf mostrou que, em 10 segundos, foram transferidos 680 MBytes, alcançando velocidade média de 560 Mbits/sec.

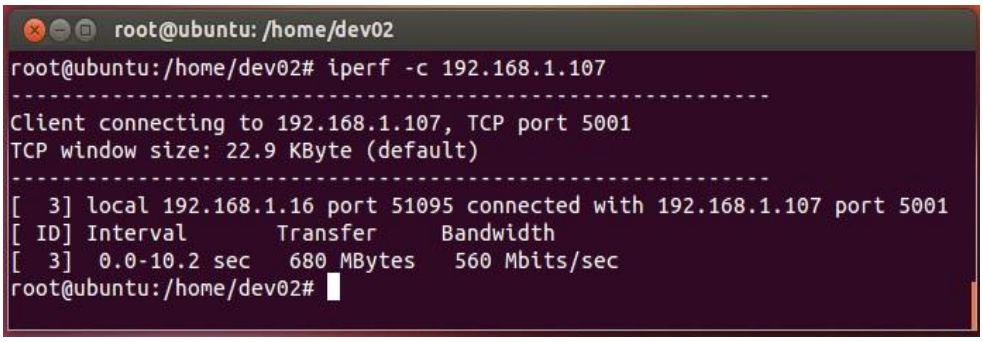

Figura 10 - iPerf Client

Fonte: autoria própria

2.6.2 Wireshark

O Wireshark é um software que captura o tráfego de rede e o apresenta agrupado por protocolo, permitindo saber tudo que entra e sai de um determinado host ou da rede em que o host está conectado.

No ambiente Linux, em distribuições derivadas do Debian, o Wireshark pode ser instalado com o comando ***apt-get install wireshark***.

Depois de feita a instalação, para executar o Wireshark, no Terminal, logado como root, basta executar o comando **wireshark**.

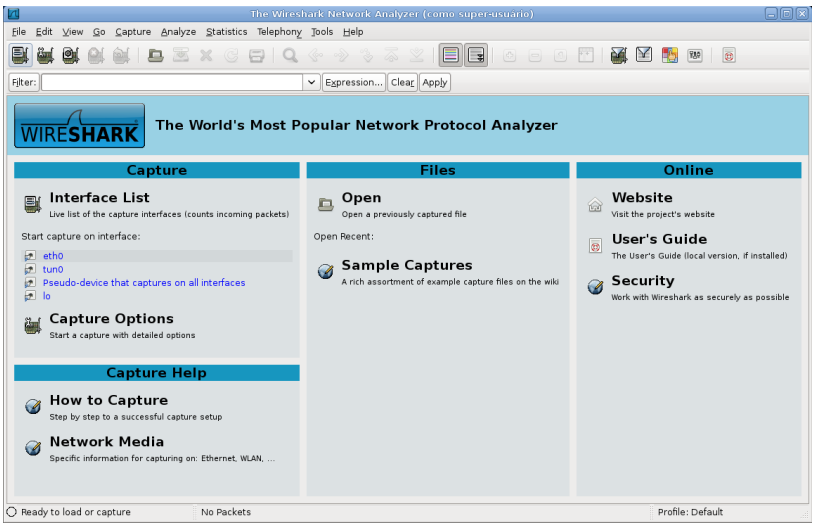

Figura 11 - Wireshark - janela inicial

Fonte: autoria própria

Para capturar o tráfego ocorrido na interface **eth0**, por exemplo, na janela inicial do Wireshark, representado pela Figura 10, acima, basta clicar no item **eth0**, abaixo de **Interface List**.

A janela abaixo é apresentada e a captura dos pacotes é, imediatamente, iniciada. Parte das colunas da janela abaixo são:

- **Source** - origem do pacote - normalmente o endereço IP do host que enviou o pacote
- **Destination** - destino do pacote - normalmente o endereço IP do host para o qual o pacote é destinado
- **Protocol** - protocolo utilizado no pacote
- **Info** - dados que estão sendo trafegados

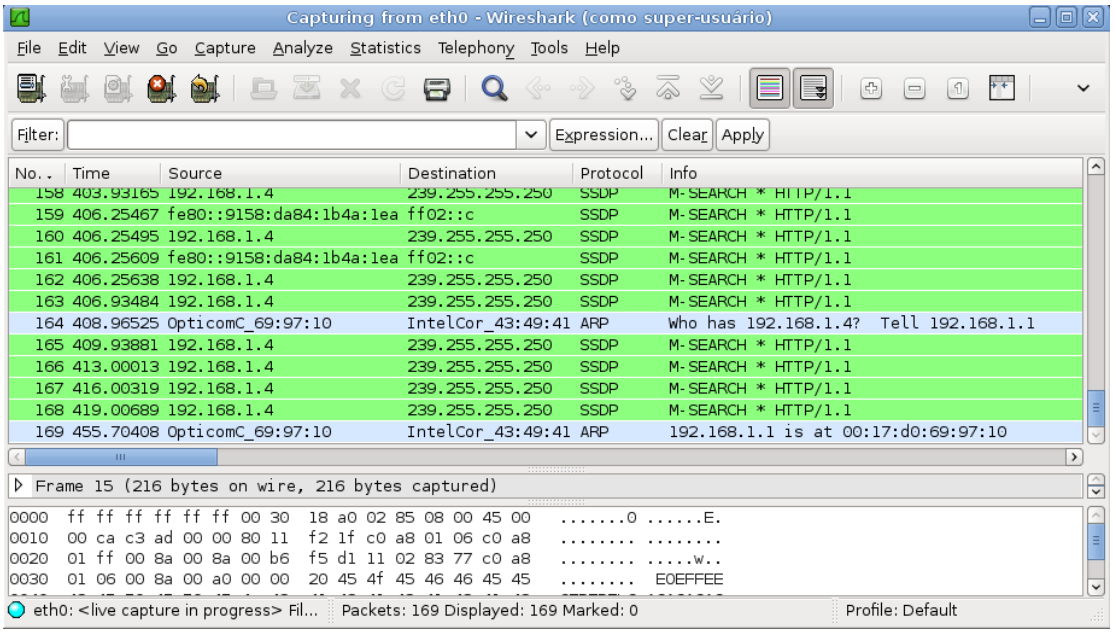

Figura 12 - Wireshark - capturando tráfego

Fonte: autoria própria

3. Implementação prática em laboratório

3.1. Topologia hierárquica

Para ilustrar uma rede hierárquica foi montada a topologia representada pela figura abaixo e implementada em laboratório. `

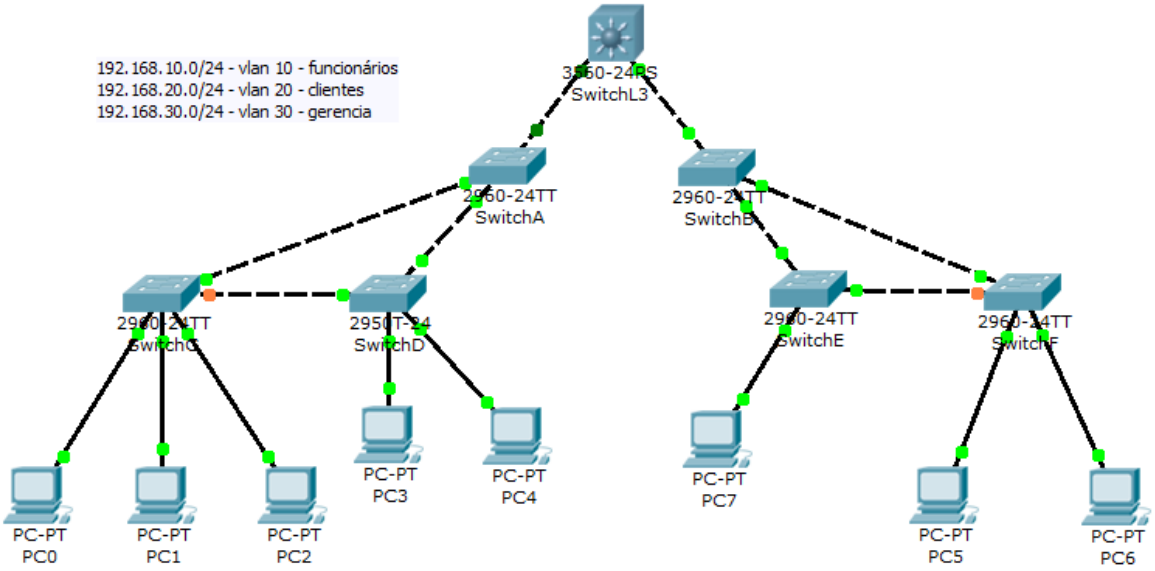

Figura 13 - Topologia hierárquica

Fonte: autoria própria

Parte das instruções do Switch Layer 3

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SwitchL3
SwitchL3(config)#interface FastEthernet 1
SwitchL3(config-if)#no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
SwitchL3(config-if)#exit
SwitchL3(config)#interface FastEthernet 1.10
SwitchL3(config-if)#encapsulation dot1q 10
SwitchL3(config-if)#exit
SwitchL3(config)#ip address 192.168.10.1 255.255.255.128
SwitchL3(config)#exit
SwitchL3#exit
```

Parte das instruções dos Switches Layer 2

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name funcionarios
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name clientes
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name gerencia
Switch(config-vlan)#exit
Switch(config)#hostname SwitchA
SwitchA(config)#spanning-tree vlan 10 root primary
SwitchA(config)#spanning-tree vlan 20 root primary
SwitchA(config)#spanning-tree vlan 30 root primary
SwitchA(config)#interface range FastEthernet 0/5-12
SwitchA(config-if-range)#switchport mode access
SwitchA(config-if-range)#switchport access vlan 10
SwitchA(config-if-range)#switchport access vlan 20
SwitchA(config-if-range)#switchport access vlan 30
SwitchA(config-if-range)#exit
SwitchA(config)#interface FastEthernet 0/2
SwitchA(config-if)#switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to
down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
SwitchA(config-if)#switchport trunk allowed vlan 10,20,30
SwitchA(config-if)#exit
SwitchA(config)#exit
SwitchA#
%SYS-5-CONFIG_I: Configured from console by console
SwitchA#exit
```

3.2. Demonstração prática da necessidade do protocolo STP

Para comprovar a necessidade do protocolo STP foi montada a topologia representada pela figura abaixo com a intenção de, com o STP desabilitado, provocar uma tempestade de broadcast. Depois com o STP habilitado mostrar que a tempestade de broadcast não ocorre.

3.2.1 Tempestade de broadcast devido à não utilização do protocolo STP

- Foi criada redundância entre Switch0 e Switch1
- O protocolo STP foi desabilitado em ambos os switches - observa-se que os links redundantes entre os dois switches estão com todas as pontas verdes, isto é, habilitadas

  Switch> enable
  Switch# configure terminal
  Switch(config)# no spanning-tree vlan 1

- Ao Switch0 foi conectado o computador **jPerfServer** que, como o nome sugere, foi configurado como servidor do jPerf para receber para receber o tráfego gerado pelo computador **jPerfClient**
- Ao Switch1 foi conectado o computador **jPerfClient** que, como o nome sugere, foi configurado como cliente do jPerf para gerar tráfego na rede
- Propositalmente, nos computadores **jPerfServer** e **jPerfClient**, foi configurado para trafegar dados em broadcast

  jPerfServer> arp -s 192.168.1.3 ff:ff:ff:ff:ff:ff
  jPerfClient> arp -s 192.168.1.2 ff:ff:ff:ff:ff:ff

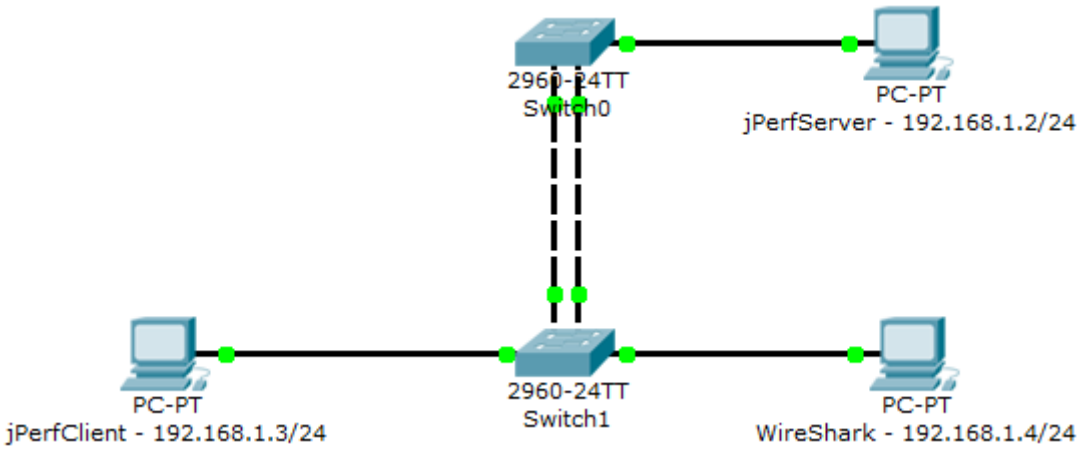

Figura 14 - STP desabilitado

Fonte: autoria própria

Os dois switches no mundo real. Se ve que há um patch cable azul conectando os dois switches através das interfaces fa0/1 e, também, um cabo amarelo fazendo o link redundante através das interfaces fa0/23.

Observa-se, também, que em ambas as conexões, fa0/1 e fa0/23, os leds estão acesos exatamente como na topologia ilustrativa. Isso indica que as interfaces estão ativas.

Figura 15 - Switches reais com STP desativado

Fonte: autoria própria

Captura da janela do jPerf Server mostra como está sendo utiliza toda a largura de banda.

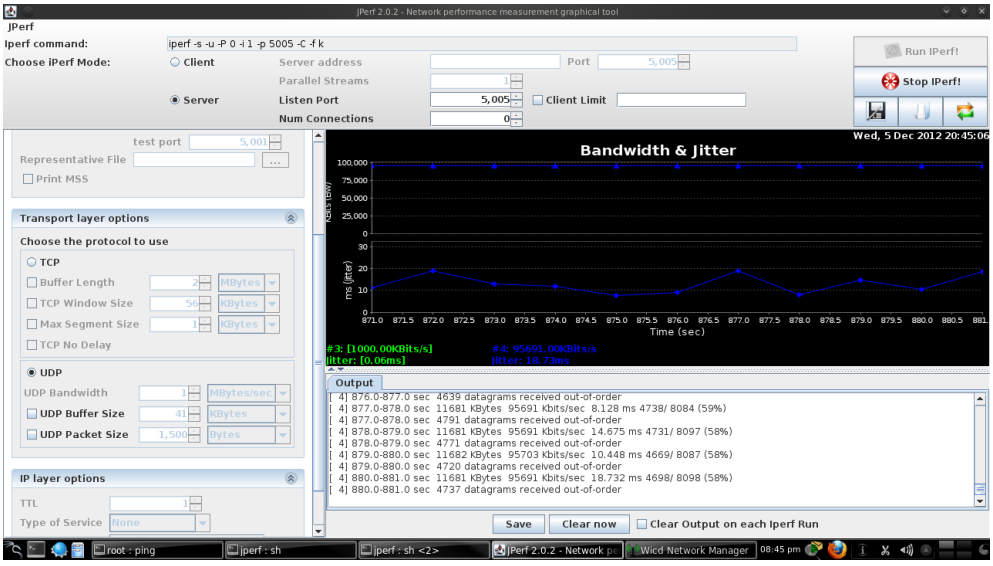

Figura 16 - jPerf utilizando toda a largura de banda

Fonte: autoria própria

Captura da janela de Interface do Switch mostrando a estatística onde se vê alta quantidade de perda de pacotes devido à tempestade de broadcast.

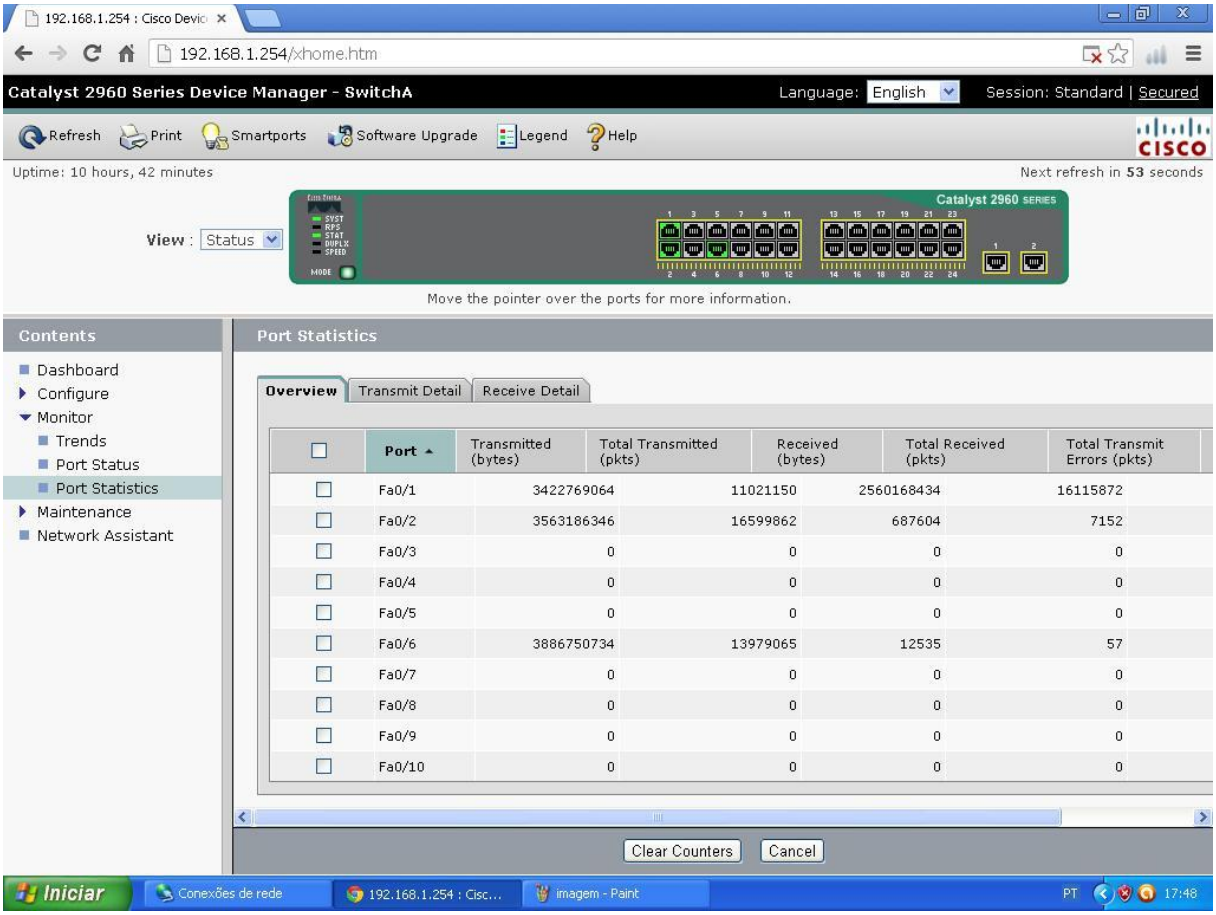

Figura 17 - Estatísticas do Switch

Fonte: autoria própria

Ao provocar a tempestade de broadcast, após poucos minutos toda a rede deixou de responder.

3.2.2 Protocolo STP desabilitando um dos links redundantes

- O protocolo STP foi habilitado em ambos os switches - observa-se que um dos links redundantes está ativo(as duas pontas em verde) e o outro está com uma das pontas em laranja indicando que o link está desabilitado

Switch> enable
Switch# configure terminal
Switch(config)# spanning-tree vlan 1

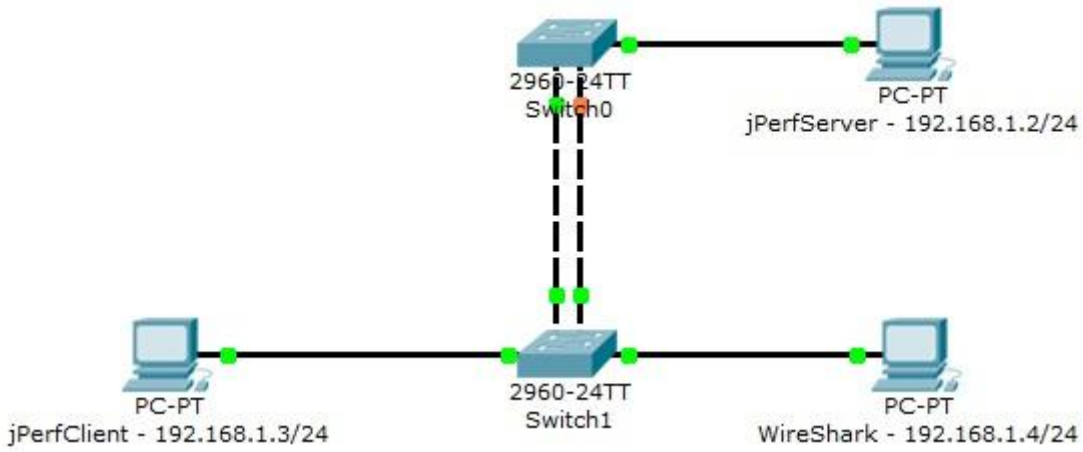

Figura 18 - STP habilitado

Fonte: autoria própria

Nos switches reais observa-se que o link do cabo amarelo está com um dos leds verde e outro em laranja indicando que este link está desabilitado.

Figura 19 - Switches reais com STP habilitado

Fonte: autoria própria

Assim foi constatado que a tempestade de broadcast deixou de ocorrer depois de ativar o protocolo STP.

4. Conclusão

O referencial teórico pesquisado proporcionou conhecimento e conscientização sobre questões importantes e que, muitas vezes são ignoradas, no universo das redes de computadores.

O conceito de VLAN(*Virtual Private Network*), por exemplo, deixa a rede melhor organizada logicamente, melhora o desempenho, visto que cada VLAN trafega no seu próprio domínio de broadcast e aumenta a segurança, pois membros de uma VLAN não tem acesso a outra VLAN.

Links redundantes, numa rede hierárquica, criam mais de um caminho para que a informação trafegue da camada de acesso até a camade de núcleo. Isso aumenta a disponibilidade da rede, pois na eventual queda de um dos caminhos, outro é, imediatamente, ativado.

Numa rede que usa links redundantes é necessário ativar o protocolo STP(*Spanning-Tree Protocol*), pois a redundância faria com que a rede entrasse em tempestade de broadcast, o que faz com que a rede deixe de responder, podendo até, em casos extremos, queimar parte dos equipamentos. O protocolo STP, quando ativado, faz com que somente um dos caminhos seja utilizado. Os outros caminhos ficam em modo de espera e, caso o caminho ativo deixe de operar, através do protocolo STP, um dos caminhos que estavam em espera é, imediatamente, acionado fazendo com que a rede se mantenha disponível, mesmo havendo ruptura de um dos caminhos.

Uma dos importantes recursos de segurança é a Segurança de Porta(*Port Security*), que pode ser configurada nos switches. Através da Segurança de porta é possível configurar cada porta de um switch para que aceite somente determinado host. No caso de um host diferente tentar acessar a porta do switch é possível rejeitar o acesso ou, até mesmo, desligar a porta para evitar tentativas posteriores.

Protocolos de roteamento fazem com que um roteador anuncie suas redes para os roteadores vizinhos e, estes, para os seus vizinhos, fazendo com que cada roteador crie uma tabela de roteamento que é usada para determinar os saltos entre um roteador e outro.

Atualmente, as empresas estão migrando seus serviços de telefonia para a tecnologia VoIP(Voz sobre IP). Através desta tecnologia utilizando um adaptador de voz é possível converter os dados de voz para pacotes IP e, então, esses pacotes IP trafegam normalmente na mesma estrutura da rede de dados.

Assim, com a pesquisa em todo o referencial teórico e as implementações práticas em laboratório, foi possível melhorar signicativamente o conhecimento na área estudada.

5. Referências

ODOM, Wendell. **CCNA ICND2.** 2ª ed. Rio de Janeiro, Alta Books, 2008.

ODOM, Wendell. **CCENT/CCNA ICND1.** 2ª ed. Rio de Janeiro, Alta Books, 2011.

STALLINGS, William. **Criptografia e Segurança e Redes**. 4ª ed. São Paulo, Pearson Education do Brasil, 2008.

TANEMBAUM, Andews S., WETHERALL David. **Redes de Computadores.** 5ª ed. São Paulo, Pearson Education do Brasil, 2011.

FILHO, André Stato. **Linux Controle de Rede**. Florianópolis, Visual Books, 2009.

MORIMOTO, Carlos Eduardo. **Servidores Linux - Guia Prático**. Porto Alegre, Meridional Ltda, 2010.

TORRES Gabriel. **Como o protocolo TCP/IP funciona,** 2007. Disponível em: http://www.infoetf.site40.net/Materias/Introducao%20a%20Redes/Protocolo_TCP_IP.pdf > Acessado em 02/12/2012

OLIVEIRA, Décio Tostes. **Gerência de Redes de Computadores,** 2002. Disponível em: http://lrodrigo.lncc.br/images/1/1f/GerRedesUmaAbordagemComUsoDoSMNP.pdf > Acessado em 03/12/2012

MILANEZ, Giovanni Folha. **Instalação Segura de um Cluster em Linux,** 2007. Disponível em: http://www.multicast.com.br/sergio/arquivos/monografia-pos-seguranca-instalacao-segura-cluster-em-linux.pdf > Acessado em 03/12/2012

SOUZA, Alessandro Goulart de. **Spanning Tree Protocol,** 2009. Disponível em: http://www.si.lopesgazzani.com.br/TFC/monografias/Monografia%20Alessandro.pdf > Acessado em 03/12/2012

ROCHA, Marcus Augusto Ribeiro da. **Voz sobre IP: Funcionamento e Cenários de Uso no Mercado Brasileiro,** 2006. Disponível em: http://www3.iesam-pa.edu.br/ojs/index.php/computacao/article/viewFile/69/64 > Acessado em 03/12/2012