

EDUARDO SALLES CUNHA PERES

**INVESTIGAÇÃO DE REDES DE
COMPUTADORES COM
COMUTADORES DE CAMADA DOIS,
CAMADA TRÊS E ROTEADORES**

Trabalho de Conclusão de Curso
apresentado à Escola de Engenharia de São
Carlos, da Universidade de São Paulo

Curso de Engenharia Elétrica com ênfase em
Eletrônica

ORIENTADOR: Ivan Nunes da Silva

São Carlos
2008

Agradecimentos

Ao **Prof. Dr. Ivan Nunes da Silva**, pela orientação, conhecimentos transmitidos e pelo apoio no desenvolvimento deste trabalho e crescimento pessoal;

Aos meus pais, **Maria Ângela Salles Cunha Peres** e **Roberto Molinari Peres**, por tudo, principalmente pelo apoio, incentivo, carinho em todas as etapas da vida;

Aos meus irmãos, **André Salles Cunha Peres** e **Fernanda Salles Cunha Peres**, pelo apoio, amizade e incentivo.

Aos meus avós, **Aparecida Homsí de Salles Cunha** e **Mário Salles Cunha**, pela dedicação e carinho em toda minha vida.

À minha avó **Olésia Maria Meira Molinari Peres**, pela dedicação e carinho em toda minha vida.

À minha namorada **Letícia Braga**, por todo amor, carinho e compreensão, que sempre me incentiva e apóia.

Aos amigos **Vinícius Cover**, **Ediléu Cardoso** e **Elisa Barbarini**, pela ajuda, incentivo e apoio para a realização deste trabalho.

A todos, que direta ou indiretamente, contribuíram para este acontecimento.

Sumário

<i>Lista de figuras</i>	v
<i>Lista de tabelas</i>	vii
<i>Lista de siglas</i>	ix
<i>Resumo</i>	xi
<i>Abstract</i>	xiii
1. Introdução	1
1.1. Breve Introdução Histórica	1
1.2. Objetivo do Trabalho	2
1.3. Organização do Texto	2
2. Introdução Teórica	5
2.1. Modelo de Referência OSI	5
2.1.1 Camada Física.....	6
2.1.2 Camada de Enlace de Dados.....	6
2.1.3 Camada de Rede.....	7
2.1.4 Camada de Transporte.....	8
2.1.5 Camada de Sessão.....	9
2.1.6 Camada de Apresentação.....	9
2.1.7 Camada de Aplicação.....	10
2.2. Interação Entre as Camadas OSI	11
2.3. Modelo de Referência TCP/IP	13
2.3.1 Camada de Aplicação.....	14
2.3.2 Camada de Transporte.....	14
2.3.3 Camada Internet.....	15
2.3.4 Camada Interface com a Rede.....	15
2.4. Críticas ao Modelo TCP/IP	16
3. Cisco Systems	17
3.1. Introdução	17
3.2. Evolução da Empresa	17
3.3. Portfolio	20
3.3.1 Comutadores de Camada Dois.....	21
3.3.2 Roteadores.....	23
3.3.3 Comutadores de Camada Três.....	26
4. Camadas Dois e Três	27
4.1. Camada Dois	27
4.2. Camada Três	31
5. Conclusão	39
6. Bibliografia	41

Lista de Figuras

Figura 1 – Rede da Arpanet em 1973 [1]	1
Figura 2 – Classes de endereçamento IP [5].....	8
Figura 3 – Resumo do modelo de referência OSI [7]	10
Figura 4 – Interação entre as camadas OSI [8]	11
Figura 5 – Modelo de camadas TCP/IP [9]	13
Figura 6 – Funcionamento da Camada de Aplicação [9]	14
Figura 7 – Cisco Catalyst 2960 [12].....	22
Figura 8 – Cisco Catalyst 3560 [12].....	23
Figura 9 – Cisco Catalyst 3750 [12].....	23
Figura 10 – Família Cisco 2800 [12].....	24
Figura 11 – Família Cisco 3800 [12].....	25
Figura 12 – Roteador Cisco 7200 [12]	26
Figura 13 – Família Cisco Catalyst 4500 [12].....	26
Figura 14 – Segmento de rede sem e com dispositivo de switching [5]	28
Figura 15 – Cabeçalho de um quadro de camada dois [13].....	30
Figura 16 – Esquema de VLAN com implementação Centrado em porta [5].....	31
Figura 17 – Tabela de roteamento [14]	31
Figura 18 – Cabeçalho camada três de um roteador tradicional [5]	36

Lista de Tabelas

Tabela 1 – Sub-redes de Classe C	34
Tabela 2 – Método binário de subdivisão de rede para uma rede de Classe B.....	35
Tabela 3 – Método decimal para listagem dos endereços IPs para uma rede de Classe B ..	35

Lista de Siglas

ACLs	<i>Access Control Lists</i>
AGS	<i>Advanced Gateway Server</i>
ARP	<i>Address Resolution Protocol</i>
ASCII	<i>American Standard Code for Information Interchange</i>
BGP	<i>Border Gateway Protocol</i>
CCIE	<i>Cisco Certified Network Expert</i>
CCNA	<i>Cisco Certified Network Associate</i>
CCNP	<i>Cisco Certified Network Professional</i>
CRS	<i>Cisco Carrier Routing System</i>
CSR	<i>Campus Switch Routers</i>
DNS	<i>Domain Name System</i>
FCS	<i>Frame Check Sequence</i>
FIFO	<i>First In First Out</i>
FTP	<i>File Transfer Protocol</i>
Gb	Giga bits
Gbps	Giga bits por segundo
HTTP	<i>HiperText Transfer Protocol</i>
ICMP	<i>Internet Control Message Protocol</i>
IEEE	<i>Institute of Electrical and Electronic Engineers</i>
IGRP	<i>Interior Gateway Routing Protocol</i>
IOS	<i>Internetwork Operating System</i>
IP	<i>Internet Protocol</i>
ISO	<i>International Organization for Standartization</i>
Kbps	Quilo bits por segundo
LAN	<i>Local Area Network</i>
MAC	<i>Medium Access Control</i>
Mbps	Mega bits por segundo
MPLs	<i>Multiprotocol Label Switching</i>
NAC	<i>Network Admission Control</i>
NCP	<i>Network Control Protocol</i>
NFS	<i>Network File System</i>
OSI	<i>Open Systems Interconnection</i>

PoE	<i>Power over Ethernet</i>
QoS	<i>Quality of Service</i>
RARP	<i>Reverse Address Resolution Protocol</i>
RPC	<i>Remote Procedure Call</i>
SDM	<i>Security Device Manager</i>
SFP	<i>Small Form-Factor Pluggable</i>
SMTP	<i>Simple Mail Transfer Protocol</i>
SQL	<i>Structured Query Language</i>
TCP	<i>Transmission Control Protocol</i>
UDP	<i>User Datagram Protocol</i>
VLAN	<i>Virtual Local Area Network</i>
VoIP	<i>Voice over Internet Protocol</i>
VPN	<i>Virtual Private Network</i>
WWW	<i>World Wide Web</i>

Resumo

No último século ocorreram grandes mudanças no método de se fazer comunicação. Com o surgimento dos computadores e dispositivos eletrônicos foi possível criar redes de comunicação, gerando o que se conhece hoje como internet. A internet é tão importante que pode-se dizer que sem ela a sociedade atual não seria como é. Para que ela chegasse a esse ponto, muitos estudos foram feitos e algumas instituições se destacaram, como a ISO (*International Organization for Standardization*) e a Cisco Systems. A primeira criou o modelo de referência OSI (*Open Systems Interconnection*) e a segunda destaca-se no ramo de dispositivos de redes, entre eles os comutadores e roteadores.

Este trabalho apresenta um estudo sobre redes de computadores, mostrando seu surgimento e sua evolução até os dias atuais. São apresentados os modelos de referência OSI e o modelo TCP/IP (*Transmission Control Protocol/Internet Protocol*) e suas funcionalidades. Além disso, é apresentada a empresa Cisco Systems e seu portfólio, bem como uma comparação entre a evolução da empresa e a evolução da internet. Por fim, são estudadas as camadas dois e três do modelo de referência OSI, suas funcionalidades e suas vantagens.

Palavras-chave: redes de computadores, modelo de referência OSI, Cisco Systems, comutadores, roteadores.

Abstract

In the last century, great changes took place on how to make communications. Since the development of the computers and electronic devices it was possible to create communication networks, that generated what is nowadays called internet. The internet is so important that, without it, the recent society couldn't be as it is. In order to improve and develop the internet, many studies were made and some companies played very important roles, as ISO (*International Organization for Standardization*) and Cisco Systems. The first created the OSI (*Open Systems Interconnection*) reference model and the last dominates the market segment of network devices, including switches and routers.

This paper presents a study of computer networks, since its creation until its evolution to the recent technologies. The OSI reference models and the TCP/IP (*Transmission Control Protocol/Internet Protocol*) model and their functionalities are presented. Besides, there is an introduction of Cisco Systems and its portfolio, as well as a comparison between the company and the internet evolution. Then, the layers two and three of the OSI reference model, its functionalities and advantages are studied.

Keywords: computer networks, OSI reference model, Cisco Systems, switches, routers.

Figura 1 – Rede da Arpanet em 1973 [1].

Em 1974 surgiu o TCP/IP (*Transmission Control Protocol / Internet Protocol*), um conjunto de protocolos de comunicação entre computadores em rede. Esse conjunto pode ser visto como um modelo de camadas, que será apresentado posteriormente, onde cada camada realiza funções específicas e bem definidas. No mesmo período em que foi desenvolvido o TCP/IP surgiu o padrão Ethernet, onde vários computadores conseguiam se conectar ao mesmo tempo em uma única rede. A partir deste ponto é introduzido o termo LAN (*Local Area Network*), muito utilizado hoje em redes de computadores. Na década de 80 a organização ISO (*International Organization for Standardization*) desenvolveu o modelo de referência OSI (*Open Systems Interconnection*). Esta arquitetura é um modelo que divide as redes de computadores em sete camadas, que será apresentado posteriormente, de forma a se obter camadas de abstração. Cada protocolo implementa uma funcionalidade assinalada a uma determinada camada [2].

A Arpanet, somada com a Ethernet, gerou uma grande ferramenta de comunicação, uma vez que a Arpanet servia para conectar diferentes redes de computadores e a Ethernet servia para criar redes locais, compartilhando arquivos e impressoras. Em 1986 a Arpanet foi substituída por uma nova rede operacional onde somente o protocolo TCP/IP foi utilizado. A partir da década de 90, com a abertura do acesso à Internet, percebeu-se que a criação de redes locais em empresas, instituições, universidades, etc., era a forma mais barata de conectar todos os computadores da rede à Internet.

Todos os componentes citados e com o avanço da tecnologia em redes de computadores contribuíram para criar a internet como é conhecida atualmente.

1.2. Objetivo do Trabalho

O trabalho tem como objetivo o estudo de redes de computadores, analisando diferentes equipamentos que atuam nas camadas dois e três do modelo de referência OSI. É também objetivo do trabalho a apresentação dos modelos de referência OSI e o modelo TCP/IP. Por fim, é ainda objetivo do estudo as camadas dois e três do modelo OSI, mostrando as atuações de rede em cada camada.

1.3. Organização do Texto

O texto está organizado na forma de capítulos seguindo a seguinte métrica. No capítulo 1 é apresentada uma breve introdução sobre comunicação e surgimento de redes de computadores, da

internet e objetivo do trabalho. No capítulo 2 é apresentado o modelo de referência OSI e TCP/IP, em detalhes, mostrando cada camada e suas aplicações. O capítulo 3 apresenta a empresa CISCO, seus produtos, suas funcionalidades e em quais camadas do modelo OSI eles atuam. No capítulo 4 são exploradas as camadas dois e três do modelo OSI a fim de se conhecer em detalhes suas aplicações e suas vantagens. Por fim, o capítulo 5 é apresentado a conclusão do trabalho.

2. Introdução Teórica

2.1. Modelo de Referência OSI

O modelo OSI se baseia em uma proposta desenvolvida pela ISO como um primeiro passo em direção à padronização internacional dos protocolos empregados nas diversas camadas. O modelo é chamado Modelo de referência ISO OSI, pois ele trata da interconexão de sistemas abertos, ou seja, sistemas que estão abertos à conexão com outros sistemas.

Este sistema possui sete camadas e para se chegar a este número utilizou-se o seguinte padrão:

- uma camada deve ser criada onde houver necessidade de outro grau de abstração;
- cada camada deve executar uma função bem definida;
- a função de cada camada deve ser escolhida tendo em vista a definição de protocolos padronizados internacionalmente;
- os limites das camadas devem ser escolhidos para minimizar o fluxo de informações pelas interfaces;
- o número de camadas deve ser grande o bastante para que funções distintas não precisem ser desnecessariamente colocadas na mesma camada e, pequeno o suficiente, para que a arquitetura não se torne difícil de se controlar [3].

As sete camadas do modelo OSI são das menores para as maiores, respectivamente:

1. Camada Física
2. Camada de Enlace de Dados
3. Camada de Rede
4. Camada de Transporte
5. Camada de Sessão
6. Camada de Apresentação
7. Camada de Aplicação

As camadas superiores do modelo OSI (sete, seis e cinco) voltam-se mais aos serviços de aplicação. As quatro camadas restantes estão mais voltadas aos fluxos de dados que passam pela rede.

2.1.1. Camada Física

A camada física trata da transmissão de bits por um canal de comunicação. O projeto da rede deve garantir que, ao se enviar um bit '1' o receptor receba um bit '1' e não '0'. Para que isto ocorra, a camada física lida com as características físicas da transmissão, ou seja, os tipos de conectores, pinos, corrente elétrica, tensão, codificação e modulação de luz. Além disso, deve-se analisar a quantidade de nanossegundos que um bit deve durar, se a conexão pode ser realizada ou não nos dois sentidos simultaneamente, a forma como a conexão inicial será realizada e de que maneira ela se encerrará quando ambos os lados tiverem terminado de transmitir, e ainda quantos pinos serão necessários e qual a função de cada. Às vezes, é necessário o uso de diferentes especificações para se ter uma completa informação da camada física. Por exemplo, RJ-45 define a forma de conector e o número de fios ou pinos no cabo. Ethernet e a norma IEEE 802.3 definem o uso de fios ou pinos um, dois, três e seis. Portanto, para se usar um cabo categoria 5 com um conector RJ-45 de conexão Ethernet, utilizam-se as especificações de Ethernet e de RJ-45 de camada física.

2.1.2. Camada de Enlace de Dados

A camada de enlace de dados é responsável por estruturar os bits da camada física em quadros, compostos por um identificador de início de quadro (padrões de bits seqüenciais), endereço de origem, endereço de destino, informações a ser enviada e um código de detecção de erros no quadro [4]. Esses quadros são formados por centenas ou milhares de bytes e são transmitidos seqüencialmente. Se a informação chegar completa para o receptor, o mesmo retorna um quadro de confirmação. Se a informação não chegar completa o transmissor retransmite a informação. Caso ele precise retransmitir várias vezes, pode-se gerar erro de duplicação de quadro. Os endereços colocados no cabeçalho do quadro são denominados MAC (*Medium Access Control*) e identificam de modo único uma máquina conectada a uma rede. Isso é necessário porque cada estação precisa ler o endereço de destino de cada quadro para saber se o quadro é destinado a ela.

Outra questão que surge na camada de enlace de dados é como impedir que um transmissor rápido envie uma quantidade excessiva de dados a um receptor lento. Com freqüência, é necessário algum mecanismo que regule o tráfego para informar ao transmissor quanto espaço no *buffer* do receptor se tem no momento. Este controle de fluxo é feito nesta camada.

O principal dispositivo que atua nessa camada é o comutador, mais conhecido como *switch*.

2.1.3. Camada de Rede

A camada de rede adiciona o endereço de rede de origem e de destino ao quadro gerado pela camada de enlace de dados, além de um identificador de qual protocolo de rede está sendo utilizado, criando uma estrutura denominada pacote. Após estruturar os pacotes, estes são endereçados, convertendo endereços lógicos (ou IP) em endereços físicos, de forma que eles consigam chegar corretamente ao destino. Essa camada também determina a rota que os pacotes irão seguir para atingir o destino, baseando-se em fatores como condições de tráfego da rede e prioridades. Estas rotas podem se basear em tabelas estáticas, “amarradas” à rede e raramente alteradas. Também podem ser determinadas ao início de cada conversação, ou podem ser altamente dinâmicas, sendo determinadas para cada pacote, com o objetivo de refletir a carga atual da rede. Além de definir as rotas, a camada de redes do modelo OSI define como elas serão aprendidas a fim de que os pacotes possam ser entregues corretamente. Outra função da camada é definir como fragmentar um pacote em pacotes menores para acomodar mídia com tamanhos de unidade de transmissão máximos menores.

O IP é o protocolo da camada de rede mais usado e sua função é justamente fazer o roteamento dos pacotes. Ele é composto por trinta e dois bits, mas, para facilitar, foi dividido em quatro octetos representados na forma decimal. Como o IP é composto por octetos na forma decimal, cada um pode possuir valor máximo de duzentos e cinquenta e cinco. Isto porque dois elevado a oitava é igual a duzentos e cinquenta e cinco. Para facilitar a administração destes endereçamentos, os projetistas distribuíram o IP em cinco classes, dentre elas apenas três são usadas para endereçamento de host (Figura 2). Os endereços da classe ‘A’ são destinados à grandes corporações e utilizam o primeiro octeto para endereços de rede e os outros octetos para hosts. Os endereços classe ‘B’ são designados à corporações de médio porte, onde os dois primeiros octetos são destinados a endereçamentos de rede e os outros dois a hosts. Por fim, os endereçamentos classe ‘C’ são destinados à pequenas corporações, onde os três primeiros octetos são destinados à rede e o último a host.

Dentro de endereçamento IP existe também o endereçamento de sub-rede, utilizado para dividir a rede existente em outras redes menores. Para entender o funcionamento da sub-rede pode-se observar o exemplo a seguir: Em um endereçamento classe ‘C’ existem duzentos e cinquenta e quatro endereços de host, pois os endereços zero e duzentos e cinquenta e cinco são utilizados para endereço de rede e *broadcast*, respectivamente. Ao fazer uma comunicação entre dois roteadores são necessários apenas dois endereços de host na rede. Portanto, ao se utilizar um

endereçamento classe 'C', duzentos e cinquenta e dois endereços serão inutilizados. Ao se fazer uma sub-rede, pode-se criar sessenta e quatro sub-redes de quatro endereços cada. Como o primeiro e último endereços são utilizados para rede e *broadcast*, restam apenas dois endereços, o que resolveria o problema acima, e não desperdiçaria os outros endereços.

O dispositivo que atua nessa camada é o roteador e será apresentado nos próximos capítulos.

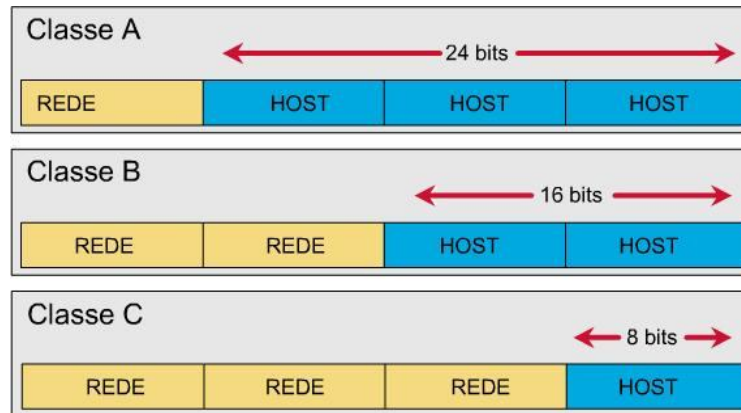


Figura 2 – Classes de endereçamento de IP [5].

2.1.4. Camada de Transporte

A camada de transporte é responsável por usar os dados enviados pela camada de sessão e dividi-los em pacotes que serão transmitidos para a camada de rede. Como receptor, a camada de transporte é responsável por pegar os pacotes recebidos da camada de rede, remontá-los formando o dado original e enviá-lo à camada de sessão. Todo esse processo deve ser feito de forma a assegurar que os fragmentos cheguem ao seu destino corretamente e de forma eficiente. Para que isto ocorra são necessários controle de fluxo, ordenação dos pacotes e correção de erros. A camada de transporte separa as camadas de aplicação (cinco, seis e sete) das camadas de nível físico (um, dois e três). Ela faz a ligação entre esses dois grupos e determina a classe de serviço necessária como orientada a conexão e com controle de erro, serviço de confirmação, sem conexões e nem confiabilidade.

Como principal exemplo de protocolo de camada de transporte orientado a conexão é o TCP. Ele utiliza várias técnicas para proporcionar uma entrega confiável de pacotes de dados, entre elas a recuperação de pacotes perdidos, a eliminação de pacotes duplicados e a recuperação de dados corrompidos. Além disso, o TCP possui controle de fluxo que é utilizado para a confirmação do recebimento de dados e, desta forma, garantir que todos os dados cheguem ao destino. O TCP é

utilizado quando é necessária a certeza da entrega, como por exemplo, a transferência de dados entre dois computadores.

Outro exemplo de protocolo da camada de transporte é o UDP (*User Datagram Protocol*) que é um protocolo não orientado a conexão, ou seja, um protocolo não confiável. O UDP faz entregas de mensagens independentes, podendo ser fora de ordem e com perdas de informações. Como não necessita de muito processamento o UDP é muito utilizado para transmitir dados poucos sensíveis, como fluxo de áudio e vídeo, uma vez que é possível a compreensão do conteúdo mesmo com a falta de algumas informações. Além disso, não seria possível a existência do VoIP (*Voice over Internet Protocol*) sem o UDP.

2.1.5. Camada de Sessão

A camada de sessão é responsável por iniciar, controlar e finalizar conversações (chamadas de sessões). Isto inclui o controle e o gerenciamento de múltiplas mensagens bidirecionais de forma que a aplicação possa ser notificada se apenas algumas de uma série de mensagens forem completadas. Isto permite à camada de apresentação ter uma visão sem interrupções de um fluxo de dados recebido. A camada de apresentação pode receber dados se houver todos os fluxos. Por exemplo, uma transação no caixa automático na qual uma pessoa saca dinheiro de sua conta corrente não deveria debitá-lo em sua conta antes de lhe dar o dinheiro, registrando a transação mesmo que ela não o tivesse recebido. A camada de sessão cria meios de se identificar que fluxos fazem parte da mesma sessão e quais deles devem estar completos antes de qualquer um ser considerado finalizado. Além disso, a camada de sessão possui sincronização que faz com que a transmissão de dados continue do ponto em que parou caso haja interrupção na transmissão [6].

Alguns exemplos de protocolos desta camada são o RPC (*Remote Procedure Call*), SQL (*Structured Query Language*) e o NFS (*Network File System*).

2.1.6. Camada de Apresentação

A camada de apresentação, também conhecida como camada de tradução, converte o formato do dado recebido pela camada de aplicação em um formato comum a ser usado na transmissão desse dado, ou seja, um formato entendido pelo protocolo usado. Um exemplo comum é a conversão do padrão de caracteres quando, por exemplo, o dispositivo transmissor usa um padrão diferente do ASCII (*American Standard Code for Information Interchange*). Além disso, a camada possui outras funções como a compressão de dados e criptografia.

A compressão de dados recebe os dados da camada superior (camada de aplicação) e os comprime, tornando mais veloz a transmissão, uma vez que menos pacotes são enviados. Por sua vez, a camada de apresentação do receptor deve descompactar os dados e enviá-los a camada de aplicação.

Para aumentar a segurança, pode-se usar algum esquema de criptografia nesse nível, sendo que os dados só serão decodificados na camada de apresentação do dispositivo receptor.

2.1.7. Camada de Aplicação

A camada de aplicação é a camada mais próxima ao usuário. Ela fornece serviços de rede aos aplicativos do usuário, tais como transferência de arquivos, correio eletrônico, acesso a terminais de computadores remotos e funções de gerência. A camada se diferencia das outras por não fornecer serviços a nenhuma outra camada OSI, mas apenas a aplicativos fora do modelo. Os programas de planilhas, de processamento de texto e programas de terminais bancários são exemplo desses processos de aplicativos. A camada de aplicação estabelece a disponibilidade dos parceiros de comunicação pretendidos, sincroniza e estabelece o acordo sobre os procedimentos para a recuperação de erros e o controle da integridade dos dados.

Na figura 3 tem-se um resumo do modelo de camadas OSI e suas aplicações:

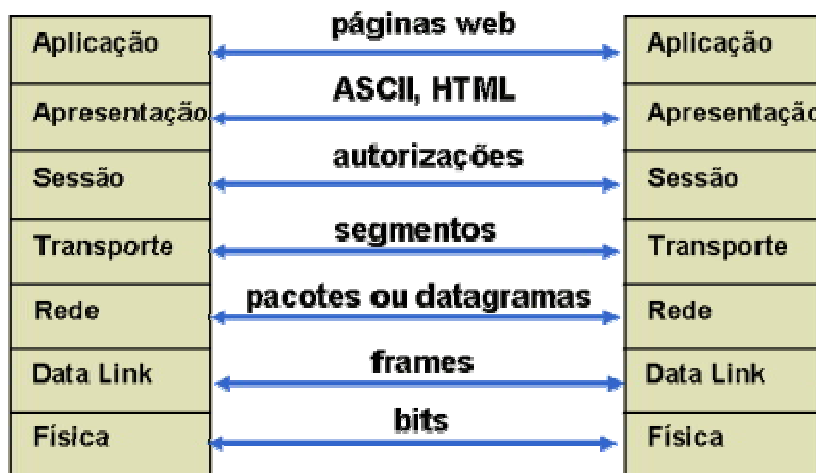


Figura 3 – Resumo do modelo de referência OSI [7].

2.2. Interação Entre as Camadas OSI

Até este ponto do trabalho foi estudado o modelo de referência OSI e suas camadas. Foram apresentadas as sete camadas e suas funcionalidades. Mesmo entendendo o comportamento de cada camada individualmente, deve-se entender o funcionamento da interação entre cada camada do modelo OSI. A figura 4 mostra a troca de informação entre dois *hosts*.

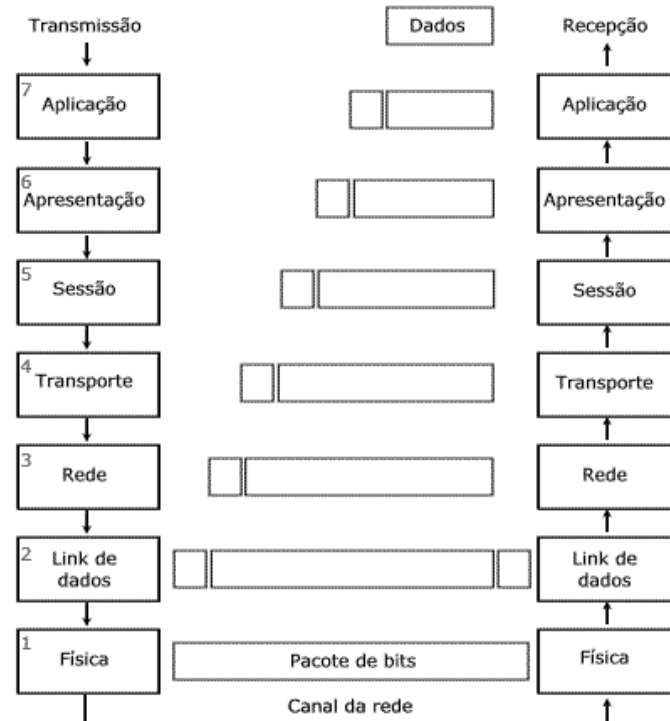


Figura 4 – Interação entre as camadas OSI [8].

A seguir será apresentado um exemplo para melhor explicar as interações entre as camadas. Um usuário (transmissor) envia uma mensagem de correio eletrônico para outro usuário (receptor). Cada camada do modelo cria um *header* e passa os dados para a próxima camada (as flechas do lado esquerdo da Figura 4 mostram a passagem dos dados entre as camadas). Passar os dados para a próxima camada significa que a camada inferior precisa realizar alguns serviços para a camada superior. Para isso, a camada inferior adiciona algumas informações em um *header* ou em um *trailer*. Da perspectiva de cada camada, os bits depois do *header* da camada são considerados dados. Por exemplo, a camada quatro considera os *headers* das camadas cinco, seis e sete juntamente com os dados do usuário originais, como um grande campo de dados.

No recebimento (lado direito da Figura 4), o receptor começa as interações com suas camadas adjacentes conforme é mostrado nas etapas a seguir:

1. a camada física assegura a sincronização de bits e coloca o padrão binário recebido em um *buffer*. Ela notifica a camada de enlace de dados que um *frame* foi recebido após se decodificar o sinal recebido em uma seqüência de bits. Por isso, a camada física ofereceu uma seqüência de bits através do meio;
2. a camada de enlace de dados examina a FCS (*Frame Check Sequence*) no *trailer* com o intuito de determinar se houveram erros na transmissão. Em caso positivo, o *frame* é descartado. O endereço do enlace de dados é examinado de forma que o receptor possa decidir se quer ou não processar os dados. Se os dados estiverem endereçados para ele, os dados entre o *header* e o *trailer* da camada de enlace são passados para o *software* da camada de rede. O enlace de dados passa os dados por meio de tal *link*;
3. examina-se o endereço de destino da camada de rede. Se ele for do receptor, o processamento continua (endereçamento lógico) e os dados depois do *header* da camada três são passados para o *software* da camada de transporte. A camada de rede ofereceu a entrega fim a fim;
4. se a recuperação de erros foi uma opção escolhida para a camada de transporte, os contadores que os identificam são codificados no *header* da camada quatro juntamente com informações de *acknowledgement* (recuperação de erro). Depois da recuperação de erro e do reordenamento dos dados de entrada, os dados são passados para a camada de sessão;
5. a camada de sessão pode ser usada para garantir que uma série de mensagens esteja completa. Por exemplo, estes dados poderiam ser inócuos, se as próximas quatro trocas não estiverem completas. O *header* da camada cinco poderia incluir campos com o intuito de dizer que isto é um fluxo intermediário em uma cadeia, e não um fluxo final. Depois que a camada de sessão assegurar que todos os fluxos estejam completos, ela passa os dados depois do *header* da camada cinco para o *software* da camada de apresentação;
6. a camada de apresentação define e manipula os formatos dos dados. Por exemplo, se os dados são binários em vez de caracteres, o *header* indica o fato. O receptor não tenta converter os dados usando o conjunto de caracteres ASCII. Este tipo de *header* costuma ser incluído apenas para fluxos de inicialização, e não para cada mensagem que está sendo transmitida (formato de dados). Depois dos formatos de dados serem

convertidos, os dados após o *header* da camada de apresentação são passados para o *software* da camada de aplicação;

7. a camada de aplicação processa o *header* final e já pode examinar os dados reais do transmissor. Este *header* significa a aceitação dos parâmetros operacionais por parte dos aplicativos no transmissor e receptor. Os *headers* são usados na sinalização dos valores para todos os parâmetros, por isso o *header* costuma ser enviado e recebido apenas no momento de inicialização da aplicação. Por exemplo, para a transferência de arquivos, o tamanho do arquivo a ser transferido e os formatos do arquivo usados seriam comunicados (parâmetros do aplicativo) [6].

2.3. Modelo de Referência TCP/IP

O modelo de referência TCP/IP (Figura 5) é um conjunto de protocolos de comunicação entre computadores em rede. Seu nome vem dos dois mais importantes do conjunto: o **TCP** (Protocolo de Controle de Transmissão) e o **IP** (Protocolo de Interconexão). O conjunto de protocolos pode ser visto como um modelo de camadas, onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo de camada superior. A camada mais alta está logicamente mais perto do usuário, chamada de camada de aplicação. Ela lida com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração.



Figura 5 – Modelo de camadas TCP/IP [9].

2.3.1. Camada de Aplicação

Como visto acima, o modelo TCP/IP não possui as camadas de sessão e apresentação, existentes no modelo OSI. Não foram incluídas essas camadas pela falta de necessidade das mesmas. Desta forma, a camada de aplicação (Figura 6) situa-se acima da camada de transporte. Ela é responsável em fazer a comunicação entre aplicativos e a camada de transporte. Ela contém todos os protocolos de nível alto. Dentre eles, o protocolo de terminal virtual (TELNET), o protocolo de transferência de arquivos (FTP – *File Transfer Protocol*), o protocolo de transferência de hipertexto (HTTP – *HiperText Transfer Protocol*), o protocolo de correio eletrônico (SMTP – *Simple Mail Transfer Protocol*) e o DNS (*Domain Name System*). O protocolo de terminal virtual permite a conexão de um usuário em um equipamento remoto.

A camada de aplicação comunica-se com a camada de transporte através de uma porta. As portas são numeradas e as aplicações padrão usam sempre uma mesma porta. Por exemplo, o protocolo SMTP utiliza sempre a porta 25, o protocolo HTTP utiliza sempre a porta 80 e o FTP sempre as portas 20 (para transmissão de dados) e 21 (para transmissão de informações de controle). O uso de um número de porta permite ao protocolo de transporte (tipicamente TCP) saber qual é o tipo de conteúdo do pacote de dados e, no receptor, saber para qual protocolo de aplicação ele deverá entregar o pacote de dados.

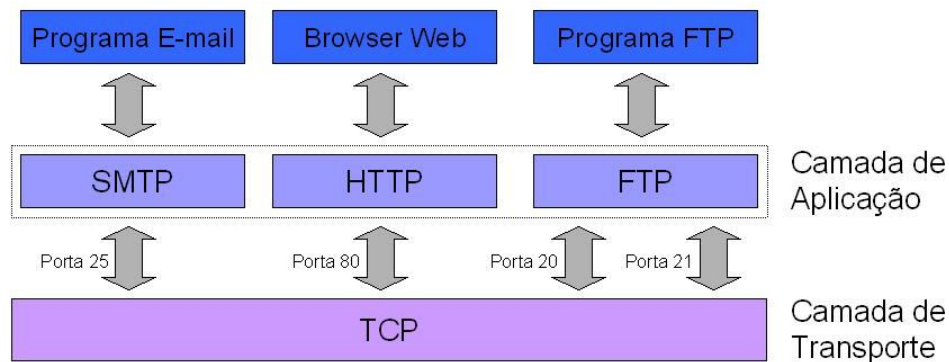


Figura 6 – Funcionamento da Camada de Aplicação [9].

2.3.2. Camada de Transporte

Na transmissão de dados, a camada de transporte é responsável por pegar os dados passados pela camada de aplicação e transformá-los em pacotes. O TCP é o protocolo mais usado na camada de transporte. Na recepção de dados, o protocolo TCP pega os pacotes passados pela

camada Internet e trata de colocá-los em ordem, uma vez que os pacotes podem chegar ao destino fora de ordem. Além disso, confere se os dados dentro dos pacotes estão íntegros e envia um sinal de confirmação chamado *acknowledge* ao transmissor, avisando que os pacotes foram recebidos corretamente. Se nenhum sinal de confirmação for recebido, o transmissor enviará novamente o pacote perdido.

O UDP é outro protocolo que opera nessa camada, porém ele não possui os mesmos recursos que o TCP. O UDP não confere se os dados possuem erros e também não envia sinal de confirmação. Por este motivo o TCP é considerado um protocolo confiável, enquanto o UDP é considerado não confiável. Mesmo não sendo um protocolo confiável, o UDP é bem mais rápido que o TCP, justamente por não enviar *acknowledge* e por seu cabeçalho ser menor que o do TCP. Enquanto o cabeçalho do UDP ocupa oito bytes, o cabeçalho do TCP utiliza vinte e quatro bytes, dependendo se um campo está sendo utilizado ou não.

2.3.3. Camada Internet

Em redes TCP/IP cada computador é identificado com um endereço virtual único, chamado endereço de IP. A camada internet é responsável por adicionar um cabeçalho aos pacotes de dados recebidos da camada de transporte onde será adicionado o endereço IP de origem e o de destino, isto é, o endereço IP do computador que está enviando os dados e o endereço IP do computador que irá recebê-los. Esta camada é responsável pelo roteamento dos pacotes. Além do protocolo IP existem outros protocolos que atuam na camada internet. Dentre eles o ICMP (*Internet Control Message Protocol*), o ARP (*Address Resolution Protocol*) e o RARP (*Reverse Address Resolution Protocol*).

2.3.4. Camada Interface com a Rede

Os datagramas gerados na camada internet serão passados para a camada interface com a rede, durante a transmissão de dados, ou a camada de interface com a rede pegará os dados da rede e os enviará para a camada de internet, na recepção de dados. Esta camada é definida pelo tipo de rede física a qual seu computador está conectado. O modelo TCP/IP não deixa muito claro a função desta camada. Comparando com o modelo OSI, esta camada se equivale as camadas física e de enlace de dados. A modelo TCP/IP se equivale as camadas três a sete do modelo OSI. Para se completar as outras duas camadas do modelo OSI é usado a Ethernet. Ela é um conjunto

de protocolos que lida com as camadas um e dois do modelo OSI. Dessa forma, utilizando o modelo TCP/IP com a Ethernet tem-se uma conexão de rede completa.

2.4. Críticas ao Modelo TCP/IP

Apesar do modelo TCP/IP ter sido adotado pela Arpanet e ser conhecido como um protocolo que permitia o crescimento praticamente ilimitado da rede, além da facilidade de sua implantação, esse modelo possui alguns pontos fracos que serão expostos a seguir.

Em primeiro lugar, o modelo não diferencia com a necessária clareza os conceitos de serviço, interface e protocolo. A boa prática da engenharia de *software* exige uma diferenciação entre especificação e implementação, algo que o OSI faz com muito cuidado, ao contrário do TCP/IP. Conseqüentemente, o modelo TCP/IP não é o melhor dos guias para a criação de novas redes com base em novas tecnologias.

Em segundo lugar, o modelo TCP/IP não é abrangente e não consegue descrever outras pilhas de protocolos a não ser a pilha TCP/IP. Por Exemplo, seria praticamente impossível tentar descrever a *Bluetooth* usando o modelo TCP/IP.

Em terceiro lugar, a camada interface com a rede não é realmente uma camada no sentido em que o termo é usado no contexto de protocolos hierarquizados, tratando-se apenas de uma interface.

Por fim, apesar de os protocolos IP e TCP terem sido cuidadosamente projetados e bem implementados, o mesmo não aconteceu com muitos outros protocolos produzidos pela comunidade acadêmica. As implementações desses protocolos eram distribuídas gratuitamente, o que acabava difundindo seu uso de tal forma que se tornou difícil substituí-las. Hoje em dia, a fidelidade as esses produtos é motivo de alguns embaraços. Por exemplo, o protocolo de terminal virtual, o TELNET, foi projetado para um terminal TTY mecânico, capaz de processar dez caracteres por segundo. Ele não reconhece o *mouse* e as interfaces gráficas do usuário. No entanto, esse protocolo é usado em larga escala ainda hoje, vinte e cinco anos após seu surgimento [3].

3. Cisco Systems

3.1. Introdução

Existem grandes empresas no mercado de roteadores, como a Juniper Networks, companhia criada em 1996, em Santa Clara (Califórnia, Estados Unidos da América) e a Alcatel Lucent, fabricante francesa. Mesmo sendo grandes, essas empresas são poucas representativas se comparadas a Cisco Systems. A Juniper representa cerca de quatorze por cento do mercado de redes, a Alcatel cerca de quatro e meio por cento e a Cisco representa cerca de setenta por cento do mercado de redes. Sendo assim, nesse capítulo será estudado o que é a Cisco, sua evolução desde o seu surgimento e o seu portfolio.

A empresa Cisco Systems, Inc. é uma companhia multinacional sediada em San Jose Califórnia, Estados Unidos da América com cerca de sessenta e três mil funcionários em todo o mundo e com faturamento anual de US\$34,9 bilhões em 2007, com crescimento de vinte e três por cento em relação a 2006. A principal atividade da Cisco é o oferecimento de soluções para redes e comunicações, quer seja na fabricação e venda (destacando-se fortemente no mercado de roteadores e *switches*) ou mesmo na prestação de serviços por meio de suas subsidiárias *Linksys*, *WebEx*, *IronPort* e *Scientific Atlanta*. No começo de suas operações, a Cisco apenas fabricava roteadores de grande porte para empresas, mas gradualmente diversificou o seu negócio passando a atender também ao consumidor final com tecnologias como o VoIP, ao mesmo tempo em que seu segmento corporativo era ampliado [10].

3.2. Evolução da Empresa

A empresa Cisco foi fundada em 1984 por Len Bosack e Sandy Lerner, que eram funcionários da área de computação da universidade estadunidense *Stanford University*. No começo a empresa era muito pequena, mas hoje é uma das cinquenta maiores empresas do mundo em apenas vinte e cinco anos de história. Além disso, é possível fazer uma comparação bem próxima entre sua evolução e a evolução da internet. A seguir, tem-se um breve resumo de como essa empresa se tornou tal potência.

– **1984:** a Cisco Systems é fundada. Número de funcionários: 2. Receita: Zero.

- **1985:** a empresa define sua identidade corporativa. O primeiro logotipo é anunciado. No mundo, os primeiros domínios .com e .edu são registrados. Número de hosts na internet: 1961. Número de funcionários: 2.
- **1986:** a Cisco contrata seu primeiro funcionário e muda sua sede para um modesto escritório em *Menlo Park* (Califórnia). A empresa lança seu primeiro produto inovador na área de roteamento, o AGS (*Advanced Gateway Server*). A primeira venda foi fechada com a Universidade de Utah. Número de funcionários: 6.
- **1987:** a empresa consegue um investimento de US\$2 milhões. A empresa lança o protocolo IGRP (*Interior Gateway Routing Protocol*), sendo o primeiro protocolo criado para rodar em redes de grande porte. Enquanto isso, na internet, o TCP/IP vai se consolidando como a tecnologia base de rede das redes de computadores. O número de *hosts* na rede ultrapassa dez mil. Número de funcionários: 9.
- **1989:** com apenas 111 funcionários e três produtos lançados, a empresa consegue obter uma receita de US\$27 milhões. Cisco desenvolve o protocolo BGP (*Border Gateway Protocol*) e completa a primeira implementação do mesmo em roteadores da empresa. Número de *hosts* na rede ultrapassa cem mil.
- **1990:** a empresa abre seu capital na bolsa eletrônica NASDAQ e consegue uma capitalização de US\$224 milhões. O consórcio que mantinha a Arpanet é desfeito, e a rede resultante é chamada de Internet pela primeira vez. Foi também neste ano que o termo WWW (*World Wide Web*) foi usado pela primeira vez. Número de funcionários: 251.
- **1991:** John Chambers obtém o cargo de vice presidente Senior para venda e operações. A Cisco inaugura seus escritórios em *Menlo Park* (Califórnia). A capitalização da empresa bate US\$1 bilhão. Número de funcionários: 503.
- **1992:** a Cisco consegue sua primeira patente. A empresa abre escritórios em Toronto (Canadá) e em Tóquio (Japão). A linha de equipamentos 3000 é lançada. O primeiro *browser* é disponibilizado anonimamente. Número de funcionários: 875.
- **1993:** a receita obtida no ano fiscal é de US\$714 milhões. A empresa completa sua primeira aquisição, a compra da *Crescendo Communications*. O programa de certificações CCIE (*Cisco Certified Internetwork Expert*) é criado. A linha de equipamentos 7000 é lançada e a Cisco começa a trabalhar com uma linha definida de produtos. Número de funcionários: 1459.
- **1994:** a empresa inaugura seus escritórios em *San Jose* e abre filiais no Brasil e China. Cinco novas linhas de produtos são lançadas, dentre elas, a linha de roteadores 2xxx. A receita obtida neste ano foi de US\$1,3 bilhão. Número de funcionários: 2269.

- **1995:** John Chambers torna-se CEO (presidente) da empresa. A Cisco lança a linha Catalyst 5000. Mais de cem mil roteadores da linha 2500 já foram vendidos. A Cisco lança a linha 7500. Na Internet, o volume de tráfego no HTTP ultrapassa, pela primeira vez, o volume do FTP. A receita neste ano foi de US\$2,2 bilhões. Número de funcionários: 3827.
- **1996:** a empresa abre escritórios na Holanda. A Cisco inicia sua incursão no segmento de *Service Providers*. O primeiro site da empresa com suporte ao idioma chinês é lançado. A Cisco compra outras empresas, como a *Stratacom*. A linha 7200 é lançada. A tecnologia MPLS (*Multiprotocol Label Switching*) é lançada pela empresa. No mundo já existem mais de quatorze milhões de *hosts* e mais de cem mil *websites*. A receita foi de US\$4,1 bilhões. Número de funcionários: 8259.
- **1997:** o programa *Cisco Networking Academy* é criado. Número de academias: 64. Número total de patentes: 34. A empresa lança a linha 12000. Primeiro produto voltado à VoIP é lançado. Mais de um milhão de roteadores da linha 25xx. A Cisco lança linha voltada aos operadores de televisão a cabo e também entra no mercado de xDSL. Primeira aparição da empresa na lista da *Fortune* 500. A receita foi de US\$6,5 bilhões. Número de funcionários: 10728.
- **1998:** primeiro anúncio na televisão é veiculado. Número de academias Cisco: 580. Patentes no ano: 60. A Cisco torna-se a primeira empresa da história a alcançar um valor de mercado acima dos US\$100 bilhões em apenas quatorze anos. A linha CSR (*Campus Switch Routers*) é lançada. Mais de mil roteadores da linha 12000 foram vendidos. Existem trinta milhões de *hosts* na Internet e mais de um milhão e oitocentos mil *websites*. A receita do ano foi de US\$8,5 bilhões. Número de funcionários: 14623.
- **1999:** a Cisco alia-se a outras dez empresas para determinar os padrões que regerão as redes locais wireless. Ela segue comprando outras empresas, dentre elas, a *Aironet* (WIFI). A receita foi de 12,2 bilhões. Número de funcionários: 20657.
- **2000:** a Cisco torna-se a empresa mais valiosa do mundo em termos de valor de mercado (US\$569 bilhões). Patentes no ano: 150. A empresa adquire mais de vinte empresas apenas neste ano. O número de academias Cisco sobe para 4901. A linha Catalyst 4000 é lançada. As linhas 2600 e 3600 são lançadas. A primeira transmissão de vídeo full-motion via rede IP é realizada. Além disso, obtém a patente para alimentar telefones IP via porta Ethernet. A receita foi de US\$18 bilhões. Número de funcionários: 34613.
- **2001:** o número de academias Cisco aumenta para oito mil. A Cisco anuncia a fase 1 da incorporação IPv6 (*Internet Protocol version six*) em seus produtos, a primeira empresa a fazê-lo. Ela lança a primeira plataforma multiserviço a operar a 10 Gb. A receita chega a US\$22,3 bilhões. Número de funcionários: 38402.

- **2002:** nesse ano ocorre a primeira queda no número de funcionários e na receita. Patentes no ano: 240. O número de academias Cisco continua crescendo com mais de dez mil. Mesmo com queda, quatorze novos modelos de roteadores de acesso são lançados. Além disso, a linha Catalyst 6500 é lançada. A empresa começa a ganhar notoriedade na área de *storage*. A receita recua para US\$18,9 bilhões e o número de funcionários para 35670.
- **2003:** há um novo corte de funcionários. Patentes no ano: 327. O número de academias chega a cerca de dez mil e quinhentos. A Cisco adquire a Linksys. A linha 7300 é anunciada. A empresa lança importantes produtos na área de segurança de rede. São anunciados o primeiro telefone IP wireless e o primeiro telefone IP com visor colorido. Existem mais de cento e setenta e dois milhões de *hosts* e mais de quarenta e seis milhões de websites na Internet. A receita da empresa foi de US\$18,9 bilhões. Número de funcionários: 34466.
- **2004:** a empresa adquire a empresa P-Cube. A linha CRS (Cisco *Carrier Routing System*) foi lançada. Este roteador foi considerado o roteador de internet com maior capacidade do planeta. A empresa lança produtos importantes nas áreas de Metro Ethernet e Wireless. Patentes no ano: 447. O número de academias recua um pouco mas continua acima de dez mil. A receita neste ano foi de US\$22 bilhões. O número de funcionário mantém estável com 34371.
- **2005:** a empresa compra a *Scientific Atlanta*, líder no segmento de vídeo digital. Patentes no ano: 469. O número de academias continua recuando, mas permanece com dez mil. A receita foi de US\$24,8 bilhões e o número de funcionários aumentou para 38813.
- **2006:** a Cisco anuncia o lançamento dos produtos de Telepresença. O número de academias permanece em dez mil. As patentes dão um salto e vão para 688 no ano. A receita aumenta para US\$28,5 bilhões e o número de funcionários vai para 51840.
- **2007:** o número de patentes continua alto com 647. O número de academias permanece constante. A Cisco firma-se como uma das maiores detentoras de patentes do mundo, com média superior a quinhentas por ano nos últimos três anos. O número de funcionários aumenta para 63050 [11].

3.3. Portfolio

A empresa possui um grande portfolio, destacando-se os comutadores de camada dois, os de camada três e os roteadores. Além dessas linhas de produtos, a Cisco possui serviços de aplicação de redes, gerenciamento de redes, software relacionado aos dispositivos de redes, o IOS (*Internetwork Operating System*), segurança de redes, entre outros. Outros produtos da Cisco são

as certificações CCNA (*Cisco Certified Network Associate*), CCNP (*Cisco Certified Network Professional*) e CCIE (*Cisco Certified Network Expert*).

3.3.1. Comutadores de Camada Dois

O comutador, também conhecido como *switch*, é um dispositivo utilizado em redes de computadores para reencaminhar frames entre diversos nós da rede. Eles operam semelhantemente a um sistema telefônico com linhas privadas. Nesse sistema, quando uma pessoa liga para outra, a central telefônica as conectará em uma linha dedicada, possibilitando um maior número de conversações simultâneas. O comutador de camada dois opera apenas na camada de enlace de dados fazendo o *switching*, ou seja, encaminhando os pacotes de acordo como endereço MAC de destino.

Os comutadores de redes locais (LAN) fazem parte do núcleo da rede, fornecendo conectividade, aplicações e sistemas de comunicação de alto desempenho. Atualmente, as redes não necessitam somente ser eficientes e seguras para transmissão de dados, voz, vídeo e aplicações de *wireless*, elas precisam prever a evolução nos padrões de tráfego, novos serviços e otimização do desempenho de aplicativos. Para satisfazer as necessidades atuais e futuras das redes, o projeto de um *switch* de rede local deve possuir seis atributos:

- **Aplicação de Inteligência:** reconhecimento, priorização e controle são referidos como aplicação de inteligência.
- **Unificação dos Serviços de Rede:** combina os melhores elementos da conexão sem fio e com fio, para conectar qualquer recurso ou pessoa através de qualquer dispositivo compatível, unificando os serviços.
- **Comunicação Sem Interrupção:** recursos existentes e capacidades que ajudam a garantir que a comunicação não pare, como por exemplo, usar um hardware redundante.
- **Virtualização:** é necessário criar redes virtuais para que alguns recursos, comuns entre segmentos, possam ser compartilhados na mesma infra-estrutura.
- **Segurança Integrada:** os LAN *switches* fornecem a primeira linha de defesa contra ataques internos e também previne usuários não autorizados de entrar na rede.
- **Gerenciamento Operacional:** para aumentar a facilidade de gerenciamento, é necessário que os funcionários possam monitorar e configurar os dispositivos remotamente.

A Cisco possui *switches* de camada dois de diferentes portes, variando de pequenos a grandes aparelhos. Entre todas as famílias de *switches* da Cisco, destacam-se três linhas: 2960, 3560 e 3750. A seguir, será apresentada cada uma das linhas e suas funcionalidades.

Catalyst 2960: a série Cisco Catalyst 2960 (Figura 7), com inteligência Ethernet com o software de LAN Base, permite atuar em mais de um nível de rede, oferecendo melhora nos serviços de LAN. Esta família de configuração fixa, autônoma e dispositivo inteligente Ethernet com PoE (*Power over Ethernet*) oferece conectividade FastEthernet e GigaEthernet. Além disso, a série oferece segurança integrada, incluindo o controle de admissão de rede, o NAC (*Network Admission Control*); qualidade de serviço avançada, o QoS (*Quality of Service*); serviços inteligentes de redes de borda; garantia limitada do tempo de vida do hardware; atualizações do software sem custos adicionais. A linha Catalyst 2960 também oferece modelos menos sofisticados para empresas de pequeno porte, oferecendo conectividade FastEthernet, o que já é suficiente para redes locais simples, onde só necessita a conectividade entre os computadores [12].



Figura 7 – Cisco Catalyst 2960 [12].

Catalyst 3560: a série Cisco Catalyst 3560 (Figura 8) é uma linha de configuração fixa, possuindo a norma IEEE 802.3af e a funcionalidade básica da Cisco de energia com Ethernet (PoE) em configurações FastEthernet e GigaEthernet. Essa linha é ideal como comutadores de camada de acesso para pequenas empresas ou para ambientes de escritório. Combinando as velocidades de acesso e da PoE é possível uma melhora na produtividade e menos custos em investimentos, uma vez que o aparelho ajuda a implementar novas tecnologias, como a telefonia IP, acesso *wireless*, construção de sistema de gestão, entre outros. Além de oferecer o tradicional *switching* de redes locais, o Catalyst 3560 ainda oferece serviços inteligentes de rede como: qualidade de serviço avançada, o QoS; limitador de taxa de transferência; listas de controle de

acesso, o ACLs (*Access Control Lists*); roteamento de IP de alta performance; gerenciamento de multiacesso [12].



Figura 8 – Cisco Catalyst 3560 [12].

Cisco Catalyst 3750: a série Cisco Catalyst 3750 (Figura 9) é um produto inovador para companhias de médio porte. Dispondo da tecnologia Cisco *StackWise*, o *switch* melhora a eficiência operacional da LAN, combinando a facilidade do uso com a maior resiliência disponível para *switches* empilháveis. A tecnologia Cisco *StackWise* é uma revolucionária arquitetura de empilhamento que traz altos níveis de resiliência, automação e performance para *switches* empilháveis. Com essa tecnologia, os clientes podem criar uma única unidade de *switching* de 32 Gbps com até nove *switches* Cisco Catalyst 3750 [12].



Figura 9 – Cisco Catalyst 3750 [12].

3.3.2. Roteadores

O roteador de rede está evoluindo rapidamente a partir de um equipamento dedicado para conectar redes diferentes, a fim de ter um dispositivo de integração de serviços capaz de múltiplas

funções, além do roteamento. Atualmente, cada vez mais está se implantado roteadores de serviços integrados, ou seja, sofisticados roteadores de rede que podem encaminhar voz, vídeo, dados e acesso a internet, *wireless* e outras aplicações. Os roteadores de rede com soluções integradas possuem algumas características primordiais que são: em um único aparelho se consegue várias funções, como transmissão de dados, voz, vídeo, *wireless*, e avançados sistemas de segurança que garantem a qualidade de serviço (QoS); o roteador permite a mesma qualidade de acesso para quem está em rede local ou rede remota; gerenciamento centralizado, que permite um funcionário gerir a rede de um único lugar; e rede de segurança integrada, que transfere a responsabilidade de segurança dos computadores pessoais para a rede propriamente dita.

A Cisco possui roteadores de diferentes portes, variando de pequenos a grandes aparelhos. Entre todas as famílias de roteadores da Cisco destacam-se três famílias: 2800, 3800 e 7200. A seguir, será apresentada cada uma das linhas e suas funcionalidades.

Cisco 2800: a série de roteadores Cisco 2800 (Figura 10), ideal para pequenas e médias empresas ou empresas filiais, são projetados para possuir alta performance na entrega de vários serviços ao mesmo tempo, fazendo-os com alta segurança. Além disso, podem acomodar várias ligações E1/T1 para serviços, incluindo dados, segurança, voz, vídeo, entre outros. A arquitetura de roteamento de serviços integrados do Cisco 2800 oferece desempenho, disponibilidade e confiabilidade necessária para aplicações críticas de negócios, nos mais exigentes ambientes de mercado. Outras características que os roteadores possuem são: gerenciador de segurança de dispositivo, o SDM (*Security Device Manager*); uma plataforma modular com grandes opções de interface; possuem até duas conexões 10/100/1000 Mbps; possuem até sessenta e quatro portas de *switches* com conexões de 10/100 Mbps; possuem até 1500 túneis de VPN (*Virtual Private Network*); o suporte para wireless em redes locais conforme o padrão 802.11 a/b/g; Suporte para o SFP (*Small Form-Factor Pluggable*) para conexão Gigabit Ethernet.



Figura 10 – Família Cisco 2800 [12].

Cisco 3800: a série de roteadores de serviços integrados Cisco 3800 (Figura 11), ideal para médias e grandes empresas, ou empresas filiais, permite simplificar a implantação e a gestão, reduzir os custos e a complexidade da rede e suportar aplicações críticas de negócios, fornecendo uma plataforma altamente segura com ligações E3/T3 para a entrega de dados, voz, vídeo, segurança e wireless. A arquitetura de roteamento de serviços integrados do Cisco 3800 oferece desempenho, disponibilidade e confiabilidade necessária para aplicações críticas de negócios, nos mais exigentes ambientes de mercado. Outras características que os roteadores possuem são: gerenciador de segurança de dispositivo (SDM); uma plataforma modular com grandes opções de interface; possuem até duas conexões 10/100/1000 Mbps; possuem até cento e doze portas de *switches* com conexões de 10/100 Mbps; possuem até 2500 túneis de VPN; possuem o *Cisco CallManager Express*, que suporta o tráfego de até 240 telefones IP da Cisco; o suporte para wireless em redes locais conforme o padrão 802.11 a/b/g; suporte para o SFP para conexão Gigabit Ethernet.



Figura 11 – Família Cisco 3800 [12].

Cisco 7200: a série de roteadores de alta performance Cisco 7200 (Figura 12), ideal para grandes empresas, suporta uma grande densidade de informações e requisitos de serviços com alto desempenho. A maioria das grandes empresas do mundo utiliza roteadores de serviços agregados em suas aplicações, em especial o Cisco 7200, que oferece: uma boa relação custo/benefício; uma gama de opções de conectividade e inúmeros recursos, incluindo manutenção e gerenciamento de redes; melhora no desempenho de VPN com o novo adaptador de serviços de VPN. Outras características que os roteadores possuem são: MPLs (*Multiprotocol Label Switching*); possuem 5000 túneis de VPN; integração de dados, voz e vídeo; projeto modular; Flexibilidade, suportando Fast Ethernet, Giga Ethernet, pacotes sobre SONET, entre outros.



Figura 12 – Roteador Cisco 7200 [12].

3.3.3. Comutadores de Camada Três

O comutador de camada três possui as funções de *switching* e de roteamento ao mesmo tempo. Ao longo dos anos noventa, os comutadores evoluíram e integraram a função de roteamento. Embora esses equipamentos sejam roteadores, eles são conhecidos como comutadores de camada três. Ganharam esse nome, pois são feitos para rotear em redes locais. A diferença entre os roteadores comuns e os comutadores de camada três é que o roteador faz o processamento da camada três via software e o comutador faz via hardware, o que acelera muito o processamento (detalhes do processamento será visto no próximo capítulo). A Cisco Systems possui várias linhas de comutadores de camada três, destacando-se o Catalyst 4500. A seguir será apresentado o equipamento e suas funcionalidades.

Catalyst 4500: a série de *switches* Catalyst 4500 (Figura 13) estende um conjunto abrangente de serviços de rede inteligentes para redes de borda, ajudando empresas de todos os tamanhos a implantar segurança, unificar dados, voz e vídeo na rede. Suas principais características são: segurança unificada de informação; serviços inteligentes; escalabilidade; resiliência; gerente embutido de evento, simplificando eventos de rotina ou eventos extraordinários através de configurações; recursos operacionais; componentes *hot-swappable*, ou seja, componentes podem ser inseridos no equipamento sem precisar desligá-lo; capacidade de operar em IPv4 e IPv6.



Figura 13 – Família Cisco Catalyst 4500 [12].

4. Camadas Dois e Três

4.1. Camada Dois

A camada dois é responsável pelo *switching* dos pacotes de dados. Switching é uma tecnologia que diminui o congestionamento nas LANs, reduzindo o tráfego e aumentando a largura de banda. Como visto, é nessa camada que se encontram os comutadores, também conhecidos como switches. Esses equipamentos fazem o *switching* e a manutenção das operações de *switching*, gerando principalmente uma melhora na eficiência das LANs. Os comutadores são projetados para trabalhar em LANs com infraestruturas de cabos que já existam nelas, para que possam ser instalados sem afetar o tráfego existente na rede. Em uma rede que não possui equipamentos de camada dois ou superior, ao se enviar uma informação, ela será enviada a todos os computadores da rede, gerando grande fluxo e causando colisões. Ao se utilizar um comutador de camada dois, ele “aprende” os caminhos das informações através do endereço MAC e cria uma tabela com o endereço MAC de cada computador que está na rede. Assim, quando um computador A enviar um pacote de informação para o computador B, o comutador não enviará para os outros computadores, apenas para o computador de destino. Com isso, há uma grande redução no tráfego de informações e colisões (Figura 14).

Existem dois métodos de switching para encaminhar um quadro através de um comutador. O primeiro método é conhecido como Armazenar e encaminhar, pois todo o quadro é recebido antes de ocorrer qualquer encaminhamento. A latência ocorrerá enquanto o quadro estiver sendo recebido, sendo maior para quadros maiores. Apesar de ocorrer uma latência relativamente alta, este método possibilita maior detecção de erros, uma vez que há mais tempo disponível para o comutador verificar os erros. O outro método é conhecido como *Cut-through*, onde o comutador lê o endereço de destino antes de receber todo o quadro. Com isso, o quadro começa a ser encaminhado antes que esteja completamente lido. Desta forma, é possível diminuir a latência de transmissão, mas em compensação há uma menor detecção de erros devido ao tempo de latência.

Existem duas formas de encaminhamento *Cut-through*, o *Fast-forward* e o *Fragment-free*. O *switching Fast-forward* oferece o nível mais baixo de latência encaminhando imediatamente um pacote após ter recebido o endereço de destino. Como o método começa a encaminhar antes que todo o pacote seja recebido, pode haver vezes em que os pacotes sejam retransmitidos com erros. Embora isso não ocorra com frequência e a placa de rede de destino descarte o pacote com defeito ao recebê-lo, o tráfego supérfluo pode ser considerado inaceitável em alguns ambientes. Neste método, a latência é medida a partir do primeiro bit recebido até o primeiro bit transmitido,

ou primeiro a entrar, primeiro a sair (FIFO, *first in, first out*). O *switching fragment-free* filtra os fragmentos da colisão, que são a maioria dos erros do pacote, antes do encaminhamento começar. Em uma rede funcionando apropriadamente, os fragmentos de colisão devem ser menores que sessenta e quatro bytes. Qualquer valor maior que sessenta e quatro bytes é um pacote válido e é normalmente recebido sem erro. Este método aguarda até que o pacote recebido seja reconhecido como não sendo um fragmento de colisão antes de encaminhá-lo. A latência também é medida pela FIFO.

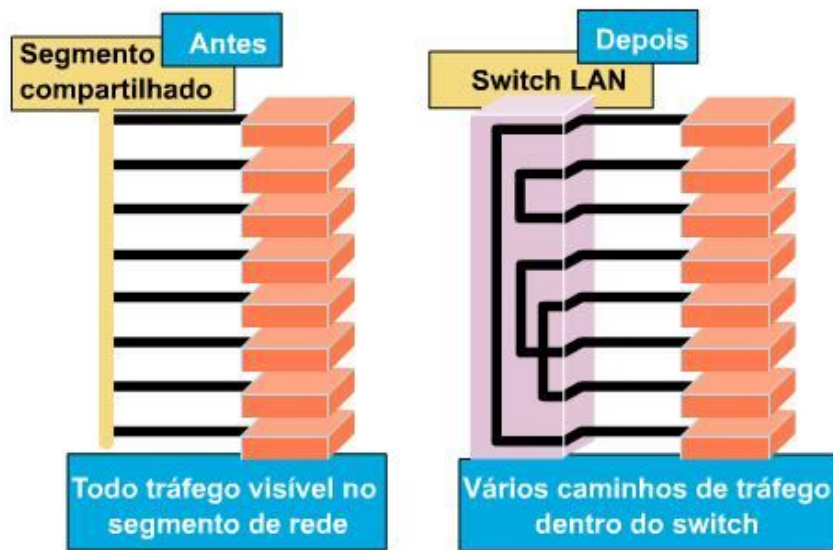


Figura 14 – Segmento de rede sem e com dispositivo de *switching* [5].

Apesar de melhorar a eficiência da rede, o uso simples de um comutador na rede não diminuiu o domínio de *broadcast*. Uma segmentação tradicional de LAN não agrupa os usuários de acordo com a associação do grupo de trabalho ou necessidade de largura de banda. Dessa forma, eles compartilham o mesmo segmento e competem pela mesma largura de banda, embora os requisitos de largura de banda variem bastante conforme o grupo de trabalho ou departamento. Com o aumento no número de usuários em uma mesma rede, a eficiência desta diminuiu muito e seu gerenciamento se torna complicado. Para solucionar este problema criou-se a VLAN (*Virtual Local Area Network*).

Uma VLAN é um agrupamento lógico de dispositivos ou usuários que podem ser agrupados por função, departamento ou aplicativo, independentemente da localização de seus segmentos físicos. A configuração da VLAN é feita no comutador através de software. As principais diferenças entre as LANs tradicionais e as VLANs são: as VLANs operam nas camadas dois e

três do modelo OSI, proporcionam métodos para controle de *broadcasts* na rede, aumentam a segurança da rede definindo quais nós da rede podem se comunicar com os outros e o administrador da rede controla o fluxo de usuários. Para se fazer a comunicação entre uma VLAN e outra é necessário um dispositivo de camada três, podendo-se utilizar roteadores ou comutadores de camada três. Essas funcionalidades dos dispositivos de camada três serão apresentadas durante o capítulo. Os comutadores são um dos principais componentes das comunicações de VLAN. Cada comutador tem inteligência para filtrar e encaminhar as decisões por quadro, baseado em métricas de VLAN definidas por gerentes da rede. O comutador também pode comunicar essas informações a outros comutadores e roteadores dentro da rede.

As maneiras mais comuns de agrupar logicamente os usuários em diferentes VLANs são a filtragem de quadros e a identificação de quadros (marcação de quadros). Ambas as técnicas examinam o quadro quando é recebido ou encaminhado pelo comutador. Baseados no conjunto de regras definidas pelo administrador, essas técnicas determinam para onde o quadro deve ser enviado, filtrado ou feito o *broadcast*. Esses mecanismos de controle podem ser administrados centralmente (com *software* de gerenciamento de rede) e são facilmente implementados por toda a rede. A filtragem de quadros examina determinadas informações sobre o quadro. Após isso, uma tabela de filtragem é desenvolvida para cada comutador, fornecendo um controle administrativo de alto nível, pois pode examinar vários atributos de cada quadro. Esse modelo não foi bem balanceado, pois cada quadro era obrigado a se referenciar a uma tabela de filtragem. A marcação de quadros atribui exclusivamente uma identificação de VLAN para cada quadro. As identificações de VLAN são atribuídas a cada VLAN na configuração do comutador através do administrador. Essa técnica foi escolhida pelo grupo de padrões do IEEE (*Institute of Electrical and Electronic Engineers*) por causa da sua escalonabilidade [5].

A marcação de quadros de VLAN é uma abordagem que foi desenvolvida especificamente para comunicações comutadas. A marcação de quadros coloca um identificador único no cabeçalho de cada quadro (Figura 15) à medida que é encaminhado através do *backbone* da rede. O identificador é reconhecido e examinado por cada comutador antes de cada *broadcast* ou transmissão para outros comutadores, roteadores ou dispositivos de final de estação. Quando o quadro sai do *backbone* da rede, o comutador retira o identificador antes que o quadro seja transmitido para a estação de destino final. A identificação de quadros requer pouco processamento ou sobrecarga administrativa.

Starting Delimiter (1 byte)	Destination Address (6 bytes)	Source Address (6 bytes)	Length (2 bytes)	LLC header and Information field (46 - 1500 bytes)	Frame Check Sequence (4 bytes)
--------------------------------	----------------------------------	-----------------------------	---------------------	---	-----------------------------------

Figura 15 – Cabeçalho de um quadro de camada dois [13].

Uma VLAN forma uma rede com comutação que é logicamente segmentada por funções, equipes de projetos ou aplicativos, sem levar em consideração a localização física dos usuários. Cada porta do comutador pode ser atribuída a uma VLAN. As portas atribuídas à mesma VLAN compartilham *broadcasts*. As portas que não pertencem a essa VLAN não compartilham esses *broadcasts*. Isso melhora o desempenho geral da rede. Há três métodos de implementação de portas de um comutador a uma VLAN, que são os Centrado em porta, Estático e o Dinâmico.

O método centrado em porta (Figura 16) consiste em um método onde uma mesma identificação de VLAN é atribuída a todos o nós conectados às portas na mesma VLAN. Este método facilita a administração da rede e a torna mais eficiente, pois os usuários são atribuídos por porta, fornecendo mais segurança entre as VLANs e os pacotes não “vazam” informações para outros domínios. As VLANs estáticas são portas em um comutador onde se atribui estaticamente a uma VLAN. Essas portas mantêm as configurações de VLAN atribuídas até que o administrador as mude. Embora as VLANs estáticas requeiram alterações do administrador, elas são seguras e fáceis de configurar. Elas operam bem em redes onde os movimentos são controlados e gerenciados. Por fim, as VLANs dinâmicas são portas de um comutador que podem determinar automaticamente suas atribuições de VLAN. As funções das VLAN dinâmicas são baseadas em endereços MAC, endereçamento lógico ou tipo de protocolo dos pacotes de dados. Quando uma estação for conectada inicialmente a uma porta de comutador não atribuída, o comutador apropriado verificará a entrada do endereço MAC no banco de dados de gerenciamento da VLAN e configurará dinamicamente a porta com a configuração de VLAN correspondente. As maiores vantagens desse método é uma menor necessidade de administração quando um usuário não reconhecido for adicionado à rede. Geralmente será necessária maior administração para configurar os dados dentro de um software de gerenciamento da VLAN e para manter um banco de dados de todos os usuários da rede.

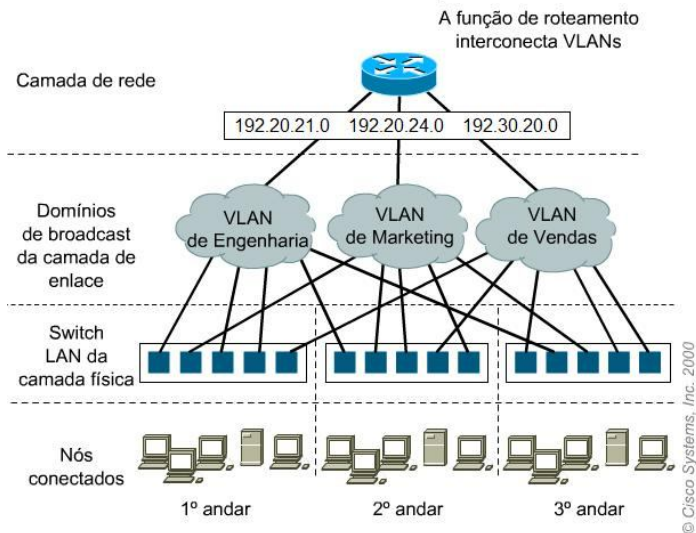


Figura 16 – Esquema de VLAN com implementação Centrado em porta [5].

4.2. Camada Três

A camada três é responsável pelo roteamento dos pacotes de dados. O roteamento é a principal forma utilizada na internet para a entrega de pacotes de dados entre *hosts*. O modelo de roteamento utilizado é o de salto-por-salto (*hop-by-hop*), onde cada roteador que recebe um pacote de dados abre-o, verifica o endereço de destino no cabeçalho IP, calcula o próximo salto que vai deixar o pacote um passo mais próximo de seu destino e entrega o pacote neste próximo salto. Este processo se repete e assim segue até a entrega do pacote ao seu destinatário. No entanto, para que este processo funcione, são necessários dois elementos: tabelas de roteamento e protocolos de roteamento. Tabelas de roteamento (Figura 17) são registros de endereços de destino associados ao número de saltos até ele, podendo conter várias outras informações.

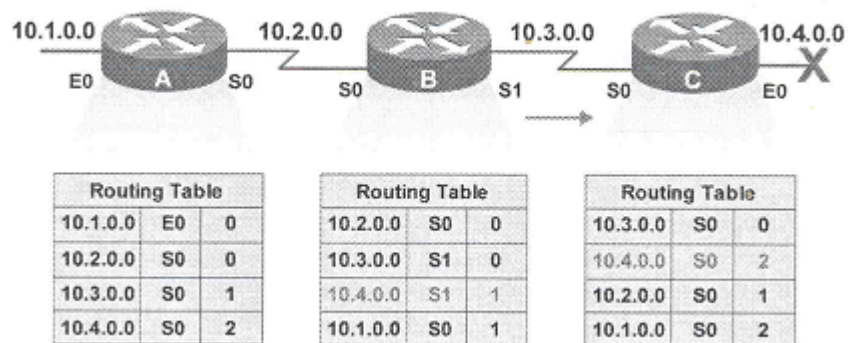


Figura 17 – Tabela de roteamento [14].

Protocolos de roteamento são protocolos que servem para trocar informações de construção de uma tabela de roteamento. É importante ressaltar a diferença entre protocolo de roteamento e protocolo roteável. Protocolo roteável é aquele que fornece informação adequada em seu endereçamento de rede para que seus pacotes sejam roteados, como o TCP/IP e o IPX. Protocolo de roteamento possui mecanismos para o compartilhamento de informações de rotas entre os dispositivos de roteamento de uma rede, permitindo o roteamento dos pacotes de um protocolo roteado. Exemplos de protocolos de roteamento são: RIP (*Routing Information Protocol*), IGRP, EIGRP (*Enhanced IGRP*), OSPF (*Open Shortest Path First*), IS-IS (*Intermediate System to Intermediate System Routing Exchange Protocol*), BGP.

O protocolo de roteamento RIP foi desenvolvido pela Xerox Corporation no início dos anos oitenta para ser utilizado nas redes XNS (*Xerox Network Systems*), e hoje em dia, é o protocolo intradomínio mais comum, sendo suportado por praticamente todos os fabricantes de roteadores e disponível na grande maioria das versões mais atuais do sistema operacional UNIX. Um dos seus benefícios é a facilidade de configuração. Além disso, seu algoritmo não necessita grande poder de comutação e capacidade de memória em roteadores ou computadores. O protocolo RIP funciona bem em pequenos ambientes, porém apresenta sérias limitações quando utilizado em grandes redes. Ele limita o número de saltos entre *hosts* a quinze. Outra deficiência é a lenta convergência, ou seja, leva relativamente muito tempo para que alterações na rede fiquem sendo conhecidas por todos os roteadores. Essa lentidão pode causar *loops* de roteamento, por causa da falta de sincronia nas informações dos roteadores. O protocolo é também um grande consumidor de largura de banda, pois, a cada trinta segundos, ele faz um *broadcast* de sua tabela de roteamento, com informações sobre as redes e sub-redes que alcança. Por fim, o RIP determina o melhor caminho entre dois pontos levando em consideração somente o número de saltos. Esta técnica ignora outros fatores que fazem diferença nas linhas entre dois pontos como, por exemplo, a velocidade de tráfego.

O IGRP também foi criado no início dos anos oitenta pela Cisco Systems Inc.. Este protocolo resolveu grande parte dos problemas associados ao uso do RIP para roteamento interno. O algoritmo utilizado pelo IGRP determina o melhor caminho entre dois pontos dentro de uma rede examinando a largura de banda e o atraso das redes entre roteadores. Ele converge mais rapidamente que o RIP, evitando *loops* de roteamento, e não tem limitação de saltos entre roteadores. Com estas características, o IGRP viabilizou a implementação de redes grandes, complexas e com diversas topologias.

A Cisco aprimorou ainda mais o protocolo IGRP para suportar maiores redes, complexas e críticas e criou o EIGRP. Este protocolo combina protocolos de roteamento baseados em vetor de

distância com os mais recentes protocolos baseados no algoritmo de estado de enlace. Ele também proporciona economia de tráfego por limitar a troca de informações de roteamento àquelas que foram alteradas. Uma desvantagem do EIGRP, assim como o IGRP, é que ambos são de propriedade da Cisco, não sendo amplamente disponíveis fora dos equipamentos deste fabricante.

O OSPF foi desenvolvido pelo IETF (*Internet Engineering Task Force*) como substituto para o protocolo RIP. Caracteriza-se por ser um protocolo intra-domínio, hierárquico, baseado no algoritmo de estado de enlace e foi especificamente projetado para operar com redes grandes. Outras características do protocolo são: A inclusão de roteamento por tipo de serviço. Por exemplo, um acesso FTP poderia ser feito por um *link* de satélite, enquanto que um acesso a terminal poderia evitar este *link*, que tem grande tempo de retardo, e ser feito através de outro enlace; O fornecimento de balanceamento de carga, que permite ao administrador especificar múltiplas rotas com o mesmo custo para um mesmo destino. O protocolo distribui o tráfego igualmente por todas as rotas; O suporte à rotas para *hosts*, sub-redes e redes específicas; A possibilidade de configuração de uma topologia virtual de rede, independente da topologia das conexões físicas. Por exemplo, um administrador pode configurar um *link* virtual entre dois roteadores mesmo que a conexão física entre elas passe através de uma outra rede; A utilização de pequenos “*hello packets*” para verificar a operação dos *links* sem ter que transferir grandes tabelas. Em redes estáveis, as maiores atualizações ocorrem uma vez a cada trinta minutos.

O protocolo ainda especifica que todos os anúncios entre roteadores sejam autenticados, ou seja, devem refletir a realidade das implementações. Permite mais de uma variedade de esquema de autenticação e que diferentes áreas de roteamento utilizem esquemas diferentes de autenticação. Duas desvantagens deste protocolo são a sua complexidade, e maior necessidade por memória e poder computacional, característica inerente aos protocolos que usam o algoritmo de estado de enlace.

O OSPF suporta, ainda, roteamento hierárquico de dois níveis dentro de um sistema autônomo, possibilitando a divisão do mesmo em áreas de roteamento. Uma área de roteamento é tipicamente uma coleção de uma ou mais sub-redes intimamente relacionadas. Todas as áreas de roteamento precisam estar conectadas ao *backbone* do sistema autônomo, no caso, a Área 0. Se o tráfego precisar viajar entre duas áreas, os pacotes são primeiramente roteados para a Área 0. Isto pode não ser bom, uma vez que não há roteamento interareas enquanto os pacotes não alcançam o *backbone*. Chegando a Área 0, os pacotes são roteados para a Área de destino, que é responsável pela entrega final. Esta hierarquia permite a consolidação dos endereços por área, reduzindo o

tamanho das tabelas de roteamento. Redes pequenas, no entanto, podem operar utilizando uma única área OSPF.

O protocolo IS-IS, assim como o OSPF, é um protocolo intra-domínio, hierárquico e que utiliza o algoritmo de estado de enlace. Pode trabalhar sobre várias sub-redes, inclusive fazendo o *broadcasting* para LANs, WANs (*Wide Area Network*) e *links* ponto-a-ponto.

O BGP é um protocolo de roteamento interdomínios, criado para uso nos roteadores principais da internet. O protocolo foi projetado para evitar *loops* de roteamento em topologias arbitrárias. Ele faz o roteamento baseado em política (*policy-based routing*), um roteamento com base em um conjunto de regras não técnicas, definidas pelos sistemas autônomos. A última versão do BGP, o BGP4, foi projetado para suportar os problemas causados pelo grande crescimento da internet [15].

Como apresentado anteriormente, o protocolo IP possui trinta e dois bits e está dividido em classes. Ele é utilizado para criar redes, uma vez *hosts* com o mesmo endereço de rede IP estão na mesma rede. Porém, às vezes, é necessário fazer com que uma rede grande se divida em redes menores a fim de diminuir o domínio de *broadcast*. Para este fim foi desenvolvida a sub-rede. Assim como a VLAN de camada dois divide a rede em partes menores, a sub-rede também o faz. Para se criar uma sub-rede é necessário três procedimentos básicos: determinar o número de bits de *hosts* a serem usados para sub-redes; listar as novas identificações de sub-redes; listar os endereços IPs para cada nova identificação de sub-rede.

O número de bits de *host* usado para sub-redes determinará o número de sub-redes possíveis e o número de *hosts* por sub-rede. Quanto mais bits de *host* forem usados para sub-redes, mais sub-redes serão criadas e menos *hosts* por sub-redes serão criados, diminuindo o tráfego de *broadcast*. Utilizando um IP de classe C pode-se dividir a rede em seis tipos de sub-redes. Os tipos serão mostrados na tabela a seguir:

Tabela 1 – Sub-redes de Classe C

Número de sub-redes	Número de bits para sub-rede	Máscara de sub-rede	Número de hosts por sub-rede
1-2	1	255.255.255.128 ou /25	126
3-4	2	255.255.255.192 ou /26	62
5-8	3	255.255.255.224 ou /27	30
9-16	4	255.255.255.240 ou /28	14
17-32	5	255.255.255.248 ou /29	6
33-64	6	255.255.255.252 ou /30	2

Após escolher o número de bits de *host* a ser usado nas sub-redes, devem-se listar as novas identificações de rede disponíveis, ou seja, listar quais endereços IPs serão conhecidos como os endereços de rede de cada sub-rede. A lista pode ser criada a partir de dois métodos: o binário e o decimal. O método binário lista todas as combinações de bits de *host* escolhidos para a subdivisão e converte cada combinação na notação decimal pontuada. O método decimal adiciona um valor incremental calculado para cada identificação de sub-rede sucessiva e converte na notação decimal pontuada. Como exemplo, tem-se a Tabela 2.

Tabela 2 – Método binário de subdivisão de rede para uma rede de Classe B

Sub-rede	Representação binária	Identificação de sub-rede
1	11000000.10101000. <u>000</u> 00000.00000000	192.168.0.0/19
2	11000000.10101000. <u>001</u> 00000.00000000	192.168.32.0/19
3	11000000.10101000. <u>010</u> 00000.00000000	192.168.64.0/19
4	11000000.10101000. <u>011</u> 00000.00000000	192.168.96.0/19
5	11000000.10101000. <u>100</u> 00000.00000000	192.168.128.0/19
6	11000000.10101000. <u>101</u> 00000.00000000	192.168.160.0/19
7	11000000.10101000. <u>110</u> 00000.00000000	192.168.192.0/19
8	11000000.10101000. <u>111</u> 00000.00000000	192.168.224.0/19

Após listar todas as identificações de sub-rede, devem-se listar os endereços IPs válidos para as novas identificações de sub-rede. Para isto, existem dois métodos de listagem: o binário e o decimal. O método binário escreve o primeiro e o último endereço para cada identificação de sub-rede e os converte para a notação decimal pontuada. O método decimal adiciona valores incrementais, correspondentes ao primeiro e ao último endereço IP para cada identificação de sub-rede e os converte para a notação decimal pontuada. Como exemplo, tem-se a tabela 3.

Tabela 3 – Método decimal para listagem dos endereços IPs para uma rede de Classe B

Sub-rede	Representação decimal	Faixa de endereços IPs
1	3232235521 - 3232243710	192.168.0.1 - 192.168.31.254
2	3232243713 - 3232251902	192.168.32.1 - 192.168.63.254
3	3232251905 - 3232260094	192.168.64.1 - 192.168.95.254
4	3232260097 - 3232268286	192.168.96.1 - 192.168.127.254
5	3232268289 - 3232276478	192.168.128.1 - 192.168.159.254
6	3232276481 - 3232284670	192.168.160.1 - 192.168.191.254
7	3232284673 - 3232292862	192.168.192.1 - 192.168.223.254
8	3232292865 - 3232301054	192.168.224.1 - 192.168.255.254

Com o uso de sub-redes, além de diminuir o domínio de *broadcast* ainda permite a sumarização de rotas, evitando tabelas de roteamento mal feitas e facilitando o trabalho dos roteadores. Por exemplo, em uma LAN existem três redes diferentes, com endereços de rede diferentes. Um roteador ao enviar informações aos roteadores vizinhos terá que mandar a sua tabela de roteamento com seus três endereços de rede. Mas ao usar sub-rede para separar essas três redes diferentes, o roteador ao enviar sua tabela para outro roteador terá que mandar apenas um endereço de rede, facilitando assim o fluxo de informações entre os roteadores e diminuindo sobrecarga de informação.

O uso de dispositivos de camada três em VLANs é indispensável, pois eles fornecem rotas de conexão entre VLANs diferentes. Além disso, fornecem firewalls, fazem o gerenciamento de *broadcast* e distribuição e processamento de rotas. Eles também se conectam a outras partes de rede, que podem ser logicamente segmentadas com uma abordagem mais tradicional de sub-rede ou que requeiram acesso a sites remotos através de *links* de longa distância. Existem dois dispositivos de camada três que possuem essa função em VLANs: o roteador tradicional e o comutador de camada três. A grande diferença entre estes dois equipamentos está contida no cabeçalho de camada três. Enquanto o processamento do cabeçalho do roteador tradicional é feito através de software, o processamento do cabeçalho do comutador de camada três é feito por hardware. Abaixo é mostrada uma figura do cabeçalho do roteador tradicional:

0	4	8	16	19	24	31
VERS	HLEN	Tipo de serviço		Tamanho total		
Identificação			Sinalizadores	Fragmento Deslocamento		
Tempo de vida		Protocolo	Checksum do cabeçalho			
Endereço IP da origem						
Endereço IP do destino						
Opções de IP (se houver)					Enchimento	
Dados						
...						

Figura 18 – Cabeçalho camada três de um roteador tradicional [5].

O processamento do cabeçalho no roteador tradicional é feito por software, pois tem que se analisar o campo Opções de IP, que não possui tamanho fixo. Com isso há uma latência no processamento até identificar em qual bit começa o campo Dados. No comutador de camada três, o campo Opções de IP é inexistente. Como todos os outros campos possuem tamanho fixo, não há necessidade de processamento algum e o comutador pode encaminhar os dados rapidamente.

5. Conclusão

As redes de computadores são de extrema importância nos dias atuais, uma vez que toda a sociedade depende dela, sejam em uma compra em um supermercado com cartão de crédito, transações bancárias, troca de informações entre pessoas, telefonia fixa e móvel, entre outros. Este trabalho apresentou os modelos de referência OSI e TCP/IP, mostrando em detalhes cada camada dos modelos e suas interações. Foi mostrado a empresa Cisco Systems e seu portfólio. Mostrou-se uma comparação entre a evolução da empresa e a evolução da internet, mostrando o quão importante é essa empresa. Foram estudadas também, as camadas dois e três do modelo OSI, mostrando algumas funções de redes de computadores, como VLAN e sub-rede. Pode-se compreender que com o uso de VLANs é possível diminuir o domínio de *broadcast* e aumentar a largura de banda de transmissão. A sub-rede possui o mesmo objetivo que as VLANs, porém, é instalada na camada três, onde há segmentação lógica das redes. Foram estudados os tipos de protocolos de roteamento e em quais ambientes trabalham, partindo do RIP que é um protocolo simples, porém muito limitado, até protocolos como o BGP, usado para grandes redes e muito complexos.

6. Bibliografia

- [1] <http://www.guiadohardware.net/tutoriais/historia-redes/>, acessado em 23/09/08
- [2] http://pt.wikipedia.org/wiki/Modelo_OSI, acessado em 04/10/08
- [3] Andrew S. Tanenbaum, Redes de Computadores, 4ª Ed, 2003, Editora Campus
- [4] Tania Regina Tronco, Redes de Nova Geração, 1ª Ed, 2006, Editora Érica
- [5] Programa Cisco Networking Academy, CCNA 1º semestre v2.1
- [6] Wendell Odom, Cisco CCNA - Guia de Certificação do Exame CCNA, 1ª Ed, 2002
- [7] http://www.projetoderedes.com.br/artigos/artigo_criptografia_simetrica.php, acessado 05/10/08
- [8] <http://www.mspc.eng.br/info/net110.shtml>, acessado em 05/10/08
- [9] <http://www.clubedohardware.com.br>, acessado em 10/10/08
- [10] http://pt.wikipedia.org/wiki/Cisco_Systems, acessado em 14/10/08
- [11] <http://blog.ccna.com.br/2008/08/20/cisco-linha-do-tempo/>, acessado em 14/10/08
- [12] <http://www.cisco.com>, acessado em 14/10/08
- [13] <http://en.wikipedia.org/wiki/Ethernet>, acessado em 03/11/2008
- [14] www.qta.ufri.br, acessado em 05/11/2008
- [15] <http://www.rnp.br/newsgen/9705/n1-1.html>, acessado em 05/11/2008