UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO
DE SERVIDORES E EQUIPAMENTOS DE REDE

CELSO ARY PIMENTEL

ESTUDO E IMPLEMENTAÇÃO DE UMA ESTRUTURA DE REDE

MONOGRAFIA

CURITIBA
2013

CELSO ARY PIMENTEL

ESTUDO E IMPLEMENTAÇÃO DE UMA ESTRUTURA DE REDE

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede, do Programa de Pós-Graduação em Tecnologia. Universidade Tecnológica Federal do Paraná. Área de Concentração: Redes de Computadores

Orientador: Prof. Dr. Augusto Foronda

CURITIBA

2013

RESUMO

PIMENTEL, Celso A. **Estudo e Implementação de uma Estrutura de Rede.** 2013. 54 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

Esta monografia aborda o estudo para a implementação de uma rede de computadores utilizando a estrutura hierárquica de camadas focando em segurança e desempenho, utilizando as tecnologias disponíveis atualmente, visando o melhor projeto, implementação e gerenciamento por parte dos administradores de redes. O tema será abordado de maneira teórica, iniciando-se pelo método bibliográfico, seguido de estudo no simulador Cisco Packet Tracer.

Palavras-chave: Redes. Estrutura hierárquica. Modelo hierárquico. Estrutura de rede.

ABSTRACT

PIMENTEL, Celso A. **Study and Implementation of a Network Structure.** 2012. 54 pages. Monograph (Specialization in Configuration and Management of Servers and Network Equipments) - Federal Technological University of Paraná. Curitiba, 2013.

This monograph discusses the study for implementing a computer network using the hierarchical structure of layers focusing on security and performance using currently available technologies, seeking the best design, implementation and management on the part of network administrators. The subject will be approached from theoretical way, starting by literature method, followed by study at Cisco Packet Tracer simulator.

Keywords: Networks. Hierarchical structure. Hierarchical model. Network structure.

LISTA DE FIGURAS

LISTA DE SIGLAS

ARP	Address Resolution Protocol
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BDR	Backup Designated Router
CHAP	Challenge Handshake Authentication Protocol
DBD	Data Bank Description
DCE	Data Communications Equipment
DHCP	Dynamic Host Configuration Protocol
DR	Designated Router
DTE	Data Terminal Equipment
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
HDLC	High-level Data Link Control
HSSI	High-Speed Serial Interface
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPX	Internetwork Packet Exchange
ISDN	Integrated Service Digital Network
IS-IS	Intermediate System-to-Intermediate System
ISO	International Organization for Standardization
ISP	Internet Solution Provider

LAN	Local Area Network
LCP	Link Control Protocol
LSA	Link-State Advertisement
LSR	Link-State Request
LSU	Link-State Update
MAC	Media Access Control
NAT	Network Address Translation
NBMA	Non Broadcast Multi Access
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PDH	Plesiochronous Digital Hierarchy
POP3	Point Of Presence 3
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
RARP	Reverse Address Resolution Protocol
RFC	Request For Comments
RIP	Routing Information Protocol
RIR	Regional Internet Registry
SDH	Synchronous Digital Hierarchy
SMTP	Simple Mail Transfer Protocol
SPF	Shortest Path First Algorithm
TCP	Transmission Control Protocol
TTL	Time To Live
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
VTP	Protocolo de entroncamento de VLAN
WAN	Wide Area Network

ÍNDICE

1 INTRODUÇÃO

Neste capítulo serão tratados os elementos introdutórios relacionados ao estudo e implementação de uma rede de computadores utilizando o modelo hierárquico.

1.1 TEMA

Atualmente, com a popularização da internet, o acesso fácil a novas tecnologias, computadores, smartphones e outros equipamentos que facilitam a comunicação de dados, podemos encontrar redes computacionais nos ambientes mais inusitados. Desde grandes corporações e empresas, até aquela residência com um único morador, é possível achar ao menos um equipamento, e este provavelmente estará ligado ao ambiente da internet.

Mais do que isso, torna-se cada vez mais comum haver diversos dispositivos interconectados em residências e pequenas empresas, compartilhando impressoras, pontos de acesso, banco de dados, entre outros.

Devido a este aumento da demanda de infraestrutura, estas redes são implementadas, na maioria das vezes, de forma inadequada e por profissionais sem o conhecimento necessário para um ótimo aproveitamento dos recursos disponíveis.

O objetivo com este estudo é auxiliar a população e operadores de redes na implementação de redes hierárquicas, que são de fácil gerenciamento e expansão, além de ser possível resolver problemas mais rapidamente.

1.2 OBJETIVOS

Nesta sessão serão trabalhados objetivo geral e objetivos específicos.

1.2.1 Objetivo Geral

O principal objetivo deste projeto é implementar uma estrutura de rede hierárquica levando em consideração a segurança, disponibilidade e integridade dos dados.

1.2.2 Objetivos Específicos

- Identificar os equipamentos que serão utilizados na implementação;
- Identificar os protocolos que serão utilizados;
- Implementar políticas de segurança;
- Implementar QoS nos equipamentos;
- Mapeamento da rede implementada;
- Agrupar setores em domínios de colisão separados.

1.3 JUSTIFICATIVA

Operadores e administradores de redes ainda tem alguma dificuldade em montar, configurar e gerenciar uma arquitetura de redes. Mesmo os tutorias disponíveis fartamente na internet possuem falhas ou não abrangem todos os tipos de equipamentos, o que acaba por causar a subutilização dos recursos existentes ou, ainda, erros de configuração, que causam paradas inesperadas.

Este estudo apresentará os recursos necessários para que sejam evitados os problemas citados, procurando priorizar a segurança, integridade e disponibilidade dos dados.

1.4 PROCEDIMENTOS METODOLÓGICOS

Este estudo será implementado com base na literatura atual sobre o assunto, conteúdos do curso CCNA Cisco e materiais didáticos obtidos na internet.

Utilizaremos também os recursos do Cisco Packet Tracer e equipamentos do Laboratório de Redes da UTFPR, a fim de testar a configuração proposta.

2. TEORIA

2.1 O Uso de Computadores em Redes

Já tem algum tempo que ouvimos falar em redes de computadores. Equipamentos que se interconectam entre si e com outros dispositivos, hoje muito comuns. Mas de onde vem essa necessidade? Como surgiu o interesse em Redes de Computadores?

Segundo (Tanenbaum, 2011), a questão aqui é o compartilhamento de recursos, deixando programas, equipamentos e, principalmente, dados ao alcance de todas as pessoas na rede, independentemente da localização física do recurso ou do usuário.

Essa necessidade de acesso a informações de maneira quase instantânea é cada vez mais necessária, tanto em ambientes de grandes corporações, quanto em pequenas empresas e escritórios.

No princípio, quando as primeiras redes de computadores surgiram, somente nos era possível conectar equipamentos de um mesmo fabricante. Isso ocorria por que não havia padronização na fabricação do hardware e no desenvolvimento de softwares e, portanto, cada fabricante utilizava seu próprio padrão.

Para facilitar a interconexão de sistemas de computadores, a ISO (*International Organization for Standardization*) desenvolveu um modelo de referência chamado OSI (*Open Systems Interconnection*), para que os fabricantes pudessem criar protocolos a partir desse modelo (Torres, 2010).

2.2 O Modelo OSI

O modelo de protocolos OSI é um modelo de sete camadas onde, em teoria, cada camada seria de responsabilidade de um protocolo específico. Na prática o que ocorre é que os protocolos existentes não seguem esse modelo de referencia ao pé da letra, usando protocolos que correspondem a mais de uma camada do modelo OSI.

Na transmissão de um dado cada camada pega as informações passadas pela camada superior, acrescenta informações pelas quais ela seja responsável e passa os dados para a camada imediatamente inferior, como mostra a figura 01. Esse processo é conhecido como encapsulamento.

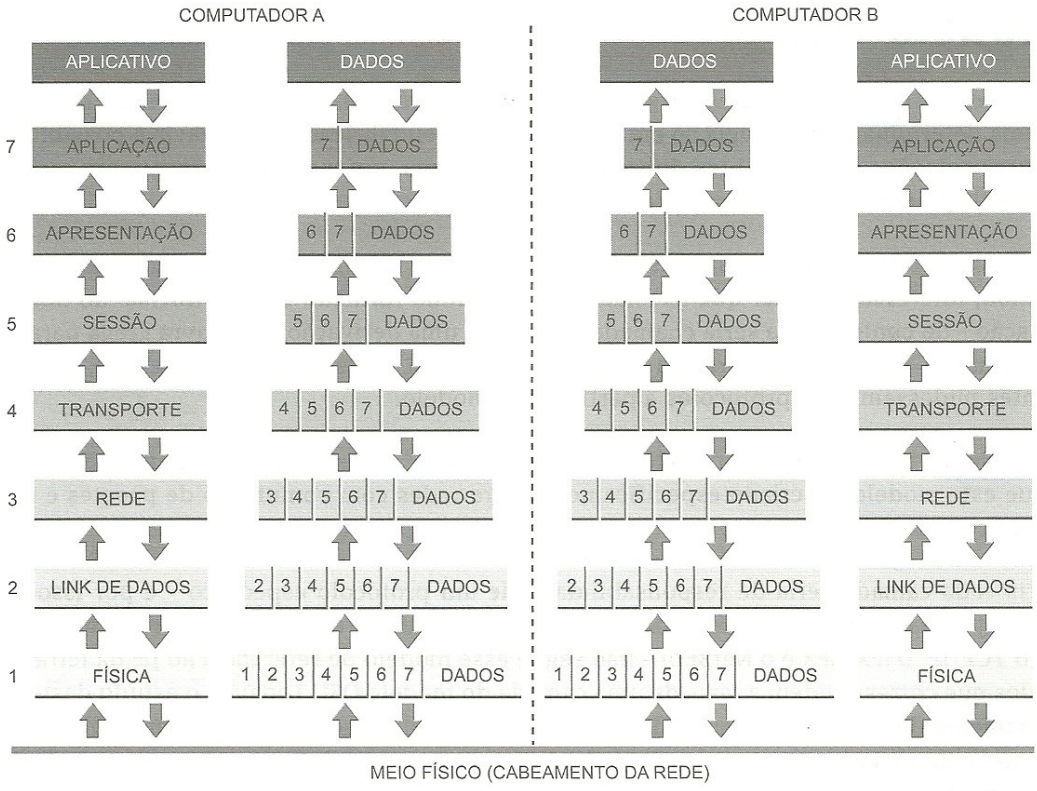

Fig. 01: Como funciona a Comunicação entre camadas no modelo OSI

Fonte: Torres (2010)

A comunicação mostrada na figura 01 é a comunicação real, ou seja, como funciona a transmissão de um dado através da rede. Na prática podemos dizer que uma determinada camada em um computador comunica-se diretamente com a camada correspondente no outro computador, ignorando o que ocorre abaixo delas.

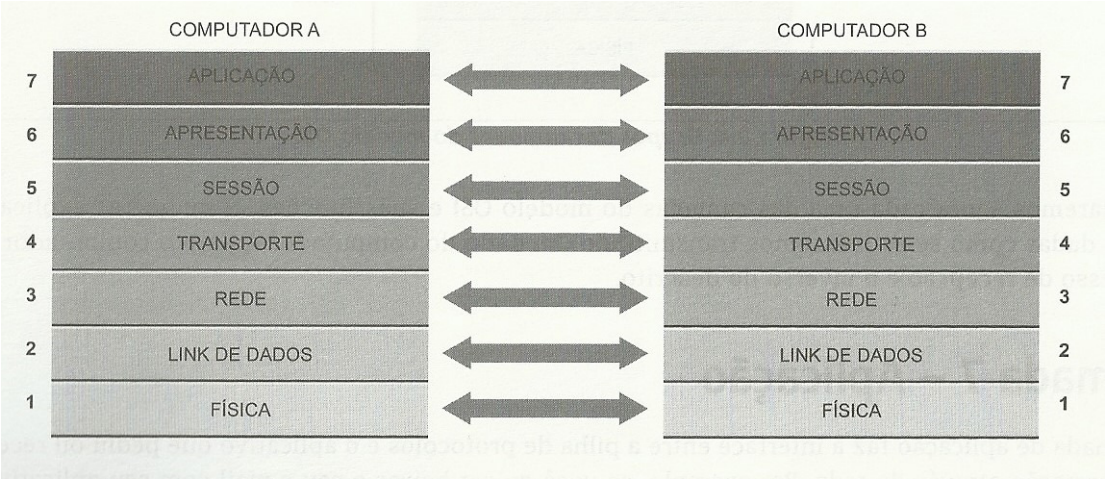

Fig. 02: Comunicação virtual no modelo OSI

Fonte: Torres (2010)

2.3 TCP/IP

Deixando de lado o modelo de referencia OSI, vamos passar ao modelo de referencia utilizado desde o princípio das redes de computadores, quando ainda era conhecida como ARPANET, a antecessora da internet mundial.

A ARPANET era uma rede de pesquisas patrocinada pelo Departamento de Defesa dos Estados Unidos, onde centenas de universidades e repartições públicas foram conectadas usando linhas telefônicas dedicadas. Quando foram criadas redes de rádios e satélite, os protocolos existentes começaram a ter problemas de interligação, o que forçou a criação de uma nova arquitetura de referencia. Assim, desde o início, a capacidade para conectar várias redes de maneira uniforme foi um dos principais objetivos do projeto. Essa arquitetura ficou conhecida com **modelo de referência TCP/IP**.

A arquitetura do TCP/IP é mostrada na figura 03. Podemos observar que é um protocolo de quatro camadas. Nessa mesma figura observamos a correlação das camadas do TCP/IP com as camadas do modelo OSI.

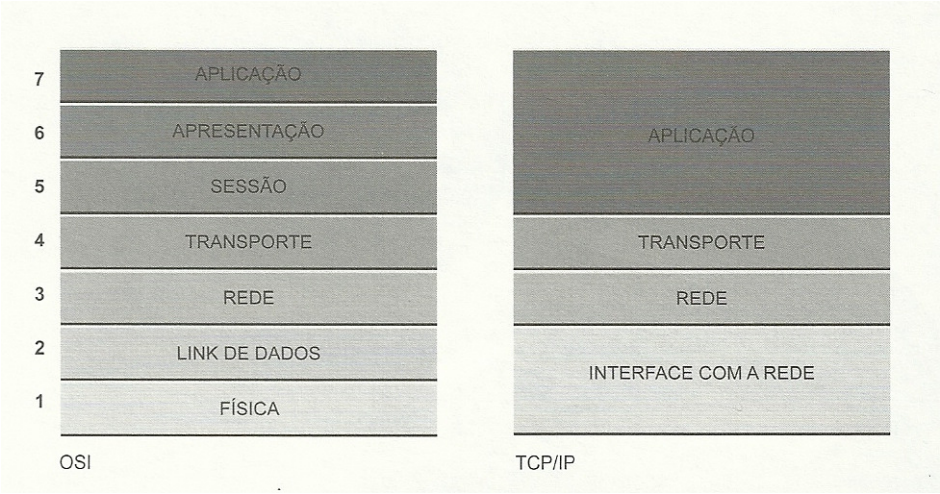

Fig. 03: Arquitetura do TCP/IP

Fonte: Torres (2010)

2.3.1 A Camada de Aplicação

Esta camada equivale às camadas 5, 6 e 7 do modelo OSI. É esta camada que "conversa" com os programas instalados em seu computador. Por exemplo, quando você clica em seu programa de e-mail para baixar e-mails, o programa faz um pedido a esta camada da pilha TCP/IP. Esta camada então prepara o pedido e/ou dados e os envia para a camada inferior, a camada de Transporte.

A camada de Aplicação contém todos os protocolos de nível mais alto, dentre eles, o protocolo de terminal virtual (TELNET), o protocolo de transferência de arquivos (FTP) e o protocolo de correio eletrônico (SMTP).

A camada de Aplicação comunica-se com a camada de transporte através de uma porta, que é um sistema de endereçamento para saber qual protocolo está transferindo os dados e, com isso, saber a que protocolo de aplicação na máquina destino os dados devem ser entregues.

Estas portas são numeradas de zero a 65.535 e no lado do servidor as aplicações padrão usam sempre a mesma porta. Por exemplo, nos servidores HTTP utiliza-se sempre a porta 80, o protocolo SMTP a porta 25 e o FTP as portas 20, para transmissão de dados, e 21, para transmissão de informações de controle. No lado do cliente, o número da porta é dinâmico e vai variar,

conforme as aplicações (programas) que estão rodando no computador do cliente.

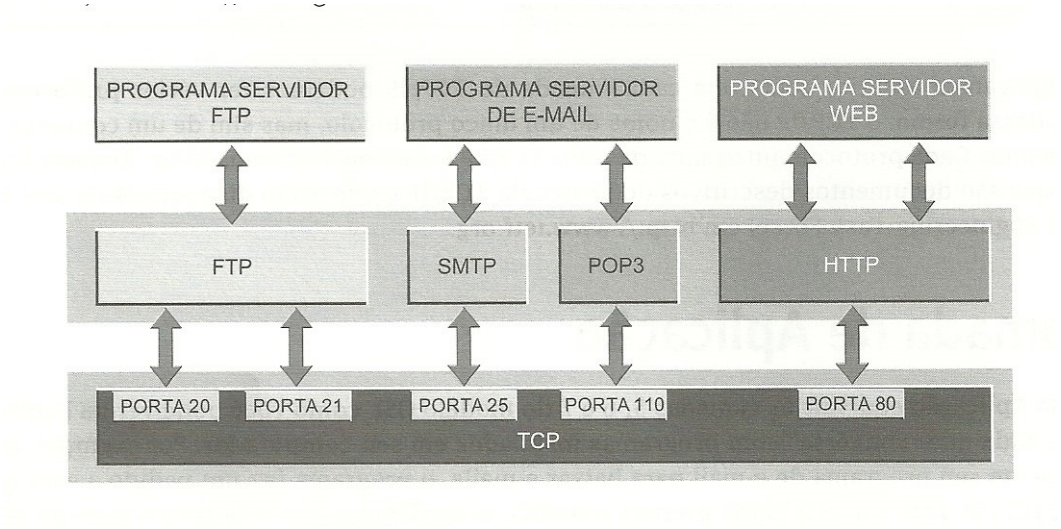

Fig. 04: Funcionamento da Camada de Aplicação em um servidor

Fonte: Torres (2010)

2.3.2 A Camada de Transporte

No modelo TCP/IP, a camada localizada abaixo da camada de aplicação é a camada de transporte. A finalidade da mesma é permitir que as entidades pares dos hosts de origem e de destino mantenham uma conversação, exatamente como acontece na camada de transporte OSI. É nessa camada que atua o protocolo que faz parte do nome do modelo: o TCP (*Transmission Control Protocol*), que é um protocolo orientado a conexões confiável que permite a entrega sem erros de um fluxo de bytes originário de uma determinada máquina em qualquer computador da internet. Ele divide o fluxo de bytes em pequenas mensagens, chamadas pacotes, e passa cada uma delas para camada seguinte, a camada de rede.

Um segundo protocolo, bastante importante, atua nessa camada. É o UDP (*User Datagram Protocol*), que é um protocolo sem conexões, não confiável, usado para aplicações que não desejam a sequencia ou o controle de fluxo do TCP. Ele é muito usado para consultas isoladas, com solicitação e resposta, tipo cliente-servidor, e aplicações em que a entrega imediata é mais

importante do que a entrega precisa, como na transmissão de voz ou vídeo. A relação entre IP, TCP e UDP é ilustrada na figura 05 (Tanenbaum, 2011).

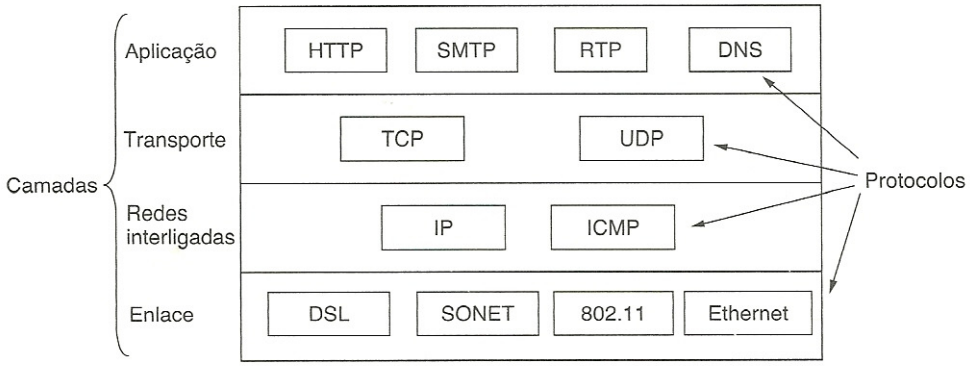

Fig. 05: Relação entre IP, TCP e UDP

Fonte: Tanenbaum (2011)

2.3.3 A Camada de Rede

A Camada de Rede do TCP/IP é equivalente à camada 3 (Rede) do modelo OSI, sendo responsável por receber os pacotes de dados provenientes da camada de transporte e dividi-los em datagramas, adicionando a informação do endereço lógico de origem e o endereço lógico de destino (endereços IP). Em seguida o datagrama é enviado à camada que estiver operando abaixo da camada de rede (camada de interface com a rede), responsável por colocar os datagramas dentro de quadros transferidos pela rede (Torres, 2010).

Segundo Tanenbaum (2011), a camada de rede integra toda a arquitetura, mantendo-a unida. Sua tarefa é permitir que os hosts injetem pacotes em qualquer rede e garantir que eles trafegarão independentemente até o destino (talvez em uma rede diferente). Eles podem chegar até mesmo em uma ordem diferente daquela em que foram enviados, obrigando as camadas superiores a reorganizá-los, caso a entrega em ordem seja desejável.

Vários protocolos operam nessa camada, como o IP (*Internet Protocol*), ICMP (*Internet Control Message Protocol*), IGMP (*internet Group Management Protocol*), ARP (*Address Resolution Protocol*), RARP (*Reverse Address Resolution Protocol*) e NDP (*Neighbor Discovery Protocol*). Os mais conhecidos são o IP, utilizado nas conexões com a internet, e o ICMP, que funciona como

um mecanismo que emite mensagens quando ocorre um erro com o datagrama enviado.

2.3.4 A Camada de Enlace

A Camada de Enlace, também conhecida como acesso à rede ou interface com a rede, é a mais baixa do modelo e descreve o que os enlaces como linhas seriais e a Ethernet clássica precisam fazer para cumprir os requisitos dessa camada de interconexão com serviço não orientado a conexões. Ela não é uma camada propriamente dita, no sentido normal do termo, mas uma interface entre os hosts e os enlaces de transmissão. O material inicial sobre o modelo TCP/IP tem pouco a dizer sobre ela (Tanenbaum, 2011).

2.4 EQUIPAMENTOS DE REDES

Existem diversos equipamentos que são responsáveis por controlar o tráfego da rede. Vamos abordar os dois mais utilizados e importantes nessa função.

2.4.1 Switches

Os switches são a evolução das pontes, que eram repetidores inteligentes de sinal. As pontes operam na camada de Link de Dados (camada 2) do modelo OSI. Isso quer dizer que elas têm a capacidade de ler e analisar os quadros de dados que estão circulando na rede.

Os switches são pontes contendo várias portas. Eles enviam os quadros de dados somente para a porta de destino do quadro, ao contrário do hub, onde os quadros são transmitidos simultaneamente para todas as portas.

Outra diferença entre hubs e switches é que hubs só operam no modo Half-duplex, enquanto que switches permitem a operação da rede no modo full-duplex, o que, em teoria, dobra a largura de banda disponível.

Os switches conseguem enviar quadros diretamente para as portas de destino porque eles são dispositivos que aprendem. Quando uma máquina

envia um quadro para a rede através do switch, este lê o campo de endereço MAC de origem do quadro e anota em uma tabela interna o endereço MAC da placa de rede do micro que está conectado àquela porta. Assim, Quando o switch recebe um quadro para ser transmitido, ele consulta sua tabela interna. Se o endereço MAC de destino constar nessa tabela, ele sabe para qual porta deve enviar o quadro (Torres, 2010).

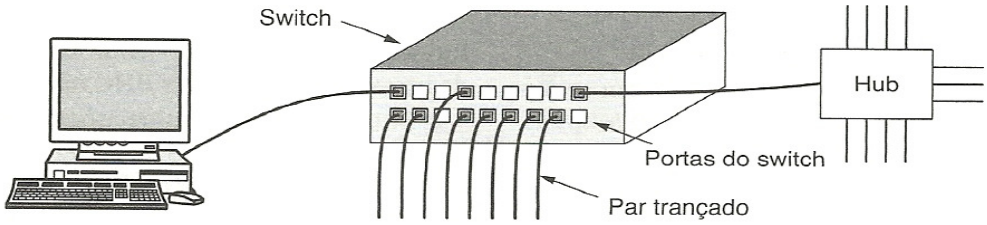

Fig. 06: Cada cabo conecta o switch a um único computador

Fonte: Tanenbaum (2011)

Atualmente os switches são divididos em duas categorias, os switches de camada 2, que acabamos de descrever, e os switches de camada 3, que tem suas características idênticas ao roteador, que será tratado no próximo item. Segundo Torres (2010), a diferença entre switches camada 3 e roteadores é a presença de uma porta chamada WAN nos roteadores, porta que não está presente nos switches camada três.

2.4.2 Roteadores

Roteadores são pontes que operam na camada de Rede do modelo OSI (camada três). Isso significa que os roteadores conseguem ler o datagrama IP, tendo acesso a todas as informações ali presentes, em especial os endereços IP de origem e destino. Além de poderem receber, enviar e analisar mensagens de controle.

Os roteadores possuem duas funções básicas: permitir a conexão de duas redes diferentes e escolher um caminho a ser usado para o datagrama chegar até o seu destino.

A conexão entre duas redes diferentes é possível porque o roteador “isola” cada rede. Enquanto que um switch faz com que todas as máquinas conectadas a ele pertençam a uma mesma rede (isto é, um único domínio de broadcast), roteadores mantêm domínios de broadcast separados para cada rede, fazendo com que dados que tenham como destino a rede local nunca saiam da rede local.

Na figura 07 comparamos o funcionamento de um switch camada dois e de um roteador (ou um switch camada três).

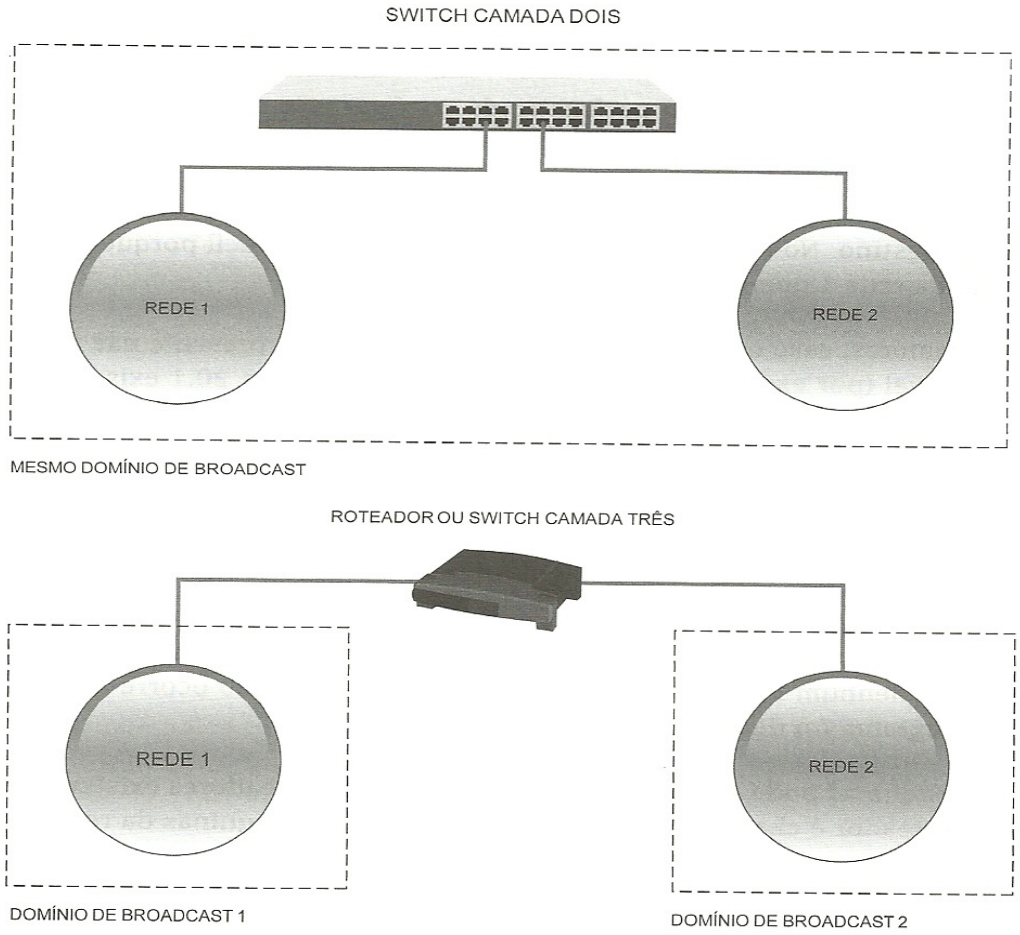

Fig. 07: Diferença entre switch e roteador

Fonte: Torres (2010)

2.4.2.1 Funcionamento básico

Os computadores da rede possuem um parâmetro de configuração, chamado default gateway (saída padrão), que indica qual é o endereço IP de saída da rede, ou seja, qual é o endereço IP do roteador da rede. Quando a máquina não sabe onde está a máquina de destino, ela envia o datagrama para o default gateway, isto é, para o roteador da rede. O roteador da rede encaminha então o datagrama para a máquina de destino.

No caso de redes de grande abrangência, caso o endereço IP de destino não esteja presente nas redes pelas quais o roteador é responsável, ele encaminhará o datagrama para o seu próprio default gateway, que é outro roteador. O outro roteador recebe o datagrama e, caso o endereço IP de destino esteja em uma rede conectada a ele, ele entregará o datagrama à máquina de destino. Caso contrário, encaminhará o datagrama para outro roteador, que é o roteador cujo endereço IP está configurado em seu parâmetro default gateway.

Este processo continua até que o datagrama chegue à máquina de destino ou então o campo Tempo de Vida (TTL) do datagrama IP chegue à zero, quando então o datagrama será descartado.

2.4.2.2 Características dos roteadores

Roteadores possuem dois tipos de portas: LAN e WAN. As portas LAN são usadas para conectar o roteador a diferentes redes locais. Já a porta WAN conecta o roteador a uma rede pública de longa distância: Internet (PPP, PPPoE), PDH, SDH, X.25, Frame Relay, ATM etc.

Como vimos, os switches camada três são roteadores sem a porta WAN. Portanto se você precisa de roteadores para conectar diferentes redes locais, mas não precisa que este roteador tenha uma conexão com uma rede pública externa, então um switch camada três é a sua melhor opção.

Os roteadores podem ter diversas características diferentes, o que influencia diretamente no preço do equipamento. As principais características são:

- Uso
- Aspecto físico (mesa ou rack/armário)
- Número de portas WAN
- Número de portas LAN
- Velocidade das portas WAN
- Velocidade das portas LAN
- Protocolos suportados
- Redundância
- Tolerância a falhas
- Balanceamento de carga
- Desempenho
- Serviços suportados (ex.: VoIP, VPN etc.)

2.5 ROTEAMENTO

2.5.1 Algoritmos de Roteamento

A principal função da camada de rede é rotear pacotes da máquina de origem para a máquina de destino. Na maioria das redes, os pacotes necessitarão de vários hops (saltos) para cumprir o trajeto. Os algoritmos que escolhem as rotas e as estruturas de dados que elas utilizam constituem um dos elementos mais importantes do projeto da camada de rede. O algoritmo de roteamento é a parte do software da camada de rede responsável pela decisão sobre a interface de saída a ser usada na transmissão do pacote de entrada.

Algumas vezes, é útil fazer distinção entre o roteamento, que é a tomada de decisão sobre quais rotas utilizar, e o encaminhamento, que acontece quando um pacote chega. Podemos imaginar que um roteador tem dois processos internamente. Um deles trata cada pacote que chega, procurando a interface de saída que será usada em sua tabela de roteamento. Esse processo é o **encaminhamento**. O outro processo é responsável pelo preenchimento e pela atualização das tabelas de roteamento. É nesse processo que o algoritmo de roteamento entra em cena.

Os algoritmos de roteamento podem ser agrupados em duas classes principais: não adaptativos e adaptativos. Os algoritmos não adaptativos não baseiam suas decisões de roteamento em medidas ou estimativas do tráfego e da topologia atuais. Em vez disso, a escolha da rota a ser utilizada para ir de uma origem até um destino (para qualquer origem e qualquer destino) é previamente calculada off-line, sendo transferida para os roteadores quando a rede é iniciada. Esse procedimento é comumente chamado de **roteamento estático**. É útil quando a escolha da rota é óbvia.

Os algoritmos adaptativos alteram as decisões de roteamento para refletir mudanças na topologia e, normalmente, também no tráfego. Esses algoritmos de **roteamento dinâmico** diferem em termos de lugar em que obtêm suas informações, do momento em que alteram as rotas e da métrica utilizada na otimização (Tanenbaum, 2011).

2.5.2 OSPF

A Internet é composta de um grande número de redes independentes, ou sistemas autônomos (*Autonomous Systems – AS*), que são operados por diferentes organizações, normalmente uma empresa, universidade ou ISP (*Internet Solution Provider* – Provedora de soluções de internet). Dentro de sua própria rede, uma organização pode usar seu próprio algoritmo para roteamento interno, ou roteamento intradomínio, como normalmente é mais conhecido.

Um protocolo de roteamento intradomínio, também chamado de protocolo gateway interior, bastante utilizado na prática é o OSPF, sobre o qual falaremos agora (Cisco 2007-2009).

2.5.2.1 Histórico

O protocolo OSPF é um protocolo de roteamento link-state que foi desenvolvido como uma substituição para o protocolo de roteamento do vetor de distância RIP. O RIP foi um protocolo de roteamento aceitável no início da Internet, mas sua confiabilidade em contagem de saltos como a única medida para escolher a melhor rota rapidamente tornou-se inaceitável em redes maiores que necessitavam de uma solução de roteamento mais robusta. O OSPF é um protocolo de roteamento classless que usa o conceito de áreas para escalabilidade. O RFC 2328 define a métrica de OSPF como um valor arbitrário chamado custo. O IOS Cisco utiliza a largura de banda como métrica de custo do OSPF. As principais vantagens do OSPF sobre o RIP são sua rápida convergência e escalabilidade para implementações de rede muito maiores.

O desenvolvimento inicial do OSPF começou em 1987 pelo Grupo de Trabalho do OSPF da Internet Engineering Task Force (IETF). Naquele tempo, a Internet era predominantemente uma rede acadêmica e de pesquisa fundada pelo governo norte-americano.

Em 1989, a especificação para o OSPFv1 foi publicada na RFC 1131. Havia duas implementações escritas: uma para executar em roteadores e outra para executar em estações de trabalho UNIX. A última implementação tornou-se mais tarde um processo UNIX difundido conhecido como GATED. O OSPFv1 foi um protocolo de roteamento experimental e nunca foi implantado.

Em 1991, o OSPFv2 foi introduzido na RFC 1247 por John Moy. O OSPFv2 ofereceu melhorias técnicas significativas sobre o OSPFv1. Ao mesmo tempo, a ISO trabalhava em um protocolo de roteamento link-state próprio chamado Intermediate System-to-Intermediate System (IS-IS). Conforme o esperado, a IETF escolheu o OSPF como seu IGP recomendado (Protocolo IGP).

Em 1998, a especificação de OSPFv2 foi atualizada na RFC 2328 e é a RFC atual para OSPF (Cisco 2007-2009).

2.5.2.2 Encapsulamento e Tipos de Pacote OSPF

Os dados de uma mensagem OSPF são encapsulados em um pacote. Este campo de dados pode incluir um dos cinco tipos de pacote OSPF. O cabeçalho do pacote OSPF é incluído em todos os pacotes OSPF, independentemente de seu tipo. Os dados específicos do cabeçalho e do tipo do pacote OSPF são então encapsulados em um pacote IP. No cabeçalho de pacote IP, o campo de protocolo é definido como 89 para indicar OSPF e o endereço de destino é definido como um dos dois endereços multicast: 224.0.0.5 ou 224.0.0.6. Se o pacote OSPF for encapsulado em um quadro ethernet, o endereço MAC de destino também será um endereço multicast: 01-00-5E-00-00-05 ou 01-00-5E-00-00-06.

A figura 08 mostra os cinco diferentes tipos de pacotes link-state OSPF. Cada pacote serve a um propósito específico no processo de roteamento OSPF:

1. Hello - Os pacotes Hello são utilizados para estabelecer e manter a adjacência com outros roteadores OSPF. O protocolo hello é discutido detalhadamente no próximo tópico.

2. DBD - O pacote de Descrição de Bancos de Dados (DBD) contém uma lista abreviada do banco de dados link-state do roteador que o está enviando, os roteadores que o recebem comparam com o banco de dados link-state local.

3. LSR - Os roteadores que recebem podem solicitar mais informações sobre qualquer entrada no DBD enviando uma Requisição Link-State (LSR).

4. LSU - Os pacotes de Atualização Link-State (LSU) são utilizados para responder às LSRs, bem como anunciar novas informações. Os LSUs contêm sete tipos diferentes de Anúncios Link-State (LSAs).

5. LSAck - Quando um LSU é recebido, o roteador envia um Link-State Acknowledgement (LSAck) para confirmar o recebimento do LSU.

Tipo	Nome do pacote	Descrição
1	Hello	Detecta vizinhos e cria adjacências entre eles
2	Descrição de banco de dados (DBD)	Verifica se há sincronização de banco de dados entre roteadores
3	Requisição Link-State (LSR)	Solicita registros de link-state específicos de roteador para roteador
4	Atualização Link-State (LSU)	Envia registros de link-state especificamente solicitados
5	Link-State Acknowledgement (LSAck)	Reconhece os outros tipos de pacote

Fig. 08: Tipos de pacotes OSPF

Fonte: CCNA Cisco (2007-2009)

2.5.2.3 Funcionamento

Antes de um roteador OSPF poder enviar seus link-states a outros roteadores, ele deverá determinar se existem outros vizinhos OSPF em algum de seus links. Para tal, os roteadores utilizam o protocolo Hello. As informações no OSPF Hello incluem a ID do roteador OSPF que envia o pacote Hello. Receber um pacote Hello de OSPF em uma interface confirma para um roteador que há outro roteador OSPF neste link. O OSPF estabelece então uma adjacência com o vizinho.

Os pacotes Hello são utilizados para:

- Detectar os vizinhos de OSPF e estabelecer as adjacências do vizinho.
- Anunciar parâmetros nos quais dois roteadores devem concordar em se tornar vizinhos.
- Eleger o Roteador designado (DR) e o Roteador designado de backup (BDR) em redes multiacesso como a Ethernet e Frame Relay.

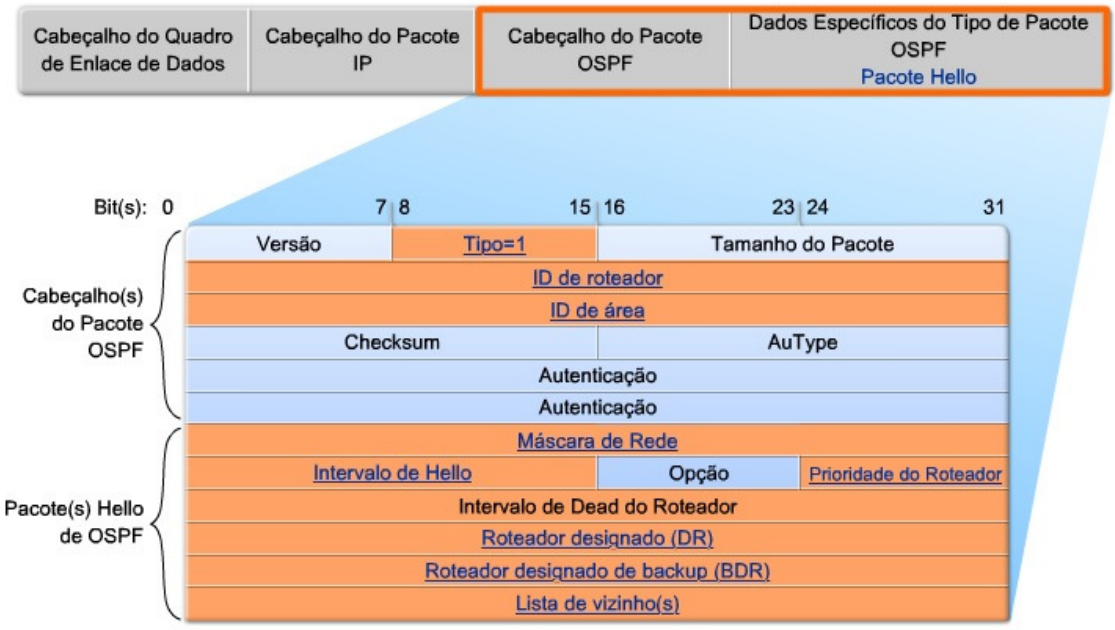

Fig. 09: Cabeçalho OSPF e Pacote Hello

Fonte: CCNA Cisco (2007-2009)

Na figura 09 podemos observar os campos importantes do cabeçalho OSPF e Pacote Hello, que incluem:

- **Tipo**: Tipo de pacote OSPF: Hello (1), DD (2), LS Request (3), LS Update (4), LS ACK (5)
- **ID do roteador**: ID do roteador de origem
- **ID da área**: área a partir da qual o pacote foi originado
- **Máscara de rede**: Máscara de sub-rede associada com a interface de envio
- **Intervalo de Hello**: número de segundos entre os hello's do roteador de envio
- **Prioridade do roteador**: Utilizado na eleição DR/BDR
- **Roteador Designado (DR)**: ID do roteador do DR se houver
- **Roteador designado de backup (BDR)** ID do roteador do BDR se houver
- **Lista de vizinhos**: lista o OSPF ID do(s) roteador (es) vizinho(s)

Antes de dois roteadores poderem formar uma adjacência de vizinho OSPF, eles deverão concordar em três valores: Intervalo de hello, intervalo de dead e tipo de rede. O intervalo de Hello de OSPF indica com que frequência o roteador OSPF transmite seus pacotes Hello. Por padrão, os pacotes Hello de OSPF são enviados a cada 10 segundos em segmentos multiacesso e ponto-a-ponto e a cada 30 segundos em segmentos de rede ponto-a-multiponto (NBMA) (Frame Relay, X.25, ATM) (NBMA).

Na maioria dos casos, os pacotes Hello de OSPF são enviados como multicast para um endereço reservado para ALLSPFRouters em 224.0.0.5. Utilizar um endereço multicast permite que um dispositivo ignore o pacote se sua interface não estiver habilitada para aceitar pacotes OSPF. Isto economiza o tempo de processamento da CPU em dispositivos não-OSPF.

O intervalo de dead é o período, expresso em segundos, que o roteador esperará para receber um pacote Hello antes de declarar o vizinho "inativo." A Cisco utiliza um padrão de quatro vezes o intervalo de Hello. Para segmentos multiacesso e ponto-a-ponto, este período é de 40 segundos. Para redes NBMA, o intervalo de Dead é de 120 segundos.

Se o intervalo de Dead expirar antes de os roteadores receberem um pacote Hello, o OSPF removerá aquele vizinho de seu banco de dados link-state. O roteador envia as informações link-state sobre o vizinho "inativo" para todas as interfaces OSPF habilitadas.

Para reduzir a quantidade de tráfego OSPF nas redes multiacesso, o OSPF elege um Roteador Designado (DR) e um Roteador Designado de Backup (BDR). O DR é responsável por atualizar todos os outros roteadores OSPF (chamados de DROthers) quando uma alteração ocorrer na rede multiacesso. O BDR monitora o DR e assume como DR se o DR atual falhar.

Cada roteador de OSPF mantém um banco de dados link-state contendo os LSAs recebidos de todos os outros roteadores. Quando um roteador recebe todos os LSAs e constrói seu banco de dados link-state local, o OSPF utiliza o algoritmo open shortest path first (SPF) de Dijkstra para criar uma árvore SPF. A árvore SPF é então utilizada para preencher a tabela de roteamento IP com os melhores caminhos para cada rede (Cisco, 2007-2009).

A distância administrativa (AD) é a confiança (ou preferência) da origem da rota. O OSPF tem uma distância administrativa padrão de 110 (Cisco, 2007-2009).

2.6 VLAN's

O desempenho da rede pode ser um fator na produtividade de uma organização e na sua reputação em cumprir o que promete. Uma das tecnologias que contribuem com a excelência do desempenho da rede é a separação dos grandes domínios de broadcast em domínios menores com VLANs. Domínios de broadcast menores limitam o número de dispositivos que participam de broadcasts e permitem separar dispositivos em agrupamentos funcionais, como serviços de banco de dados para um departamento de contabilidade e de transferência de dados em alta velocidade para um departamento de engenharia.

VLAN é uma sub-rede IP separada logicamente. As VLANs permitem a existência de várias redes IP e sub-redes na mesma rede comutada. Para que os computadores se comuniquem na mesma VLAN, cada um deve ter um endereço IP e uma máscara de sub-rede correspondentes a essa VLAN. O switch precisa ser configurado com a VLAN e cada porta correspondente deve ser atribuída a essa VLAN. Uma porta de switch com uma única VLAN configurada é chamada de porta de acesso. Dois computadores conectados fisicamente ao mesmo switch não significa que eles podem se comunicar. Os dispositivos separados por redes ou sub-redes devem se comunicar por meio de um roteador (Camada 3), independentemente das VLANs serem usadas ou não (Cisco, 2007-2009).

Os benefícios primários de usar VLANs são os seguintes:

- **Segurança** – Grupos que têm dados confidenciais são separados do restante da rede, o que diminui as chances de violações das informações confidenciais.

- **Redução de custo** – Economia de custos é resultante da menor necessidade das atualizações de rede caras e do uso mais eficiente da largura de banda e dos uplinks existentes.
- **Desempenho mais alto** – Dividir as redes da Camada 2 simplesmente em vários grupos de trabalho lógicos (domínios de broadcast) reduz um tráfego desnecessário na rede e aumenta o desempenho.
- **Atenuação da tempestade de broadcast** – Dividir uma rede em VLANs reduz o número de dispositivos que podem participar de uma situação de descontrole por excesso de broadcast. A segmentação de rede local impede uma situação de descontrole em uma rede devido a excesso de broadcast.
- **Maior eficiência do pessoal de TI** – VLANs simplificam o gerenciamento da rede porque os usuários com requisitos de rede semelhantes compartilham a mesma VLAN. Quando você provisiona um novo switch, todas as políticas e procedimentos já configurados para a VLAN específica são implementados quando as portas são atribuídas. Também é fácil para o pessoal de TI identificar a função de uma VLAN, dando a ela um nome apropriado.
- **Projeto mais simples ou gerenciamento de aplicativo** – VLANs agregam usuários e dispositivos de rede para suportar requisitos de negócios ou geográficos. Ter funções separadas simplifica o gerenciamento de um projeto ou o trabalho com um aplicativo especializado, por exemplo, uma plataforma de desenvolvimento de e-learning para os funcionários. Também é mais fácil determinar o escopo dos efeitos de atualizar os serviços de rede.

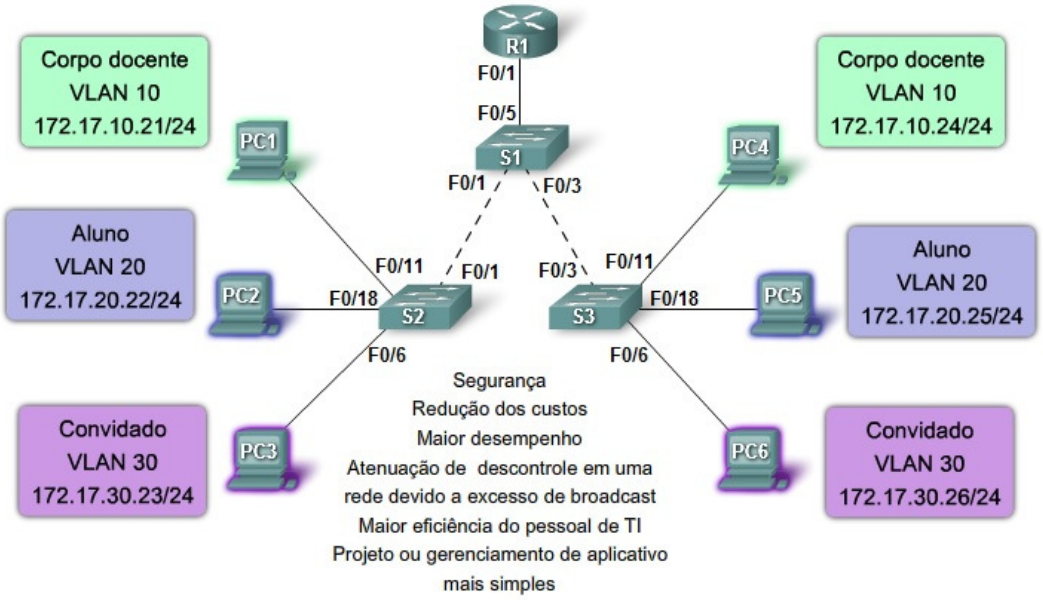

Fig. 10: Benefícios de usar VLAN

Fonte: CCNA Cisco (2007-2009)

As VLANs são identificadas pelos seus ID's, que são divididos em normal e estendido:

VLANs de intervalo normal

- Usadas em redes corporativas de pequeno e médio porte.
- Identificadas por uma ID VLAN entre 1 e 1005.
- As ID's 1002 até 1005 são reservadas para VLANs Token Ring e FDDI.
- As ID's 1 e 1002 a 1005 são criadas automaticamente, não podendo ser removidas.
- As configurações são armazenadas em um arquivo do banco de dados de VLAN, chamado vlan.dat. O arquivo vlan.dat é localizado na memória flash do switch.
- O protocolo de entroncamento VLAN (VTP), que ajuda a gerenciar configurações de VLAN entre switches, só pode aprender VLANs de

intervalo normal e as armazenar no arquivo de banco de dados da VLAN.

VLANs de intervalo estendido

- Permite a operadoras estender sua infraestrutura para um número maior de clientes. Algumas empresas globais podem ser grandes o bastante para precisar de ID's de VLAN de intervalo estendido.
- Elas são identificadas por uma ID VLAN entre 1006 e 4094.
- Elas suportam menos recursos VLAN que as VLANs de intervalo normal.
- Elas são salvas no arquivo de configuração de execução.
- VTP não aprende VLANs de intervalo estendido.

As VLANs podem identificadas com alguns termos comumente utilizados que indicam uma função específica executada por esta VLAN:

VLAN de dados

Uma VLAN de dados é uma VLAN configurada para transportar apenas o tráfego gerado pelo usuário. Uma VLAN pode transportar o tráfego baseado em voz ou o tráfego usado para gerenciar o switch, mas esse tráfego não faria parte de uma VLAN de dados. É uma prática comum separar o tráfego de voz e de gerenciamento do tráfego de dados. A importância de separar dados de usuário dos dados de controle de gerenciamento do switch e do tráfego de voz é realçada pelo uso de um termo especial para identificar VLANs que só transportam dados de usuário – uma "VLAN de dados". Às vezes, uma VLAN de dados é conhecida como VLAN de usuário.

VLAN padrão

Todas as portas de switch se tornam um membro da VLAN padrão após a inicialização do switch. Ter todas as portas de switch participando da VLAN

padrão torna essas portas parte do mesmo domínio de broadcast. Isso permite a qualquer dispositivo conectado a qualquer porta de switch se comunicar com outros dispositivos em outras portas. A VLAN padrão de switches Cisco é VLAN 1. A VLAN 1 tem todos os recursos de qualquer VLAN, exceto por não ser possível renomeá-la e excluí-la. Por padrão, o tráfego de controle da Camada 2, como CDP e o tráfego de protocolo spanning tree, é associado à VLAN 1.

Alguns administradores de rede usam o termo "VLAN padrão" para se referir a uma VLAN, diferente da VLAN 1, definida pelo administrador de rede como a VLAN a que todas as portas são atribuídas quando não estão em uso. Nesse caso, a única função que a VLAN 1 desempenha é a de tratar o tráfego de controle da Camada 2 da rede.

VLAN nativa

Uma VLAN nativa é atribuída a uma porta de tronco 802.1Q. Uma porta de tronco 802.1Q oferece suporte ao tráfego de muitas VLANs (tráfego marcado), bem como também ao tráfego que não vem de uma VLAN (tráfego sem marcação). A porta de tronco 802.1Q posiciona o tráfego sem marcação na VLAN nativa. O tráfego sem marcação é gerado por um computador conectado a uma porta de switch configurada com a VLAN nativa. As VLANs nativas são definidas na especificação IEEE 802.1Q para manter a compatibilidade com versões anteriores com tráfego sem marcação comum em cenários de rede local antigos. Uma VLAN nativa serve como um identificador comum em extremidades opostas de um link de tronco. É uma prática recomendada usar uma VLAN diferente da VLAN 1 como a VLAN nativa.

VLAN de gerenciamento

VLAN de gerenciamento é uma VLAN configurada para acessar os recursos de gerenciamento de um switch. A VLAN 1 serviria como a VLAN de gerenciamento se você não tivesse definido alguma outra para este propósito. Você atribui à VLAN de gerenciamento um endereço IP e uma máscara de sub-rede. Um switch pode ser gerenciado por HTTP, Telnet, SSH ou SNMP. Pelo

fato de a VLAN 1 ser a padrão para gerenciamento do switch, ela não é a melhor opção em função de possibilitar a um usuário arbitrário se conectar ao switch para usar o gerenciamento.

VLAN de voz

O trafego de voz exige algumas características específicas e por isso a VLAN de voz deve ser implementada separadamente de qualquer outra VLAN:

- Largura de banda assegurada para garantir qualidade de voz
- Prioridade de transmissão sobre outros tipos de tráfego da rede
- Capacidade de roteamento em áreas congestionadas na rede
- Atraso inferior a 150 milissegundos (ms) através da rede

Para atender a esses requisitos, toda a rede precisa ser projetada para suportar VoIP. Os detalhes de como configurar uma rede para suportar VoIP estão além do escopo deste estudo.

Mas, e se quiséssemos conectar mais de uma VLAN pelo mesmo caminho físico? Nós teríamos que utilizar o que se chama de **Tronco de VLAN**. Tronco é um link ponto-a-ponto entre dois dispositivos de rede que transporta mais de uma VLAN. Um tronco de VLAN permite estender as VLANs através de uma rede inteira. A Cisco suporta IEEE 802.1Q para coordenar troncos em interfaces Fast Ethernet e Gigabit Ethernet. Um tronco de VLAN não pertence a uma VLAN específica, sendo mais um canal para VLANs entre switches e roteadores (Cisco, 2007-2009).

2.7 NAT

Os endereçamentos IP utilizados em redes são divididos em Endereços Públicos e Endereços Privados. Todos os endereços de Internet públicos devem ser registrados com um Registro de internet regional (RIR, Regional Internet Registry). As organizações podem emprestar os endereços públicos de um ISP. Somente o proprietário registrado de um endereço público de internet pode atribuir esse endereço a um dispositivo de rede.

Diferentemente dos endereços IP públicos, os endereços IP privados são um bloco reservado de números que podem ser usados por qualquer um. Isso significa que duas redes ou dois milhões de redes podem usar os mesmos endereços privados. Para proteger a estrutura de endereços da Internet pública, os ISPs geralmente configuram os roteadores de borda para impedir que o tráfego endereçado exclusivamente a eles seja encaminhado pela Internet.

Ao fornecer um maior espaço de endereços do que a maioria das organizações pode obter através de um RIR, o endereçamento privado confere às empresas uma flexibilidade considerável no design da rede. Isso permite a obtenção de esquemas de endereçamento operacional e administrativamente convenientes, além de um crescimento mais fácil.

Entretanto, como não é possível rotear endereços privados pela Internet e como não existem endereços públicos suficientes para permitir que as organizações forneçam um para todos os hosts, as redes precisam que um mecanismo traduza os endereços privados para endereços públicos na extremidade de sua rede que funcionar em ambas as direções. Na ausência de um sistema de tradução, os hosts privados de um roteador na rede de uma organização não podem conectar-se a hosts privados de um roteador em outras organizações pela Internet.

A Tradução de endereços de rede (NAT, *Network Address Translation*) fornece esse mecanismo. Antes da NAT, um host com um endereço privado não podia acessar a Internet. Usando a NAT, as empresas individuais podem designar a alguns ou todos os seus hosts com endereços privados e usar a NAT para fornecer acesso à Internet.

Assim, enquanto o servidor DHCP designa os endereços IP dinâmicos para os dispositivos dentro da rede, os roteadores habilitados pela NAT retêm um ou muitos endereços IP de Internet válidos fora da rede. Quando o cliente enviar pacotes pela rede, a NAT traduzirá o endereço IP interno do cliente para um endereço externo. Para usuários externos, todo o tráfego destinado para a rede e proveniente dela possui o mesmo endereço IP ou vem do mesmo conjunto de endereços.

A NAT tem muitos usos, mas o principal é salvar os endereços IP, permitindo que as redes usem os endereços IP privados. A NAT traduz endereços privados, não roteáveis e internos em endereços públicos e

externos. A NAT tem um benefício adicional de proporcionar um nível maior de privacidade e segurança para uma rede porque ela oculta endereços IP internos de redes externas. Um dispositivo habilitado para NAT funciona normalmente na borda de uma rede. Quando um host dentro da rede deseja transmitir um pacote para um host externo, esse pacote é encaminhado para o roteador de borda, que executa o processo de NAT, traduzindo o endereço privado interno do host para um endereço público, roteável e externo.

Na terminologia de NAT, a rede interna é o conjunto de redes que estão sujeitas à tradução. A rede externa se refere a todos os outros endereços. Os endereços IP possuem designações diferentes dependendo de estarem na rede privada ou na rede pública (Internet) e de o tráfego estar chegando ou saindo (Cisco, 2007-2009).

A NAT oferece muitos benefícios e vantagens. Porém, existem algumas desvantagens de usá-la, inclusive a falta de suporte para alguns tipos de tráfego:

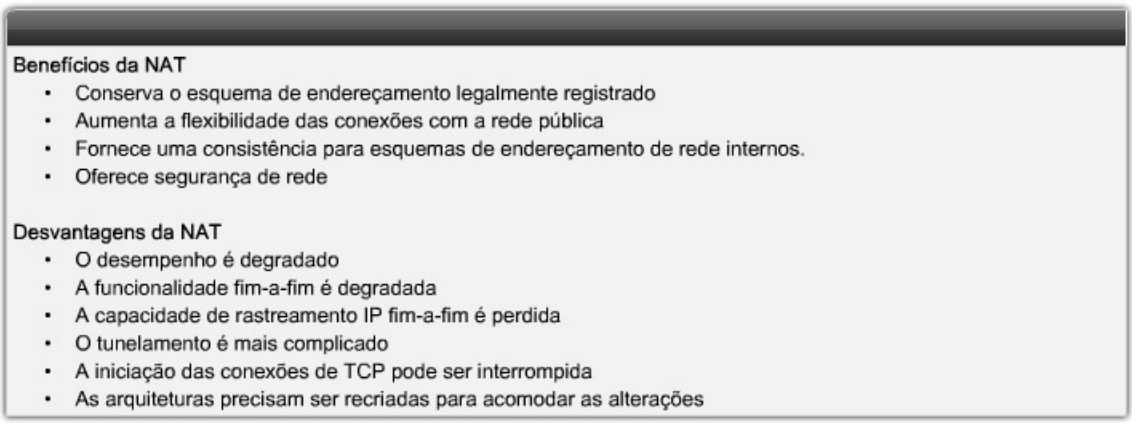

Fig. 11: Vantagens e desvantagens da NAT

Fonte: CCNA Cisco (2007-2009)

2.8 PPP

Um dos tipos mais comuns de conexão WAN é a ponto-a-ponto. As conexões ponto-a-ponto são utilizadas em redes locais com WANs de operadora e na conexão de segmentos de rede local dentro de uma rede empresarial. Uma conexão ponto-a-ponto entre rede local e WAN também é conhecida como uma conexão serial ou conexão de linha alugada, porque as

linhas são alugadas de uma operadora (normalmente uma companhia telefônica) e de uso dedicado ao uso pela empresa locadora das linhas.

O Protocolo ponto a ponto (PPP, *Point-to-Point Protocol*) fornece conexões de rede local para WAN com vários protocolos que lidam com TCP/IP, Intercâmbio de pacotes de redes interconectadas (IPX, *Internetwork Packet Exchange*) e Appletalk simultaneamente. Ele pode ser usado em linhas de par trançado, de fibra óptica e na transmissão via satélite. O PPP fornece transporte em links ATM, Frame Relay, ISDN e ópticos. Em redes modernas, a segurança é uma grande preocupação. O PPP permite autenticar conexões usando o Protocolo de autenticação de senha (PAP, *Password Authentication Protocol*) ou o mais eficiente Protocolo avançado de autenticação de reconhecimento (CHAP, *Challenge Handshake Authentication Protocol*).

O encapsulamento PPP foi projetado cuidadosamente para manter a compatibilidade com o hardware de suporte mais utilizado. O PPP encapsula quadros de dados para transmissão em links físicos da Camada 2. O PPP estabelece uma conexão direta utilizando cabos seriais, linhas telefônicas, linhas de tronco, telefones celulares, links de rádio especiais ou links de fibra óptica. Há muitas vantagens em utilizar PPP, inclusive o fato de não ser propriedade de ninguém. Além disso, ele inclui muitos recursos não disponíveis em outros protocolos:

- O recurso de gerenciamento de qualidade do link monitora a qualidade do link. Se forem detectados muitos erros, o PPP desativará o link.
- O PPP suporta a autenticação PAP e CHAP.

PPP contém três componentes principais:

- O protocolo HDLC para encapsulamento de datagramas em links ponto-a-ponto.
- Protocolo de controle do link extensível (LCP, *Link Control Protocol*) para estabelecer, configurar e testar a conexão do link de dados.

- Família de Protocolos de controle de rede (NCP, *Network Control Protocol*) para estabelecer e configurar protocolos da camada de rede diferentes. O PPP permite a utilização simultânea de vários protocolos da camada de rede. Alguns dos NCPs mais comuns são os Protocolos de controle de protocolo da internet, Protocolo de controle Appletalk, Protocolo de controle Novell IPX, Protocolo de controle Cisco Systems, Protocolo de controle SNA e Protocolo de controle de compressão.

Arquitetura PPP

Uma arquitetura de camadas é um modelo lógico, design ou plano que auxilia na comunicação entre camadas de interconexão. A figura 12 mapeia a arquitetura de camadas do PPP em relação ao modelo Open System Interconnection (OSI). PPP e OSI têm a mesma camada física, mas PPP distribui as funções de LCP e NCP de maneira diferente.

Na camada física, você pode configurar o PPP em várias interfaces, incluindo:

- Serial assíncrona
- Serial síncrona
- HSSI
- ISDN

O PPP funciona em qualquer interface DTE/DCE (RS-232-C, RS-422, RS-423 ou V.35). O único requisito absoluto imposto pelo PPP é um circuito bidirecional, dedicado ou comutado, capaz de funcionar em modos seriais de bits assíncronos ou síncronos, transparentes para quadros de camada de enlace PPP. O PPP não impõe nenhuma restrição quanto à taxa de transmissão que não seja a imposta pela interface DTE/DCE em particular sendo utilizada.

Grande parte do trabalho feito pelo PPP acontece nas camadas de enlace e de rede pelo LCP e pelos NCPs. O LCP configura a conexão PPP e

seus parâmetros, os NCPs lidam com configurações de protocolo da camada superior e o LCP encerra a conexão PPP (CCNA Cisco, 2009).

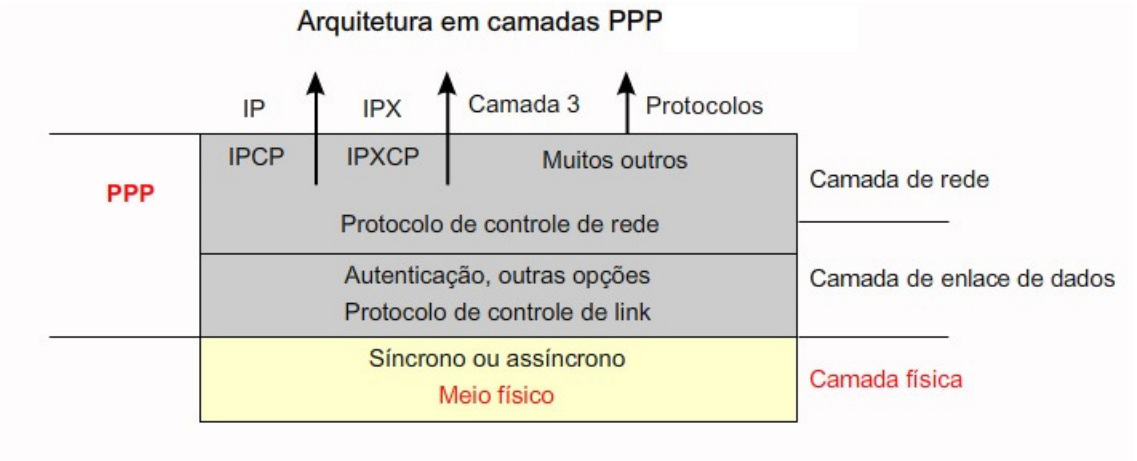

Fig. 12: Camadas do PPP

Fonte: CCNA Cisco (2007-2009)

3. TOPOLOGIA

Abaixo apresentamos a topologia que foi montada em laboratório e no simulador Cisco Packet Tracer, para realização dos estudos apresentados neste texto:

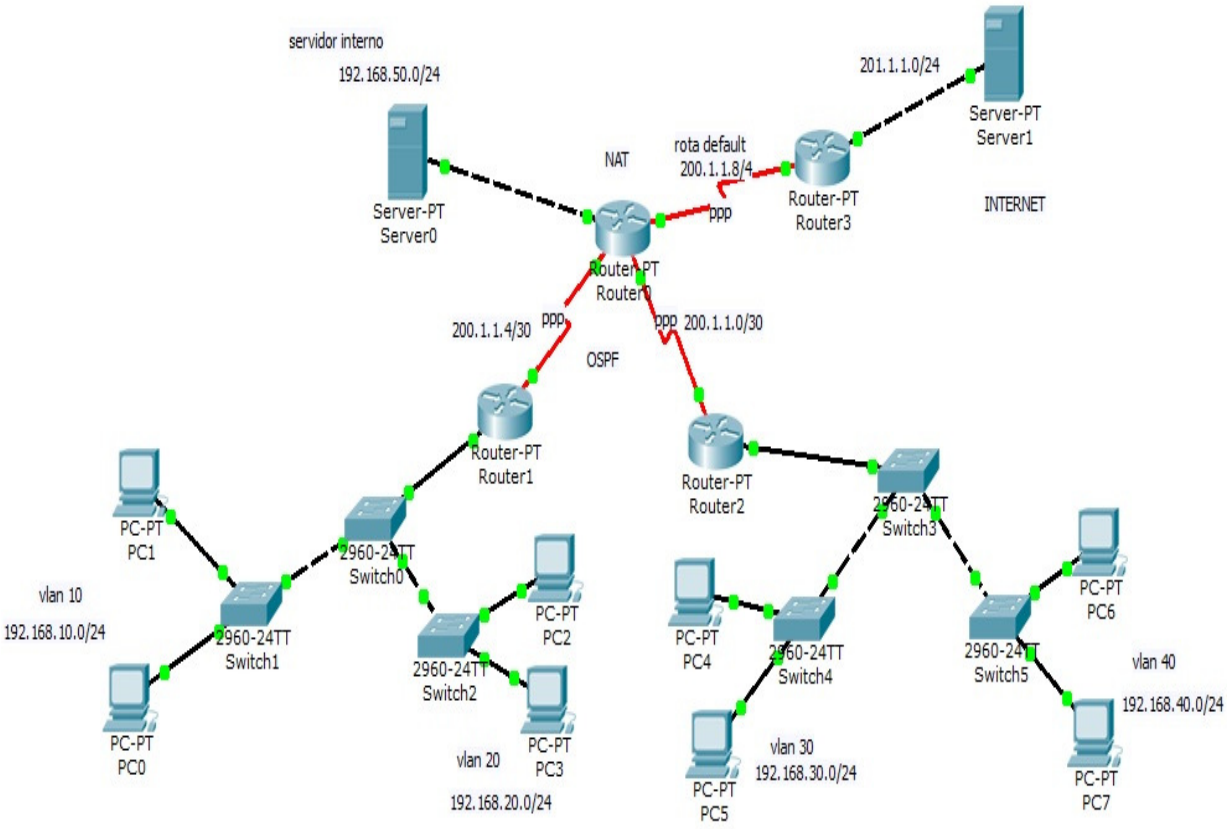

Fig. 13: Topologia

Fonte: Autoria própria

Na estrutura observamos um servidor interno, conectado às VLANs através do Router0, que também fornece o serviço de NAT, além de possuir a rota padrão que leva para a internet, passando pelo roteador de borda, Router3.

Internamente a rede é dividida através dos roteadores Router0, Router1 e Router2, onde vemos o protocolo de roteamento OSPF atuando.

3.1 Endereçamento

Os usuários desta LAN (*Local Area Network*) foram divididos em 4 VLANs, e a estrutura apresenta os seguintes endereçamentos:

- VLAN 10 – 192.168.10.0/24
- VLAN 20 – 192.168.20.0/24
- VLAN 30 – 192.168.30.0/24
- VLAN 40 – 192.169.40.0/24

As conexões WAN (*Wide Area Network*), têm os seguintes endereços:

- 200.1.1.0/30
- 200.1.1.4/30
- 200.1.1.8/30

O servidor interno utiliza à rede 192.168.50.0/24 e o acesso à internet se dá através da rede 201.1.1.0/24.

3.2 VLANs

Em nossa topologia observamos que são utilizados 6 Switches, para divisão e gerenciamento das VLANs, levando em consideração futuras ampliações dos setores. A seguir verificamos as configurações dos Switches, onde temos as portas trunk, que interconectam os switches entre si e com o roteador que está imediatamente acima na hierarquia e as portas configuradas para suas respectivas VLANs.

Parte das configurações do Switch0:

```
Switch#
Switch#sh run
!
```

```
interface FastEthernet0/3
switchport mode trunk
!
interface FastEthernet0/4
switchport mode trunk
!
interface FastEthernet0/5
switchport mode trunk
!
end
```

Parte das configurações do Switch1:

```
Switch#sh run
!
interface FastEthernet0/1
switchport access vlan 10
!
interface FastEthernet0/2
switchport access vlan 10
!
interface FastEthernet0/3
switchport mode trunk
!
end
```

Parte das configurações do Switch2:

```
Switch#sh run
!
interface FastEthernet0/1
switchport access vlan 20
!
```

```
interface FastEthernet0/2
switchport access vlan 20
!
interface FastEthernet0/4
switchport mode trunk
!
end
```

Parte das configurações do Switch3:

```
Switch#sh run
!
interface FastEthernet0/3
switchport mode trunk
!
interface FastEthernet0/4
switchport mode trunk
!
interface FastEthernet0/5
switchport mode trunk
!
end
```

Parte das configurações do Switch4:

```
Switch#sh run
interface FastEthernet0/1
switchport access vlan 30
!
interface FastEthernet0/2
switchport access vlan 30
!
interface FastEthernet0/3
switchport mode trunk
```

```
!
end
```

Parte das configurações do Switch5:

```
Switch#sh run
interface FastEthernet0/1
switchport access vlan 40
!
interface FastEthernet0/2
switchport access vlan 40
!
interface FastEthernet0/3
switchport mode trunk
!
end
```

3.3 Roteamento

O roteamento dos dados é realizado por 4 roteadores, sendo 3 (Router0, Router1 e Router2) que utilizam o OSPF, para roteamento interno. O roteador Router3 é chamado de roteador de borda, pois ele é que fornece a conexão para a internet e/ou outras redes. Vejamos suas configurações:

Parte das configurações do Roteador0:

```
Router#sh run
interface FastEthernet0/0
ip address 192.168.50.1 255.255.255.0
ip nat inside
duplex auto
speed auto
interface Serial2/0
ip address 200.1.1.5 255.255.255.252
```

```
encapsulation ppp
ip nat inside
!
interface Serial3/0
ip address 200.1.1.1 255.255.255.252
encapsulation ppp
ip nat inside
interface Serial6/0
ip address 200.1.1.9 255.255.255.252
encapsulation ppp
ip nat outside
!
router ospf 1
log-adjacency-changes
network 200.1.1.0 0.0.0.3 area 0
network 200.1.1.4 0.0.0.3 area 0
network 192.168.50.0 0.0.0.255 area 0
default-information originate
!
ip nat inside source list 1 interface Serial6/0 overload
ip nat inside source static 192.168.50.2 200.1.1.9
ip classless
ip route 0.0.0.0 0.0.0.0 200.1.1.10
!
!
access-list 1 permit any
!
end
```

Tabela de Roteamento do Router0:

```
Router#sh ip route
O IA 192.168.10.0/24 [110/65] via 200.1.1.6, 01:28:14, Serial2/0
```

```
O IA 192.168.20.0/24 [110/65] via 200.1.1.6, 01:28:14, Serial2/0
O    192.168.30.0/24 [110/65] via 200.1.1.2, 01:28:14, Serial3/0
O    192.168.40.0/24 [110/65] via 200.1.1.2, 01:28:14, Serial3/0
C    192.168.50.0/24 is directly connected, FastEthernet0/0
     200.1.1.0/24 is variably subnetted, 6 subnets, 2 masks
C       200.1.1.0/30 is directly connected, Serial3/0
C       200.1.1.2/32 is directly connected, Serial3/0
C       200.1.1.4/30 is directly connected, Serial2/0
C       200.1.1.6/32 is directly connected, Serial2/0
C       200.1.1.8/30 is directly connected, Serial6/0
C       200.1.1.10/32 is directly connected, Serial6/0
S*   0.0.0.0/0 [1/0] via 200.1.1.10
```

Parte das configurações do Roteador1:

```
Router#sh run
interface FastEthernet0/0.1
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/0.2
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
!
interface Serial2/0
ip address 200.1.1.6 255.255.255.252
encapsulation ppp
!
router ospf 1
log-adjacency-changes
network 200.1.1.4 0.0.0.3 area 0
network 192.168.10.0 0.0.0.255 area 1
network 192.168.20.0 0.0.0.255 area 1
!
```

```
end
```

Tabela de Roteamento do Router1:

```
Router#sh ip route
C    192.168.10.0/24 is directly connected, FastEthernet0/0.1
C    192.168.20.0/24 is directly connected, FastEthernet0/0.2
O    192.168.30.0/24 [110/129] via 200.1.1.5, 01:45:52, Serial2/0
O    192.168.40.0/24 [110/129] via 200.1.1.5, 01:45:52, Serial2/0
O    192.168.50.0/24 [110/65] via 200.1.1.5, 01:45:52, Serial2/0
     200.1.1.0/24 is variably subnetted, 3 subnets, 2 masks
O       200.1.1.0/30 [110/128] via 200.1.1.5, 01:45:52, Serial2/0
C       200.1.1.4/30 is directly connected, Serial2/0
C       200.1.1.5/32 is directly connected, Serial2/0
O*E2 0.0.0.0/0 [110/1] via 200.1.1.5, 01:45:52, Serial2/0
```

Parte das configurações do Roteador2:

```
Router#sh run
interface FastEthernet0/0.1
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
!
interface FastEthernet0/0.2
encapsulation dot1Q 40
ip address 192.168.40.1 255.255.255.0
!
interface Serial3/0
ip address 200.1.1.2 255.255.255.252
encapsulation ppp
!
router ospf 1
log-adjacency-changes
network 200.1.1.0 0.0.0.3 area 0
```

```
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
!
ip classless
!
end
```

Tabela de Roteamento do Router2:

```
Router#sh ip route
O IA 192.168.10.0/24 [110/129] via 200.1.1.1, 02:03:38, Serial3/0
O IA 192.168.20.0/24 [110/129] via 200.1.1.1, 02:03:38, Serial3/0
C    192.168.30.0/24 is directly connected, FastEthernet0/0.1
C    192.168.40.0/24 is directly connected, FastEthernet0/0.2
O    192.168.50.0/24 [110/65] via 200.1.1.1, 02:03:38, Serial3/0
     200.1.1.0/24 is variably subnetted, 3 subnets, 2 masks
C       200.1.1.0/30 is directly connected, Serial3/0
C       200.1.1.1/32 is directly connected, Serial3/0
O       200.1.1.4/30 [110/128] via 200.1.1.1, 02:03:38, Serial3/0
O*E2 0.0.0.0/0 [110/1] via 200.1.1.1, 02:03:38, Serial3/0
```

Parte das configurações do Roteador3:

```
Router#sh run
interface FastEthernet0/0
ip address 201.1.1.1 255.255.255.0
duplex auto
speed auto

interface Serial2/0
ip address 200.1.1.10 255.255.255.252
encapsulation ppp
!
end
```

Tabela de Roteamento do Router3:

Router#sh ip route

200.1.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 200.1.1.8/30 is directly connected, Serial2/0
C 200.1.1.9/32 is directly connected, Serial2/0
C 201.1.1.0/24 is directly connected, FastEthernet0/0

Podemos confirmar através da tabela de roteamento dos roteadores, observando as linhas que iniciam com a letra 'O', que o protocolo de roteamento OSPF está ativo e funcionando corretamente, além das redes conectadas diretamente ('C') e a rota default.

3.4 PPP

Nos enlaces seriais utilizamos o protocolo PPP, como podemos verificar através das informações em destaque, retiradas dos roteadores:

Roteador0:

interface Serial2/0
ip address 200.1.1.5 255.255.255.252
encapsulation ppp
interface Serial3/0
ip address 200.1.1.1 255.255.255.252
encapsulation ppp
interface Serial6/0
ip address 200.1.1.9 255.255.255.252
encapsulation ppp

Roteador1:

interface Serial2/0
ip address 200.1.1.6 255.255.255.252

encapsulation ppp

Roteador2:

interface Serial3/0
ip address 200.1.1.2 255.255.255.252
encapsulation ppp

Roteador3:

interface Serial2/0
ip address 200.1.1.10 255.255.255.252
encapsulation ppp

3.5 NAT

O serviço de tradução de endereços de rede, NAT, é fornecido pelo Router0, como podemos observar na configuração abaixo:

interface FastEthernet0/0
ip address 192.168.50.1 255.255.255.0
ip nat inside
interface Serial2/0
ip address 200.1.1.5 255.255.255.252
ip nat inside
interface Serial3/0
ip address 200.1.1.1 255.255.255.252
ip nat inside
ip nat outside
interface Serial6/0
ip address 200.1.1.9 255.255.255.252
!
ip nat inside source list 1 interface Serial6/0 overload
ip nat inside source static 192.168.50.2 200.1.1.9
ip classless
ip route 0.0.0.0 0.0.0.0 200.1.1.10
!

```
!
access-list 1 permit any
```

Como mostrado, as redes internas 192.168.x.x, configuradas como VLANs, poderão acessar serviços de internet através do uso da NAT.

4. CONCLUSÃO

A pesquisa do material bibliográfico utilizado, trouxe o embasamento teórico necessário para compreender fatos bastante relevantes no momento do projeto de uma rede de computadores.

A utilização das VLANs nos traz grandes benefícios, como a organização lógica das redes, o planejamento das expansões e melhoria do desempenho, uma vez que, com elas, limitamos o broadcast na LAN.

Outro ponto importante é a escolha do equipamento adequado para função pretendida. Pudemos observar que, atualmente, existe uma gama de equipamentos utilizados com as mais diversas configurações de hardware. A escolha correta trará benefícios como versatilidade, alto desempenho, possibilidade de crescimento e o investimento justo para execução do projeto.

Após a tomada de decisão sobre que equipamentos utilizar, os protocolos de que serão utilizados para roteamento, enlaces WAN, acessos à internet, entre outros, precisam ser corretamente configurados, pois, é através deles que obteremos o desempenho esperado e, consequentemente, o retorno do investimento realizado.

Atualmente contamos com protocolos e algoritmos muito eficientes, que se tornam adaptativos, ou seja, alteram automaticamente suas configurações para que o sistema, como um todo, continue funcionando adequadamente, mesmo apresentando alguma falha na rede.

Desta forma, utilizando dos recursos disponíveis em laboratório, simuladores e a bibliografia pesquisada, foi possível melhorar significativamente e aplicar de forma coerente o conhecimento adquirido ao longo deste período de estudo da área de redes de computadores.

5 REFERÊNCIAS

CISCO, Networking Academy. **CCNA Exploration – Fundamentos de Rede.** Cisco Systems, Inc., 2007-2009.

TANENBAUM, Andrew. S. **Redes de Computadores**. 4ª ed. Rio de Janeiro: Editora Campus (Elsevier), 2003.

SOARES, Luiz Fernando G. **Redes de Computadores: das LAN's, MAN's e WAN's às redes ATM**. Luiz Fernando Gomes Soares, Guido Lemos, Sergio Colcher. 2ª ed. Rio de Janeiro: Editora Campus, 1995.

TANENBAUM, Andrew S. **Redes de Computadores.** 5ª ed. São Paulo: Pearson Prentice Hall, 2011.

TORRES, Gabriel. **Redes de Computadores,** Versão Revisada e Atualizada. Novaterra Editora, 2010.