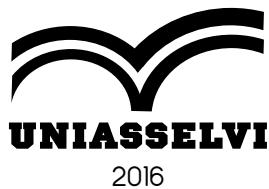


FUNDAMENTOS DE REDES DE COMPUTADORES

Unidade 1: Prof. Edemilson Bay

Unidades 2 e 3: Prof. Paulo Henrique Bluning





Copyright © UNIASSELVI 2016

Elaboração:

Unidade 1: Prof. Edemilson Bay

Unidades 2 e 3: Prof. Paulo Henrique Bluning

Revisão, Diagramação e Produção:

Centro Universitário Leonardo da Vinci – UNIASSELVI

Ficha catalográfica elaborada na fonte pela Biblioteca Dante Alighieri
UNIASSELVI – Indaial.

004.6
B356f Bay; Edemilson

Fundamentos de redes de computadores/ Edemilson
Bay; Paulo Henrique Bluning : UNIASSELVI, 2016.

215 p. : il.

ISBN 978-85-7830-963-3

1. Redes de computadores.
I. Centro Universitário Leonardo Da Vinci.

APRESENTAÇÃO

Caro(a) acadêmico(a)!

Seja bem-vindo(a) ao Caderno de Estudos da disciplina de Fundamentos de Redes de Computadores.

Estamos iniciando os estudos nesta disciplina, cuja importância para um profissional na área de informática é bastante grande. Atualmente os sistemas computacionais estão cada vez mais integrando diversas máquinas, que podem estar próximas entre si ou muito distantes fisicamente. Aplicações as mais diversas são desenvolvidas levando em consideração a necessidade de troca de informações entre os computadores e também entre seus usuários.

Hoje em dia, são as redes de computadores que suportam o desenvolvimento de praticamente todos os ramos de negócios, como indústria, comércio, financeiro, serviços etc. As atividades de empresas privadas são baseadas no funcionamento de redes de comunicação privativas ou na rede Internet, que é uma rede pública, assim como as atividades de órgãos públicos também o são. Dessa forma, os profissionais envolvidos com tecnologia da informação devem ter no mínimo conhecimentos básicos sobre redes de computadores. Esta disciplina objetiva proporcionar uma aprendizagem autônoma sobre fundamentos de redes de computadores, estando este caderno dividido em três unidades.

A Unidade 1 apresenta os principais conceitos sobre comunicação de dados e redes de computadores para facilitar o entendimento do conteúdo existente nas Unidades 2 e 3. Os componentes das redes de computadores, essenciais para o funcionamento das mesmas, também são estudados nessa unidade.

A Unidade 2 do caderno relaciona e descreve as normas desenvolvidas para utilização em redes e os órgãos responsáveis pelas mesmas, assim como os principais protocolos para comunicação de dados em ambiente de rede. Também, os principais equipamentos e dispositivos que permitem a construção e funcionamento das redes de computadores são estudados.

A Unidade 3 contém conceitos importantes sobre as redes locais (LAN), redes de longa distância (WAN) e redes sem fio (Wireless), além de apresentar princípios e noções sobre a segurança em redes de computadores, muito importante para garantir a disponibilidade e inviolabilidade das informações de empresas, órgãos públicos e usuários em geral.

Temos o objetivo, com os assuntos abordados, de contribuir com sua formação acadêmica e com o desenvolvimento de competências, habilidades e atitudes que tornem você um profissional mais preparado e alinhado com as necessidades do mercado.

Desejamos bons estudos e sucesso na sua vida acadêmica e profissional!

Prof. Edemilson Bay
Prof. Paulo Henrique Bluning



Você já me conhece das outras disciplinas? Não? É calouro? Enfim, tanto para você que está chegando agora à UNIASSELVI quanto para você que já é veterano, há novidades em nosso material.

Na Educação a Distância, o livro impresso, entregue a todos os acadêmicos desde 2005, é o material base da disciplina. A partir de 2017, nossos livros estão de visual novo, com um formato mais prático, que cabe na bolsa e facilita a leitura.

O conteúdo continua na íntegra, mas a estrutura interna foi aperfeiçoada com nova diagramação no texto, aproveitando ao máximo o espaço da página, o que também contribui para diminuir a extração de árvores para produção de folhas de papel, por exemplo.

Assim, a UNIASSELVI, preocupando-se com o impacto de nossas ações sobre o ambiente, apresenta também este livro no formato digital. Assim, você, acadêmico, tem a possibilidade de estudá-lo com versatilidade nas telas do celular, *tablet* ou computador.

Eu mesmo, UNI, ganhei um novo *layout*, você me verá frequentemente e surgirei para apresentar dicas de vídeos e outras fontes de conhecimento que complementam o assunto em questão.

Todos esses ajustes foram pensados a partir de relatos que recebemos nas pesquisas institucionais sobre os materiais impressos, para que você, nossa maior prioridade, possa continuar seus estudos com um material de qualidade.

Aproveito o momento para convidá-lo para um bate-papo sobre o Exame Nacional de Desempenho de Estudantes – ENADE.

Bons estudos!



Olá acadêmico! Para melhorar a qualidade dos materiais ofertados a você e dinamizar ainda mais os seus estudos, a Uniasselvi disponibiliza materiais que possuem o código *QR Code*, que é um código que permite que você acesse um conteúdo interativo relacionado ao tema que você está estudando. Para utilizar essa ferramenta, acesse as lojas de aplicativos e baixe um leitor de *QR Code*. Depois, é só aproveitar mais essa facilidade para aprimorar seus estudos!

BATE SOBRE O PAPO ENADE!



Olá, acadêmico!



Você já ouviu falar sobre o ENADE?

Se ainda não ouviu falar nada sobre o ENADE, agora você receberá algumas informações sobre o tema.

Ouviu falar? Ótimo, este informativo reforçará o que você já sabe e poderá lhe trazer novidades.



Vamos lá!



Qual é o significado da expressão ENADE?

EXAME NACIONAL DE DESEMPENHO DOS ESTUDANTES

Em algum momento de sua vida acadêmica você precisará fazer a prova ENADE.



Que prova é essa?



É **obrigatória**, organizada pelo INEP – Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira.

Quem determina que esta prova é obrigatória... O **MEC – Ministério da Educação**.

O objetivo do MEC com esta prova é o de avaliar seu desempenho acadêmico assim como a qualidade do seu curso.



Fique atento! Quem não participa da prova fica impedido de se formar e não pode retirar o diploma de conclusão do curso até regularizar sua situação junto ao MEC.

Não se preocupe porque a partir de hoje nós estaremos auxiliando você nesta caminhada.



Você receberá outros informativos como este, complementando as orientações e esclarecendo suas dúvidas.



Você tem uma trilha de aprendizagem do ENADE, receberá e-mails, SMS, seu tutor e os profissionais do polo também estarão orientados.

Participará de webconferências entre outras tantas atividades para que esteja preparado para #mandar bem na prova ENADE.

Nós aqui no NEAD e também a equipe no polo estamos com você para vencermos este desafio.

Conte sempre com a gente, para juntos mandarmos bem no ENADE!



SUMÁRIO

UNIDADE 1 – INTRODUÇÃO À COMUNICAÇÃO DE DADOS E REDES DE COMPUTADORES	1
TÓPICO 1 – CONCEITOS BÁSICOS DE COMUNICAÇÃO DE DADOS	3
1 INTRODUÇÃO	3
2 A COMUNICAÇÃO	4
2.1 O SISTEMA DE COMUNICAÇÃO	4
2.2 SINAIS ANALÓGICOS E SINAIS DIGITAIS	5
3 A TRANSMISSÃO DE DADOS	7
3.1 TÉCNICAS E TIPOS DE TRANSMISSÃO	7
3.2 MODOS DE TRANSMISSÃO	11
3.3 SENTIDOS DE TRANSMISSÃO	13
3.4 LARGURA DE BANDA E TAXA DE TRANSMISSÃO	14
4 MULTIPLEXAÇÃO	15
RESUMO DO TÓPICO 1	19
AUTOATIVIDADE	20
TÓPICO 2 – CONCEITOS BÁSICOS DE REDES DE COMPUTADORES	21
1 INTRODUÇÃO	21
2 DEFINIÇÃO E APLICAÇÕES DE REDE	23
3 CLASSIFICAÇÕES E TOPOLOGIAS DE REDES	28
3.1 CLASSIFICAÇÃO CONFORME A ABRANGÊNCIA GEOGRÁFICA	28
3.2 CLASSIFICAÇÃO CONFORME O OBJETIVO	32
3.3 TOPOLOGIAS DE REDES	34
4 OUTRAS CLASSIFICAÇÕES DE REDES	37
4.1 QUANTO AO ENDEREÇAMENTO	37
4.2 QUANTO AO TIPO DE COMUTAÇÃO	38
4.3 QUANTO À ARQUITETURA DE COMPARTILHAMENTO	41
RESUMO DO TÓPICO 2	44
AUTOATIVIDADE	45
TÓPICO 3 – COMPONENTES DAS REDES DE COMPUTADORES	47
1 INTRODUÇÃO	47
2 OS MEIOS FÍSICOS DE REDE	48
2.1 OS MEIOS GUIADOS	48
2.2 OS MEIOS NÃO GUIADOS	53
3 O HARDWARE DE REDE	56
4 O SOFTWARE DE REDE	59
LEITURA COMPLEMENTAR	60
RESUMO DO TÓPICO 3	62
AUTOATIVIDADE	63

UNIDADE 2 – NORMAS, PROTOCOLOS E EQUIPAMENTOS	65
TÓPICO 1 – NORMAS E ÓRGÃOS NORMATIZADORES	67
1 INTRODUÇÃO	67
2 PADRÕES	67
3 ÓRGÃOS NORMATIZADORES	68
4 PRINCIPAIS NORMAS EM REDES	69
RESUMO DO TÓPICO 1	72
AUTOATIVIDADE	73
TÓPICO 2 – PROTOCOLOS DE COMUNICAÇÃO	75
1 INTRODUÇÃO	75
2 SURGIMENTO DOS PROTOCOLOS	75
3 SERVIÇO X PROTOCOLO	76
4 MODELO DE REFERÊNCIA	77
4.1 MODELO DE REFERÊNCIA OSI	77
4.1.1 Camada Física	78
4.1.2 Camada de Enlace	79
4.1.3 Camada de Rede	79
4.1.4 Camada de Transporte	80
4.1.5 Camada de Sessão	80
4.1.6 Camada de Apresentação	80
4.1.7 Camada de Aplicação	81
4.2 MODELO DE REFERÊNCIA TCP/IP	81
4.2.1 Camada Internet	82
4.2.2 Camada de Transporte	83
4.2.3 Camada de Aplicação	83
4.2.4 Camada de Rede (ou Acesso à Rede)	84
5 PROTOCOLO DE COMUNICAÇÃO DA CAMADA DE TRANSPORTE (TCP E UDP)	84
5.1 UDP – User Datagram Protocol	85
5.2 TCP – Transmission Control Protocol	88
6 PROTOCOLOS DA CAMADA DE APLICAÇÃO	92
6.1 DNS – DOMAIN NAME SYSTEM	92
6.2 SMTP - Simple Mail Transfer Protocol	94
6.3 POP3 – POST OFFICE PROTOCOL VERSION 3	95
6.4 HTTP – PROTOCOLO DE TRANSFERÊNCIA DE HIPERTEXTO	97
6.5 FTP – FILE TRANSFER PROTOCOL	99
6.6 DHCP	100
7 PROTOCOLO IP (INTERNET PROTOCOL)	101
7.1 IPV4	102
7.1.1 Endereçamento IPv4	105
7.1.2 Sub-redes	110
7.2 IPV6	113
7.2.1 Cálculo de rede com IPv6	117
LEITURA COMPLEMENTAR	121
RESUMO DO TÓPICO 2	123
AUTOATIVIDADE	124
TÓPICO 3 – EQUIPAMENTOS DE REDE	125
1 INTRODUÇÃO	125
2 EQUIPAMENTOS DE REDE	125
2.1 HUB	125

2.2 <i>Switch</i>	127
2.3 ROTEADOR	129
LEITURA COMPLEMENTAR	133
RESUMO DO TÓPICO 3	136
AUTOATIVIDADE	137
UNIDADE 3 – REDES LANS, WANS, REDES SEM FIO E SEU GERENCIAMENTO	139
TÓPICO 1 – CONCEITO DE REDES LAN	141
1 INTRODUÇÃO	141
2 REDES LAN	141
3 ETHERNET	143
3.1 CSMA/CD: PROTOCOLO DE ACESSO MÚLTIPLO DA ETHERNET	145
3.2 SERVIÇOS ORIENTADOS E NÃO ORIENTADOS A CONEXÕES	146
RESUMO DO TÓPICO 1	149
AUTOATIVIDADE	150
TÓPICO 2 – CONCEITO DE REDES WAN	151
1 INTRODUÇÃO	151
2 REDE WAN	151
3 QoS (QUALITY OF SERVICE – QUALIDADE DE SERVIÇO)	153
4 MPLS (<i>Multi-Protocol Label Switching</i>)	154
RESUMO DO TÓPICO 2	157
AUTOATIVIDADE	158
TÓPICO 3 – CONCEITOS DE REDES WIRELESS	161
1 INTRODUÇÃO	161
2 CONCEITOS	161
3 HARDWARE SEM FIO	163
4 SEGURANÇA EM REDES SEM FIO	166
4.1 SEGURANÇA POR ENDEREÇO FÍSICO	166
4.2 SEGURANÇA POR CRIPTOGRAFIA	168
4.3 SEGURANÇA POR OCULTAÇÃO DE SSID	170
LEITURA COMPLEMENTAR	172
RESUMO DO TÓPICO 3	175
AUTOATIVIDADE	176
TÓPICO 4 – NOÇÕES DE GERENCIAMENTO DE REDES	177
1 INTRODUÇÃO	177
2 VISÃO GERAL	177
3 SOFTWARES DE GERENCIAMENTO	179
4 MONITORAMENTO E CONTROLE	190
5 PROTOCOLOS DE GERENCIAMENTO	190
5.1 SNMP	191
5.2 ICMP	196
6 INTERLIGAÇÃO DE REDES	200
LEITURA COMPLEMENTAR	207
RESUMO DO TÓPICO 4	209
AUTOATIVIDADE	210
REFERÊNCIAS	211

UNIDADE 1

INTRODUÇÃO À COMUNICAÇÃO DE DADOS E REDES DE COMPUTADORES

OBJETIVOS DE APRENDIZAGEM

A partir do estudo desta unidade você será capaz de:

- descrever conceitos relativos à comunicação de dados;
- relacionar e definir conceitos sobre redes de computadores;
- citar e explicar as classificações de redes e as topologias;
- entender os componentes que formam uma rede;
- relacionar os tipos de meios de transmissão mais utilizados;
- compreender os conceitos básicos sobre o *hardware* e o *software* de rede.

PLANO DE ESTUDOS

Esta unidade está dividida em três tópicos. Ao final de cada tópico você encontrará autoatividades, cujo objetivo é auxiliar na fixação dos principais conteúdos apresentados.

TÓPICO 1 – CONCEITOS BÁSICOS DE COMUNICAÇÃO DE DADOS

TÓPICO 2 – CONCEITOS BÁSICOS DE REDES DE COMPUTADORES

TÓPICO 3 – COMPONENTES DAS REDES DE COMPUTADORES



Assista ao vídeo
desta unidade.



CONCEITOS BÁSICOS DE COMUNICAÇÃO DE DADOS

1 INTRODUÇÃO

Caro(a) acadêmico(a), é muito importante que profissionais da área de TI (Tecnologia da Informação) conheçam os princípios de funcionamento das redes de comunicação, que hoje em dia não trafegam somente voz, mas evoluíram, e conseguem trafegar dados, imagens e vídeo.

Uma rede de comunicação é a base para que ocorra o processo de comunicação entre computadores ou entre dispositivos diversos. Essa comunicação pode ocorrer entre equipamentos que estejam a alguns metros de distância entre si, ou que estejam a milhares de quilômetros de distância entre si, no entanto o processo de comunicação é sempre o mesmo, com algumas pequenas variações conforme a tecnologia utilizada.

Neste tópico veremos o princípio de funcionamento da comunicação, que é baseado num modelo de processo genérico, sendo que este utiliza recursos semelhantes, não importando se a comunicação é entre seres humanos ou entre máquinas. Será estudada a diferença entre sinais analógicos e digitais, já que os equipamentos eletrônicos podem utilizar as duas formas de sinais, dependendo da aplicação.

Também serão apresentados vários conceitos importantes referentes à técnica de transmissão de dados em sistemas de comunicação, que são aplicados na comunicação entre redes de computadores. Por fim, neste tópico vamos estudar técnicas de multiplexação que viabilizaram o crescimento do volume de troca de informações nos sistemas de comunicação, através da otimização dos recursos de transmissão e redução dos custos envolvidos nas redes de telecomunicações, os quais são grandes.

Então, caro(a) acadêmico(a), vamos iniciar os estudos dessa fascinante e importante disciplina do mundo da informática?

2 A COMUNICAÇÃO

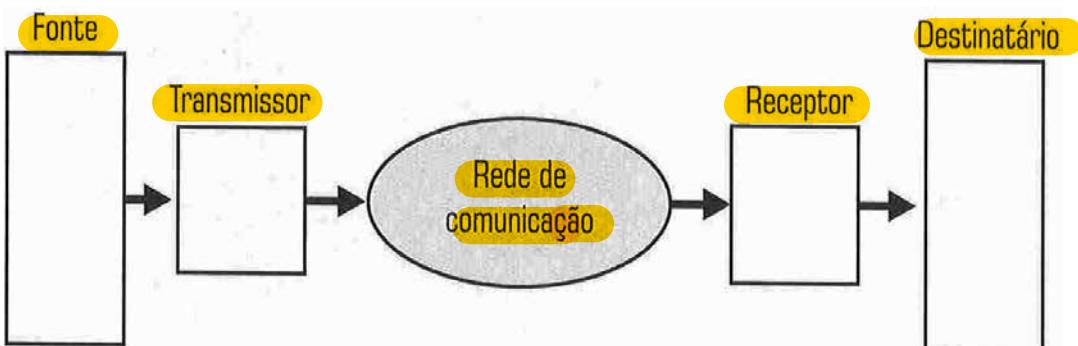
O ser humano, desde os primórdios, necessita comunicar-se. No passado utilizava processos de comunicação gestual e verbal somente, aprimorando o processo até chegar na comunicação escrita. Esta possui um conjunto de símbolos que, arranjados de maneira correta e seguindo regras, permitem a troca de informações e o registro das mesmas.

Observamos que, independente do processo de comunicação utilizado, sempre existe um formato semelhante para que seja viabilizada a comunicação, conforme veremos a seguir. Importante ressaltar que uma comunicação só ocorre quando a informação enviada é recebida e perfeitamente entendida.

2.1 O SISTEMA DE COMUNICAÇÃO

Quando existe a necessidade de troca de informações entre duas pessoas, ou entre dois computadores, por exemplo, sempre é adotado um formato semelhante para que ocorra o processo de comunicação. Isso pode ser representado através da Figura 1.

FIGURA 1 – MODELO GENÉRICO DE COMUNICAÇÃO



FONTE: Dantas (2002, p. 8)

O que podemos observar e concluir analisando a Figura 1? Que existem elementos definidos: a fonte, o transmissor, a rede de comunicação, o receptor e por fim o destinatário; e que o fluxo de informação é sempre de uma fonte para um destinatário. A fonte é responsável por gerar a informação que deve ser enviada, e pode ser uma pessoa, um computador ou outro equipamento. De acordo com Dantas (2010), deve existir um tratamento da informação gerada antes de ser enviada através da rede para se adequar ao meio de transmissão utilizado pela mesma.

Segundo Dantas (2010), o transmissor é responsável pela conversão da informação em alguma forma de sinal que possa ser transportado pela rede de comunicação, através de um processo de modulação para sinais analógicos ou um processo de codificação para sinais digitais. Isso pode ser feito por aparelhos telefônicos, *modems*, *codecs* (codificadores/decodificadores) de sinal e transmissores digitais ou analógicos. O sinal analógico ou digital será estudado mais adiante.

A rede de comunicação é responsável pelo transporte do sinal que contém a informação, do transmissor ao receptor, sendo o coração do sistema de comunicação. Existem diversos tipos de redes, como redes de computadores locais (LAN) e de longa distância (WAN), redes de telefonia, redes de TV a cabo e por satélite, entre outras.

O receptor é responsável por converter o sinal que vem da rede em informação que possa ser entendida pelo destinatário, conforme Dantas (2010), podendo utilizar um processo de demodulação para sinais analógicos ou um processo de decodificação para sinais digitais. Por fim, o último elemento do sistema de comunicação é o destinatário, que recebe efetivamente a informação gerada pela fonte.



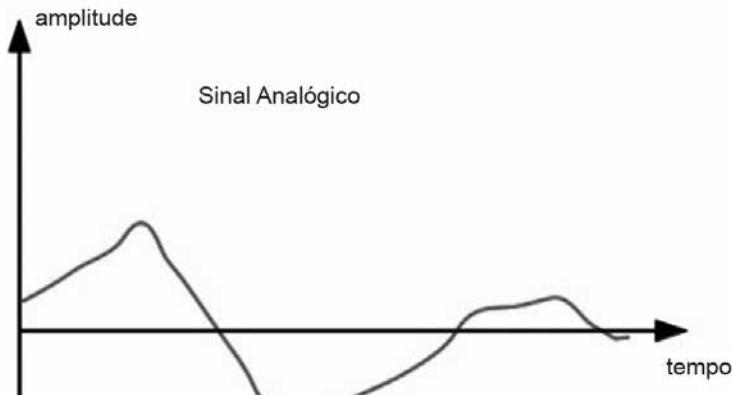
Para que o processo de comunicação possa ser dito completo, através do sistema de comunicação, é estritamente necessário que o destinatário, além de receber a informação, consiga entender a mesma. Será considerada informação pelo destinatário somente aquela que é efetivamente entendida, compreendida pelo mesmo.

2.2 SINAIS ANALÓGICOS E SINAIS DIGITAIS

As redes de comunicação normalmente são suportadas por sistemas de telecomunicações, os quais são desenvolvidos para transmitir sinais a distâncias diversas, como centenas de metros, quilômetros ou até milhares de quilômetros. Mas que tipos de sinais os sistemas de telecomunicações conseguem transmitir?

Os tipos de sinais transmitidos são sinais analógicos ou sinais digitais. Um sinal na forma analógica é apresentado na Figura 2, onde podemos observar que a variação do sinal ao longo do tempo é contínua. Em outras palavras, a amplitude, ou intensidade do sinal, varia continuamente com o passar do tempo. No mundo da matemática, é classificada como uma função contínua.

FIGURA 2 – EXEMPLO DE SINAL ANALÓGICO

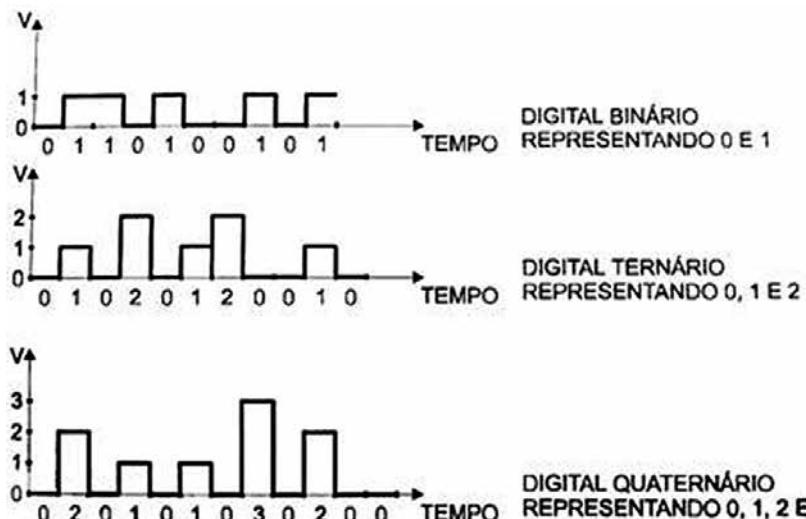


FONTE: Disponível em: <<http://wiki.sj.ifsc.edu.br/wiki/index.php/Gabarito>>. Acesso em: 15 fev. 2016.

Já um sinal na forma digital apresenta descontinuidades ou variações abruptas de amplitude, ou intensidade, com o passar do tempo. Os sinais digitais mais conhecidos são os binários, aqueles que possuem somente duas possibilidades de amplitude, por exemplo, assumem os valores 0 (zero) ou 1 (um), configurando um sinal semelhante a uma sequência de pulsos. No mundo da matemática seria classificada como uma função discreta (aquele que possui descontinuidades ao longo do tempo).

Na Figura 3 temos três gráficos com exemplos de sinais digitais. O primeiro é um sinal digital binário, que tem duas possibilidades de amplitude. O segundo é um sinal digital ternário, que tem três possibilidades de amplitude, e o terceiro é um sinal digital quaternário, que tem quatro possibilidades de amplitude.

FIGURA 3 – EXEMPLOS DE SINAIS DIGITAIS



FONTE: Disponível em: <http://www.teleco.com.br/tutoriais/tutorialcamerap1/pagina_2.asp>. Acesso em: 15 fev. 2016.



Caro(a) acadêmico(a): cabe aqui ressaltar que os sinais digitais podem assumir valores negativos também. Um exemplo seria um sinal discreto assumindo, alternadamente, os valores +5 V (volts) e -5 V (volts) com o passar do tempo.

3 A TRANSMISSÃO DE DADOS

Conforme vimos, para que a comunicação possa acontecer, é necessário que a informação seja transportada pela rede de comunicação, do transmissor da fonte até o receptor do destinatário. Essa função é executada pelos sistemas de transmissão, já que na maioria das vezes o transmissor e o receptor estão bastante distantes entre si. Podemos então definir a transmissão, segundo Dantas (2010, p. 45), “como sendo a transferência (elétrica ou óptica) de uma informação de um determinado local para outro”.

Na sequência, vamos estudar os principais conceitos relativos ao sistema de transmissão, como os tipos de transmissão, os sentidos e os modos de transmissão, a largura de banda e a taxa de transmissão.

3.1 TÉCNICAS E TIPOS DE TRANSMISSÃO

Os sistemas de transmissão utilizam basicamente duas técnicas, chamadas de transmissão via portadora, ou transmissão guiada; e transmissão via ondas de rádio, ou transmissão não guiada. A técnica de transmissão guiada é sempre utilizada quando o meio de transmissão é um meio físico, como, por exemplo, um cabo metálico de cobre (usado na rede telefônica), ou uma fibra óptica (usada em redes de dados de longa distância). No caso de cabos metálicos, a transmissão acontece através da circulação de corrente elétrica (energia elétrica), ao passo que no caso de fibras ópticas, a transmissão acontece através da propagação de luz (energia óptica) no seu interior.

Já a técnica de transmissão não guiada é utilizada quando a implantação de uma rede de cabos metálicos ou cabos ópticos é inviável, principalmente pelos altos custos. Como exemplo, para atingir regiões mais remotas, muito distantes dos centros urbanos, a solução mais viável é a transmissão não guiada. Neste caso, a transmissão acontece através da radiação e propagação de ondas eletromagnéticas pelo ar (energia eletromagnética). Sistemas de rádio, de televisão e redes wireless (sem fio) fazem uso dessa técnica.

Outro conceito que deve ser conhecido é quanto aos tipos de transmissão, que podem ser analógicos ou digitais. A transmissão analógica é apresentada por Dantas (2010, p. 26) como segue:

Podemos dizer, simplificando, que a informação quando for transmitida como um sinal analógico terá variações de estados (ex.: amplitude, frequência e fase, dentre outras características) de uma forma não discreta. Exemplos de sinais analógicos típicos são as ondas das estações de rádio (AM e FM) e TV. Interessante de se comentar que o vídeo utiliza modulação por amplitude, o som faz a modulação por frequência e a cor é modulada por fase. Todos os sinais comentados estão em formatos analógicos.

Neste momento é bom esclarecer que a transmissão analógica sempre faz uso de um modulador, cuja função é modular o sinal de uma onda portadora conforme a informação que deve ser transmitida. Modular o sinal da portadora significa alterar alguma característica dessa portadora (amplitude, frequência ou fase, por exemplo), de forma contínua no tempo, baseado na informação original a ser transmitida. Essa portadora modulada é que será transmitida, e no lado do receptor deverá existir um demodulador, cuja função é resgatar a informação original a partir da análise da portadora modulada/alterada que foi recebida. A modulação pode ser do tipo AM (Amplitude Modulada), FM (Frequência Modulada) ou PM (Fase Modulada), mas neste caderno não estudaremos esses tipos de modulação.

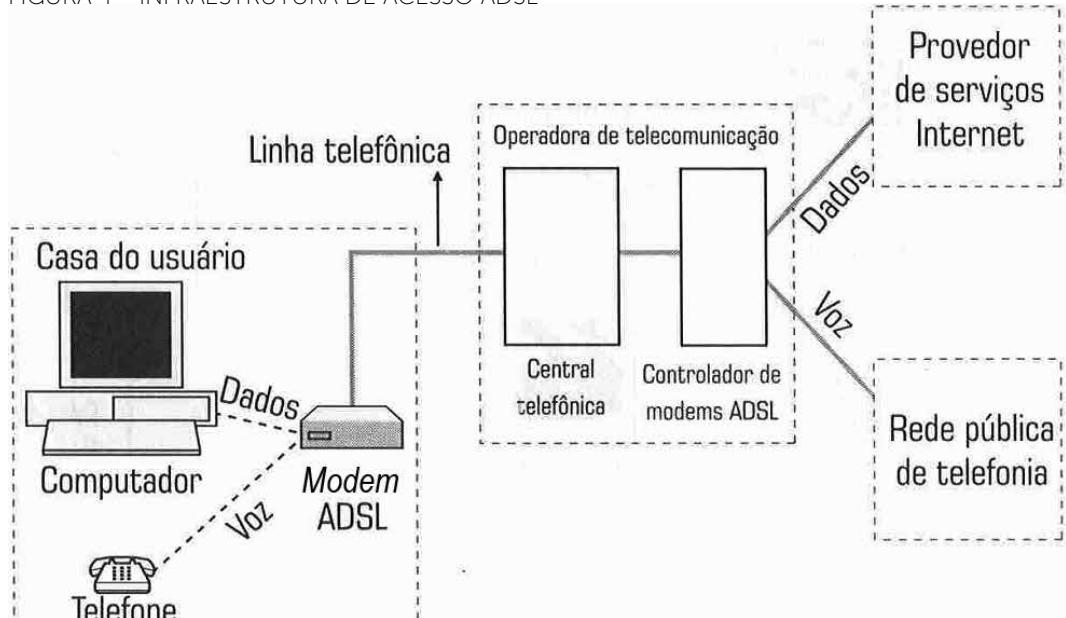
Com relação à transmissão digital, podemos afirmar que é muito mais simples do que a transmissão analógica. Isso porque a transmissão é feita através do envio de sinais discretos, com níveis muito bem definidos, em geral 0 (zero) e um (um), tornando os equipamentos de transmissão e recepção bem menos complexos que aqueles utilizados na transmissão analógica. Dessa forma, a transmissão digital torna-se muito mais econômica e atualmente é a mais empregada em redes de telecomunicações, responsáveis pela infraestrutura de transporte para as redes de comunicação de computadores.

No entanto, caro(a) acadêmico(a), a transmissão digital necessita de sincronia entre os sistemas transmissores e receptores, para que seja possível a correta identificação dos níveis digitais dos sinais e no tempo correto. Assim, mais adiante iremos estudar os modos de transmissão que definem duas técnicas de sincronização na transmissão digital.

Vimos que na transmissão analógica são utilizados moduladores (no transmissor) e demoduladores (no receptor), e, analogamente, na transmissão digital existe o codificador no lado transmissor. Sua função é alterar o sinal digital para um formato mais adequado à transmissão no meio físico, e este formato, ou tipo de codificação, vai depender do meio físico que está sendo utilizado na transmissão. No lado receptor deverá existir um decodificador, cuja função é resgatar o sinal digital original, eliminando a codificação usada durante a transmissão. Existem diversos tipos de CODECs (Codificadores/Decodificadores), mas não os estudaremos neste caderno.

Visando ilustrar para você uma situação prática das transmissões analógicas e digitais, apresentamos a Figura 4. Nela temos um esquema de infraestrutura utilizada para o serviço ADSL, utilizado em muitas residências e empresas, no Brasil e no mundo.

FIGURA 4 – INFRAESTRUTURA DE ACESSO ADSL



FONTE: Dantas (2002, p. 13)

Podemos verificar na Figura 4 que o *modem* ADSL na casa do usuário é responsável por multiplexar (agrupar) os sinais de dados (digitais) do computador e os sinais de voz (analógicos) do telefone, e enviar através da linha telefônica para a operadora de telecomunicações. De modo semelhante, quando chega informação da operadora para a casa do usuário, o *modem* ADSL faz a demultiplexação (desagrupar) dos sinais de dados que vão para o computador e os sinais de voz que vão para o telefone. O tipo de transmissão entre o *modem* ADSL e a operadora de telecomunicações, ou seja, na linha telefônica, é a analógica.

Ainda analisando a Figura 4, na operadora de telecomunicações existe conexão com a Internet, chegando nos provedores de serviços, por exemplo, e existe conexão com a rede pública de telefonia, na qual se conectam outras operadoras também. Agora, neste caso, além dos sinais de dados serem digitais, também os sinais de voz são digitais, e o tipo de transmissão utilizado é o digital. E você? Saberia dizer por que os sinais de voz são digitais na operadora?

Porque as operadoras de telecomunicações trabalham internamente em suas redes de telefonia com a voz digitalizada, ou seja, sempre que a voz chega na operadora vinda de uma linha telefônica (que é analógica), a operadora executa um processo de digitalização da voz, transformando a voz analógica em voz no formato digital, uma sequência de 0s (zeros) e 1s (uns). Quando a operadora precisa enviar

voz para uma linha telefônica, ela faz a transformação da voz digital (de sua rede interna) para voz analógica, e somente então envia para a linha telefônica.

Já que estamos falando em transmissão digital, e sabemos que os computadores são máquinas essencialmente digitais, vamos aproveitar e apresentar a forma de representação binária utilizada pelos mesmos. Ou seja, como um computador, ou impressora, ou outra máquina digital, consegue trabalhar com letras, números e sinais de pontuação?

Isso é possível utilizando códigos, como o ASCII (*American Standard Code for Information Interchange*) ou o EBCDIC (*Extended Binary Coded Decimal Interchange Code*). O código ASCII foi desenvolvido pelo órgão de padronização ITU-T (International Telecommunication Union – T) e é o mais usado atualmente. Este código permite representar letras, números e caracteres especiais (sinais de pontuação) e caracteres de controle. Estes últimos são usados para controlar um dispositivo a partir de outro, e podemos exemplificar com o caractere LF (*Line Feed*), que ao ser recebido por uma impressora, faz com que a mesma vá para a próxima linha.

FIGURA 5 – TABELA ASCII

Posição dos Bits				7	0	0	0	0	1	1	1	1
4	3	2	1									
0	0	0	0	NUL	DLE	SP	0	@	P	\	P	
0	0	0	1	SOH	DC1	!	1	A	Q	a	q	
0	0	1	0	STX	DC2	"	2	B	R	b	r	
0	0	1	1	ETX	DC3	#	3	C	S	c	s	
0	1	0	0	EOT	DC4	\$	4	D	T	d	t	
0	1	0	1	ENQ	NAK	%	5	E	U	e	u	
0	1	1	0	ACK	SYN	&	6	F	V	f	v	
0	1	1	1	BEL	ETB	'	7	G	W	g	w	
1	0	0	0	BS	CAN	(8	H	X	h	x	
1	0	0	1	HT	EM)	9	I	Y	i	y	
1	0	1	0	LF	SUB	*	:	J	Z	j	z	
1	0	1	1	VT	ESC	+	;	K	[k	{	
1	1	0	0	FF	FS	,	<	L	\	l		
1	1	0	1	CR	GS	-	=	M]	m	}	
1	1	1	0	SO	RS	.	>	N	^	n	~	
1	1	1	1	SI	US	/	?	O	-	o	DEL	

FONTE: Dantas (2002, p. 28)

Como exemplo, vamos supor que a palavra “Ontem” seja digitada no teclado de um computador. A representação binária com a qual o computador vai trabalhar, usando o código ASCII, é a seguinte para cada letra, lembrando que a posição do *bit* 7 é mais à esquerda:

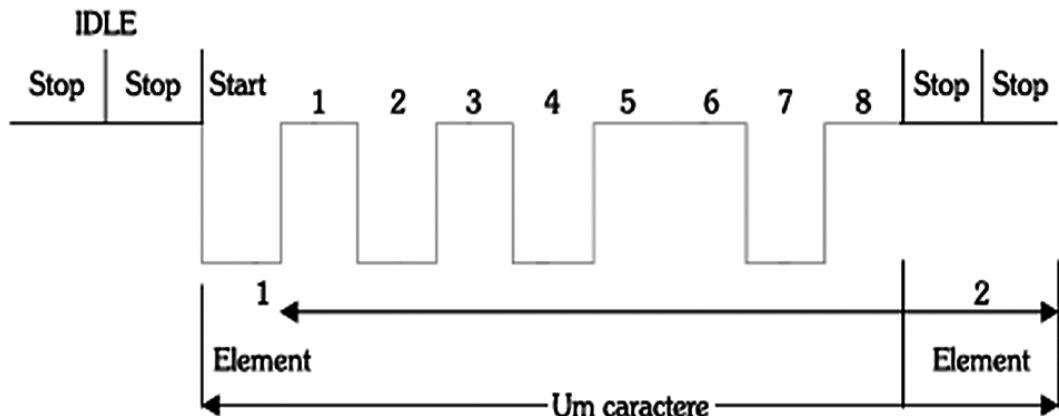
letra O = **1001111** ; letra n = **1101110** ; letra t = **1110100** ; letra e = **1100101** ; letra m = **1101101**

3.2 MODOS DE TRANSMISSÃO

Como informamos anteriormente, os sistemas transmissores e receptores necessitam de alguma informação de sincronia entre eles. Isto porque o receptor obrigatoriamente deve saber quando inicia a transmissão do primeiro *bit* do caractere da informação e qual será sua duração antes que venha o próximo *bit*. Somente com essa sincronização o receptor estará preparado para receber corretamente os dados enviados.

Inicialmente era utilizado o modo de transmissão assíncrono, já que os relógios (*clock*) do transmissor e do receptor não estão sincronizados no tempo, e, portanto, cada caractere transmitido deve levar a informação específica de sincronismo. Sistemas digitais trabalham com relógios (*clock*) para determinar instantes de tempo importantes, como o instante de tempo no qual o primeiro *bit* deverá ser lido pelo receptor, o instante de tempo para o segundo *bit* ser lido e assim por diante. Este modo de transmissão é mostrado na Figura 6.

FIGURA 6 – TRANSMISSÃO ASSÍNCRONA



FONTE: Moraes (2014, p. 32)

Observamos que no modo de transmissão assíncrono são inseridos *bits* adicionais ao caractere que está sendo transmitido. O *start bit* indica para o receptor que um caractere está iniciando, portanto, os próximos oito *bits* referem-se aos *bits* de informação útil, no caso da Figura 6. Em seguida vem o *stop bit*, que poderá ter o tempo de um ou dois *bits*, conforme previamente configurado no sistema,

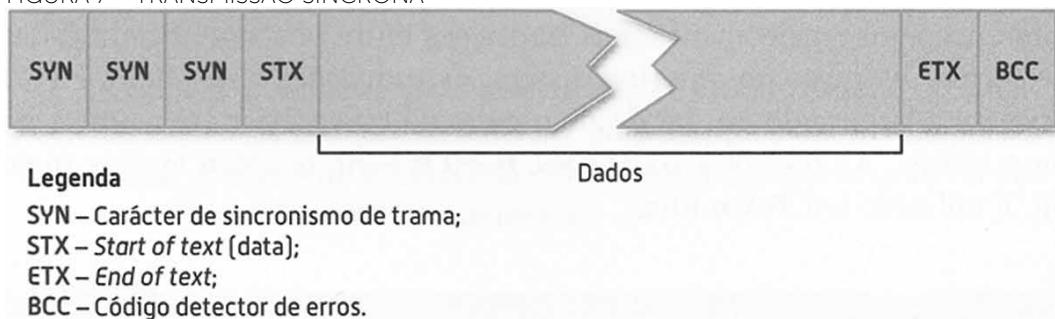
indicando que acabou a transmissão desse caractere. Assim, sucessivamente para todos os *bytes*, ou caracteres, da informação que deverá ser transmitida. Isso gera um *overhead* considerável, já que para oito *bits* de informação útil, teremos três *bits* adicionais para o modo assíncrono. Isso faz com que a taxa de utilização do sistema de transmissão seja apenas 62% em média.

Por outro lado, o **modo de transmissão síncrono** consegue uma taxa de utilização bem maior, pois utiliza uma técnica de sincronismo através da inserção de caracteres, e não *bits*. Conforme informado em Moraes (2014, p. 31):

A transmissão síncrona é baseada na transmissão de blocos de informação de uma única vez, entretanto os blocos de informação não podem ser transmitidos a qualquer instante, mas apenas no momento determinado pelo sinal do *clock* de sincronismo. Esse tipo de transmissão tem uma série de vantagens, entre elas que o *overhead* é muito pequeno e possui caracteres de sincronismo entre blocos de informação e não mais para cada *byte*, como na transmissão assíncrona.

O modo de transmissão síncrona é mostrado na Figura 7, onde observamos a existência de caracteres de sincronismo (SYN) e um caractere de início de texto (STX) antes do bloco de dados/informação. Após existe um caractere de fim de texto (ETX) e um caractere para detecção de erros (BCC).

FIGURA 7 – TRANSMISSÃO SÍNCRONA



FONTE: Disponível em: <<https://goncalolopes14.wordpress.com/2012/11/05/transmissao-sincrone/>>. Acesso em: 17 fev. 2016.

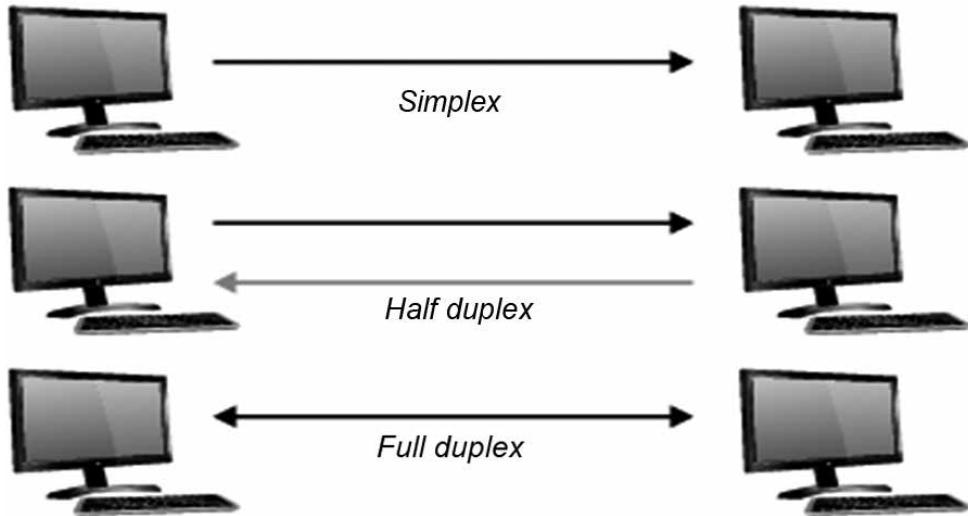


Existem processos para detecção e correção de erros que usam técnicas diversas, como *bit* de paridade, somas de verificação (*checksum*), verificação de redundância cíclica (CRC) e verificação e correção de erro (ECC). Esses assuntos não serão tratados neste caderno, mas sugerimos a você obter esse conhecimento consultando o item 1.4 do livro *Rede de Computadores*, de Barret e King (2010).

3.3 SENTIDOS DE TRANSMISSÃO

Em redes de computadores e outras redes de comunicação, a troca de informações entre dois dispositivos pode acontecer baseada em três sentidos de transmissão. Eles são mostrados na Figura 8, e recebem os nomes de transmissão *Simplex*, *Half-duplex* e *Duplex ou Full-duplex*.

FIGURA 8 – SENTIDOS DE TRANSMISSÃO



FONTE: Moraes (2014, p. 30)

Conforme informado por Torres (2001), a transmissão *Simplex* é constituída por um dispositivo que é sempre transmissor e outro dispositivo sempre receptor, configurando uma comunicação unidirecional somente. Como exemplo temos os sistemas de rádio AM e FM, além da TV aberta que somente transmite programação, mas não recebe nada dos telespectadores.

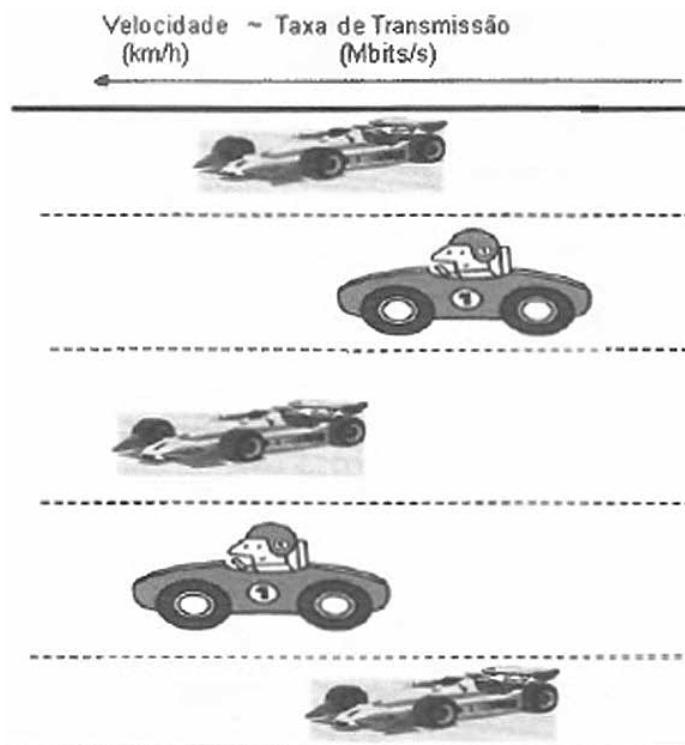
Segundo Torres (2001), na transmissão *Half-duplex*, quando um dispositivo transmite o outro não pode transmitir, porque compartilham um mesmo canal de comunicação, apesar da transmissão ser bidirecional. Ou seja, os dois dispositivos podem transmitir, desde que não seja ao mesmo tempo. Como exemplo clássico temos os comunicadores *walk-talk*, onde duas pessoas podem conversar, mas somente uma por vez. Também os sistemas de radioamador e alguns sistemas de comunicação de dados.

Para Ross (2008), na transmissão *Full-duplex* ocorre a transmissão de informações nos dois sentidos de forma simultânea, ou seja, os dois dispositivos trocam dados ao mesmo tempo, conforme a última ilustração da Figura 8. Um dispositivo pode enviar informação e receber outra informação no mesmo instante. Como exemplo temos os próprios telefones e muitos sistemas de comunicação de dados modernos, como os acessos à Internet via serviços ADSL ou via *Cable-Modem* das operadoras de TV a cabo.

3.4 LARGURA DE BANDA E TAXA DE TRANSMISSÃO

É bastante comum observarmos nos meios acadêmicos, e também profissionais, uma dificuldade no entendimento dos conceitos e da diferença entre largura de banda e taxa de transmissão. Muitos utilizam esses termos de forma trocada, ou seja, falam em largura de banda mas querem expressar a taxa de transmissão e vice-versa. Para entendermos os conceitos e sua diferença, vamos utilizar a Figura 9, onde relaciona-se largura de banda e taxa de transmissão.

FIGURA 9 – LARGURA DE BANDA x TAXA DE TRANSMISSÃO



FONTE: Dantas (2010, p. 55)

Na Figura 9 devemos fazer uma analogia entre uma estrada, por onde trafegam automóveis, e um meio de transmissão, por onde trafegam dados digitais. A largura da estrada (medida em metros) corresponde à largura de banda (medida em Hz) do meio físico de transmissão, enquanto que a velocidade dos carros na estrada (medida em Km/h) corresponde à taxa de transmissão dos dados (medida em bps=bits por segundo) pelo meio de transmissão.

Conforme Dantas (2010), deve-se lembrar que a largura de banda é sempre relativa à capacidade máxima de transmissão do meio físico que está sendo usado, sendo diferente da taxa de transmissão. É possível aumentar a taxa de transmissão com a mesma largura de banda, basta aumentar a potência do carro ou a pressa do motorista. Numa rede de computadores, isso poderia ser a troca da interface de *hardware* da rede e do protocolo por um mais rápido.

Para finalizar esse comparativo, apresentamos a Figura 10, onde observamos que a taxa de transmissão, sempre medida em bps, normalmente pode ser maior que a largura de banda, sempre medida em Hz (Hertz). Entenda que essa figura é somente um exemplo, e a taxa de transmissão obtida num meio de transmissão com fibra ótica pode ser bem maior que 2 Gbps.

FIGURA 10 – RELAÇÃO ENTRE MEIO, A TAXA E A LARGURA

Meio de transmissão	Taxa de transmissão	Largura de banda
Par trançado	4 Mbps	3MHz
Cabo coaxial	550 Mbps	350 MHz
Fibra óptica	2 Gbps	2 Gbps

FONTE: Dantas (2002, p. 32)

4 MULTIPLEXAÇÃO

Com o passar dos anos, a quantidade de comunicação de voz, dados e imagem aumentou muito. Dessa forma, as operadoras de telecomunicações precisaram otimizar a utilização dos canais dos sistemas de transmissão. Foi então desenvolvida pela Bell Labs uma técnica para que vários usuários pudessem compartilhar o mesmo canal de comunicação, ou seja, várias conversas telefônicas poderiam acontecer usando o mesmo canal de comunicação, obtendo maior capacidade e redução de custos na infraestrutura física das redes.

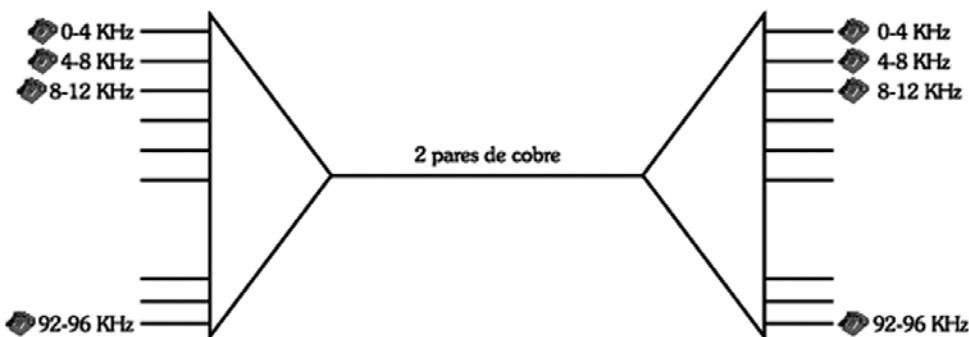
Essa técnica é chamada multiplexação, e os equipamentos responsáveis por agrupar os sinais de vários usuários sobre um mesmo canal de comunicação são chamados multiplexadores (MUX). Já os demultiplexadores (DEMUX) executam a operação inversa, recebem os sinais num único canal e desagrupam em sinais independentes, como era antes da multiplexação.

NOTA

Caro(a) acadêmico(a), todo o processo de multiplexação e demultiplexação é transparente para o usuário, ou seja, o usuário nada percebe. Exemplo: se você faz uma ligação telefônica de Florianópolis/SC para Belo Horizonte/MG, a sua conversa vai utilizar determinados canais de transmissão entre Florianópolis e Belo Horizonte que também estarão sendo utilizados por outras ligações telefônicas simultaneamente. Uma conversa não interfere na outra, mesmo utilizando o mesmo canal de transmissão, graças aos sistemas multiplex. Obs.: aqui estamos falando do serviço telefônico fixo comutado (STFC) utilizado nas redes de telefonia convencional das operadoras de telecomunicações, não estamos falando de telefonia IP (VoIP).

As técnicas básicas de multiplexação são FDM (Multiplexação por Divisão de Frequência) e TDM (Multiplexação por Divisão do Tempo). No FDM, a técnica mais adequada para sinais analógicos, a largura de banda do canal de transmissão é dividida em vários canais menores, conforme exemplo da Figura 11. Nesta figura, um canal com largura de banda de 96 KHz é subdividido em 24 canais de 4KHz cada. Dessa forma, 24 conversas telefônicas podem compartilhar o mesmo canal de 96 KHz, constituído por apenas dois pares de cobre, já que cada conversa telefônica analógica ocupa uma largura de 4 KHz.

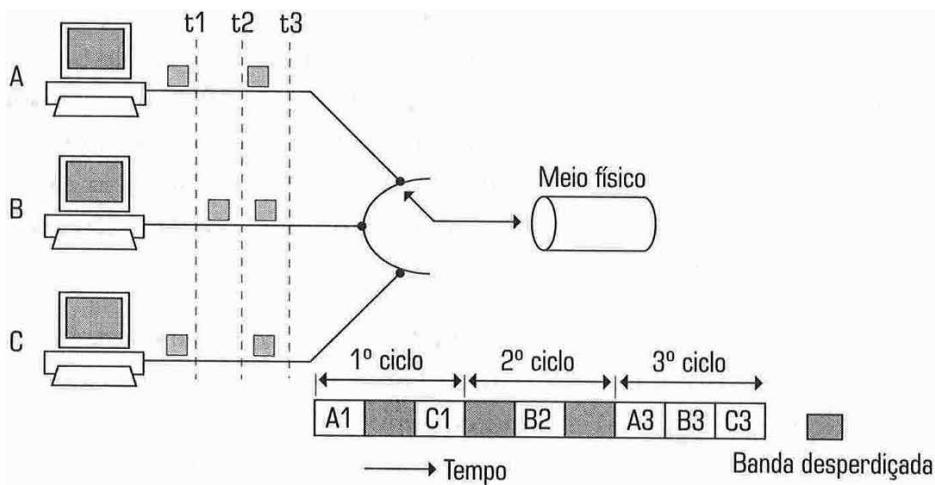
FIGURA 11 – APLICAÇÃO DO FDM



FONTE: Moraes (2014, p. 34)

No TDM, a técnica mais adequada para sinais digitais, o tempo de transmissão do canal é dividido em pequenos intervalos de tempo, chamados *time slots*. Existe o TDM comum, também chamado TDM Síncrono, onde cada usuário de canal é alocado a um *time slot* fixo, no qual fará sua transmissão. No caso de um usuário não tiver sinal para transmitir quando vier seu *time slot*, esse intervalo de tempo será desperdiçado no canal multiplexado. Veja isso na Figura 12, onde no 1º ciclo transmitem A1 e C1, no 2º ciclo somente B2 tem dados para transmitir, existindo desperdício de dois *time slots* de tempo neste ciclo, e no 3º ciclo todos transmitem dados.

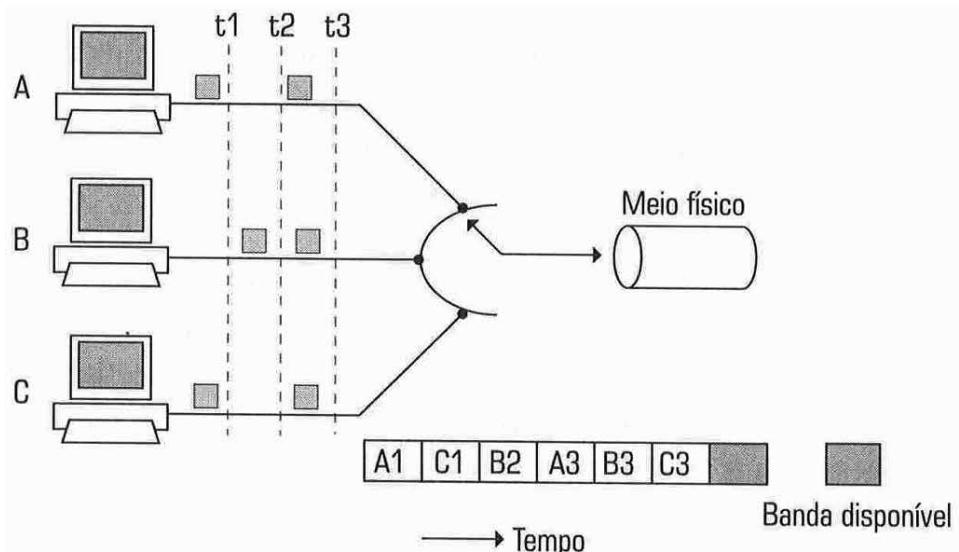
FIGURA 12 – TDM COMUM OU TDM SÍNCRONO



FONTE: Dantas (2002, p. 44)

Com o uso do TDM foi identificado que até 30% do tempo não era utilizado pelos usuários, ou seja, não havia transmissão de informação, ficando esses *time slots* vazios. Foi desenvolvido, então, o TDM Estatístico, também chamado TDM Assíncrono. Neste, o usuário não é alocado a um *time slot* fixo, mas pode acessar aleatoriamente *time slots* que estejam vazios no momento que desejar transmitir. Entenda isso melhor analisando a Figura 13.

FIGURA 13 – TDM ESTATÍSTICO OU TDM ASSÍNCRONO



FONTE: Dantas (2002, p. 44)

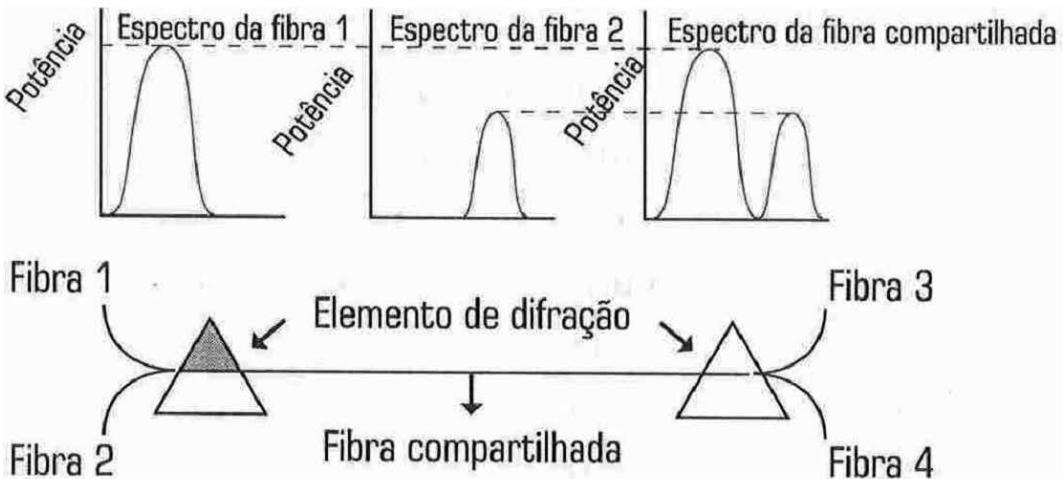
Podemos notar na Figura 13 que o 2º *time slot* foi ocupado pelo usuário C, e o 3º *time slot* foi ocupado pelo usuário B. Dessa forma, consegue-se otimizar o uso do meio de transmissão, já que poucos *time slots*, ou nenhum, ficam vazios. Isso significa redução de custos, pois reduz a necessidade de ampliação de canais de transmissão que possuem custos elevados.

Existe outra técnica de multiplexação, chamada WDM (Multiplexação por Divisão de Onda), utilizada em sistemas onde o meio físico é a fibra óptica. Seu objetivo é agrupar muitos sinais ópticos numa única fibra óptica e seu funcionamento é semelhante ao FDM. Conforme explicado em Dantas (2010, p. 69):

No caso da WDM, temos uma (ou mais) fibra(s) chegando a um dispositivo passivo chamado de grade de difração. Este equipamento faz uma divisão dos espectros para que os mesmos possam passar por uma fibra compartilhada. No ponto destinatário existe outra grade de difração que efetua a operação inversa, ou seja, cada espectro é novamente dividido.

Na Figura 14 temos uma ilustração sobre WDM, onde duas fibras chegam no elemento de difração. Este atua como MUX, juntando os espectros do sinal da fibra 1 e da fibra 2, e transmitindo pelo meio que é uma fibra óptica compartilhada. No receptor existe um DEMUX, cuja responsabilidade é separar os espectros para as fibras 3 e 4, respectivamente.

FIGURA 14 – A TÉCNICA WDM



FONTE: Dantas (2002, p. 44)

Existem sistemas que conseguem combinar centenas de fibras, e são chamados de DWDM (Multiplexação por Divisão de Onda Densa), muito utilizados por operadoras de telecomunicações e provedores de serviços de comunicação de dados.

RESUMO DO TÓPICO 1

Neste tópico vimos que:

- Existe um modelo genérico de processo de comunicação, com elementos bem definidos, que representa todos os tipos de troca de informações.
- Os sinais eletroeletrônicos podem ser analógicos ou digitais, e possuem características bastante distintas.
- As técnicas de transmissão de sinais podem ser guiadas ou não guiadas, e existem as transmissões analógicas ou digitais.
- É importante conhecer a diferença entre os modos de transmissão assíncrono e síncrono.
- Os sentidos de transmissão são classificados em *simplex*, *half-duplex* e *full-duplex*.
- Largura de banda e taxa de transmissão são conceitos diferentes, apesar de muitos utilizarem erroneamente o termo largura de banda como se fosse taxa de transmissão.
- As principais técnicas de multiplexação são FDM, TDM e WDM, sendo que atualmente as mais utilizadas são TDM e WDM.

AUTOATIVIDADE



- 1 Relacione os cinco elementos do modelo de comunicação genérico e descreva os mesmos com as suas palavras.
- 2 Descreva com suas palavras os tipos de transmissão analógica e digital.
- 3 Cite e descreva com suas palavras os três tipos de sentidos de transmissão.
- 4 Explique com suas palavras a diferença entre taxa de transmissão e largura de banda.



*Assista ao vídeo de
resolução da questão 4*



CONCEITOS BÁSICOS DE REDES DE COMPUTADORES

1 INTRODUÇÃO

As redes de computadores são utilizadas massivamente nos dias de hoje, mas nem sempre foi assim. Havia uma época, décadas de 70 e 80, onde, para transferir informações de um computador para outro, era necessário, por exemplo, inserir um disquete (havia alguns modelos com capacidades entre 1M e 5MBytes) na unidade de discos do computador, copiar os dados desejados para esse disquete, então levar fisicamente o mesmo até o outro computador, inserir na unidade de discos e copiar dos dados para esse computador. Nos anos 70 e início de 80 nem mesmo computadores pessoais eram comuns, somente algumas empresas tinham condições de adquirir esses microcomputadores.

Para profissionais da área de TI, além de ser importante estudar os fundamentos das redes de computadores, é interessante que conheçam ao menos um resumo da história das redes. Essa história das redes se confunde, em termos cronológicos, com a história da evolução dos computadores em si. Nesta unidade vamos conhecer um pouco da história das redes e estudar as classificações e topologias de redes de computadores. Também vamos entender algumas características das redes que determinam suas formas de funcionamento.

Um dos importantes marcos da história da comunicação aconteceu no século XIX, quando o Código Morse foi utilizado no telegrafo com fios. Na sequência, foi desenvolvido o Telex na primeira metade do século XX, que transmitia e recebia um conjunto de 32 caracteres alfanuméricos, utilizando-se de um código binário com 5 bits, e foi utilizado até os anos 80.

Os primeiros computadores foram desenvolvidos entre 1930 e 1940. O famoso computador ENIAC foi desenvolvido nos anos 40, nos Estados Unidos, durante a Segunda Guerra Mundial. Nessa época, também a Alemanha e Inglaterra desenvolveram projetos de computadores. Após a guerra, o ENIAC passou a ser o primeiro computador a ser vendido comercialmente com o nome de UNIVAC, sendo responsável a empresa Remington.

Na década de 60, três centros de pesquisa começaram a desenvolver conceitos para interligar computadores e formar redes através de troca de mensagens usando comutação de pacotes. Os centros eram o MIT (Instituto de Tecnologia de Massachusetts), o Rand Institute e o National Physical Laboratory da Inglaterra. Em 1969, a ARPA (Advanced Research Projects Agency) – Agência de Projetos de Pesquisa Avançados, dos Estados Unidos, implementou a primeira rede interligando quatro computadores, e foi chamada ARPAnet.

Em 1972 a ARPAnet já tinha 15 nós (computadores) conectados, e foi desenvolvido o primeiro programa de *e-mail* por Ray Tomlinson, assim como foi desenvolvido também o protocolo NCP (*Network Control Protocol*), que deu origem posteriormente ao conhecido TCP/IP. Em 1976, foi desenvolvido por Robert Metcalfe e David Boggs, na Xerox Corporation, o padrão *Ethernet*, cujos conceitos são utilizados até hoje em redes de computadores.

Na década de 70, nas grandes empresas, já eram conectados terminais (vídeo e teclado) aos *mainframes*, que eram os grandes computadores da época, e que centralizavam todo o processamento e armazenamento de dados nos CPDs (Centro de Processamento de Dados). No entanto, os *mainframes* e os CPDs tinham custos elevados para aquisição e manutenção.

Os microcomputadores PC (Computadores Pessoais) surgiram na década de 80, e algumas aplicações poderiam agora serem feitas no próprio PC, e não mais no *mainframe*, iniciando o processo de descentralização do processamento. Em 1983 o protocolo TCP/IP passa a ser adotado na ARPAnet. No final da década de 80, a ARPAnet já contava com nove países interconectados, além dos Estados Unidos, iniciando a Internet de abrangência mundial.

Na década de 90 surgiu o processamento distribuído, que era a descentralização com integração entre PCs e *mainframe* já utilizando conceitos de redes de computadores. Nessa época, em 1991, começou a utilização comercial da Internet, quando a ARPAnet deixou de existir e passou a chamar-se NSFNET, administrada pelo NSF dos Estados Unidos, que era um órgão de pesquisa e projetos de inovação tecnológica. Em 1992 já existiam 7.500 redes interconectadas, formando a Internet da época. Em 1993 surge o MOSAIC, primeiro navegador para Internet usando interface gráfica.

No Brasil, a Internet comercial teve início em 1995, com sua operação pela Embratel. A partir daí o crescimento da Internet foi extremamente grande, e contribuiu também para o crescimento do uso de redes de computadores privativas, locais e de longa distância.



Caro(a) acadêmico(a), para que você possa ter uma visão mais completa sobre o histórico das redes de computadores e da internet, sugerimos consultar o item 1.7 do livro **Redes de computadores e a Internet: uma abordagem top-down**, referência: Kurose e Ross (2010).

2 DEFINIÇÃO E APLICAÇÕES DE REDE

Sempre que desejamos criar uma definição para determinado elemento ou assunto, surgem várias possibilidades para sua redação e conceito, que devem visar à mais fácil compreensão para quem vir a estudar tal definição.

Para o caso de redes de computadores, muitas definições existem, mas nós poderíamos definir as redes de computadores como sendo um conjunto de recursos que, corretamente interligados e configurados, permitem a efetiva troca de informações entre computadores distintos, ou equipamentos correlatos, que estejam fisicamente próximos ou muito distantes entre si; além de permitir o compartilhamento de alguns recursos.

Outra definição para redes de computadores é apresentada por Barrett e King (2010, p. 31), como segue:

Uma rede é um grupo de computadores que podem se comunicar uns com os outros para compartilhar informações. Isso pode variar, em sua forma mais simples, desde dois computadores em uma casa, que estão conectados por um cabo, até a rede mais complexa contendo muitos computadores, cabos e dispositivos espalhados por continentes.

Por outro lado, para Dantas (2010, p. 189), as redes têm a seguinte definição:

As redes de comunicação são ambientes que se caracterizam pela interligação de um conjunto de elementos com capacidade computacional através de enlaces físicos guiados e não guiados. Em adição, pacotes de software são empregados para permitir uma transparência na utilização da configuração.

É interessante observarmos, nesse momento, a relação que existe entre duas áreas diferentes, mas que possuem muitos conceitos e formas de implementação semelhantes. Essas são as áreas de redes de comunicação e redes de computadores, que tecnologicamente cresceram de forma muito rápida nas últimas décadas. Segundo Dantas (2010), os profissionais dessas áreas vivem um distanciamento entre si, já que situações referentes à área de redes de comunicação, ou telecomunicações, são tratados por engenheiros; enquanto situações referentes

a computadores são tratadas por profissionais de computação. É preciso uma visão moderna sobre esse tema para os envolvidos em processo de integração de sistemas locais e geograficamente distribuídos.

Sobre as características e a relação existente entre as redes de comunicação (redes de telecomunicações) e as redes de computadores, Dantas (2010, p. 18) conclui que:

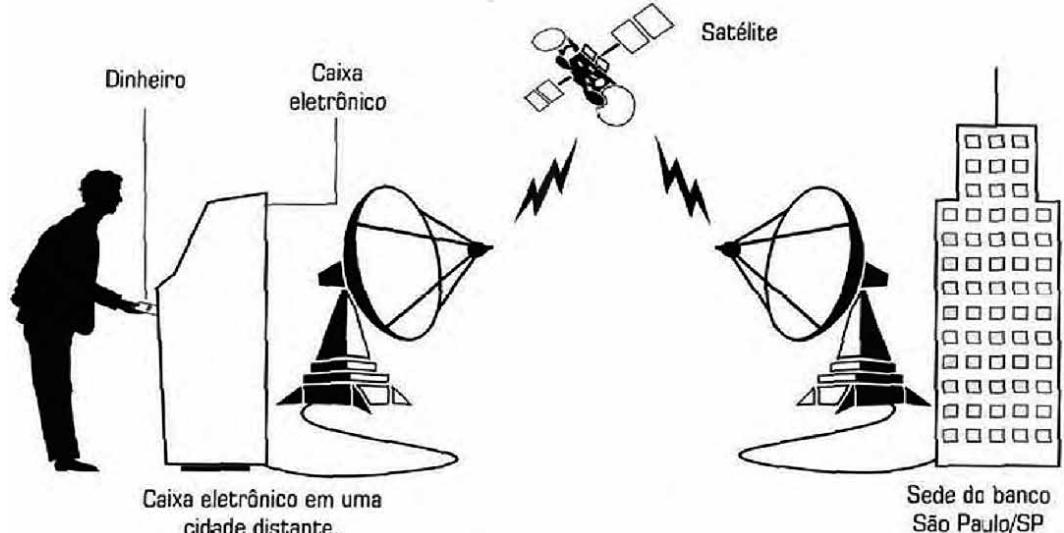
Em uma primeira análise, muitas vezes, por causa dos equipamentos conectados às redes [telefones, TVs, computadores] e do tipo diferente de informação transmitida, somos levados a crer que as redes de comunicação e redes de computadores têm características disíspares [características diferentes]. Entretanto este raciocínio é um engano, pois os princípios que orientam a transmissão da informação de uma forma geral são semelhantes nos dois ambientes de rede [portanto, não pode existir uma separação entre essas duas áreas].

Vamos apresentar agora alguns exemplos de aplicações de redes de computadores, já que a utilização das mesmas se tornou um recurso indispensável nos ambientes empresariais e também nos residenciais. O custo dos computadores e do próprio acesso à Internet diminuiu consideravelmente nos últimos anos, contribuindo para a disseminação das redes e desenvolvimento de aplicações diversas. Praticamente 100% das empresas possuem acesso à Internet e o percentual de residências conectadas à Internet cresce a uma taxa grande.

Uma empresa pode ter computadores para diversas atividades, como controlar a produção, monitorar e controlar estoques, desenvolver a folha de pagamento, entre outros. É possível compartilhar recursos físicos, como gravadores de CDs, impressoras e *scanners*, mas principalmente informação, como compartilhamento de arquivos de trabalho, compartilhamento de programas e compartilhamento de acesso à Internet.

Como exemplo de aplicação de redes, podemos citar os caixas eletrônicos de bancos, instalados nas agências bancárias ou em outros locais, como supermercados, postos de gasolina, *shopping centers*. A comunicação do(s) caixa(s) eletrônico(s) com os computadores centrais do banco é feita através de uma rede de computadores, como representa a Figura 15. Nesta, o caixa eletrônico se comunica com o computador central, instalado na sede do banco ou em algum *Datacenter*, através de uma rede via satélite, mas poderia ser uma rede via cabos metálicos ou via fibra óptica. Solução via satélite somente é utilizada quando não existe solução via meio físico, pois o custo de soluções via satélite é alto.

FIGURA 15 – APLICAÇÃO DE REDES: CAIXA ELETRÔNICO

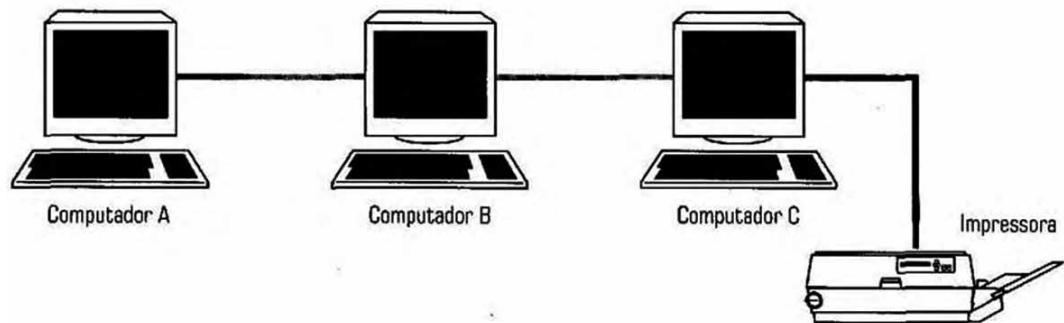


FONTE: Torres (2001, p. 4)

Outro exemplo de aplicação de redes seria num supermercado. Neste caso existe a rede interna de computadores dos setores, como administração, compras, financeiro e inclusive dos caixas, que são máquinas com capacidade computacional que, além de totalizar o valor da compra, ainda podem e devem atualizar o sistema responsável pelo estoque. Pode existir também uma rede externa, interligando todas as filiais desse supermercado à sua matriz, trocando e atualizando dados de forma *on-line* em todos os sistemas existentes. Somente dessa forma é possível uma perfeita operação das filiais e matriz desse supermercado.

Segundo Torres (2001), além da troca de informações entre os equipamentos, o compartilhamento de periféricos é uma das aplicações de redes que traz grandes vantagens, como redução de custos, quando uma única impressora é compartilhada por vários computadores ou, ainda, o acesso à Internet é compartilhado entre computadores utilizando um único *modem* para conexão com a operadora do serviço de Internet. Na Figura 16 está representada uma rede simples, mas que permite, além da troca de informações, o compartilhamento de uma impressora.

FIGURA 16 – COMPARTILHAMENTO DE IMPRESSORA

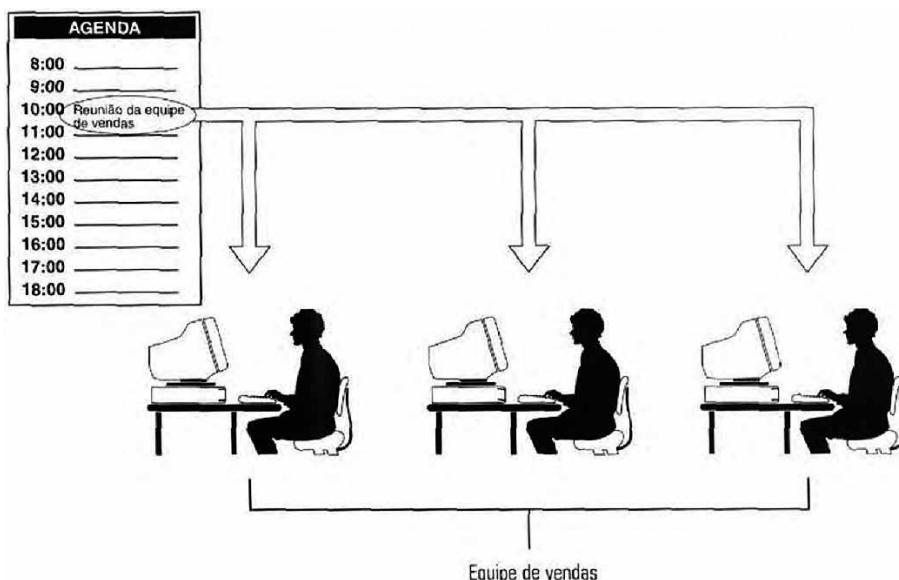


FONTE: Torres (2001, p. 4)

O compartilhamento de programas também é uma aplicação de redes muito utilizada, já que permite aos computadores acessar programas instalados fisicamente em HDs (discos rígidos) de outras máquinas. Isso traz como vantagens a padronização dos programas utilizados, libera espaço para armazenamento no HD local, e a consequente redução de custos muito bem vista pelas empresas. Inclusive existe a redução de custos com o próprio programa, já que versões para operação em rede têm custo menor do que a compra individual para cada máquina da rede.

Nos é informado por Torres (2001) que outras duas aplicações de redes são bastante utilizadas no meio empresarial, sendo o caso do correio eletrônico e da agenda de compromissos. A comunicação entre os funcionários da empresa é muito agilizada com a utilização do correio, e a agenda facilita a marcação de compromissos como reuniões, áudio ou videoconferências entre os funcionários e os níveis de gerência ou diretoria. Na Figura 17 representamos uma agenda marcando reunião com a equipe de vendas, sendo que outros funcionários da empresa não terão esse compromisso definido em suas agendas.

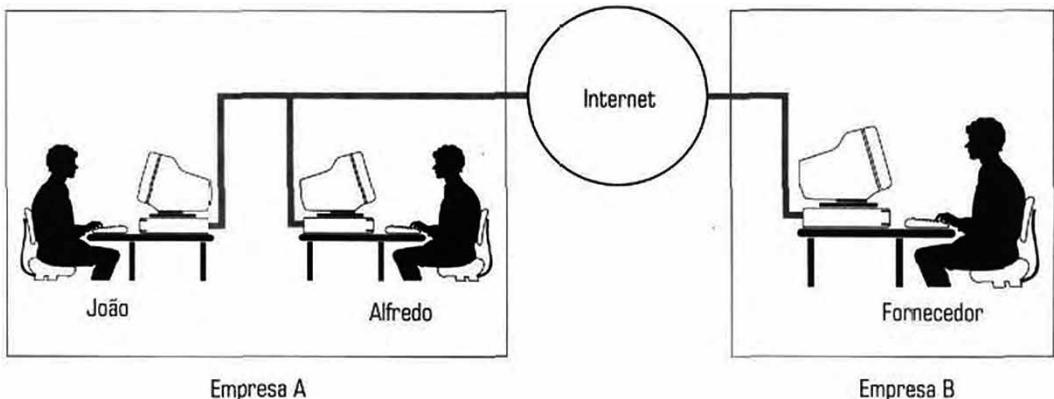
FIGURA 17 – APLICAÇÃO DE AGENDA DE COMPROMISSOS



FONTE: Torres (2001, p. 6)

Com relação ao correio eletrônico, praticamente todas as empresas utilizam a partir de servidores de correio instalados na rede interna da empresa, ou a partir de serviços de correio terceirizados como Gmail, Yahoo, cujos servidores estão instalados em alguns países, mas através da Internet conseguem atender empresas no mundo inteiro. Assim, os funcionários conseguem enviar mensagens e arquivos entre si e também com fornecedores, clientes, etc. É necessário que a empresa tenha um acesso à Internet, e normalmente esse acesso é compartilhado entre alguns ou todos os computadores da empresa. Na Figura 18 temos um exemplo simplificado de rede interna numa empresa, com acesso compartilhado à Internet e viabilizando a comunicação com fornecedores, ou então clientes ou outras empresas e órgãos do governo, por exemplo.

FIGURA 18 – APLICAÇÃO DE ACESSO COMPARTILHADO À INTERNET



FONTE: Torres (2001, p. 7)

As grandes empresas fazem uso das chamadas redes corporativas, que nada mais são do que a integração entre computadores de usuários, servidores diversos (como Windows NT, SunOS, Unix/Linux), *mainframes* que ainda são utilizados por algumas empresas e a própria Internet. Essas redes viabilizam a utilização de diversos sistemas operacionais de rede e diversos aplicativos, como banco de dados, ERP (sistema de Planejamento de Recursos da Empresa), CRM (sistema de Gerenciamento de Relacionamento com Clientes), entre outros. Permitem uma infraestrutura padronizada para acessar todas as informações necessárias e trazem a vantagem da redução de custos na utilização dos recursos computacionais.

Por outro lado, é preciso ter em mente que a utilização de redes de computadores pode trazer alguns inconvenientes, como ataques de vírus que podem se espalhar por toda a rede, causando problemas e até a interrupção do funcionamento dos sistemas, problemas com os equipamentos de *hardware* da rede podem gerar lentidão ou interrupções indesejadas, invasão de *hackers*, principalmente nas redes que estão conectadas com a Internet 24 horas, podendo ocasionar perda e vazamento de informações importantes e até confidenciais da empresa. Devemos, portanto, implantar meios ou sistemas que minimizem a probabilidade de ocorrência dos inconvenientes citados.

Existem incontáveis aplicações de redes e aqui foram apresentadas apenas algumas e de forma resumida. As redes estão presentes em muitos lugares, lugares que às vezes nem imaginamos, como, por exemplo, dentro de um automóvel mais moderno, onde existem algumas redes interligando os processadores, sensores e atuadores responsáveis pelo perfeito funcionamento deste automóvel. Alguns automóveis permitem inclusive a comunicação dos sistemas computacionais internos com a fábrica/montadora do mesmo.

Assim, para finalizar esse item, quanto à atual situação de utilização e aplicações das redes de computadores, Dantas (2010, p. 22) afirma que:

[...] estamos vivendo a era dos agregados computacionais (*clusters*), que podemos traduzir como a abordagem de evolução da simples interconexão física de computadores para uma forma distribuída de operação. Em outras palavras, não só a rede deve nos permitir ligar os computadores, mas temos que ter garantias de que as aplicações de diferentes fornecedores devem interoperar de uma forma única, transparente e com bom desempenho. Mais recentemente, o paradigma de *cluster* computacional ganha a dimensão das redes geograficamente distribuídas, que são desenvolvidas sob o paradigma de grade (*grid*) e nuvem computacional (*cloud computing*).

3 CLASSIFICAÇÕES E TOPOLOGIAS DE REDES

As redes de computadores são muito diversificadas, podendo ser construídas em diferentes formatos, dependendo das aplicações e necessidades dos usuários. Mesmo assim, para facilitar os estudos e sua compreensão, as redes foram classificadas em grupos baseados em algumas características das mesmas.

Vamos estudar os tipos e classificações das redes, entender o que são as redes Intranet, Extranet e Internet, e, além disso, vamos conhecer as diferentes topologias físicas e lógicas de redes de computadores.

3.1 CLASSIFICAÇÃO CONFORME A ABRANGÊNCIA GEOGRÁFICA

As redes de computadores, segundo Dantas (2010), são classificadas geralmente levando em consideração o aspecto da abrangência geográfica, ou dispersão. Assim, as redes se classificam em redes pessoais (PAN - *Personal Area Networks*), redes locais (LAN - *Local Area Networks*), redes metropolitanas (MAN - *Metropolitan Area Networks*) e redes de longa distância (WAN - *Wide Area Networks*).

Ressaltamos que, com o surgimento e crescimento na utilização das redes *wireless* (sem fio), novas classificações relativas às redes *wireless* foram definidas, e são elas: redes pessoais sem fio (WPAN - *Wireless Personal Area Networks*), redes locais sem fio (WLAN - *Wireless Local Area Networks*), redes metropolitanas sem fio (WMAN - *Wireless Metropolitan Area Networks*) e redes de longa distância sem fio (WWAN - *Wireless Wide Area Networks*).

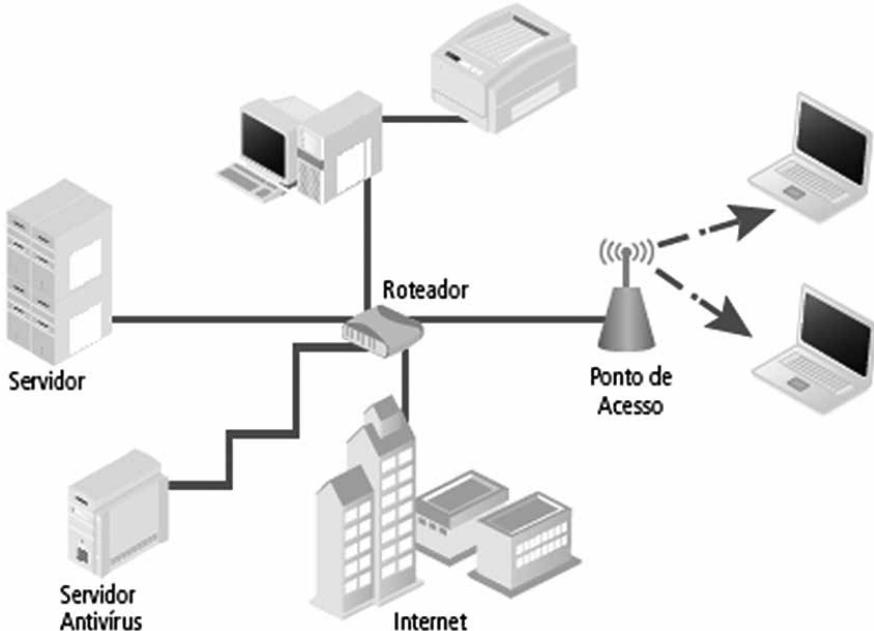
As redes PAN, conforme Dantas (2010), são redes que viabilizam a comunicação entre pequenos dispositivos pessoais, como *smartphone*, *tablets*, relógios, sensores, GPSs etc. Esses podem pertencer, ou não, à pessoa. No caso de uma rede RFID (Identificação por Radiofrequência), composta por sensores e outros equipamentos, esses provavelmente não pertenceriam à pessoa.

O alcance de uma rede PAN é limitado a alguns metros. Existe a possibilidade de conectar uma rede PAN a uma rede de maior abrangência, como uma WAN, segundo Dantas (2010). Um exemplo seria uma rede de monitoração da saúde de uma pessoa numa UTI, classificada como PAN, enviando os dados coletados para um centro médico estabelecido numa cidade em outro estado da federação.

As redes LAN são as que existem em maior quantidade, e uma definição, conforme Dantas (2010), seria: “Uma rede local (LAN) é uma facilidade de comunicação que provê uma conexão de alta velocidade entre processadores, periféricos, terminais e dispositivos de comunicação de uma forma geral em um único prédio (ou *campus*)”.

A Figura 19 apresenta um exemplo simplificado de uma rede LAN conectada a uma rede WLAN. Essa rede possui dois servidores, um microcomputador e sua impressora multifuncional que representam a LAN em si, e um roteador que interliga a LAN com a Internet, representada por um prédio de operadora de telecomunicações, e com o ponto de acesso que forma a rede WLAN, que possui dois notebooks.

FIGURA 19 – REDE LAN E REDE WLAN



FONTE: Amaral (2012, p. 19)

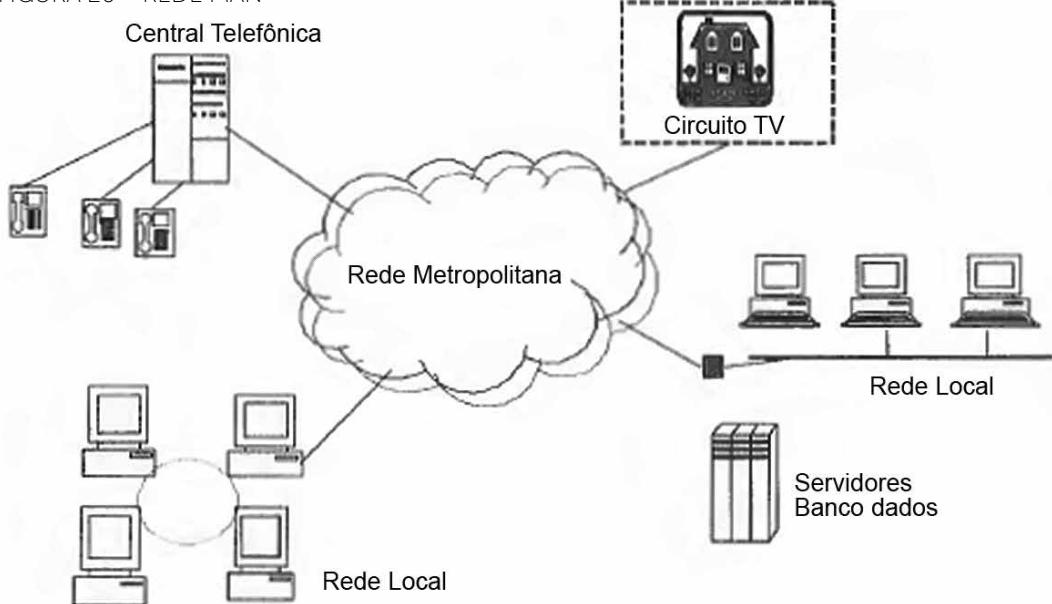
As redes LAN possuem algumas características importantes, segundo Dantas (2010):

- Abrangência geográfica – usam tecnologias que permitem alcance de centenas de metros ou alguns quilômetros no máximo, limitando seu uso a no máximo um *campus* de uma universidade ou prédios de uma empresa que estejam num mesmo terreno físico.

- Propriedade – os equipamentos e sistemas são de propriedade da empresa que utiliza a LAN.
- Tecnologia de Transmissão – a forma de comunicação é multiponto entre os computadores. Já os *switches* (comutadores de rede) fornecem ligações temporárias do tipo ponto-a-ponto.
- Topologia – a interligação entre os computadores é feita usando ligações físicas em estrela, barra ou anel, que ainda serão estudadas no decorrer deste caderno.
- Taxa de transmissão – bastante alta, da ordem de 1G ou 10G ou 100Gbps.
- Latência e Taxa de erros – baixas quando comparadas com MANs ou WANs.

As redes MAN são redes com abrangência geográfica de uma única região metropolitana, e são usadas para interligar redes locais que estejam nessa região. Também podem fornecer serviços como acesso à Internet, transmissão de TV, conexão entre centrais telefônicas etc. Na Figura 20 temos um exemplo de rede MAN que está interligando duas redes locais, uma delas possuindo servidores de banco de dados. Além disso, essa rede MAN fornece serviços de TV e telefonia.

FIGURA 20 – REDE MAN



FONTE: Dantas (2010, p. 254)

As redes MAN normalmente são oferecidas por operadoras de telecomunicações ou prestadoras de serviços autorizadas pela Anatel, órgão que regulamenta as telecomunicações no Brasil.



Uma região metropolitana é constituída por um grupo de municípios próximos entre si fisicamente. Eles devem estar integrados socioeconomicamente a um município central, que é denominado metrópole. Os serviços públicos e de infraestrutura da região metropolitana, ou seja, desses municípios, devem ser planejados regionalmente.

As redes MAN possuem como principais características a velocidade igual ou menor do que as redes LAN, os equipamentos de conexão com a MAN normalmente são locados da operadora de telecomunicações ou prestador de serviços, e a topologia normalmente é em anel.

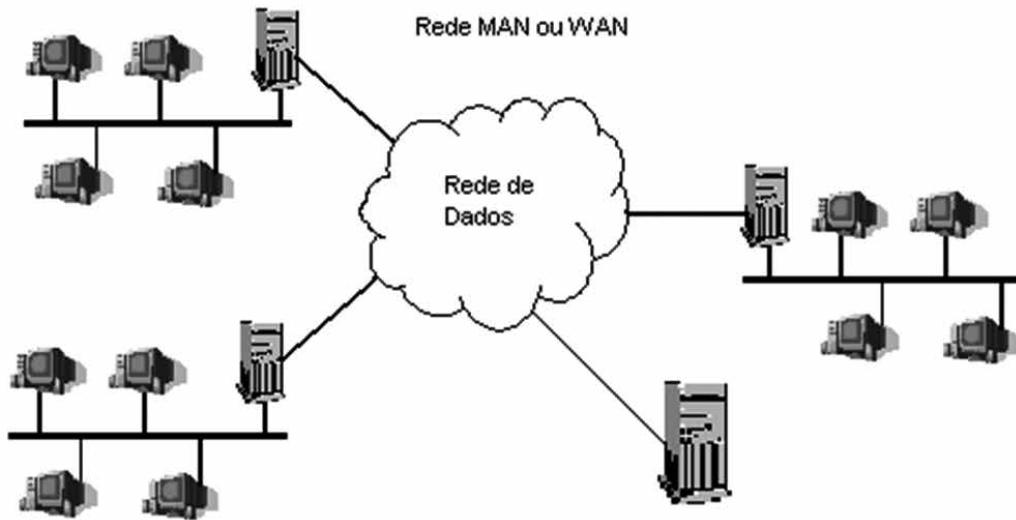
Já as redes WAN, de acordo com Amaral (2012), têm o conceito de redes de longa distância devido à sua abrangência geográfica, que pode ser imensurável, ou seja, podem interligar continentes, países e regiões através de enlaces mais longos utilizando tecnologias com satélites ou fibras ópticas (terrestres ou submarinas).

As redes WAN oferecem taxas de transmissão menores que as redes LAN e MAN, mas atualmente já chegam a dezenas de Gbps, sendo o custo do serviço, nessas velocidades altas, bastante grande. Também possuem as WANs uma latência maior (tempo que a informação leva dentro da rede para sair da origem e chegar no destino) que as LANs e MANs, além de uma taxa de erro um pouco maior. Essas duas características, latência e taxa de erro, normalmente têm seus números acrescidos conforme aumenta a distância que a informação precisa percorrer na rede para ir de sua origem ao seu destino.

Normalmente são utilizadas para interligar redes LAN ou MAN entre si, sendo que as redes WAN são redes privativas em sua maioria, mas oferecidas por operadoras de telecomunicações ou prestadores de serviços autorizados pela Anatel. São oferecidas redes com tecnologia *Frame-Relay*, mais antigas, e com tecnologia MPLS (*Multi-Protocol Label Switching*), mais modernas. Essa última tecnologia, quando aliada ao padrão DIFFSERV (*Differentiated Services*), consegue fornecer serviços de rede com garantia de QoS (*Quality of Service*) para as aplicações dos usuários dessa rede WAN MPLS. A rede Internet também é um exemplo de rede WAN, porém não existe fornecimento de QoS atualmente na rede Internet, ou seja, as informações e aplicações são transmitidas pela rede Internet sem garantias de desempenho.

As redes WAN e LAN usam atualmente, em sua maioria, a fibra óptica como meio físico de transmissão, e dessa forma acabam tendo características muito semelhantes, ficando a principal diferença entre elas a distância abrangida pelas mesmas. Dessa forma, na Figura 21 temos uma representação de redes de dados que serve tanto para WAN como para MAN, já que não está especificada a abrangência geográfica da rede representada, apenas nos mostra que está interligando três redes locais e um servidor independente, que poderia ser um *Data Center*, por exemplo.

FIGURA 21 – REDES WAN / MAN



FONTE: Disponível em: <http://www.teleco.com.br/Cbrede/pagina_3.asp>. Acesso em: 19 fev. 2016.



Um *Data Center* é um ambiente específico, normalmente um prédio dedicado a essa função, com uma excelente infraestrutura instalada para centralizar os equipamentos e as operações de TI das organizações que forem clientes dessa *Datacenter*. São prestados serviços como armazenamento, gerenciamento e disponibilização das informações aos clientes num período de 24 horas por dia, 365 dias por ano, com um percentual de falhas extremamente baixo. As grandes operadoras de telecomunicações são os principais fornecedores de serviços de *Data Center* no Brasil.

Segundo Dantas (2010), uma nova abordagem visando atender aplicações que necessitam processamento de alto desempenho está crescendo. Trata-se das redes **SAN (System Area Networks)**, que visam compartilhar sistemas de memória dos distintos sistemas computacionais que estejam ligados na SAN. **Clusters** de computadores, onde é necessário uma menor latência, alta disponibilidade e grande largura de banda, são exemplos de ambientes onde as SANs são utilizadas. Essas redes suportam distâncias de apenas poucos metros e, portanto, são bastante específicas para as aplicações mencionadas.

3.2 CLASSIFICAÇÃO CONFORME O OBJETIVO

As redes de computadores também podem ser classificadas quanto ao seu objetivo de utilização. Essa classificação não é uma classificação com base técnica, mas com base mercadológica. Nesse sentido, temos as redes Internet, Intranet e Extranet.

Antes de mais nada, é interessante analisar a diferença de significados das palavras Internet e internet. Segundo Mendes (2007, p. 20):

A Internet, com “I” maiúsculo, refere-se à rede que começou como ARPAnet, e continua como, grosseiramente falando, a confederação de todas as redes TCP/IP interligadas direta ou indiretamente. Nessa interligação, temos os *backbones* TCP/IP comerciais norte-americanos, brasileiros, europeus, redes TCP/IP regionais, redes TCP/IP governamentais, sendo todas interconectadas por circuitos digitais de alta velocidade. A internet com inicial minúscula, por sua vez, é simplesmente qualquer rede feita por múltiplas redes menores, que usam o mesmo protocolo de comunicação. Uma internet não precisa obrigatoriamente estar conectada à Internet, nem necessita usar o modelo de referência TCP/IP como protocolo de comunicação. Existem ainda Internets isoladas de corporações, conhecidas como Intranets e Extranets.

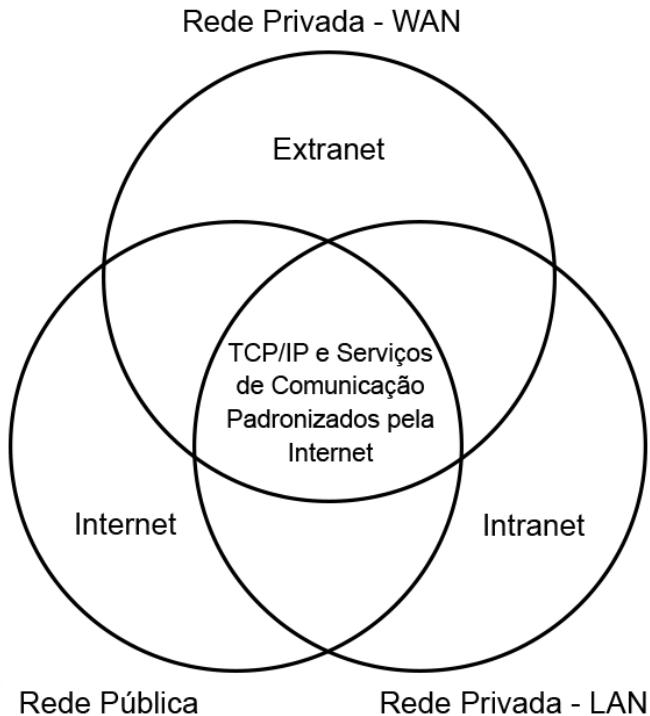
A Internet é uma rede mundial de computadores, pública, formada pela interligação de inúmeras redes menores, com milhões e milhões de usuários pelo mundo comunicando-se através da arquitetura do protocolo TCP/IP (*Transport Control Protocol/Internet Protocol*). O acesso à Internet é público, sendo que qualquer pessoa ou organização pode utilizá-la, e as informações contidas na Internet são públicas e pulverizadas pela rede. É a forma mais barata e simples para as pessoas e organizações do mundo inteiro se comunicarem, no entanto não é a mais segura nem a mais confiável.

Já as redes Intranet são redes privativas e fechadas, ou seja, seu uso é restrito a um público autorizado. Normalmente são utilizadas em organizações com o objetivo de melhorar a comunicação e a disponibilidade das informações necessárias para sua operação. Seu funcionamento e serviços são semelhantes aos da Internet, usando o protocolo TCP/IP, porém as informações ficam restritas ao ambiente da Intranet, ou seja, restrito aos usuários que tenham acesso à rede local Internet (LAN Intranet).

Quanto às Extranets, são redes privativas também, que funcionam como as Intranets, porém agora as informações podem ser acessadas do mundo externo, por funcionários, clientes e fornecedores, desde que tenham autorização de acesso, que é controlado por senhas. Assim, através da Internet é possível acessar uma Extranet, proporcionando facilidade para comunicação e novos negócios com fornecedores e clientes, visando agilidade, redução de custos e crescimento da organização que disponibiliza a Extranet.

No entanto, como o acesso pode ser feito de qualquer lugar do mundo via Internet, é necessário tomar cuidado com aspectos de segurança para evitar invasões indesejadas. Deve ser feito um planejamento específico sobre as tecnologias que serão adotadas, fornecendo vários níveis distintos de acessibilidade aos usuários externos, através de *logins* e senhas que vão determinar quais partes e informações da Extranet você poderá acessar. Na Figura 22 podemos observar a relação que existe entre as redes Internet, Intranet e Extranet, todas utilizam o mesmo protocolo TCP/IP e disponibilizam os mesmos serviços para comunicação.

FIGURA 22 – RELAÇÃO ENTRE INTERNET, INTRANET E EXTRANET



FONTE: Mendes (2007, p. 21)

3.3 TOPOLOGIAS DE REDES

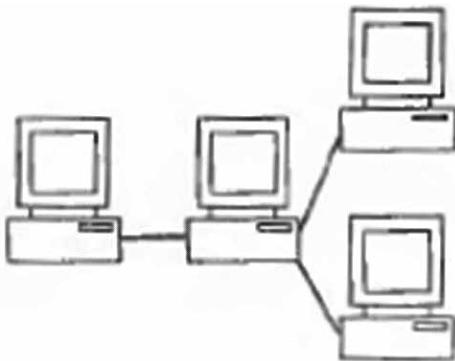
Para descrever como as redes de computadores estão interligadas, ou como seus elementos estão interligados, tanto do ponto de vista físico como do ponto de vista lógico, utilizam-se as definições de tipos de topologias de redes. Segundo Dantas (2010, p. 197), “[...] a topologia pode ser entendida como a maneira pela qual os enlaces de comunicação e dispositivos de comutação estão interligados, provendo efetivamente a transmissão do sinal entre os nodos da rede”.

A topologia de uma rede de computadores é definida através da topologia física e da topologia lógica utilizada nessa rede. A topologia física compreende a forma como os meios de transmissão (cabos metálicos, fibras ópticas etc.) conectam os elementos da rede entre si, como computadores, switches e roteadores, por exemplo. Por outro lado, a topologia lógica trata da maneira como os elementos da rede se comunicam, utilizando os meios de transmissão da mesma, ou seja, refere-se ao modo como os dados circulam entre os elementos da rede.

A topologia física e a topologia lógica, numa mesma rede, podem ser iguais ou distintas, conforme nos informa Dantas (2010, p. 197): “[...] a topologia física de uma rede pode ser representada por uma configuração estrela e a topologia lógica ser uma barra”. As redes *Token Ring*, por exemplo, usam uma topologia lógica de anel, mas usam uma topologia física de estrela. Vamos conhecer mais à frente as principais topologias de rede, que são: barramento, estrela, anel e malha.

Mas antes, caro(a) acadêmico(a), vamos falar sobre a tecnologia de transmissão. Normalmente, as redes adotam a abordagem ponto-a-ponto ou multiponto para a transmissão dos dados. No caso de redes ponto-a-ponto a transmissão dos dados é sempre feita de entre dois computadores que estejam interligados entre si, conforme mostrado na Figura 23. Neste caso, um computador A não pode transmitir dados diretamente para outro computador C que não esteja conectado fisicamente ao primeiro computador A.

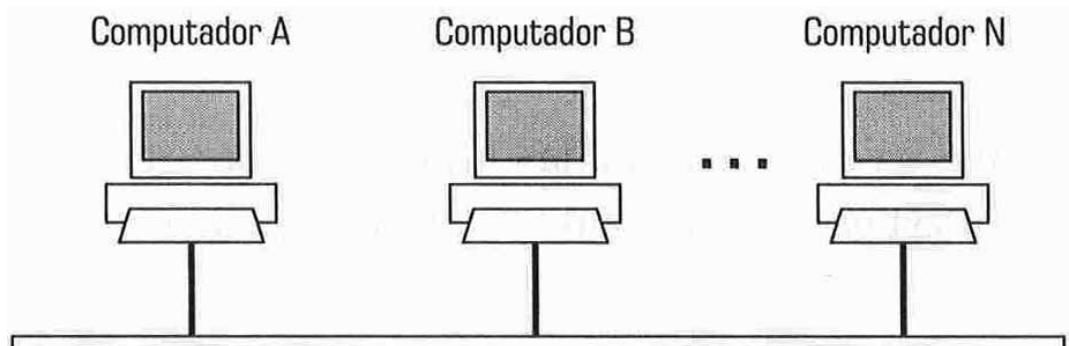
FIGURA 23 – REDE PONTO-A-PONTO



FONTE: Dantas (2010, p. 196)

Já nas redes com transmissão multiponto, os computadores estão ligados a um ponto único, como um cabo ilustrado na Figura 24 ou um equipamento *Hub*. Neste caso, um computador pode transmitir diretamente para qualquer outro computador da rede. A rede local *Ethernet* é um exemplo de rede multiponto.

FIGURA 24 – REDE MULTIPONTO



FONTE: Dantas (2002, p. 19)

Agora que vimos as tecnologias de transmissão ponto-a-ponto e multiponto, vamos falar então das topologias de redes. Começando com a topologia em barramento, também conhecida como topologia *bus*, podemos dizer que é a mais antiga e na qual os computadores ficam todos conectados ao mesmo *backbone*, ou barramento, que é constituído normalmente por um cabo tipo coaxial (falaremos sobre esse cabo no próximo tópico deste caderno). Essa topologia já foi praticamente

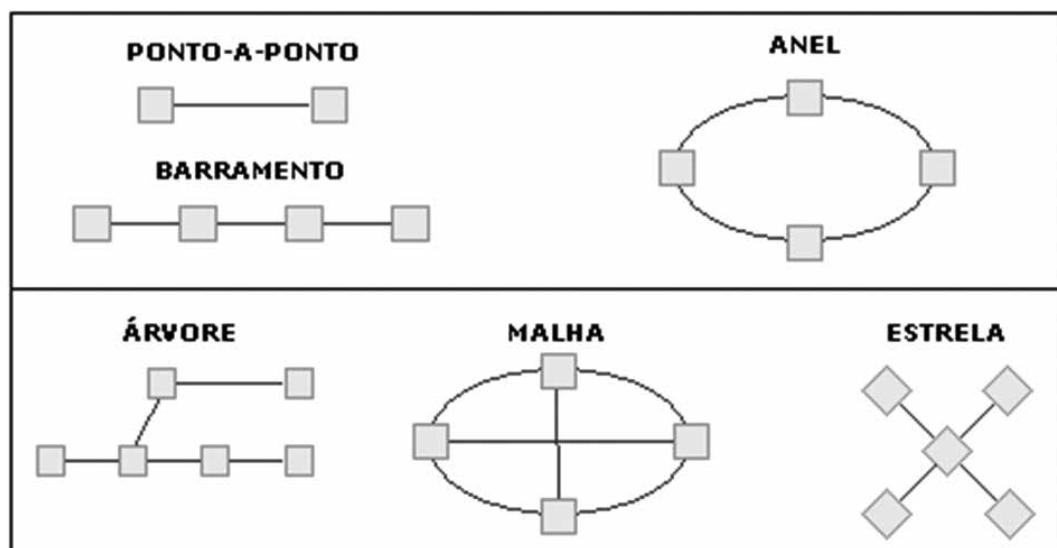
toda substituída pela topologia estrela, porque caso aconteça algum problema no *backbone*, todos os computadores deixam de comunicar-se.

Já a topologia em estrela tem como característica principal a conexão independente de cada computador a um equipamento central, chamado de concentrador, e que nos dias de hoje é o dispositivo chamado *switch* (significa comutador em inglês). No passado essa função de concentrador era feita pelos *hubs*, mas por questões de desempenho foram gradativamente sendo substituídos pelos *switches*, que possuem diversas vantagens, como será visto na Unidade 2 deste caderno.

Como vantagens principais, a topologia estrela provê uma manutenção da rede simplificada, possui baixo custo, já que o cabo utilizado é o par trançado, e caso aconteça o rompimento de um cabo, somente o computador daquele cabo deixará de funcionar.

A Figura 25 apresenta exemplos das topologias barramento e estrela, que vimos anteriormente, além das topologias anel e malha, que veremos em seguida. Ainda são apresentadas as topologias ponto-a-ponto e árvore, que não serão vistas neste caderno.

FIGURA 25 – TOPOLOGIAS DE REDES



FONTE: Disponível em: <http://www.teleco.com.br/tutoriais/tutorialsdh/pagina_3.asp>. Acesso em: 19 fev. 2016.

Na topologia em anel, cada computador da rede é conectado a dois nós (computadores) adjacentes em círculo, formando um anel fechado. A comunicação entre os computadores normalmente é feita numa determinada direção, mas em topologias mais modernas, como as utilizadas em redes de telecomunicações, essa direção poderá ser alterada no caso de alguma falha, mantendo o funcionamento da rede. Normalmente o meio físico de interligação é a fibra óptica, já que a topologia

em anel é mais indicada para redes que precisam ter alta disponibilidade (poucos períodos de interrupção). Existem protocolos de acesso ao meio, rede em anel, que trabalham de forma ordenada, e cada computador tem um tempo limite de acesso à rede, e dessa forma não ocorre piora de desempenho da rede quando existe um aumento grande de nós, ou computadores. Por outro lado, a gerência (ou controle) dessa rede em anel é complexa.

Por fim, a topologia em malha define que todos os nós da rede estão interconectados uns aos outros, formando um desenho semelhante a uma malha. Essa topologia somente é usada para conexão de equipamentos de rede, como roteadores numa rede de comunicação de uma operadora de telecomunicações. A tecnologia MPLS, que será vista no decorrer do caderno, trabalha com o conceito de topologia em malha, que também é chamada de *full-mesh*. Uma grande vantagem da topologia *mesh* é que sempre existem rotas (ou caminhos) alternativas para permitir a transferência de dados entre dois nós da rede.

4 OUTRAS CLASSIFICAÇÕES DE REDES

Além da classificação básica das redes, que é feita conforme a abrangência geográfica em **LAN, MAN e WAN**, existem diversas outras classificações, definidas com base em diversos parâmetros ou características distintas das redes de computadores. A seguir veremos mais quatro tipos de classificações de redes.

4.1 QUANTO AO ENDEREÇAMENTO

Como será visto mais à frente neste caderno, para que a informação originada num computador da rede possa chegar ao computador destino, é necessário que seja definido o endereço lógico do computador destino, ou também conhecido como endereço IP nas redes que trabalham com o protocolo TCP/IP, a grande maioria. Nesse contexto, uma rede pode ser classificada de acordo com **três tipos de endereçamento da comunicação: *Unicast*, *Multicast* e *Broadcast***. Vale ressaltar que uma rede pode implementar os três tipos de endereçamento, ou funcionar somente com um tipo de endereçamento, por exemplo.

Nas redes *Unicast* a comunicação, ou transmissão da informação, acontece sempre de uma origem para um destino. De acordo com Ghoddosi (2009), a transferência das informações é realizada com endereçamento tipo “1 para 1”, e mesmo a mensagem passando por vários nós da rede, somente um destinatário existe no endereçamento da informação. Um exemplo poderia ser um *download* de arquivo de uma máquina origem para uma máquina destino.

Já nas redes *Multicast*, a comunicação é feita partindo de uma origem e chegando num grupo de destinatários, sendo realizado o endereçamento tipo “1 para N”. Somente aquele grupo que foi endereçado irá receber efetivamente

a informação transmitida. Segundo Ghoddosi (2009), os computadores devem possuir na composição do seu endereço, além do seu endereço IP padrão, a definição de qual grupo a que pertencem. Um exemplo seria uma videoconferência entre Matriz e algumas filiais da mesma.

Para as redes Broadcast, a comunicação será feita de uma origem para todos os computadores da rede, através de endereçamento tipo “1 para todos”. O endereçamento é obtido colocando um endereço predefinido por norma internacional, e a informação chegará a todas as máquinas da rede, que deverão ler a informação recebida. Como exemplo, alguns protocolos de rede enviam broadcasts para a rede, visando obter algum retorno para montar tabelas de conversão de endereços e tabelas de roteamento, por exemplo. Na Figura 26 são representados os três tipos de endereçamento de comunicação.

FIGURA 26 – TIPOS DE ENDEREÇAMENTO DA COMUNICAÇÃO



FONTE: Disponível em <<http://www.dltec.com.br/blog/cisco/voce-conhece-mesmo-o-endereco-mac-va-alem-do-trivial-para-ir-bem-no-ccna-ou-ccent/>>. Acesso em 19 mar. 2016.

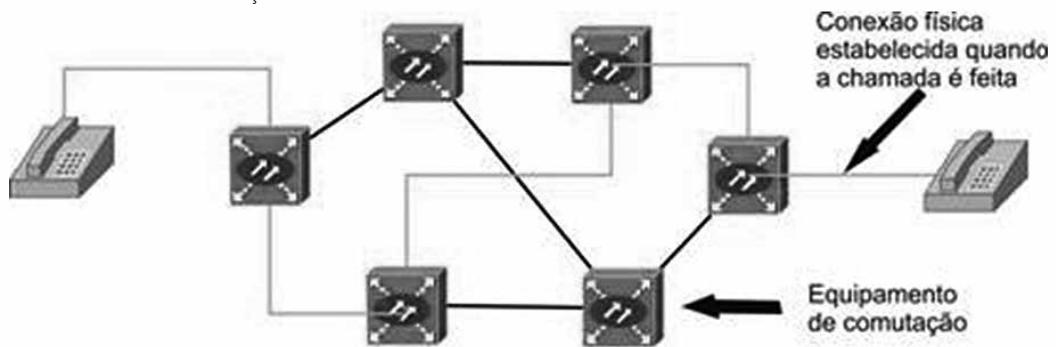
4.2 QUANTO AO TIPO DE COMUTAÇÃO

Para que uma rede consiga encaminhar uma informação de uma origem até um destino, muitas vezes precisará utilizar diversos equipamentos da rede e caminhos, ou rotas, para atingir seu objetivo. Esses equipamentos de rede são responsáveis por fazer a comutação, ou escolha de caminhos, para que a informação possa chegar no seu destino. Um exemplo é a rede telefônica atual, onde as centrais telefônicas são responsáveis por encontrar caminhos para viabilizar uma conversa telefônica entre a pessoa que efetua a ligação e a pessoa que deve receber essa ligação. As centrais estão fazendo a função de comutação, ou seja, na rede telefônica os equipamentos comutadores são as centrais telefônicas. De modo semelhante, as redes de dados possuem equipamentos, como roteadores, que

fazem a comutação na rede para que os dados possam partir da origem e chegar no seu destino. Existem dois tipos de comutação mais utilizados: a comutação de circuitos e a comutação de pacotes.

Na comutação de circuitos, mais utilizada na rede telefônica, os equipamentos comutadores devem encontrar um caminho físico entre a origem e o destino, caminho esse chamado de circuito, por onde vai fluir toda a comunicação. Na Figura 27 é apresentada uma rede baseada em comutação de circuitos, onde foi estabelecido, como exemplo, um possível caminho entre o telefone origem e o telefone destino.

FIGURA 27 – COMUTAÇÃO DE CIRCUITOS



FONTE: Disponível em: <http://www.teleco.com.br/tutoriais/tutorialvoipconv/pagina_3.asp>. Acesso em 19 mar. 2016.

Segundo Soares, Lemos e Colcher (1995), a comutação de circuitos possui três fases definidas, que são:

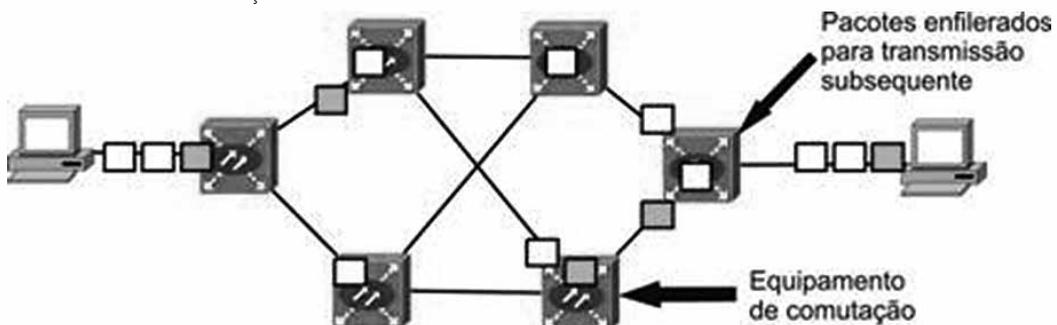
- Estabelecimento do circuito – um circuito fim-a-fim entre origem e destino é definido antes que os terminais iniciem a troca de informações. O circuito é formado por cada canal, ou enlace, entre os equipamentos comutadores, e o circuito é reservado de forma dedicada e exclusiva para essa comunicação, até que ela se encerre.
- Transferência da informação – esta fase só acontece após o estabelecimento do circuito, e somente nela pode ocorrer o processo de comunicação, ou seja, o envio e recebimento da informação entre origem e destino.
- Desconexão do circuito – nesta fase um dos terminais gera uma ação para desconexão, e os canais ou enlaces que suportavam o circuito serão liberados, ficando disponíveis para estabelecimento de novos circuitos quando necessário.

Na comutação de pacotes, mais utilizada em redes de comunicação de dados, de acordo com Soares, Lemos e Colcher (1995), não existe o estabelecimento de um circuito, sendo a comunicação viabilizada através do endereço de destino adicionado à informação que a origem deseja transmitir. Essa informação é fragmentada em pacotes, caso seja maior que um limite preestabelecido em Bytes. Assim, em cada nó, ou comutador da rede, é feita a análise do pacote, verificando o endereço de destino e encaminhando tal pacote para o próximo nó, até que chegue

no seu destino. Esse processo realizado pelos nós da rede, recebendo o pacote, analisando o endereço e então encaminhando o mesmo, é denominado de *store-and-forward*.

Nas redes que usam comutação de pacotes, quando o tráfego de informação nos enlaces for muito alto, pode acontecer que pacotes sejam enfileirados nos comutadores até que consigam ser transmitidos, e, caso esse tempo seja muito grande, poderá ocorrer o descarte de alguns ou vários pacotes, gerando a conhecida perda de pacotes. Na Figura 28 temos uma rede baseada em comutação de pacotes com tráfego de informação (pacotes) entre uma origem e um destino.

FIGURA 28 – COMUTAÇÃO DE PACOTES



FONTE: Disponível em: <http://www.teleco.com.br/tutoriais/tutorialvoipconv/pagina_3.asp>. Acesso em 19 mar. 2016.

Como não existe o estabelecimento de um circuito fixo, dedicado, os pacotes podem ser transmitidos através de caminhos diversos, desde que cheguem ao destino. Assim, a comutação de pacotes torna-se mais tolerante às falhas do que a comutação de circuitos, já que os pacotes podem utilizar rotas alternativas para alcançar o destino, e isso é muito desejável. Por outro lado, os pacotes poderão chegar fora da ordem de transmissão, pois é possível que diferentes pacotes percorram diferentes caminhos, e isso não é muito bom. Entretanto, dependendo da aplicação é possível corrigir essa ordem dos pacotes através de *software*, resolvendo esse problema.

Existem várias diferenças entre a comutação de circuitos e a comutação de pacotes, mas, para Tanenbaum (1994, p. 106):

A diferença fundamental é que a comutação de circuitos reserva antecipadamente a banda passante necessária [circuito físico], [...], enquanto que a comutação de pacotes adquire e libera a banda passante conforme necessário. Com a comutação de circuitos, qualquer banda passante não utilizada em um circuito alocado é simplesmente desperdiçada. Na comutação de pacotes, ela pode ser utilizada por pacotes vindos de origens não relacionadas, seguindo para destinos também não relacionados, visto que os circuitos não são dedicados.

Existem dois modos de funcionamento nas redes comutadas por pacotes, que são o modo orientado à conexão e o modo não orientado à conexão. Segundo Almeida (2011), no modo não orientado à conexão, os pacotes são encaminhados através da rede levando em consideração somente a informação existente no cabeçalho do pacote, como seu endereço de destino. Ou seja, não existe nenhum tipo de negociação sobre conexão origem/destino, feita anteriormente pelos nós de origem, nós intermediários e nó de destino. Neste modo, os pacotes são roteados na rede com base nos algoritmos de roteamento existentes em cada nó, podendo as rotas variarem instantaneamente conforme o *status* da rede naquele momento, de forma imprevisível.

No modo orientado à conexão, de acordo com Almeida (2011), os pacotes são encaminhados na rede através de técnicas predefinidas de negociação e reserva de recursos entre os nós da rede. Neste modo existe, portanto, uma fase de configuração da conexão, gerando uma rota definida por onde passarão todos os pacotes dessa conexão, e somente depois dessa fase é que pode acontecer a transferência de informações. Ao final da transferência existe a fase de liberação dos recursos, ou seja, é desfeita a conexão previamente configurada. Em caso de falha da rede, o tráfego é transferido (re-roteado) para um novo caminho que pode ser definido anteriormente pelo administrador da rede.

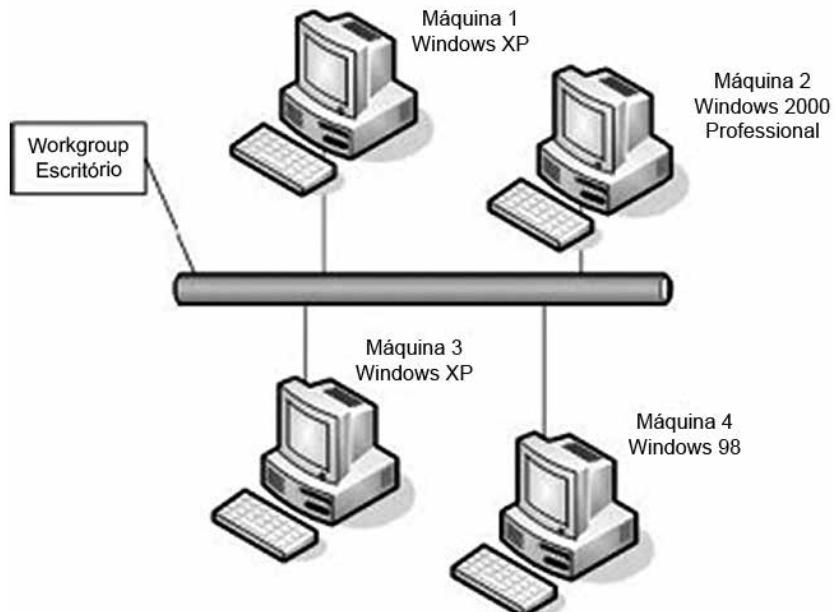
Um exemplo de protocolo de rede de pacotes, baseado em modo não orientado à conexão, é o protocolo IP (*Internet Protocol*), utilizado na rede Internet. Exemplo de protocolo baseado em modo orientado à conexão é o protocolo MPLS (*Multiprotocol Label Switching*), utilizado em redes privativas oferecidas por operadoras de telecomunicações.

4.3 QUANTO À ARQUITETURA DE COMPARTILHAMENTO

Com relação à forma com que as informações são compartilhadas numa rede de computadores, existem basicamente duas, que são as redes ponto-a-ponto e as redes cliente/servidor. Essa classificação depende da configuração feita em *software*, e não da topologia física com a qual a rede está implementada.

As redes ponto-a-ponto, também chamadas P2P (*peer-to-peer*), conforme Torres (2001), são redes nas quais todos os computadores podem compartilhar dados e periféricos com os outros computadores da rede, ou seja, todos os computadores podem ser clientes ou servidores, dependendo da necessidade dos usuários e dos recursos disponíveis em cada computador. A Figura 29 apresenta uma possível rede ponto-a-ponto utilizada num escritório, por exemplo.

FIGURA 29 – REDE PONTO-A-PONTO

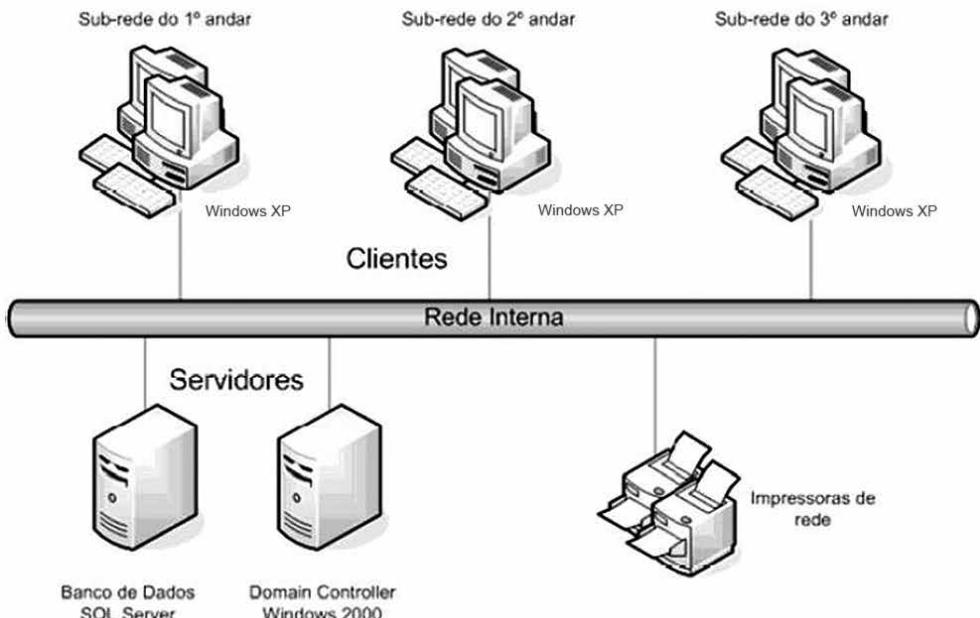


FONTE: Ross (2008, p. 13)

De acordo com Torres (2001), as principais características dessa arquitetura são: utilização em redes pequenas com no máximo 10 computadores, oferece baixo custo de implantação e manutenção, fácil implementação, baixa segurança da informação, não existe a figura do administrador de redes e não existem computadores servidores.

Por outro lado, nas redes cliente/servidor existe no mínimo um computador com *status* de servidor, mas pode existir mais de um servidor numa mesma rede. Recursos são compartilhados com os computadores da rede a partir do(s) servidor(es). Importante notar que o servidor fica dedicado para as tarefas que a ele foram definidas, ou seja, ele não vai executar outros processos que possam atrapalhar seu objetivo principal de ser o servidor de determinados recursos. Dessa forma, considerando que a função de um servidor é responder requisições dos clientes, sua velocidade no atendimento aos clientes torna-se bem melhor do que um computador temporariamente servidor numa rede ponto-a-ponto. Na Figura 30 temos a representação de uma rede cliente/servidor, onde podemos notar a existência de dois servidores, impressoras de rede e três subredes representadas pelos conjuntos de dois computadores.

FIGURA 30 – REDE CLIENTE/SERVIDOR



FONTE: Ross (2001, p. 14)

Os servidores podem oferecer recursos de aplicações, de arquivos, de impressão, de backup, de comunicação, de e-mail, entre outros recursos que podem ser úteis em redes de computadores. As principais características das redes cliente/servidor, segundo Torres (2008), são: utilização em redes com mais de 10 computadores ou redes menores cuja segurança deve ser mais alta, maior custo de implantação e manutenção, maior desempenho que as redes ponto-a-ponto, necessita dos serviços de um profissional administrador de redes e viabiliza utilização de aplicações com banco de dados que não são suportadas em redes ponto-a-ponto.

RESUMO DO TÓPICO 2

Neste tópico vimos que:

- Existem várias definições para redes de computadores, mas podemos resumir como um conjunto de recursos que permitem a efetiva troca de informações entre computadores que estejam fisicamente próximos ou muito distantes entre si.
- Aplicações de redes de computadores existem as mais diversas, e novas são desenvolvidas constantemente sempre com o objetivo de trazer benefícios para os usuários.
- As redes podem ser classificadas conforme sua abrangência geográfica em PAN, LAN, MAN e WAN, cada uma com suas características e funcionalidades.
- Existem diferenças importantes entre as redes chamadas Internet, Intranet e Extranet, onde cada uma possui objetivos diferenciados.
- As principais topologias de rede são barramento, estrela, anel e malha, e o tipo de transmissão entre os computadores pode ser ponto-a-ponto ou multiponto.
- A comunicação entre computadores pode ser feita usando endereçamentos tipo *Unicast*, *Multicast* e *Broadcast*, que define para quantos computadores a informação é destinada.
- As redes, quanto ao tipo de comutação nos equipamentos responsáveis, podem ser comutadas por circuitos ou comutadas por pacotes. Estas últimas podem ser orientadas à conexão ou não orientadas à conexão.
- As redes podem compartilhar ou trocar informações no formato ponto-a-ponto ou no formato cliente/servidor, devendo ser corretamente configuradas para tanto.

AUTOATIVIDADE



- 1 Apresente uma definição para redes de computadores usando as suas palavras.
- 2 As redes podem ser classificadas conforme sua abrangência geográfica. Nesse sentido, disserte sobre as redes LAN e WAN utilizando as suas palavras.
- 3 Explique as diferenças entre comunicação *Multicast* e *Broadcast* usando as suas palavras.
- 4 Explique as diferenças entre Internet, Intranet e Extranet usando as suas palavras.
- 5 Explique as diferenças que existem entre as redes ponto-a-ponto e redes cliente/servidor.



Assista ao vídeo de
resolução da questão 4



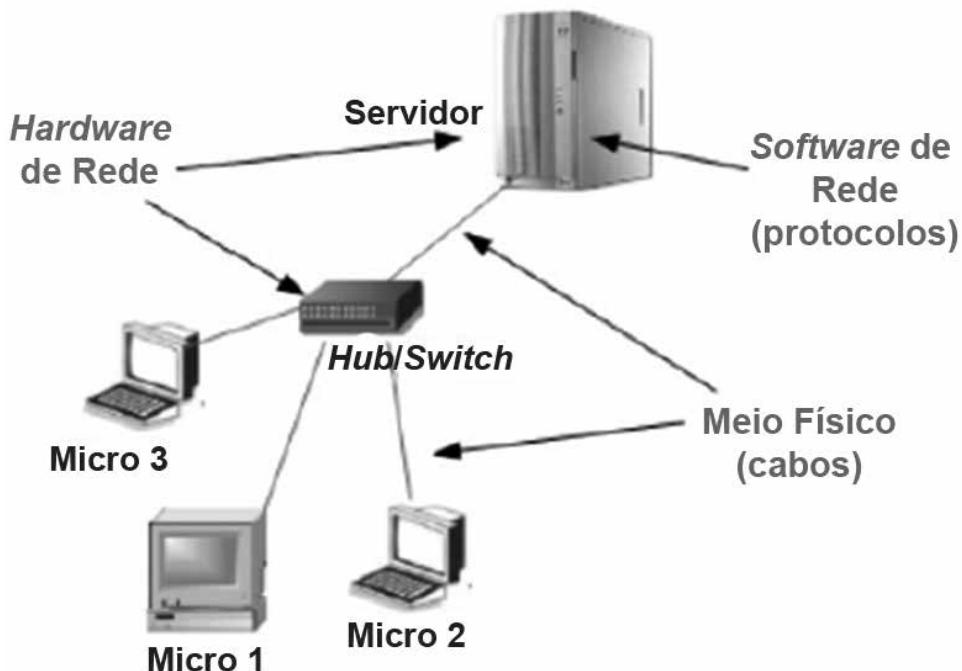
COMPONENTES DAS REDES DE COMPUTADORES

1 INTRODUÇÃO

Caro(a) acadêmico(a), até aqui estudamos conceitos básicos de comunicação de dados e também conceitos básicos de redes de computadores. Foram vistos definição e aplicação de redes, topologias de redes e além disso, diversas classificações e tipos de redes. Mas quais são os componentes ou dispositivos que tornam o funcionamento das redes possível?

Para que uma rede de computadores funcione adequadamente, é necessário que um conjunto mínimo de componentes esteja instalado e operacional, ou seja, corretamente configurado e ativado. Os grupos de componentes básicos que formam uma rede de computadores podem ser vistos na Figura 31.

FIGURA 31 – COMPONENTES DAS REDES DE COMPUTADORES



FONTE: Latzke e Gross (2013, p. 9)

O meio físico, o *hardware* de rede e o *software* de rede são os grupos básicos de componentes de uma rede de computadores. O meio físico é responsável pelo transporte do sinal que contém a informação a ser entregue no destino. O *hardware* de rede engloba todos os equipamentos de rede, como *hub*, *switch*, roteador, e também os computadores servidores e clientes. Quanto ao *software* de rede, é o grupo de programas responsável por viabilizar a troca de informações entre máquinas, composto por sistemas operacionais de rede e também os protocolos da arquitetura de comunicação em rede.

Segundo Latzke e Gross (2013), pode-se identificar os grupos de componentes básicos de uma rede inclusive analisando um exemplo antigo, a comunicação usando telégrafos. Vejam que o fio do telegrafo correspondia ao meio físico por onde o sinal elétrico correspondente à mensagem era transportado, o aparelho telegrafo correspondia ao *hardware* de rede e o Código Morse, desenvolvido para representar as letras do alfabeto através de sinais distintos, correspondia ao *software* de rede.

2 OS MEIOS FÍSICOS DE REDE

Os meios físicos de rede, também chamados mídias de transmissão, são os canais ou enlaces pelos quais trafega o sinal físico, responsável por transportar a informação entre uma origem e um destino. Os diversos meios físicos possuem características físicas diferentes, e por isso cada meio é adequado para certa aplicação, já que influencia diretamente na velocidade máxima da transmissão e na distância máxima alcançada por este enlace.

Podemos classificar os meios de transmissão em meios guiados e meios não guiados. Cada meio de transmissão possui suas propriedades intrínsecas, que consistem em fatores limitantes para a capacidade da rede. Para obtermos os melhores resultados com os meios de transmissão numa rede, devemos observar certos pontos, pois conforme Dantas (2010, p. 76):

Numa transmissão guiada, por exemplo, o cuidado que devemos observar para atingir uma qualidade de transmissão aceitável é o tipo de meio físico empregado na transmissão. Este é o fator limitante do ambiente. Por outro lado, numa comunicação onde utilizamos os meios não guiados (ou ambientes sem fio), a intensidade do sinal e os ruídos durante a transmissão são pontos onde devemos concentrar nossa atenção para obtermos uma transmissão com melhor qualidade.

2.1 OS MEIOS GUIADOS

Os meios de transmissão guiados podem ser separados em dois grupos, sendo um grupo dos meios com fio de cobre e outro grupo dos meios ópticos. No grupo dos meios com fio de cobre os principais são o cabo coaxial e o par trançado, enquanto que no grupo dos meios ópticos temos como principais os cabos de fibras ópticas.

O cabo coaxial é formado por um condutor interno e outro externo, sendo este uma malha de cobre trançado, separados fisicamente por um material isolante, conforme pode ser visto na Figura 32. Sobre a malha, cujo objetivo é evitar interferências externas, existe uma capa flexível com objetivos de proteção física e antichamas.

FIGURA 32 – CABO COAXIAL



FONTE: Disponível em <<http://radiocomunicacaopxvhf.blogspot.com.br/2011/04/cabo-coaxial.html>>. Acesso em: 19 mar. 2016.

Os cabos coaxiais já caíram em desuso, sendo substituídos pelo par trançado, mas ainda existem aplicações como nos serviços prestados pelas empresas de TV a cabo (CATV). Esses cabos podem ser usados para transmitir sinais analógicos, com uso de amplificadores a distâncias regulares de alguns quilômetros, ou sinais digitais com repetidores de sinal a cada quilômetro. Vale ressaltar que quanto maior a frequência analógica ou taxa de transmissão digital utilizada, menor será a distância alcançada.

O par trançado é o meio de transmissão mais simples e vem desde o início da década de 90 substituindo o cabo coaxial. O cabo de pares trançados é mais flexível do que o cabo coaxial, suporta velocidades maiores, propicia uma instalação mais fácil, além de ter menor custo.

O par trançado consiste de dois fios de cobre entrelaçados em forma helicoidal, sendo que esse entrelaçamento tem o objetivo de reduzir a interferência eletromagnética que existiria se fossem pares paralelos. A qualidade do cabo de pares trançados será maior, quanto maior for o número de tranças por centímetro existente no cabo, porque maior será o efeito do cancelamento da interferência eletromagnética entre os pares. A Figura 33 mostra um cabo com quatro pares trançados, onde podemos ver claramente as tranças que existem nos pares de fios.

FIGURA 33 – CABO DE PAR TRANÇADO COM QUATRO PARES

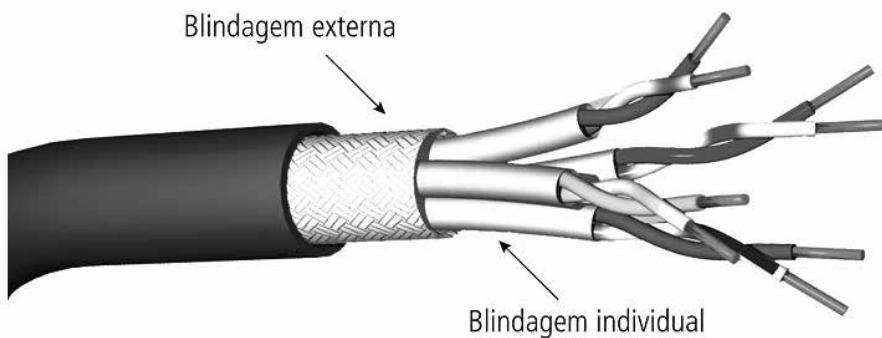


FONTE: Amaral (2012, p. 55)

Existem dois tipos de cabos de par trançado, classificados conforme a blindagem do cabo (existente ou não). De acordo com Amaral (2012), são eles:

- STP (*Shielded Twisted Pair* – Par Trançado Blindado) – este cabo tem uma malha em volta de cada par para protegê-lo individualmente contra interferências externas, e também possui uma malha externa protegendo todo o conjunto de pares do cabo. Esse tipo de cabo, portanto, é mais imune a interferências do meio externo, porém tem um custo mais alto que o outro tipo de cabo, chamado UTP, e é menos flexível, sendo mais trabalhoso passá-lo por tubulações. Seu uso é mais indicado para ambientes industriais onde o nível de interferências geradas pelo ambiente é maior. A Figura 34 mostra um cabo STP com quatro pares trançados.

FIGURA 34 – CABO DE PAR TRANÇADO TIPO STP



FONTE: Amaral (2012, p. 57)

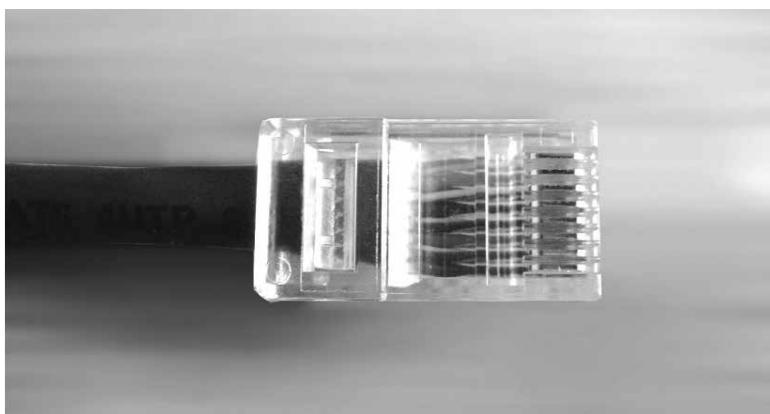
- UTP (*Unshielded Twisted Pair* – Par Trançado Não Blindado) – esse cabo não possui malha individual nem malha externa de proteção. É o cabo mais simples e mais barato, muito utilizado em redes locais empresariais e residenciais. Como é um cabo mais leve e mais flexível que o STP, torna-se mais fácil sua passagem por tubulações. Um exemplo de cabo de par trançado UTP já foi apresentada na Figura 33.

Os cabos de pares trançados são classificados em categorias, e atualmente o padrão TIA/EIA 568-B define as seguintes categorias:

- Categoria 3 – velocidade até 10 Mbps, uso em redes *Ethernet*.
- Categoria 5 – velocidade até 100 Mbps, para uso em redes *Fast Ethernet*.
- Categoria 5e – velocidade até 1 Gbps, para uso em redes *Gigabit Ethernet*.
- Categoria 6 – velocidade até 1 Gbps, para uso em redes *Gigabit Ethernet*.
- Categoria 6A – velocidade até 10 Gbps, para uso em redes *10 Gigabit Ethernet*.
- Categoria 7 e 7A – padrões em desenvolvimento, mas devem chegar a 40 e 100 Gbps.

Nas pontas dos cabos UTP são instalados, ou crimpados, conectores tipo RJ-45 para conectar nas interfaces de rede ou nas portas dos equipamentos de rede (*switches* ou roteadores). Na Figura 35 podemos ver um conector RJ-45 crimpado num cabo de par trançado tipo UTP categoria 5.

FIGURA 35 – CONECTOR RJ-45 PARA CABOS DE REDES

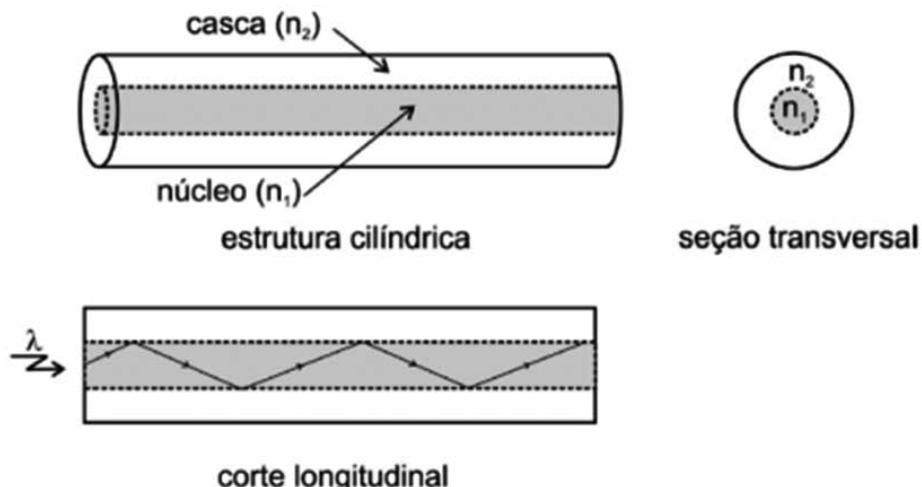


FONTE: Amaral (2012, p. 58)

Os cabos de fibra óptica não transmitem energia elétrica (na forma de elétrons), como fazem os cabos coaxial e par trançado, mas transmitem energia luminosa (na forma de fótons). A composição da fibra óptica é simples, tratando-se de um cilindro interno chamado de núcleo, muito fino, flexível, e com capacidade de conduzir raios de luz; feito de sílica, vidro ou plástico; e revestido por uma casca cujo material tem índice de refração da luz diferente do núcleo.

Na fibra óptica é utilizado o conceito de reflexão do sinal luminoso na casca da fibra, que deve possuir um índice de refração da luz (n_2) diferente do índice de refração do núcleo (n_1), obtendo dessa forma o transporte da luz que fica confinada no núcleo da fibra, e assim a fibra consegue alcançar longas distâncias de transporte. A Figura 36 mostra o princípio de funcionamento da fibra óptica, onde um raio de luz com comprimento de onda lambda (λ) entra na fibra e através da reflexão na casca é conduzido para o outro lado da fibra. É mostrado também que os índices de refração no núcleo e na casca devem ser diferentes, além do diâmetro da casca ser bem maior que do núcleo.

FIGURA 36 – LUZ NA FIBRA ÓPTICA



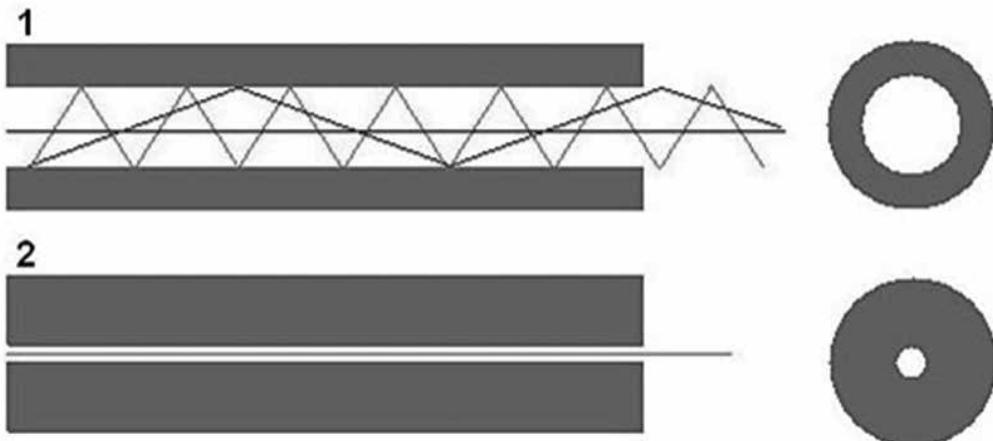
FONTE: Disponível em: <http://osfundamentosdrafisica.blogspot.com.br/2013/10/cursos-do-blog-termologia-optica-e-ondas_8.html>. Acesso em: 19 mar. 2016.

É feita uma classificação das fibras ópticas de acordo com a forma que a luz é transportada no núcleo da fibra. A explicação apresentada por Dantas (2010, p. 86) é a seguinte:

Temos a classificação das fibras como monomodo e multimodo. No tipo da classe monomodo, um único sinal de luz é transportado de uma forma direta no núcleo do cabo. O sinal pode atingir distâncias maiores sem repetição nesta forma de tráfego da luz, quando comparado com a transmissão da segunda classe de fibra. Uma fibra multimodo tem como característica um feixe de luz que viaja ao longo do seu trajeto fazendo diferentes refrações ao longo das paredes do núcleo do cabo.

Na Figura 37 mostramos o transporte do sinal luminoso numa fibra multimodo e numa fibra monomodo, onde podemos ver que na fibra multimodo um sinal de luz trafega com muitos modos ao longo do núcleo, gerando maior atenuação e menor velocidade de transmissão.

FIGURA 37 – FIBRAS MULTIMODO E MONOMODO



FONTE: Disponível em <<http://d705243685.tecla337.tecla.com.br/blog/165-tecnologia-optica>>. Acesso em: 20 mar. 2016

Portanto, a fibra monomodo é melhor, consegue alcançar dezenas de quilômetros de transmissão, enquanto a multimodo fica por volta de centenas de metros de alcance. Também ressaltamos que na fibra monomodo o diâmetro do núcleo é bem menor, por volta de 8 a 10 micrômetros, enquanto que na fibra multimodo o diâmetro fica entre 50 e 60 micrômetros. A fibra monomodo tem um custo maior pela sua qualidade e maior é a dificuldade para sua fabricação, sendo mais utilizada por operadoras de telecomunicações para redes de transmissão de longa distância, enquanto que a fibra multimodo é mais utilizada em redes locais. Além das distâncias consideráveis que alcançam, as fibras ópticas têm a vantagem de serem bastante flexíveis, facilitando a instalação, e ainda são totalmente imunes a interferências eletromagnéticas do meio externo.

2.2 OS MEIOS NÃO GUIADOS

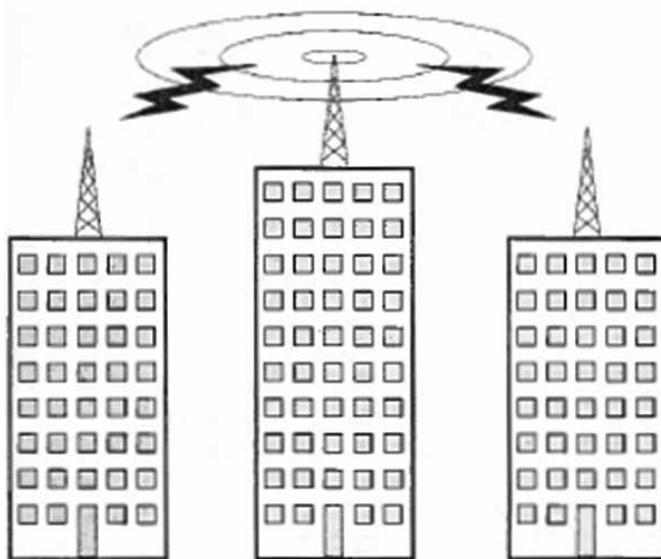
Na categoria dos meios não guiados, ou seja, os meios de transmissão que não utilizam fios ou cabos, existem três grupos, basicamente: os baseados em RF (Radiofrequências), os baseados em infravermelho e os baseados em laser. Dessa forma, os meios não guiados utilizam o próprio ar (ou espaço livre) como meio físico de transmissão.

Segundo Amaral (2012), para viabilizar uma comunicação sem fio é necessário utilizar transmissores e receptores, acoplados às antenas com tamanhos adequados, que utilizam frequências emitidas no ar para se comunicar. Frequência é o número de oscilações por segundo de uma onda eletromagnética, sendo medida em Hz (Hertz).

Sobre a utilização dos meios guiados, Dantas (2010) nos diz que a preferência de utilização deve ser dada aos meios guiados, pois possuem baixa latência, custo menor e são mais imunes a interferências externas. Os meios não guiados devem ser usados quando existe impedimento do uso dos meios guiados, como, por exemplo, uma transmissão em desertos, pântanos ou cidades nas quais não seja permitida a instalação de cabos por alguma razão legal (e isso acontece de fato).

Os meios baseados em RF (Radiofrequências) são bastante utilizados e existem dois modos de transmissão. O primeiro modo é a transmissão omnidirecional, na qual as ondas se propagam em todas as direções ao redor da antena transmissora, permitindo que antenas receptoras diversas que estejam na região de alcance consigam captar as informações. Assim, esse modo não é seguro, mas tem suas aplicações para os casos em que a informação é pública. Se for necessário segurança, pode-se ativar sistemas de criptografia nas informações. A Figura 38 mostra um exemplo de transmissão omnidirecional externa, mas pode ser utilizada internamente em prédios ou residências também.

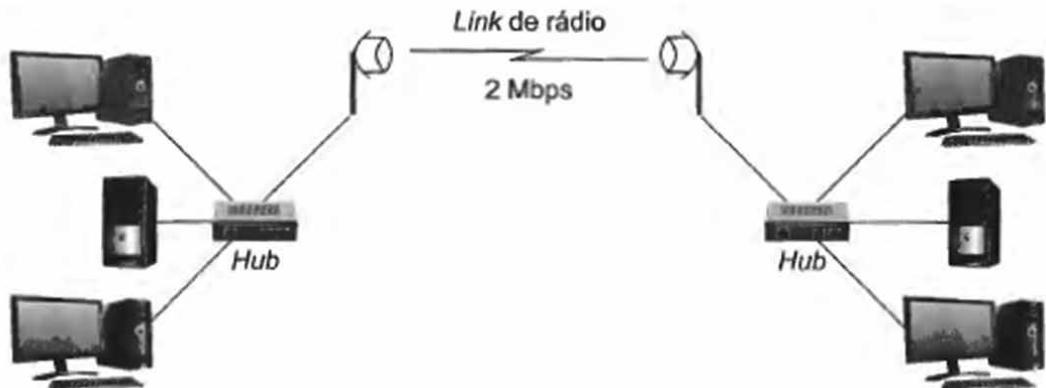
FIGURA 38 – TRANSMISSÃO DE RÁDIO TIPO OMNIDIRECIONAL



FONTE: Torres (2001, p. 254)

O modo de transmissão direcional faz uso de duas antenas que formam um único enlace, ou seja, somente um sistema receptor vai captar as informações. É mais seguro, portanto, mas é necessário que as duas antenas estejam alinhadas perfeitamente, ou, em outras palavras, estejam em visada direta. Na Figura 39 temos um exemplo de transmissão direcional, onde está viabilizada uma comunicação de dados na velocidade de 2Mbps.

FIGURA 39 – TRANSMISSÃO DE RÁDIO DIRECIONAL



FONTE: Sousa (2014, p. 32)

Foram desenvolvidas diversas tecnologias para transmissão de dados através de radiofrequências, operando em frequências distintas, como sistemas de comunicação via satélite para comunicações a grandes distâncias, sistemas de comunicação WiFi que permitem a implementação de redes locais sem fio (Wireless), entre outros.



Para conhecer mais sobre os sistemas e tecnologias de transmissão de dados via ondas de rádio, sugerimos as páginas 260 até 267 da bibliografia Torres (2001), além de acessar o artigo “O que é Wi-Fi (IEEE 802.11)?”, que você, caro(a) acadêmico(a), pode encontrar em <<http://www.infowester.com/wifi.php>>. Veja o espectro completo de frequências em Moraes (2014, p. 104).

Os sistemas baseados em infravermelho não necessitam de licença para operação, diferentemente de alguns sistemas de RF que precisam de licença da Anatel para operar. A luz infravermelha, não visível ao ser humano, é utilizada para comunicação entre os dispositivos. A frequência do infravermelho fica acima das micro-ondas e abaixo da luz visível. Sua maior utilização é doméstica, em aparelhos de TV e som, mas também pode ser utilizada para redes de computadores em dispositivos pequenos, como um smartphone, por exemplo.

A transmissão em sistemas de infravermelho pode ser em visada ou em difusão. Na primeira, os dispositivos precisam estar praticamente alinhados, pois o sinal é enviado de forma direcional pelo transmissor. Na segunda, o sinal é enviado em todas as direções e, dessa forma, os dispositivos não precisam estar alinhados, no entanto, o alcance será menor que na transmissão em visada.

A limitação de distância é uma desvantagem, assim como o fato da luz infravermelha não atravessar barreiras sólidas, como paredes, por exemplo. O alcance do infravermelho pode chegar a 30 metros em visada, e a capacidade de dispositivos até 15.

Já os sistemas baseados em laser, que utilizam técnica semelhante ao infravermelho, mas operando em outra faixa de frequência, são altamente direcionais. Isto faz com que os dispositivos transmissor e receptor devam estar precisamente alinhados entre si, além de estarem fixos para que não seja perdido o alinhamento e, consequentemente, a comunicação.

Também não necessitam de licença da Anatel e como aplicação podemos citar a interconexão de LAN's entre prédios, por exemplo, desde que a visada seja perfeita. O sistema laser tem como vantagem em relação ao infravermelho o fato de obter um alcance muito maior devido à potência e direcionalidade dos transmissores. Por outro lado, sistemas laser são muito sensíveis a condições climáticas, como chuva e neblina, as quais podem prejudicar a visada e interromper a comunicação.

3 O *HARDWARE* DE REDE

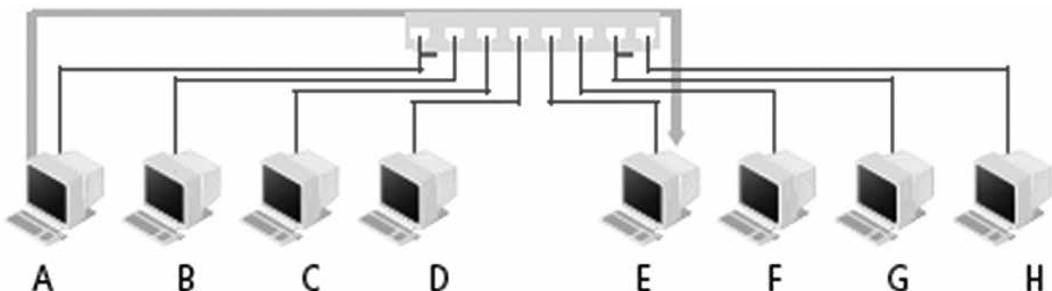
O *hardware* de rede é o grupo de componentes de rede que contém os dispositivos, ou equipamentos, utilizados para viabilizar fisicamente uma comunicação em rede. Deve-se ter o cuidado para não confundir com os meios físicos de transmissão, já que estes são responsáveis por transportar os sinais físicos (elétricos, luminosos, eletromagnéticos) entre os dispositivos. **Os principais dispositivos do grupo *hardware* de rede são o *hub*, o *switch*, o roteador, o *modem*, as placas de rede, as estações de trabalho e os servidores.**

O *hub* é um dispositivo mais antigo, sendo o primeiro utilizado para implementar as redes locais (LAN) na topologia estrela, interligando os computadores através de cabos de pares trançados. Trabalha na camada física sendo basicamente um repetidor, cuja função é regenerar, amplificar e retransmitir o sinal recebido numa porta, para todas as suas outras portas. Dessa forma, um pacote que chega numa porta do *hub* é enviado para todas as outras portas do mesmo, e, assim, todos os segmentos da LAN receberão tal pacote. No entanto, somente o computador com o endereço de destino do pacote irá processá-lo, os demais vão desconsiderar o pacote.

Os *hubs* são muito rápidos, já que fazem somente uma repetição em *hardware* de um sinal, no entanto, todos os dispositivos conectados ao *hub* vão compartilhar a velocidade do mesmo, e isso faz com que o desempenho da rede seja reduzido. Assim, caso tenhamos três dispositivos conectados a um *hub* de 10Mbps, cada dispositivo terá disponível somente 3,33 Mbps quando estiverem transmitindo ao mesmo tempo. O *hub* será melhor estudado na Unidade 2.

Já os *switches* não trabalham com velocidade compartilhada, ou seja, se tivermos três dispositivos conectados a um *switch* de 10Mbps, todos os três podem usar a velocidade de 10Mbps. O *switch* trabalha na camada de enlace do modelo OSI, como será melhor visto na Unidade 2 deste caderno, e por isso um pacote que chega é enviado somente para a porta na qual está conectado o computador destinatário desse pacote. Isso reduz, ou praticamente extingue, a quantidade de colisões que podem ocorrer na rede, melhorando o desempenho da mesma. Na Figura 40 temos uma representação de rede com oito computadores conectados a um *switch*, onde a estação “A” envia uma informação para a estação “E”, sendo que o *switch* não envia essa informação para outras portas, somente para a porta na qual está a estação “E”.

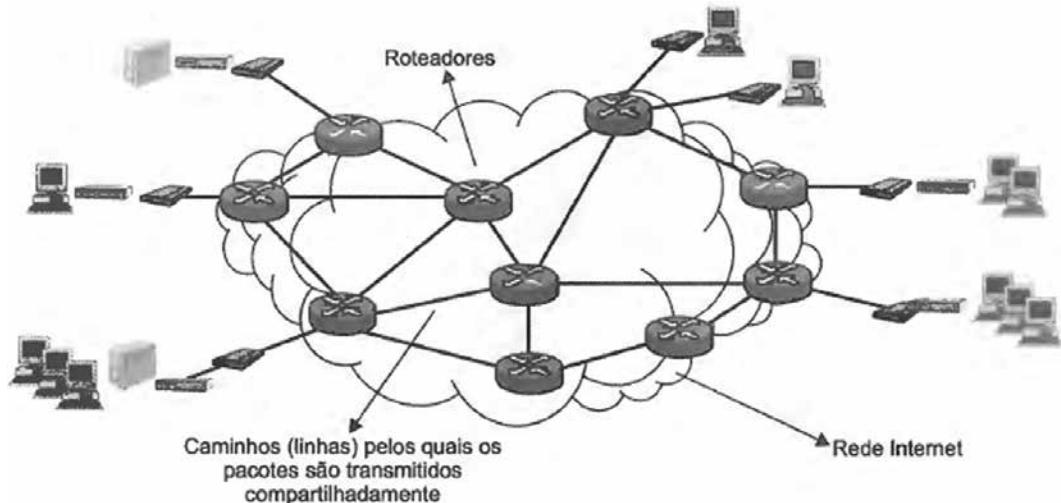
FIGURA 40 – REDE COM SWITCH



FONTE: Amaral (2012, p. 43)

Os roteadores têm a função de viabilizar a troca de informações entre redes, sendo que normalmente essas redes estão distantes entre si, ou seja, os roteadores interligam redes WAN. A identificação do caminho na rede WAN para chegar à rede de destino é feita pelos roteadores através dos protocolos de roteamento, como será visto mais adiante. A rede Internet, por exemplo, é formada pela interligação de inúmeras redes e através de inúmeros roteadores de grande, médio e pequeno porte espalhados pelo nosso planeta Terra, sob responsabilidade das operadoras de telecomunicações nos diversos países, e também prestadores de serviços (provedores de acesso e provedores de conteúdo), como representa a Figura 41.

FIGURA 41 – ROTEADORES NA REDE INTERNET



FONTE: Sousa (2013, p. 16)

O *modem*, abreviação de modulador/demodulador, tem a função de adequar e transmitir os dados através do meio físico de transmissão. Se o meio for fibra óptica, utiliza-se um *modem* óptico; se o meio for rede metálica, utiliza-se um *modem* para par metálico; se o meio for radiofrequência, utiliza-se um *modem* rádio, e assim por diante.

No caso do serviço ADSL (ou Banda Larga) que utilizamos em nossas residências, muitas vezes, emprega-se um *modem* analógico que compartilha os serviços de voz (telefonia convencional) e dados (ADSL-Assimetric Digital Subscriber Line). Atualmente os serviços ADSL usando par metálico chegam a velocidades de até 30Mbps, mas já é possível chegar a 100Mbps usando como meio de transmissão a fibra óptica. Neste caso, a operadora de telecomunicações leva uma fibra óptica até a residência do usuário, mas é óbvio que o preço do serviço será maior.

As placas de rede, também conhecidas como interface de rede ou como NIC (*Network Interface Card*), são necessárias nos computadores para que possam se conectar à rede local. São responsáveis por adequar a informação a ser transmitida na rede montando o quadro conforme o protocolo de rede utilizado e enviando pela rede. Também o processo contrário é executado, ou seja, quando uma informação chega pela rede a placa identifica através do MAC address (endereço MAC) se essa informação deve ser recebida pelo computador no qual está a placa, e caso positivo, encaminha a informação utilizando o protocolo de rede para o nível superior que é o computador.



O endereço MAC, ou MAC address, é um endereço que existe em cada placa de rede (ou dispositivo de rede) para identificar esse hardware. É formado por seis octetos, sendo que os três primeiros identificam o fabricante do hardware e os outros três octetos referem-se a uma identificação interna definida pelo fabricante para esse hardware. Não existem, no mundo, dois endereços MAC iguais.

A placa de rede faz a comunicação com o computador no qual está instalada usando um *driver* de comunicação, que se comunica com o sistema operacional instalado no mesmo. Existem placas para diversos padrões de redes, sendo as principais *Ethernet* a 10Mbps, *Fast Ethernet* a 10 ou 100Mbps, *Gigabit Ethernet* a 1Gbps, 10 *Gigabit Ethernet* a 10Gbps, entre outras tecnologias.

Servidores e estações de rede nada mais são do que computadores, que numa rede tipo Cliente/Servidor, como vimos no Tópico 2, item 4.3, executam funções distintas e definidas. Um servidor (de arquivos, de impressão, de aplicações, de e-mail etc.) fica dedicado somente à sua função principal, aguardando que os clientes da rede solicitem os serviços disponibilizados pelo servidor. Ele normalmente tem boa capacidade de processamento, grande capacidade de disco e memória RAM, *hardware* interno mais robusto e tolerante às falhas, como, por exemplo, duas fontes de alimentação e/ou duas placas de processadores. A parte mais pesada do *software* da aplicação roda no servidor.

As estações de rede, ou estações de trabalho, ou estações cliente, por sua vez, são computadores mais simples e que utilizam os recursos da rede solicitando os serviços aos servidores e ficando no aguardo das respostas. A parte mais simples do *software* da aplicação roda na estação cliente. Podem ter pequena capacidade de disco e memória RAM. Não devemos esquecer que, como vimos, também existem as redes tipo Ponto-a-Ponto (P2P), onde os computadores podem ser clientes e servidores, dependendo da sua necessidade, da necessidade das outras estações e dos recursos disponíveis em cada estação.

4 O SOFTWARE DE REDE

O *software* de rede é o grupo de componentes de rede composto principalmente pelos Sistemas Operacionais de Rede (SOR) e pelos protocolos de comunicação. Adicionalmente existem os aplicativos para redes e *softwares* de segurança e acesso a redes, mas esses não fazem parte do escopo deste caderno. Os protocolos de comunicação serão vistos na Unidade 2.

Assim, os SORs são responsáveis por executar duas funções principais, segundo Amaral (2012, p. 49):

A primeira é funcionar como um sistema operacional comum, fazendo o controle dos recursos do computador servidor, como o acesso a disco rígido ou memória. A segunda função é fazer o controle do uso das redes que estão instaladas; por exemplo, o SOR pode controlar se você, como usuário da rede, pode ou não ter acesso a um arquivo no disco rígido do servidor.

Os sistemas operacionais de rede podem ser classificados como ponto-a-ponto ou cliente/servidor, e de acordo com Amaral (2012), nas redes ponto-a-ponto os SORs instalados em todos os computadores são do tipo cliente, já que não existe a figura de servidor dedicado nessas redes. Não devem ser utilizados em redes com mais de 20 computadores devido à dificuldade de controlar a organização e segurança da rede. Por outro lado, têm como vantagem a maior simplicidade para instalação e configuração.

Nas redes cliente/servidor, conforme Amaral (2012), os computadores cliente possuem SOR cliente e solicitam serviços dos servidores. Os servidores possuem SOR servidor, como Windows Server 2012 ou distribuições Linux para servidores, e atendem às solicitações dos clientes. Essas redes são mais caras porque são mais complexas, exigindo SOR servidor, e requerem equipe técnica especializada para instalação, configuração e manutenção dos serviços disponibilizados pelos servidores.

LEITURA COMPLEMENTAR

SDN (*Software Defined Network*): realidade do mundo virtual?

A Rede Definida por *Software* (em inglês *Software-Defined Networking* ou SDN) é uma arquitetura emergente para atender às demandas da Terceira Plataforma de TI e resolver alguns problemas das atuais arquiteturas de rede existentes.

A SDN propõe uma arquitetura dinâmica, gerenciável, adaptável e com um custo-benefício adequado, tornando-se a plataforma ideal para a alta largura de banda e a natureza dinâmica das aplicações de hoje.

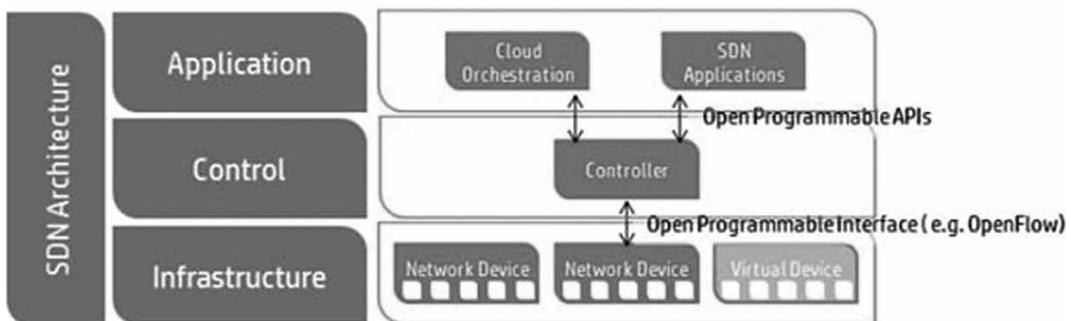
O principal motivador para substituir a arquitetura de rede convencional para uma Rede Definida por *Software* é o seu desenho alinhado com as principais tendências de mercado:

- Nuvem Híbrida: Sistemas distribuídos geograficamente através de nuvens públicas e privadas demandam um gerenciamento de tráfego extremamente flexível e acesso à largura de banda sob demanda.

- Consumerização de TI: A tendência de BYOD (*Bring Your Own Device*) requer redes que sejam flexíveis e seguras.
- *Big data*: A era do *zettabyte* significa mais largura de banda, conectividade e acesso aos sistemas do *Data Center*.

Ainda é possível atribuir como vantagem da arquitetura SDN a dificuldade das atuais redes convencionais em crescer na escala e na dinâmica que a TI precisa, a complexidade na implementação de políticas e readaptação do desenho e a dependência de fabricantes.

Figura 1. Estrutura de uma Rede definida por Software.



Um dos elementos-chave da arquitetura de SDN é o protocolo *OpenFlow*, padronizado pela ONF. O *OpenFlow* é a primeira interface padronizada projetada especificamente para SDN, proporcionando alto desempenho, controle de tráfego granular através de dispositivos de rede de diferentes fornecedores. O protocolo também proporciona a melhoria de automação e gerenciamento, usando APIs comuns para abstrair os detalhes de infraestrutura básica de rede dos sistemas de orquestração e aplicações de aprovisionamento. Com esses recursos é possível melhorar a experiência do usuário final, com aplicações que podem explorar as informações das condições da rede para adaptá-la perfeitamente ao comportamento e às necessidades do usuário.

A arquitetura SDN e o protocolo *Openflow* também influenciam diretamente na confiabilidade e segurança da rede, uma vez que a gestão centralizada e automatizada de dispositivos de rede permite a aplicação de políticas uniformes, reduzindo possíveis erros de configuração.

O instituto de pesquisa IDC estima que o mercado de SDN movimente mundialmente cerca de US\$3,7 bilhões em 2016, sendo 58% desse investimento relacionado à infraestrutura e controle da rede de dados. É, portanto, uma tendência e irá proporcionar os benefícios aqui já citados.

FONTE: Disponível em: <<http://www.vert.com.br/blog-vert/sdn-software-defined-network-realidade-do-mundo-virtual/>>. Acesso em: 20 mar. 2016.

RESUMO DO TÓPICO 3

Neste tópico vimos que:

- Os componentes das redes de computadores podem ser divididos em três grupos, que são os grupos do meio físico de transmissão, do *hardware* de rede e do *software* de rede.
- Os meios físicos de transmissão de rede são responsáveis por transmitir fisicamente os sinais entre os equipamentos, *hardware* de rede. Podem ser divididos em meios físicos guiados e não guiados.
- Os meios físicos guiados dividem-se nos grupos dos meios com fios de cobre e dos meios ópticos. O cabo coaxial e o cabo de pares trançados são meios físicos do grupo com fios de cobre, enquanto que as fibras ópticas são os meios físicos do grupo óptico.
- O cabo de pares trançados é o mais utilizado atualmente nas redes locais, substituindo o cabo coaxial, que ainda tem algumas aplicações em ambientes externos, como redes de TV a cabo. Existem os cabos de pares trançados tipo UTP e STP.
- As fibras ópticas estão cada vez mais sendo utilizadas, porque possuem grande alcance, têm boa flexibilidade e seus custos estão diminuindo. Existem as fibras ópticas tipo monomodo e tipo multimodo.
- Os meios não guiados utilizam o ar como meio físico de transmissão, existindo os grupos baseados em RF (radiofrequência), baseados em infravermelho e baseados em laser. Existem algumas aplicações de longa distância onde a transmissão usando radiofrequência é a solução com melhor custo-benefício.
- O *hardware* de rede é composto pelos equipamentos físicos como *switch*, roteador, servidor, estação de trabalho ou cliente etc. É preciso não confundir com os meios físicos.
- O *software* de rede é composto principalmente pelos SORs (Sistemas Operacionais de Rede) cliente e servidor, e pelos protocolos de comunicação.

AUTOATIVIDADE



- 1 Apresente uma definição para os meios físicos de rede usando as suas palavras.
- 2 Descreva com suas palavras as características do cabo de pares trançados e cite os dois tipos existentes.
- 3 Explique as diferenças que existem entre as fibras ópticas monomodo e multimodo.
- 4 Explique com suas palavras a diferença entre transmissão via rádio omnidirecional e transmissão via rádio direcional. Cite as vantagens de cada uma.
- 5 Explique o que é *hardware* de rede com suas palavras e relate alguns dispositivos que fazem parte deste grupo.



Assista ao vídeo de
resolução da questão 1



UNIDADE 2

NORMAS, PROTOCOLOS E EQUIPAMENTOS

OBJETIVOS DE APRENDIZAGEM

Esta unidade tem por objetivos:

- conhecer as principais normas e órgãos normalizadores das redes de computadores;
- compreender a estrutura em camadas das redes de computadores;
- conhecer os principais protocolos de rede e suas camadas de funcionamento;
- estudar os principais componentes de uma rede e suas funções.

PLANO DE ESTUDOS

Esta unidade está dividida em três tópicos. No final de cada um deles você encontrará atividades visando à compreensão dos conteúdos apresentados.

TÓPICO 1 – NORMAS E ÓRGÃOS NORMATIZADORES

TÓPICO 2 – PROTOCOLOS DE COMUNICAÇÃO

TÓPICO 3 – EQUIPAMENTOS DE REDE



Assista ao vídeo
desta unidade.



NORMAS E ÓRGÃOS NORMATIZADORES

1 INTRODUÇÃO

Durante o estudo das redes de computadores, várias vezes foram mencionadas estruturas, políticas de utilização, definição de padrões, entre outras funcionalidades que são comuns a diferentes equipamentos e fabricantes. Padrões que foram desenvolvidos e aplicados com a intenção de melhorar o desempenho das redes de computadores e diminuir os problemas de comunicação existentes entre diferentes ativos e fabricantes.

Estes padrões e normas foram estudados e desenvolvidos por entidades especializadas e são constantemente atualizados, para cada vez mais facilitar a comunicação.

2 PADRÕES

As redes de computadores são formadas por vários dispositivos interligados, que realizam a comunicação de diferentes faixas de IPs, possibilitando assim a troca de informações de maneira eficiente e rápida.

Porém, nem sempre isso foi assim, pois, por se tratar de uma estrutura muito complexa, a mesma está repleta de diferentes equipamentos e cada qual com o seu sistema operacional. Esta diversidade de ambientes no início das redes foi um grande problema, pois cada fabricante de *hardware* e *software* realizava o tratamento das informações da maneira que entendia ser mais adequado, o que acabava por inviabilizar a comunicação entre diferentes equipamentos.

Devido a estes constantes problemas de conectividade, surgiram as primeiras normas e padrões referentes às redes de computadores, que mais tarde vieram a dar origem aos primeiros protocolos de comunicação, pois, até o presente momento, cada desenvolvedor ou fabricante tinha o seu próprio protocolo de rede.

Esta padronização e normatização das redes de computadores surgiu com a intenção de garantir a produção de ativos e suprimentos de rede, onde todos pudessem vir a realizar a comunicação de maneira eficiente e confiável. Garantir a interoperabilidade, ou seja, garantir a troca de informação entre as aplicações que estão sendo processadas nos computadores e equipamentos, e assim vir a garantir de forma total a interconectividade em um ambiente com tanta heterogeneidade.

Os padrões criados têm como objetivo garantir que diferentes *hardwares*, ao estarem ligados dentro do mesmo ambiente, possam realizar a comunicação sem que haja perda de informação ou colisão de dados devido a maneiras diferentes de tratamento do dado. Para tanto, constituição do pacote, formatos de conexão física e lógica, modelos de transmissão foram padronizados, e hoje, obedecem estas normas garantindo assim a comunicação entre os dispositivos.

Esta padronização e criação de regras só foram possíveis graças a uma cooperação entre diferentes órgãos que se uniram com a intenção de definir regras e modelos para facilitar a integração de diferentes *hardwares* e *softwares*. Em resumo, foi o momento-chave para as redes de computadores, onde surgiram as leis em um mundo até então sem leis.

3 ÓRGÃOS NORMATIZADORES

A partir de agora vamos falar um pouco mais sobre os principais órgãos que realizam a regulamentação e planejamento das redes de computadores.

- ISO -->*International Standard Organization*, a ISO é a entidade máxima quando se fala em padronização. A mesma foi fundada em 1946 e é constituída por diferentes órgãos e entidades de diferentes países. Seu objetivo é criar normas e padrões para com isso estabelecer metas e uma maior qualidade de serviços e produtos.
- ANSI -->*American National Standards Institute*, é uma organização privada, que administra e coordena o sistema norte-americano de conformidades. Esta organização foi fundada em 1918, onde sua principal missão tem sido o incremento da competitividade do setor comercial dos EUA. Promovendo assim um maior desenvolvimento voluntário e consensual de sistemas de conformidade.
- IEEE -->*Institute of Electrical and Electronic Engineers*, tem por objetivo definir os padrões de utilização das redes sem fio. Entre os seus trabalhos, podemos destacar a constituição do padrão 802.11 que ficou amplamente conhecido como *WI-FI*, e, teve como objetivo a normatização da conexão entre cliente e ponto de acesso.
- EIA/TIA -->*Electronic Industries Association/Telecommunications Industries Association*, estabelece padrões para sistemas de cabeamento de comunicação.

- IANA --> *Internet Assigned Number Authority*, é a autoridade máxima que atua na atribuição dos números IP's na Internet. Ficam sob sua responsabilidade também o registro das portas de serviços utilizadas pelas aplicações e sua homologação, além dos registros de nomes na rede (Internet).
- IETF --> *Internet Engineering Task Force*, é um grupo que tem como foco o desenvolvimento de padrões voltados para a internet. Dessa forma, acabam por contribuir na evolução das tecnologias utilizadas no desenvolvimento da internet como um todo, englobando *hardware* e *software*.

4 PRINCIPAIS NORMAS EM REDES

Agora que já conhecemos as principais entidades normativas, vamos estudar algumas das principais normas que atuam diretamente nas redes de computadores.

- Norma ANSI/TIA/EIA 568-A NBR 14565 (2001) --> esta norma é utilizada para a instalação do cabeamento de rede, topologia da rede e outros quesitos relacionados à estrutura física da rede, o que é denominado popularmente como cabeamento estruturado. A seguir, a tabela referente à padronização para a instalação de redes locais.

TABELA 1 - NORMAS

NORMA	TEMA
ANSI/TIA/EIA 568-A	Padrões de cabeamento
ANSI/TIA/EIA 569-A	Infraestrutura
ANSI/TIA/EIA 570-A	Cabeamento Residencial
ANSI/TIA/EIA 606	Administração
ANSI/TIA/EIA 607	Aterramento

FONTE: Disponível em: <<http://www.ansi.org/>>. Acesso em: 10 jan. 2016.

- Modelo OSI --> este modelo surgiu baseado em uma proposta desenvolvida pela ISO e foi o primeiro passo na direção de uma padronização internacional dos protocolos empregados nas diversas camadas da estrutura de rede. Este modelo foi denominado de OSI (*Open Systems Interconnection*), pois trata da interconexão de sistemas abertos, ou seja, sistemas que estão abertos à comunicação com outros sistemas. Este modelo é composto por uma estrutura composta por sete camadas, como pode ser observado na Figura 42.

FIGURA 42 - MODELO DE REFERÊNCIA OSI



FONTE: O autor

Tais camadas e suas funcionalidades estudaremos mais à frente, no decorrer da disciplina.

- **Modelo TCP/IP** --> o modelo TCP/IP surgiu baseado na necessidade de interconectar redes distintas de maneira uniforme, o que até então não era possível. Este modelo possui como uma diferença básica o seu número de camadas, muito mais simplificado, como pode ser observado na imagem a seguir:

FIGURA 43 - MODELO DE REFERÊNCIA TCP/IP



FONTE: O autor

Este novo modelo garante à rede maior flexibilidade e agilidade em suas trocas de arquivos, pois utiliza um esquema de endereçamento universal, o que possibilita o roteamento e encaminhamento das informações entre redes distintas. Tais camadas e funcionalidade existentes em cada uma delas serão estudadas mais adiante neste caderno.



Semelhanças entre TCP/IP e OSI --> ambos os modelos são divididos em camadas e a tecnologia de comutação de pacotes é utilizada em ambos;

Diferenças entre TCP/IP e OSI --> quantidade de camadas existente. A Internet se desenvolveu baseada no modelo TCP/IP, enquanto nenhuma rede se desenvolveu utilizando o modelo OSI, porém é muito utilizado como base de estudos.

- Padrão *Ethernet* --> este modelo é baseado no conceito de que todos os pontos da rede têm capacidade de enviar e receber informações, onde cada ponto da rede possui uma chave de 48 bits única, chave a qual é denominada de MAC. Este endereço (chave) garante que não exista nenhum tipo de duplicidade dentro da rede. Tal endereço MAC será estudado mais adiante.
- Padrão IEEE 802.13E --> trata-se de um conjunto de padrões desenvolvidos para definir métodos de acesso e controle para as redes locais.
- Padrão IEEE 802.3 --> é um padrão de transmissão de dados para a rede local, considerando que todos os *hosts* estão conectados a uma mesma linha de comunicação constituída por cabos cilíndricos.
- Padrão 802.11 --> este padrão, como já mencionado anteriormente, é popularmente conhecido como *Wi-Fi*, possui algumas variações, tais como 802.11b, 802.11a, 802.11g, 802.11i, 802.11n e 802.11x. Todos estão diretamente relacionados com formato de comunicação sem fio, suas diferenças estão nas suas velocidades de transmissões, criptografia e segurança, larguras de banda e, consequentemente, alcance de seu poder de transmissão.

Em resumo, os padrões e normas atribuídos às redes de computadores e à comunicação de forma geral são algo de suma importância para que as trocas de informações entre diferentes dispositivos possam ser bem-sucedidas. Na ausência desta abordagem, as redes seriam uma grande desordem, onde diferentes ativos não teriam êxito ao realizar qualquer sincronização ou troca de informação. Tais premissas também são válidas para as estruturas físicas das redes, pois o ambiente físico é uma extensão do ambiente lógico e ambos necessitam estar alinhados para que assim seja possível realizar as transmissões de dados de maneira eficiente e confiável.

RESUMO DO TÓPICO 1

Neste tópico você viu:

- A importância da padronização dos conceitos utilizados nas redes de computadores, a qual permite uma comunicação entre *hosts* de forma eficiente e confiável.
- O surgimento de organizações como entidades padronizadoras de comunicação, que obrigaram os desenvolvedores de *hardware* e *software* a trabalharem na mesma linha de pensamento.
- A criação de regras e padrões para a estruturação das redes de computadores, definindo normas e métodos para a estrutura lógica e física das redes, minimizando assim possíveis indisponibilidades de comunicação e facilitando toda e qualquer manutenção neste meio computacional.

AUTOATIVIDADE



Prezado(a) acadêmico(a), vamos praticar o que estudamos até agora.

- 1 A definição de normas e padrões foi algo muito importante para as redes de computadores. Qual o grande problema que esta abordagem veio resolver?
- 2 Dentre vários estudos, podemos destacar os dois modelos de referência que nortearam todo o surgimento das redes. Desta forma, diga quais são estes modelos, no que se diferem e como funcionam de maneira simplificada.



*Assista ao vídeo de
resolução da questão 2*



PROTOCOLOS DE COMUNICAÇÃO

1 INTRODUÇÃO

A principal função de uma rede de computadores é realizar a comunicação entre diferentes pontos de maneira rápida e eficiente, garantindo segurança e disponibilidade das informações que estão sendo trocadas.

Os protocolos de rede surgiram dentro dessa estrutura de redes, com a intenção de regrar essa comunicação e assegurar que esta comunicação entre dois pontos distintos aconteça da forma mais simples para o usuário, porém, garantindo ao mesmo que todos os dados que por ele forem enviados cheguem ao seu destino da mesma forma que saíram da sua origem, garantindo, desse modo, a integridade das informações.

2 SURGIMENTO DOS PROTOCOLOS

Com o surgimento das redes de computadores, os protocolos de comunicação surgiram com a intenção de padronizar as comunicações entre os diferentes *hardwares* envolvidos.

Desta forma, os protocolos de comunicação podem ser facilmente definidos como as regras utilizadas para dois ou mais dispositivos interconectados estabelecerem comunicação e, consequentemente, realizar uma troca de dados entre si. Sendo assim, sem uma sintaxe e parâmetros muito bem definidos e esclarecidos, esta comunicação entre diferentes *hosts* não poderia acontecer. É através destas regras que a comunicação estabelece seus enlaces, permitindo o fluxo da informação.

Para realizar a comunicação entre diferentes *hosts* dentro de uma rede de computadores, são utilizados diferentes tipos de protocolos de rede, onde cada um possui uma função específica e de suma importância ao todo. Desta maneira, a comunicação acontece utilizando várias regras (protocolos) distintas simultaneamente, onde teremos protocolos responsáveis pela comunicação direta dos *hosts*, controles de congestionamento e fluxo da informação, segurança dos dados, velocidade na entrega das informações, entre outras funções existentes nas comunicações.

Assim sendo, todos os protocolos são importantes e um depende diretamente do outro para realizar seus procedimentos e assim atingir máxima eficiência do seu desempenho.

Para reduzir a complexidade das redes de computadores, a grande maioria das redes é organizada como uma pilha de camadas, colocadas umas sobre as outras. A ideia fundamental dessa arquitetura é que uma camada forneça um determinado serviço a seus usuários, mas também venha a manter ocultos os detalhes de seu estado interno e de seus algoritmos.

Assim, a camada N de uma máquina se comunica com a camada N de outra máquina. Estas regras de comunicação entre as camadas são os chamados protocolos de comunicação. Este conjunto de camadas e serviços oferecidos por cada delas é denominado de arquitetura de rede. A lista de protocolos utilizados para realizar a comunicação entre dois *hosts* distintos é conhecida como pilha de protocolos, ou seja, todos os protocolos envolvidos em cada camada para realizar a comunicação entre os *hosts*.

Utilizando esta abordagem de camadas, cada camada existente dentro da arquitetura de rede virá a servir a camada superior. Para tanto, existem dois modelos de arquitetura de rede, o modelo de referência OSI e o modelo de referência TCP, os quais serão abordados a seguir.

3 SERVIÇO X PROTOCOLO

Antes de estudarmos os modelos de referência para entendermos o funcionamento das arquiteturas de redes, é necessário compreender e diferenciar os conceitos de serviços e protocolos, pois os mesmos serão de suma importância para o andamento do estudo.

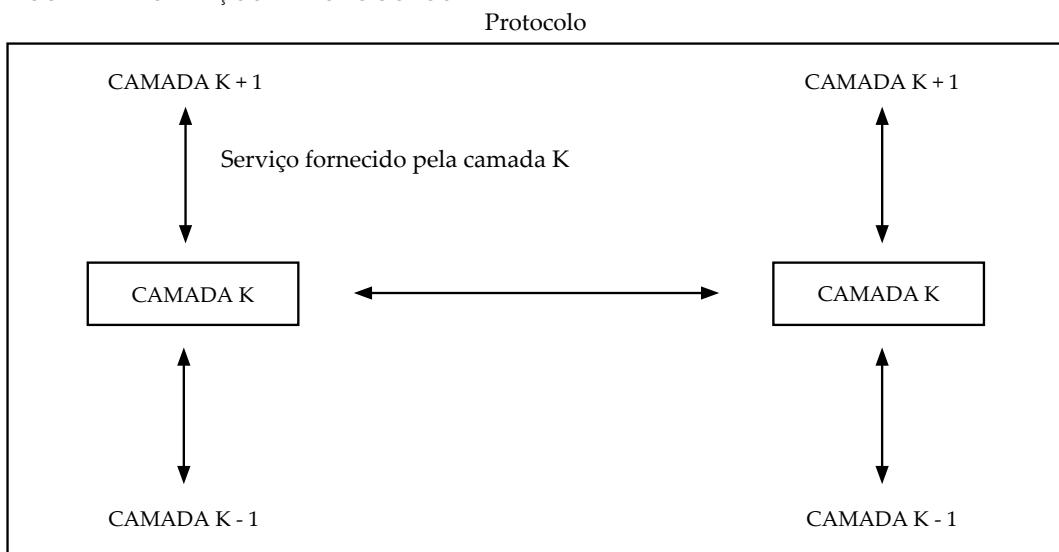
Segundo Tanenbaum (2003, p. 37),

um serviço é um conjunto de operações que uma camada oferece à camada situada acima dela. O serviço define as operações que a camada está preparada para executar em nome de seus usuários, mas não informa absolutamente nada sobre como essas operações são implementadas. Assim, um serviço se relaciona a uma interface entre duas camadas, sendo a camada inferior o fornecedor do serviço e a camada superior o usuário do serviço.

Quando mencionamos um protocolo, podemos definir o mesmo como um conjunto de regras que controla o formato e o significado dos pacotes ou mensagens que são trocadas pelas entidades pares contidas em uma camada. As entidades utilizam protocolos com a finalidade de implementar suas definições de serviço. Elas possuem a liberdade de trocar seus protocolos, desde que não alterem o serviço visível para seus usuários. Desta forma, o serviço e o protocolo são independentes um do outro (TANENBAUM, 2003, p. 39).

Observe a imagem a seguir.

FIGURA 44 – SERVIÇOS E PROTOCOLOS



FONTE: Tanenbaum (2003, p. 40)

4 MODELO DE REFERÊNCIA

Agora que já temos uma breve noção geral da arquitetura de uma rede de computador, vamos estudar mais detalhadamente a constituição dos dois modelos.

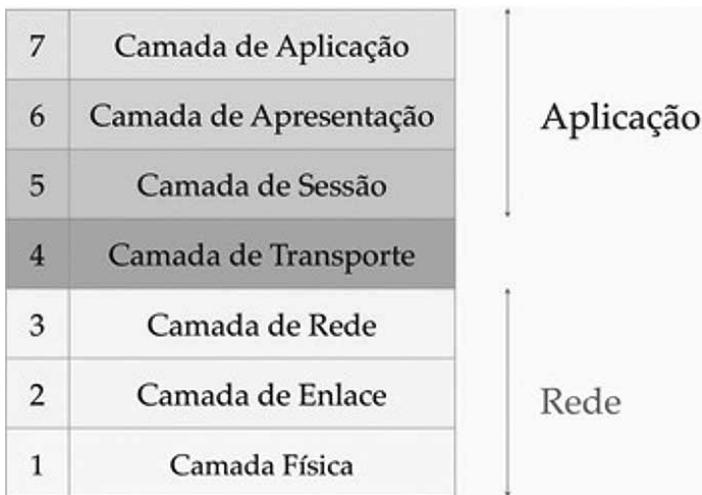
4.1 MODELO DE REFERÊNCIA OSI

O modelo de referência OSI foi desenvolvido pela ISO (*International Standards Organization*), foi o primeiro modelo com a ideia de realizar a padronização das comunicações entre *hosts* distintos.

Sua principal função é realizar o tratamento das conexões de sistemas abertos, ou seja, sistemas que estão conectados e disponíveis para realizar a transmissão de dados.

Este modelo foi desenvolvido com sete camadas, onde cada uma delas possui uma finalidade muito bem definida, como pode ser observado na imagem que segue:

FIGURA 45 - MODELO DE REFERÊNCIA OSI



FONTE: Disponível em: <<http://professorgilberson.blogspot.com.br/2010/02/modelo-de-referencia-osi.html>>. Acesso em: 10 fev. 2016.

O modelo apresentado nos mostra como é realizado o processo de comunicação entre dois *hosts* distintos dentro da rede, ou seja, como a informação é tratada e transmitida.

A partir de agora iremos realizar um maior detalhamento sobre cada camada, com a intenção de facilitar o entendimento do fluxo de informação e as responsabilidades de cada camada envolvida no processo.

4.1.1 Camada Física

A camada física é responsável pela gerência física da conexão, dessa maneira, ela determina a quantidade de pinos existentes dentro um conector, por exemplo, um RJ45, e realiza a padronização dessa conexão, de tal maneira que chega a indicar e determinar a finalidade de cada um dos pinos existentes nos conectores.

É nesta camada que se inicia a conexão entre *hosts* distintos, ou seja, a validação do meio físico que será utilizado para a transmissão dos dados. Esta camada é responsável pela sincronização inicial e final de todas as conexões estabelecidas.

Além de realizar a sincronização final e o encerramento da conexão, a camada física realiza a transmissão dos *bits* no meio físico e é de responsabilidade da mesma a garantia de entrega desses *bits*, onde ao enviar um *bit* 1 o destino receba o mesmo *bit* 1 e não um *bit* 0, por exemplo. Para tanto, ela irá gerenciar a voltagem aplicada no meio físico para realizar a transmissão do dado e tempo de entrega desse dado, para que assim o mesmo possa vir a alcançar o seu objetivo e não venha a ser perdido pelo caminho.

4.1.2 Camada de Enlace

A função da camada de enlace é transformar um canal de comunicação bruto, ou seja, o canal oferecido pela camada física em um ambiente seguro e estável, sem nenhum tipo de erro para realizar a transmissão dos dados.

Para realizar esta função de maneira correta, a camada de enlace encontrou a seguinte saída: dividir os dados que serão enviados em pequenos quadros, ou seja, realizar a fragmentação da informação, e após esta fragmentação, realizar o envio do pacote, pois desta forma a probabilidade de erros fica muito restrita, e caso ocorra qualquer tipo de erro durante a transmissão, será somente um fragmento de informação comprometido, sendo muito mais simples a sua recuperação ou até o seu reenvio.

Além de realizar a fragmentação da informação, a camada de enlace tem outra função de suma importância para o bom andamento das redes. É ela que realiza a negociação entre os dois *hosts* para determinar a velocidade com que os dados serão transmitidos dentro da rede. Dessa forma, se um *host* possui alta capacidade de transmissão e o *host* que irá receber estas informações não possui a mesma capacidade, a camada de enlace entra em ação para determinar a velocidade com que a informação será trocada, para que assim não seja gerado nenhum tipo de congestionamento de informações, ou por uma alta velocidade no envio do dado ou até mesmo uma falta de informações a serem processadas pelo *host* de recebimento.

4.1.3 Camada de Rede

A camada de rede tem por responsabilidade realizar a gestão das operações da sub-rede, ou seja, determinar de maneira lógica qual o melhor caminho para determinado pacote alcançar o seu destino final.

Em resumo, é na camada de rede que o pacote irá definir o caminho que ele irá seguir dentro da rede. Como esta camada é responsável por indicar o caminho, ela também deve realizar o controle de congestionamento desses caminhos, para evitar que muitos pacotes fiquem na espera para serem processados, onde esta espera pode vir a acontecer na saída, chegada ou no trânsito, pois, como sabemos, muitas vezes, para alcançar o seu destino final, um determinado pacote pode passar por N equipamentos de rede, fazendo com que seu tempo de resposta seja maior e assim comprometendo a performance da rede.

Dessa maneira, a camada de rede deve processar a informação e tratar seus possíveis problemas quanto a tamanho. Em seguida, definir o melhor caminho ou rota para que esta informação tenha êxito em sua transmissão.

4.1.4 Camada de Transporte

A camada de transporte tem por principal funcionalidade receber as informações geradas pela camada superior, fragmentá-las em pequenas unidades quando necessário e realizar o encaminhamento destas unidades, garantindo que todos os fragmentos cheguem ao seu destino de maneira íntegra e correta.

Esta camada é conhecida pela sua conexão fim a fim, pois ela realiza uma conexão direta com o *host* final que irá receber as informações, enquanto as outras camadas deste modelo apenas realizam a comunicação com o próximo *host* envolvido no encaminhamento da informação.

Desta maneira, é função da camada de transporte determinar as regras e normas de como será realizada a comunicação entre os pontos inicial e final da comunicação, para garantir assim a integridade das informações a serem trafegadas.

4.1.5 Camada de Sessão

Esta camada vem permitir o estabelecimento de sessões entre diferentes *hosts* dentro da rede. Dentro dessas sessões é onde realiza-se o controle de diálogo (mantendo o controle de quem deve transmitir em cada momento), a sincronização que realiza a verificação e análise periódica do meio de comunicação com a intenção de minimizar os erros, e, por fim, o gerenciamento do *token*, o qual impossibilita que os dois *hosts* envolvidos na troca de mensagem tentem realizar a mesma operação crítica dentro do túnel de comunicação ao mesmo tempo, e assim acaba por evitar possíveis colisões ou erros de sinalização de sincronização.

4.1.6 Camada de Apresentação

A camada de apresentação tem por função realizar o gerenciamento da sintaxe e semântica das informações transmitidas.

Nesta camada é realizada a padronização da forma como os dados serão transmitidos, ou seja, ela é responsável por determinar a forma ou linguagem com que as informações serão transmitidas e recebidas, para que todos os ativos envolvidos nesta comunicação possam realizar a interpretação dos dados e assim acabar por realizar o encaminhamento da informação correta e, consequentemente, realizar a transcrição da informação que está de maneira abstrata para uma informação legível novamente.

4.1.7 Camada de Aplicação

A camada de aplicação é muito conhecida por possuir muitos protocolos conhecidos pelos usuários, dentre os quais podemos citar o HTTP, SSH, POP, SMTP, entre outros.

Desta maneira, a camada de aplicação realiza a interação entre o usuário e o serviço que o mesmo deseja utilizar, é ele que realizará o tratamento da informação e o encaminhamento da solicitação a quem é de direito. Um exemplo muito simples destes protocolos é o HTTP (*Hyper Text Transfer Protocol*), o qual envia o nome da página que o usuário deseja acessar para o servidor detentor da página. Então, o servidor recebe esta transmissão e envia as informações da página para que o navegador do usuário possa realizar a apresentação do *site*. Todo este processo ocorre utilizando o protocolo HTTP.

4.2 MODELO DE REFERÊNCIA TCP/IP

O modelo de referência OSI foi utilizado durante o início do surgimento das redes de computadores, quando as conexões ainda eram muito simplificadas, as interconexões de redes distintas ainda não eram uma realidade e ainda não existiam diferentes meios de transmissão de dados além do cobre.

A partir do momento em que as redes de computadores começaram a evoluir, passando a utilizar outros meios de comunicação, como satélites e rádio, por exemplo, a abrangência das redes em nível territorial cresceu e assim as sub-redes começaram a surgir. Este modelo de referência OSI passou a encontrar vários problemas para realizar a comunicação entre os *hosts* com essas características.

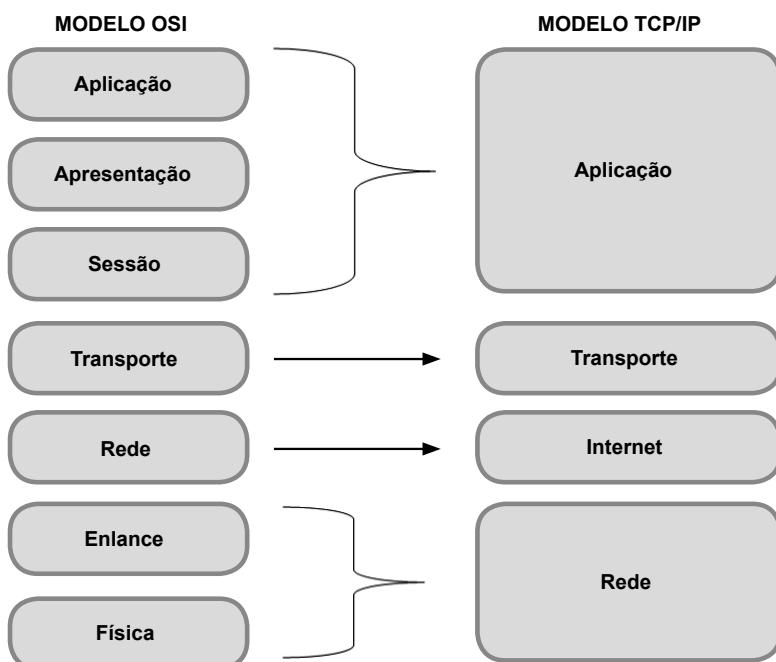
Como o modelo de referência OSI já não atendia de forma eficiente às redes de computadores, foi então desenvolvido um novo modelo de comunicação, o qual foi denominado de modelo de referência TCP/IP, e sua estrutura pode ser observada nas Figuras 46 e 47:

FIGURA 46 - MODELO DE REFERÊNCIA TCP/IP



FONTE: Disponível em: <<https://jbgsom.wordpress.com/2010/05/31/camadas-tcpip/>>. Acesso em: 10 fev. 2016.

FIGURA 47 - COMPARATIVO ENTRE MODELO OSI E MODELO TCP/IP



FONTE: O autor

4.2.1 Camada Internet

Toda a evolução das redes de computadores, com a interligação das redes, tornou necessário o desenvolvimento de uma forma com que *hosts* pudessem vir a se comunicar com todos os *hosts* conectados em qualquer rede à qual estivessem conectados.

Dessa maneira, a camada internet veio a suprir esta necessidade. Ela permite que um determinado *host* tenha condição de injetar pacotes dentro da rede com destino a diferentes redes/*range* de rede.

Para tanto, foi desenvolvido um modelo específico de comunicação para esta camada, o protocolo IP (*Internet Protocol*), o qual será estudado mais a fundo. Assim, a tarefa da camada internet é realizar a entrega dos pacotes IP ao seu destino final, onde o controle de congestionamento e os protocolos de roteamento (direcionamento de pacotes) são de suma importância para o bom andamento da informação. Sendo assim, pode-se dizer que a camada internet do modelo de referência TCP/IP é muito similar à camada de rede do modelo de referência OSI, o qual foi estudado anteriormente.

4.2.2 Camada de transporte

A camada de transporte existente no modelo TCP/IP é exatamente idêntica à existente no modelo OSI. É ela que é responsável pela comunicação fim a fim existente entre os *hosts* de uma rede, ou seja, é esta camada que realiza a sincronização da conexão e determina como serão realizadas as transmissões de dados entre os *hosts* envolvidos.

Para tanto, foram desenvolvidos dois protocolos de comunicação utilizados por esta camada, o protocolo TCP (*Transmission Control Protocol*) e o protocolo UDP (*User Datagram Protocol*), os quais serão estudados adiante.

4.2.3 Camada de Aplicação

Como pode ser observado na imagem anterior, o modelo TCP/IP, diferentemente do modelo de referência OSI, não possui as camadas de sessão e apresentação, as quais foram removidas deste novo modelo por serem julgadas de pouca utilização e sem necessidade para esta nova abordagem.

Esta nova camada de aplicação, da mesma forma que a anterior, continua a gerenciar os protocolos de comunicação de nível mais alto, ou seja, aqueles com os quais o usuário possui contato direto, como é o caso do HTTP, DNS, FTP, POP, entre outros.

4.2.4 Camada de Rede (ou Acesso à Rede)

A camada de rede (ou acesso à rede) é responsável pela conexão física do dispositivo, ou seja, faz a inserção das informações a serem transmitidas dentro do meio de comunicação, realizando as funções das camadas de enlace e física do modelo OSI.

5 PROTOCOLO DE COMUNICAÇÃO DA CAMADA DE TRANSPORTE (TCP E UDP)

Como já mencionado anteriormente, a camada de transporte realiza a conexão fim a fim entre os *hosts* para que, assim, possa-se realizar a transmissão das informações entre dois pontos. Para tanto, foram desenvolvidos dois protocolos de comunicação para realizar a transmissão de maneira eficiente e controlar o fluxo desses dados no meio.

Estes protocolos de comunicação são denominados de *Transmission Control Protocol* (TCP) e *User Datagram Protocol* (UDP). Cada conexão existente em um *host* obrigatoriamente precisa fazer uso de um destes protocolos para assim realizar a troca de dados.

Porém, antes de estudarmos mais a fundo o funcionamento destes dois protocolos de comunicação, é preciso esclarecer outro conceito muito utilizado quando nos referimos a conexões. Este conceito refere-se aos soquetes, popularmente conhecidos por portas.

Estas portas proporcionam um ponto de encontro por meio dos quais processos podem passar dados. Desta forma, cada processo fica vinculado a uma determinada porta de serviço, sendo esta porta representada por um número de 16 bits. Dessa maneira, sempre que um determinado *host* deseja enviar uma informação para outro, a informação será vinculada ao *host* de recebimento e também a uma porta, a qual servirá de guia para o destinatário realizar o encaminhamento correto desta informação para o processo que irá tratá-la.

Assim, uma porta só pode estar associada a um único processo. Não é permitido e é tecnicamente inviável a utilização da mesma porta em dois processos diferentes do mesmo *host*, pois caso aconteça, não será possível realizar o encaminhamento dos dados corretamente ao processo que irá tratá-los.

Uma determinada porta ou soquete pode receber mais de uma conexão de forma simultânea e realizar o encaminhamento ao processo respectivo, porém um soquete não pode representar dois processos ao mesmo tempo, como já descrito anteriormente.

Na estrutura atual de serviços de transmissão de dados existem 65.535 portas (soquetes) disponíveis para utilização, porém, algumas delas já estão associadas a determinados processos. Esta associação é realizada através da IANA (*Internet Assigned Numbers Authority*), organização que realizou o cadastro das principais aplicações e, consequentemente, as portas que as mesmas utilizariam para realizar a comunicação.

Sendo assim, nada impede que um determinado gestor altere as configurações das portas do seu processo, porém isso dificultará bastante a comunicação dele com outros usuários existentes na rede.

Muitas vezes, esta abordagem de alteração da configuração da porta de serviço pode ser considerada como uma forma ou premissa de segurança, na tentativa de inibir algumas formas de tentativas de ataque ao seu ambiente. Porém, esta alteração só pode ser efetuada se todos os usuários que irão utilizar este determinado serviço tenham conhecimento desta alteração ou se ele não seja algo de suma importância para organizações, pois devido a esta alteração, alguns usuários podem vir a perder comunicação ou ter uma grande dificuldade para o estabelecimento da mesma.

Qualquer pessoa pode cadastrar sua aplicação/processo junto à IANA e assim ter a definição e padronização de uma porta específica para o seu serviço, porém, como já mencionado, isto não garante exclusividade para o mesmo. Segue uma lista de algumas portas já catalogadas junto à IANA:

TABELA 2 - PORTAS E SERVIÇOS

Porta	USO
21	<i>File transfer</i> (transferência de arquivos)
23	<i>Login</i> remoto
25	Correio eletrônico
80	<i>World wide web</i>
110	Acesso remoto a correio eletrônico
119	Notícias da USENET

FONTE: Disponível em: <<http://iana.org>>. Acesso em: 15 jan. 2016.

5.1 UDP – *User Datagram Protocol*

O protocolo UDP proporciona comunicação sem o estabelecimento de uma conexão entre programas aplicativos, ou seja, ele permite que um determinado programa envie um determinado dado para outro *host* da rede, sem a necessidade

de, antes de enviar o dado, existir uma sincronização entre os *hosts* envolvidos e uma sinalização de liberação para que o dado seja encaminhado. Mesmo sem estes princípios de conexão, o dado é enviado e o destinatário o recebe sem maiores problemas.

Baseado nesta característica descrita acima, o protocolo UDP é caracterizado como um protocolo não orientado à conexão, pois, como já mencionamos, não realiza qualquer tipo de conexão com o destinatário antes de enviar a informação para o mesmo.

Por se tratar de um protocolo não orientado à conexão, como já explicado, o mesmo não apresenta nenhum tipo de controle de congestionamento de dados e, por consequência, não tem qualquer comprometimento com a entrega do pacote, ou seja, quando o dado é enviado utilizando este protocolo de comunicação, o mesmo é inserido na rede pelo remetente, porém, não existe nenhuma garantia ou confirmação de que o dado chegou ao seu destino. Desta forma, este protocolo acaba por não ser muito confiável para a transmissão das informações.

Porém, por outro lado, por este protocolo não exigir qualquer tipo de confirmação de chegada do dado ou de integridade do dado que foi transmitido, isso faz com que o protocolo UDP ganhe muita agilidade e performance no momento da transmissão, fazendo com que o mesmo seja o protocolo mais rápido para realizar transmissões de dados. Assim, o mesmo passou a ser amplamente utilizado em transmissões de informações que precisam de alta performance, como o caso das transmissões de vídeo em tempo real ou mesmo ligações utilizando voz sobre IP.

Esta analogia da utilização do protocolo UDP em transmissões em *real time* é muito simples de compreender, pois se o protocolo em questão viesse a possuir qualquer tipo de garantia de entrega do dado, o destinatário necessariamente seria obrigado a enviar um pacote ao remetente confirmando cada um dos pacotes recebidos, e só poderia receber o próximo pacote após a confirmação do anterior. Isto acarretaria, para uma transmissão de vídeo ou voz, a perda da continuidade da transmissão, pois ao perder um pacote ou somente em atraso no recebimento do mesmo, a transmissão seria interrompida até que o próximo pacote chegasse, deixando de ser assim uma transmissão em *real time*, ou até interrompendo o fluxo de uma determinada conversa no caso de voz sobre IP.

Como descrito acima, o protocolo UDP é amplamente utilizado para realizar as transmissões em tempo real (RTP – *Real Time Protocol*). Para tanto, no início das comunicações, as velocidades de transferência entre pontos eram muito pequenas, o que, mesmo com a grande velocidade do protocolo UDP, era um grande problema para estes tipos de aplicações. Assim, foi desenvolvida uma abordagem diferenciada para que as aplicações em *real time*, ou mesmo as reproduções de vídeos e sons, obtivessem maior eficiência em suas apresentações. Esta abordagem, ou melhor, esta solução para este problema de transmissão foi denominada de *buffer*.

O *buffer* é uma espécie de área de armazenamento de dados dinâmica, que age como um controle da conexão. Desta forma, ao iniciar uma aplicação que fará

uso do UDP para uma transmissão de vídeo, por exemplo, o *buffer* entra em ação realizando o recebimento do pacote e gerenciamento do início da transmissão. Sua principal função é controlar a apresentação para o usuário ao ponto que ela não seja interrompida por falta de pacotes recebidos. Assim, no momento em que o *buffer* passa a receber os pacotes, o mesmo calcula quanto tempo ele demorou para receber esta quantidade de pacotes e quanto tempo de vídeo esta quantidade de pacotes poderia proporcionar ao usuário. Ao final desta análise, se a quantidade de vídeo é suficiente para receber a mesma quantidade de pacotes, o vídeo em questão é liberado ao usuário, caso contrário o *buffer* segura o início da apresentação até que receba uma quantidade suficiente para apresentar o dado e tenha tempo para receber outra quantidade similar à primeira para que, assim, possa dar continuidade sem interrupção no vídeo apresentado ao usuário.

Muitas vezes esta abordagem garante uma transmissão sem nenhum problema para o usuário, porém em outros casos, mesmo com todo este controle durante o tempo de recebimento, pode variar durante a transmissão, fazendo com que o *buffer* tenha que recalcular o seu tempo de espera para liberar a apresentação ao usuário, fazendo com que a apresentação em questão venha a ser interrompida por um determinado período até que o *buffer* venha a estar preenchido novamente e, assim, libere a apresentação novamente.

Por garantir esta grande agilidade das transmissões, o protocolo UDP não possui nenhum tipo de controle de congestionamento, pois, como não estabelece qualquer tipo de conexão com o *host* final, ele não conhece o *status* do seu destinatário, tendo somente a informação de que deve enviar da forma mais rápida possível estes dados para a rede, e assim o destinatário deve se preocupar em realizar o recebimento e o tratamento mais rápido possível dos dados.

Mas, se durante o recebimento destes dados não for possível realizar o recebimento de um determinado pacote, seja por um congestionamento na interface de rede, ou simplesmente porque o pacote foi perdido em trânsito, a própria aplicação que está realizando a solicitação deve realizar o tratamento deste erro, ou seja, pular o pacote faltando, por exemplo, e assim dar continuidade à aplicação, pois no caso de aplicações de *real time*, o importante é a continuidade e fluidez da apresentação.

Outro ponto com que as aplicações devem se preocupar ao utilizar este tipo de protocolo de comunicação é a questão da ordenação das informações, ou seja, por mais que os pacotes sejam enviados de forma ordenada pelo remetente, não necessariamente o destinatário irá receber-los de forma ordenada, assim, quem deve realizar a ordenação dos pacotes é a aplicação que os solicitou.

Neste pensamento, caso uma determinada aplicação venha a receber uma sequência X de pacotes, e durante este processo um pacote não tenha sido recebido, porém o seu sucessor já está disponível, o mesmo passa a ser ignorado para, assim como já mencionando anteriormente, possa-se dar maior fluidez à aplicação/vídeo em questão.

Desta forma, podemos resumir o protocolo UDP como um protocolo de grande velocidade, porém sem garantia de entrega de dados, sem estabelecimento de conexão (não orientado à conexão) e sem qualquer tipo de controle de congestionamento ou fluxo das informações a serem transmitidas e recebidas, porém amplamente utilizado para *real time*.

5.2 TCP - *Transmission Control Protocol*

O protocolo TCP (*Transmission Control Protocol*) foi desenvolvido com a intenção de realizar uma comunicação fim a fim, ou seja, direta entre dois *hosts* de forma confiável dentro de uma rede, e inter-rede não confiável. Não confiável, pois os pontos de troca entre redes e dentro de uma rede local são muito suscetíveis a interferências externas e internas e, consequentemente, às interrupções.

Uma conexão TCP tem o seu funcionamento básico a partir do momento em que transmissor e receptor realizam e estabilizam uma conexão direta entre eles. Para realizar essa comunicação é utilizado, juntamente com o IP dos *hosts*, um soquete de comunicação (porta), para desta forma o remetente realizar a identificação correta do processo que irá realizar o tratamento do dado.

Assim, o destinatário irá realizar o envio da informação após a sincronização da comunicação, chamando o IP do *host* destinatário e a porta que faz referência ao processo solicitado. Neste momento o remetente abre também uma porta de serviço, porém esta porta não é a mesma que será utilizada no destinatário, e sim uma diferente, pois este remetente pode vir a ser um destinatário para outra conexão cuja porta seja utilizada.

Dessa maneira, de forma simplificada, ao realizar uma solicitação de um *site*, por exemplo, um *host* (origem) abre uma conexão na porta 4000, a qual foi escolhida pelo *host* de maneira aleatória, porém considerando os serviços que o mesmo possui, para que assim os mesmos não sejam comprometidos. Esta conexão iniciada será sincronizada com o *host* de destino na porta 80 do mesmo, para que este *host* saiba que se trata de uma solicitação HTTP e assim encaminhe as informações para o processo correto. Este processo irá realizar o tratamento desta solicitação e retornará a informação pelo mesmo caminho que recebeu. Assim, a informação será devolvida ao solicitante pela porta 4000 que foi aberta anteriormente, no início do pedido.

No protocolo TCP, todas as conexões são de caráter *FULL-DUPLEX* e ponto a ponto. Uma conexão ponto a ponto significa que cada conexão possui exatamente dois pontos terminais, neste protocolo não são permitidos processos multidifusão e difusão. Quando nos referimos a conexões *full-duplex*, estamos nos referindo ao sentido do fluxo da informação. Neste caso em específico, existem informações sendo transmitidas e recebidas nos dois sentidos ao mesmo tempo, ou seja, um *host* pode enviar e receber dados simultaneamente. Quando isto não é possível, ou seja,

ou o *host* envia dados ou recebe, não executando as duas operações juntas, temos um tipo de comunicação denominada de *Half-Duplex*.

As entidades transmissoras e receptoras que fazem uso do protocolo TCP realizam essa transmissão e recepção dos dados de forma fragmentada. Um fragmento TCP consiste em um cabeçalho fixo de 20 *bytes*, o qual carrega as informações de origem, destino, tipo do protocolo, endereço MAC, tamanho, número de sequência do pacote, parâmetros de segurança do pacote, entre outras informações, e um fragmento do dado que está sendo transmitido.

Para determinar o tamanho de formação desse pacote, cada rede possui um tamanho máximo de MTU (*Maximum Transfer Unit*), ou seja, a unidade máxima de transferência por pacote da rede. Geralmente esta unidade máxima é de 1500 *bytes*, sendo assim, um pacote de informação que irá circular por dentro da rede não pode ser maior que este valor, pois caso seja, o mesmo não será transmitido de maneira correta e não alcançará o seu destino final.

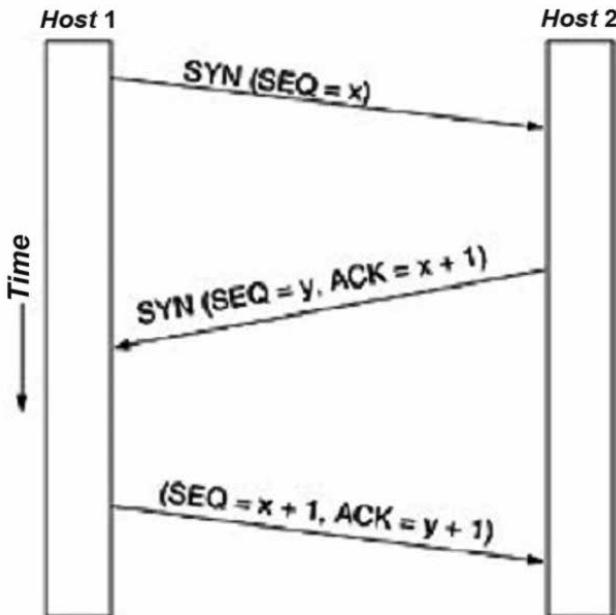
Então, um pacote contendo 1500 *bytes*, descontando sua carga de cabeçalho, terá 1480 *bytes* destinados a informações. O valor deste MTU pode ser ajustado pelo usuário, porém, ao realizar qualquer ajuste neste sentido, todo o meio de transmissão utilizado por este pacote deve ser capaz de transmitir este pacote alterado, tanto para mais quanto para menos. Em ambos os casos, se a alteração não for suportada pela infraestrutura atual, o pacote não chegará ao destino.

Em outra situação onde é reduzido consideravelmente o tamanho do MTU, o mesmo também irá apresentar problemas, pois exigirá uma maior fragmentação dos pacotes, e assim, a quantidade de pacotes gerados para transmitir a mesma informação será muito maior, o que pode vir a ocasionar congestionamento de rede e perda de pacotes no meio.

As conexões TCP são estabelecidas por meio do *handshake* de três vias, ou seja, o popularmente conhecido como triplo aperto de mão. Para estabelecer uma conexão, um lado (servidor) aguarda passivamente por uma conexão de entrada, executando as funções *LISTEN* e *ACCPEL*, o outro *host* (cliente) executa uma primitiva *CONNECT*, especificando o endereço IP e a porta à qual deseja se conectar, e o tamanho máximo de segmento de rede que deseja aceitar. A solicitação de *CONNECT* envia um segmento TCP com o bit SYN ativando um bit ACK desativado, e aguarda uma resposta.

Quando o pacote chega ao destino, o protocolo TCP verifica se existe uma primitiva *LISTEN* na porta informada, caso não haja ele envia um bit RST ativado para rejeitar a conexão. Caso contrário, havendo um processo escutando na porta solicitada, o mesmo pode recusar a conexão ou aceitar. Caso ele escolha aceitar, um segmento de confirmação será retornado, como pode ser observado na Figura 48:

FIGURA 48 - ESTABELECIMENTO DE CONEXÃO TCP



FONTE: Tanenbaum (2003, p. 575)

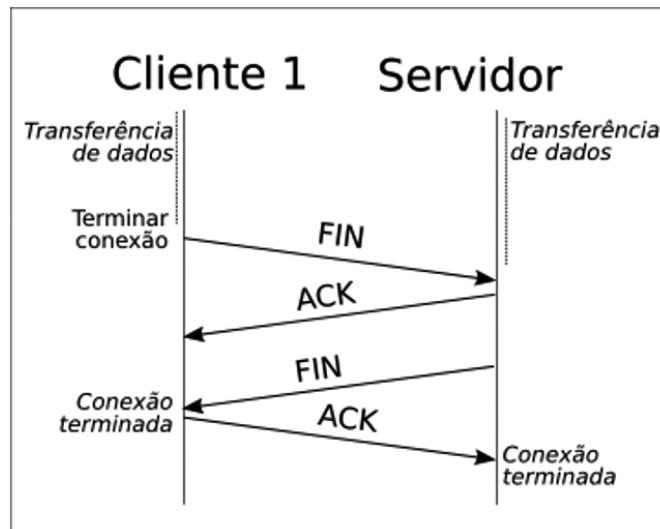
Para realizar o encerramento da conexão TCP, qualquer um dos lados pode vir a realizar, ou seja, basta enviar um segmento com o bit FIN ativado, o que significa que não há mais dados a serem transmitidos. Quando o FIN é confirmado, esse sentido é desativado para novos dados, porém a conexão somente é totalmente encerrada quando ambos os lados realizarem a confirmação do bit FIN.



BIT RST é responsável por controlar a conexão, e sempre que o mesmo tem seu valor alterado para 1, a conexão é reiniciada.

Assim, para realizar o fechamento de uma conexão são necessários quatro segmentos TCP, isto é, um FIN e um ACK para cada sentido, porém, é possível reduzir a três segmentos realizando o agrupamento do primeiro ACK e o segundo FIN, como pode ser observado na figura a seguir:

FIGURA 49 - ENCERRAMENTO DA CONEXÃO TCP



FONTE: Tanenbaum (2003, p. 575)

Como já mencionado anteriormente, o protocolo TCP, entre outras funcionalidades, se difere do protocolo UDP por possuir um controle de congestionamento de tráfego. Este controle é utilizado quando a carga oferecida a qualquer rede é maior que sua capacidade.

Para realizar tal controle, ao efetuar uma conexão TCP, são abertas duas janelas de transmissão, uma para realizar a troca de dados e outra para realizar o controle do tráfego. Dessa forma, no momento em que um dado é solicitado, a janela de controle entra em ação e realiza o acompanhamento dessa informação até seu destino. Baseado nesse fluxo, tempo de resposta, tempo de transmissão, a janela de congestionamento ajusta o tempo de envio entre um pacote e outro, para que, assim, nenhum dos dois *hosts* envolvidos no fluxo dessa informação fique sobrecarregado.

Esta análise e acompanhamento dos pacotes são realizados durante todo o processo de atividade da conexão, pois a velocidade de transmissão entre dois pontos pode alterar durante a transferência de um determinado arquivo, fazendo com que os controles de fluxo sejam todos recalibrados a ponto de evitar falhas nas transmissões e possíveis colisões de pacotes.

Em resumo, o protocolo de transporte TCP é um protocolo mais lento em relação ao protocolo UDP, porém, por possuir o triplo aperto de mão no momento do estabelecimento da conexão, oferece uma garantia sobre os dados trafegados dentro da rede, garantia que é baseada em seu estabelecimento de conexão entre os *hosts* envolvidos, controle de congestionamento do meio, solicitação e confirmação de recebimento dos pacotes que foram enviados. Assim, sempre que não há necessidade de alta performance no momento da transmissão e os dados devam alcançar o seu destino de maneira eficiente e íntegra, a melhor escolha em nível de transporte é a utilização do protocolo TCP.

6 PROTOCOLOS DA CAMADA DE APLICAÇÃO

As aplicações são a grande razão para as redes de computadores existirem. A fim de garantir que todas as aplicações funcionem de maneira correta, foram desenvolvidos protocolos de comunicação para que os mesmos venham a dar suporte às aplicações existentes.

6.1. DNS – DOMAIN NAME SYSTEM

A estrutura das redes de computadores, como já sabemos, é baseada em endereços IP, os quais estudaremos mais a fundo adiante, porém, o mesmo consiste em que todos dispositivos que estejam ligados à rede venham a ter um número específico que os identifique.

Sendo assim, os acessos aos serviços fornecidos por cada *host* dentro da rede ficam acessíveis através do seu endereço IP. Porém, como dentro de uma rede existem vários endereços IP, ficaria muito difícil de lembrar todos eles para assim poder usufruir de seus serviços.

Para resolver este problema, foram atribuídos nomes aos serviços, com a finalidade de facilitar o seu acesso e assim garantir maior acessibilidade ao mesmo. Mas, como fazer um nome ASCII corresponder a um endereço IP? Foi aí que o serviço de DNS surgiu.



American Standard Code for Information Interchange é um código binário composto por um conjunto de 128 símbolos. Dentre estes, 95 são gráficos (letras do alfabeto latino, sinais de pontuação e sinais matemáticos) e 33 sinais de controle.

A função do DNS dentro de uma rede consiste em realizar a conversão e, por consequência, a identificação de cada *host*, para que assim seja possível realizar o encaminhamento da informação ao local correto.

Segundo Tanenbaum (2003),

A essência do DNS é a criação de um esquema hierárquico de atribuição de nomes baseado no domínio e de um sistema de bancos de dados distribuídos para implementar esse esquema de nomenclatura. Ele é usado principalmente para mapear nomes de *hosts* e destinos de mensagens de correio eletrônico em endereços IP, mas também pode ser usado para outros objetivos. O DNS é definido nas RFCs 1034 e 1035.

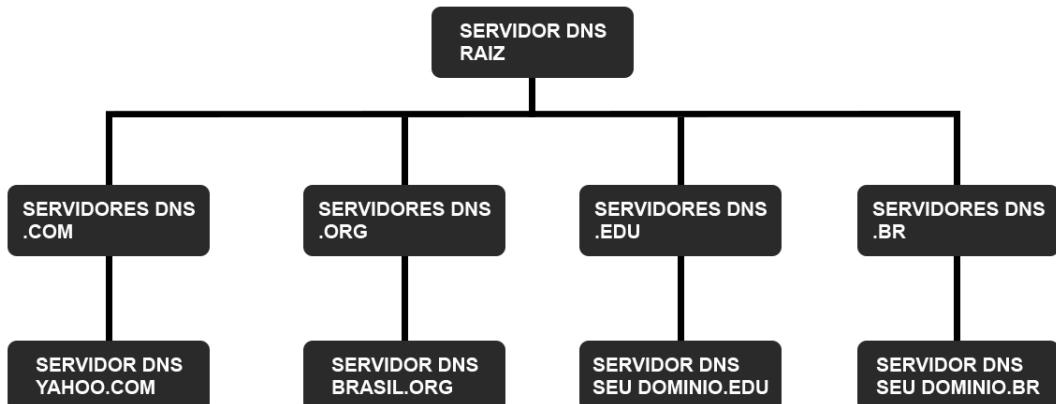
Em resumo, é função do DNS realizar a conversão de tudo o que é informado em forma de caracteres (letras) para números, pois as redes de computadores fazem o processamento dos caminhos e destino através de números (IP), e não baseado em nomes ou domínios. Sem o DNS as redes ficariam restritas aos acessos diretos, ou seja, informando e buscando os serviços através do IP e portas, como já estudamos.

No mundo existem muitos servidores DNS espalhados, desta forma, para que todos possam realizar a resolução de nomes de forma correta, foi desenvolvida uma abordagem de anúncios, onde cada servidor DNS se comunica com outro servidor DNS para realizar a propagação de suas informações, ou seja, ao registrar um domínio na internet, é necessário adquirir um servidor para que o mesmo possa ser responsável pela conversão desse determinado nome em um IP.

Para tanto, este servidor irá se comunicar com os servidores DNS da organização que regulamenta a Internet nesta localidade, no caso do Brasil, o Registro.br. Para realizar a propagação desse nome adquirido, os servidores DNS do Registro.br irão realizar a propagação desse anúncio para os servidores Raiz, ou seja, os servidores DNS mundiais, que são os detentores das classes de IP de todo mundo.

Assim, todos os servidores passam a conhecer todos os domínios de forma recursiva, como pode ser observado na Figura 50:

FIGURA 50 - ESTRUTURA DE DNS RAIZ



FONTE: O autor

Baseados nesta sincronização de DNS, os mesmos possuem uma função denominada de DNS *cache*, a qual é responsável por armazenar de forma temporária todos os endereços convertidos recentemente. Devido a este *cache*, quando realizamos qualquer tipo de alteração de servidor de um respectivo domínio na Internet, o mesmo pode ficar inacessível por determinado período, pois o servidor, que até então respondia pelo mesmo, não responde mais, e o novo servidor ainda não é conhecido por todos os servidores. Desta maneira, é necessário realizar a

limpeza do DNS *cache* do seu servidor ou esperar um tempo indeterminado até que o servidor novo de DNS realize a propagação de suas novas informações e passe as mesmas para todos os servidores de DNS do mundo, e assim, todos possam vir a atualizar o seu DNS *cache* e, consequentemente, liberar novamente o acesso a este conteúdo.

Podemos dizer que o DNS é algo fundamental para as redes de computadores e, mais precisamente, a Internet. Sem ele seria inviável qualquer tipo de serviço de localização de conteúdo ou acesso dentro das redes, devido à grande quantidade de IP's e serviços disponíveis.

6.2 SMTP - *Simple Mail Transfer Protocol*

O protocolo SMTP é o coração do serviço de *e-mail*. Sua função é realizar a transferência de mensagens de correio eletrônico do remetente para servidores de correio destinatários. No início do seu funcionamento estas mensagens transportavam somente texto, atualmente elas realizam o transporte de diferentes tipos de arquivos, tais como: áudio, vídeo, imagens, documentos etc.

Em seu lançamento e até pouco tempo atrás, este serviço de envio de mensagens era representado pela porta 25, porta que ainda se encontra em funcionamento, porém, muitos administradores estão realizando a troca da porta de serviço para 587, com a intenção de diminuir o fluxo de *spams* na Internet.



Spam é o termo usado para referir-se aos *e-mails* não solicitados que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamado de UCE (do inglês, *Unsolicited Commercial E-mail*).

FONTE: Registro.br. Disponível em: <<http://antispam.br/conceito/>>. Acesso em: 15 mar. 2016.

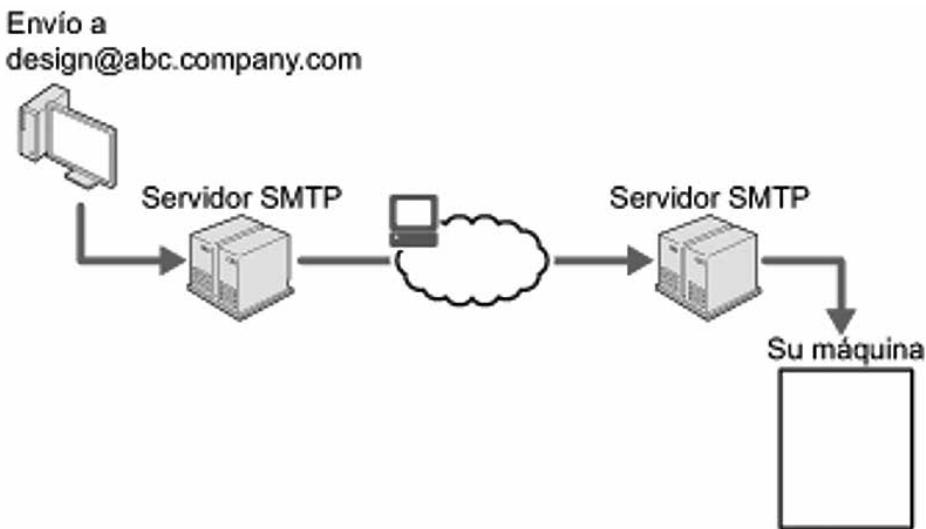
Esta simples troca de porta de serviço e a evolução do protocolo SMTP com a incorporação de métodos de autenticação do usuário para enviar mensagens vem fazendo com que vários aplicativos de envio de *spam* que utilizavam a porta 25 deixem de funcionar, fazendo com que o volume de *spams* na Internet diminua consideravelmente.

Como estamos tratando de uma troca de mensagem de forma confiável, o SMTP faz uso do protocolo de transporte TCP para realizar o envio das suas mensagens.

O funcionamento do SMTP acontece da seguinte forma: primeiramente o cliente SMTP (que funciona no hospedeiro do servidor de correio remetente) faz com que o TCP estabeleça uma conexão na porta 25 (caso esteja ainda no padrão antigo) com o servidor SMTP (que funciona no hospedeiro do servidor de correio destinatário). Se o servidor não estiver em funcionamento, o cliente tenta novamente mais tarde. Uma vez estabelecida a conexão, o servidor e o cliente trocam alguns procedimentos de apresentação antes de transferir as informações (técnica padrão de conexão utilizando TCP). Cliente e servidor SMTP, depois da conexão estabelecida, realizam outra troca de apresentações entre si, nessa fase, o cliente SMTP indica os endereços de *e-mail* do remetente e do destinatário. Assim que a etapa de apresentação entre os servidores é finalizada, a mensagem é enviada, e o servidor destinatário realiza a confirmação de recebimento da mensagem ao servidor remetente.

A partir desse momento, a mensagem enviada está armazenada no servidor de correio eletrônico do destinatário e está disponível para que o usuário proprietário da mensagem possa realizar seu *login* no servidor e assim realizar a visualização da mesma, como pode ser observado na Figura 51.

FIGURA 51 - SERVIÇO SMTP



FONTE: Disponível em: <http://support.ricoh.com/bb_v1oi/pub_e/oi_view/0001043/0001043279/view/fax/int/0121.htm>. Acesso em: 20 fev. 2016.

6.3 POP3 - POST OFFICE PROTOCOL VERSION 3

O POP3 é um protocolo de acesso de correio eletrônico extremamente simples e suas funcionalidades são bastante limitadas.

Segundo Kurose (2010, p. 93),

O POP3 começa quando o agente de usuário (cliente) abre uma conexão TCP com o servidor de correio (o servidor) na porta 110. Com a conexão TCP ativada, o protocolo passa por três fases: autorização, transação e atualização. Durante a primeira fase, autorização, o agente de usuário envia um nome de usuário e uma senha para autenticar o usuário. Na segunda fase, transação, recupera mensagens; é também nessa fase que o agente de usuário pode marcar mensagens que devem ser apagadas, remover essas marcas e obter estatísticas de correio. A terceira fase, atualização, ocorre após o cliente ter dado o comando *quit*, que encerra a sessão POP3.

Segue uma imagem ilustrativa do funcionamento deste protocolo:

FIGURA 52 - SERVIÇO POP



FONTE: Disponível em: <http://support.ricoh.com/bb_v1oi/pub_e/oi_view/0001043/0001043279/view/fax/int/0121.htm>. Acesso em: 20 fev. 2016.

Como citado, o POP responde na porta de comunicação 110 por padrão, porém, da mesma forma que o protocolo SMTP, o mesmo vem evoluindo e as novas versões desse protocolo já passam a utilizar a porta 995. Tal alteração está sendo realizada não somente motivada pelos altos índices de *spams*, mas também pela implementação de novos itens de segurança para a realização da autenticação do usuário.

Estes novos modelos de segurança deixam de utilizar o *login* e senha em texto puro como eram utilizados, e passam a implementar a criptografia de dados, e ainda, em alguns casos, a incorporação de certificados digitais para dar mais segurança aos usuários e suas mensagens armazenadas.

O processo de funcionamento base não sofreu nenhum tipo de alteração, somente novas premissas de segurança é que foram adotadas, para assim garantir a confiabilidade e integridade das informações de cada conta.

6.4 HTTP – PROTOCOLO DE TRANSFERÊNCIA DE HIPERTEXTO

O protocolo HTTP é um protocolo existente dentro da camada de aplicação, e, é responsável pelo funcionamento da *web*. Seu funcionamento é dividido em cliente e servidor, os quais, são independentes e diferentes. O cliente HTTP gera as solicitações que são recebidas e respondidas pelo servidor HTTP, dessa forma acontece a troca de informações entre eles.

Este protocolo define a estrutura das mensagens e o modo como o cliente e o servidor as trocam.

Uma página na Internet nada mais é do que um documento construído e disponível dentro da rede, o que muda dele para outro documento qualquer é a forma como o mesmo foi desenvolvido e como será exibido. Este documento normalmente é desenvolvido a partir de uma linguagem de programação, como HTML, PHP, JAVA, entre outras, e conta com imagens, fotos e outros elementos gráficos.

Dessa forma, no momento em que um determinado usuário busca com ajuda do servidor de DNS um determinado domínio, o servidor respectivo que responde por este domínio recebe esta solicitação, a qual busca dados na porta 80, que representa o protocolo HTTP.

Esta solicitação ou pedido é constituída por uma URL, ou seja, o endereço do documento que se deseja acessar. Assim, cada URL é composta de duas partes, o nome do servidor que se deseja buscar e nome do objeto (arquivo) que se deseja abrir, como pode ser observado no exemplo:

HTTP://www.nead.com.br/hp-2.0/home/index.php

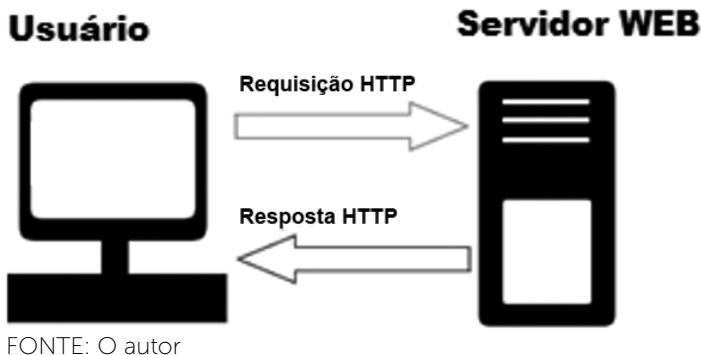
No exemplo acima, NEAD é nome do *host* que queremos acessar e /hp-2.0/home/index.php é o caminho para chegar ao conteúdo requerido.

Este protocolo determina como clientes WEB (*browsers*) requisitam as páginas *web* aos servidores e como eles as transferem a clientes. Esta conexão entre cliente e servidor faz uso do protocolo da camada de transporte TCP, pois as informações trafegadas nesse canal de comunicação não podem ser perdidas ou alteradas, e não podemos nos esquecer do controle de congestionamento existente no TCP, que neste momento é de suma importância para garantir a alta performance do protocolo.

O funcionamento do protocolo HTTP é muito simples, ele acontece da seguinte forma: um cliente em seu navegador (*browser*) realiza uma solicitação de uma determinada informação a um determinado *host* através do seu endereço, neste momento vamos desconsiderar a interação com o servidor DNS para localizar o

host. Esta solicitação, ou melhor, esta requisição HTTP, é enviada ao servidor com o nome do *host*, o endereço do arquivo a ser acessado, porta de serviço ou *socket* (80). Ao realizar esta solicitação, o *host* inicial deixa uma porta de comunicação aberta para essa sincronização, porém, como já estudamos, esta porta não é a mesma a ser utilizada pelo servidor remoto. Ao receber a requisição, o servidor remoto analisa o pacote e retorna uma resposta HTTP para remetente já na porta específica de conexão, a qual foi determinada no momento da sincronização do protocolo TCP entre os dois *hosts*, como pode ser observado na Figura 53.

FIGURA 53 - HTTP REQUISIÇÃO E RESPOSTA



FONTE: O autor

A partir dessa sincronização, os dados começam a ser transferidos e o *browser* do remetente dá início ao processo de interpretação dos códigos contidos dentro do arquivo recebido, passando a realizar a montagem no *site* para o usuário.

Em resumo, a *web*, também conhecida como WWW (*World Wide Web*), é uma estrutura arquitetônica que permite o acesso a documentos vinculados e espalhados por milhões de máquinas na Internet, tudo isso utilizando como base o protocolo HTTP para realizar as trocas de mensagens e sincronização entre cliente e servidor (KUROSE, 2010, p. 72).

Para fazer uso da *web*, o usuário deve possuir um navegador, sendo os mais conhecidos Internet Explorer, Google Chrome, Mozilla, Edge, entre outros. Cada navegador já possui incorporado dentro de sua arquitetura o protocolo HTTP para realizar a comunicação entre cliente e servidor e os *plugins* necessários para a interpretação das linguagens de programação utilizadas para o desenvolvimento dos conteúdos que foram disponibilizados.



Um *plugin* é um programa instalado no navegador que permite a utilização de recursos não presentes na linguagem HTML, no qual é criada a grande maioria das páginas.

Como já mencionamos anteriormente, cada aplicação possui uma porta de referência, uma porta de comunicação, no caso do HTTP não é diferente. O HTTP tem por padrão a porta 80 como interface de comunicação, desta maneira, todas as requisições devem chegar ao servidor de conteúdo buscando esta interface para assim receber os dados.

Porém, como já mencionamos, muitas vezes os administradores, por segurança, acabam por alterar a porta dos seus serviços. O mesmo pode vir a acontecer no HTTP, não é algo muito comum, mas pode acontecer. Esta alteração não é considerada comum, pois ao realizá-la, todos os navegadores que buscarem informações deste *host* na porta 80 não terão êxito, dificultando assim a exibição dos conteúdos. Para que esta alteração funcione de maneira correta, todos os usuários que tenham a necessidade de buscar conteúdo neste servidor remoto terão de conhecer a porta de serviço do mesmo, para, desta maneira, informar em seu navegador a nova porta de serviço, como pode ser observado no exemplo a seguir:

HTTP://www.nead.com.br:8080

NEAD é o *host* a ser acessado, e o número 8080 consiste na porta de serviço onde o protocolo HTTP está respondendo no *host*.

O protocolo HTTP possui uma variação denominada de HTTPS. Esta variação do protocolo surgiu com a intenção de aumentar os índices de segurança da Internet de forma geral. Este protocolo traz agregado às suas funcionalidades já conhecidas o certificado digital. Este certificado tem a intenção de trazer maior confiabilidade ao serviço que está sendo acessado.

Esta confiabilidade é garantida para o usuário final a partir de algumas entidades certificadoras que realizam a criação dos certificados. Para que este conceito de autenticidade venha a ter êxito, os navegadores (*browsers*) devem possuir dentro de sua arquitetura uma lista com todas as unidades certificadoras verídicas existentes, para que no momento de sua utilização, ao receber um certificado de um determinado *site*, o mesmo possa ser analisado e assim comparado com a base do navegador e, desta maneira, seja validado, garantindo um alto índice de confiabilidade e autenticidade das informações ali trafegadas.

Podemos finalizar o protocolo HTTP descrevendo que ele é o principal responsável pela troca de informações entre cliente e servidor, e sem ele a Internet como a conhecemos não existiria.

6.5 FTP – FILE TRANSFER PROTOCOL

O FTP é um protocolo destinado à transferência de arquivos direta entre cliente e servidor, onde, para ter acesso ao local de troca de arquivo entre ambos, o usuário deve se identificar.

Esta identificação nada mais é do que uma solicitação de usuário e senha. Baseado nestas informações, o servidor lhe dará acesso ou não aos dados e, juntamente com o acesso, os privilégios concedidos a este determinado usuário.

Os privilégios de acesso podem variar entre somente leitura e escrita/leitura dentro do servidor, sem falar nos níveis de acesso a conteúdo que podem ser criados pelo gestor para garantir a confidencialidade das informações ali armazenadas.

Esta conexão criada entre cliente e servidor faz uso do protocolo TCP da camada de transporte, pois estamos tratando de informações que estão sendo transferidas de um local para outro e, assim, devem chegar de forma íntegra e confiável ao seu destino final.

Uma conexão FTP acontece da seguinte maneira: o usuário informa o endereço do *host* que deseja acessar, ao enviar a solicitação e a conexão será aceita pelo servidor, o mesmo responde ao usuário solicitando suas credenciais para acesso (*login/senha*). Ao informar tais dados, os mesmos são conferidos pelo servidor remoto, e assim que os dados de autenticação são validados, são entregues para o usuário seus privilégios de acesso. Estes privilégios, como já mencionado, consistem no que o usuário pode ver e alterar dentro do local acessado.

A grande parte dos serviços de FTP está vinculada à porta de serviço 21, porém, como não foge à regra, a mesma pode vir a ser alterada de acordo com a necessidade do administrador, por segurança ou simplesmente por padronização interna na rede.

O serviço de FTP é amplamente utilizado para enviar arquivos para servidores remotos, na grande maioria das vezes são documentos e arquivos utilizados no abastecimento dos *sites* organizacionais. Porém, uma abordagem muito utilizada é o FTP como uma forma de armazenamento de arquivos de *backup* das organizações, tirando estes dados de dentro da organização e alocando os mesmos na nuvem, com a intenção de aumento de segurança e replicação das informações para garantir a disponibilidade das informações.

6.6 DHCP

DHCP é a abreviatura de *Dynamic Host Configuration Protocol*, e visa automatizar as configurações TCP/IP enviadas aos dispositivos na rede (impressoras, computadores, *switches*). Sem a automatização desse serviço, os administradores de rede teriam que configurar manualmente dispositivo por dispositivo. O uso deste serviço pode trazer diversos benefícios, dentre os quais se destacam:

- A configuração de forma automática de todos os *hosts* ligados à rede.

- Praticidade de gestão da rede e dos recursos oferecidos por ela no sentido de alterações de configurações e possíveis erros de configuração, caso fossem realizadas manualmente.

O DHCP pode prover um controle centralizado para o endereçamento do protocolo TCP/IP. Com um servidor DHCP é possível fornecer informações vitais para o exercício de uma rede baseada no padrão TCP/IP. O DHCP pode incluir: o IP, máscara de *sub-net*, *gateways*, DNS primário e secundário e WINS. O serviço de DHCP pode também fornecer endereços IPV4 e IPV6 para qualquer uma das interfaces de rede dos computadores.



WINS - *Windows Internet Name Service* ou *Net Bios Name Service* (NBNS) é um protocolo muito similar ao DNS. Fornecendo endereços TCP/IP em função de nomes e garantindo a manutenção e replicação de dados de nomes existentes na rede local.

O DHCP age da seguinte forma: considere uma estação de trabalho configurada para utilizar o DHCP. Durante a inicialização, esta estação de trabalho entra em um processo de “descobrir” um servidor DHCP na rede. Uma vez que a estação de trabalho consegue se comunicar com o servidor DHCP, ela recebe todas as configurações do protocolo TCP/IP, diretamente do servidor DHCP, ou seja, com o uso do DHCP, o administrador pode automatizar as configurações do protocolo TCP/IP em todos os computadores da rede sem a necessidade de realizar a configuração manual em cada dispositivo conectado.

7 PROTOCOLO IP (*INTERNET PROTOCOL*)

O elemento que mantém a Internet unida é o protocolo da camada de rede denominado de *Internet Protocol* (IP). Este protocolo, desde sua origem, foi desenvolvido com a intenção de realizar a interligação das redes. Pois, como já sabemos, a Internet nada mais é do que uma grande rede formada pela interligação de todas as pequenas redes existentes.

Atualmente, o protocolo IP possui duas versões, sendo elas a versão 4 e a versão 6. Dentre as versões, damos maior destaque inicialmente à versão 4, devido à sua ampla disseminação e utilização.

Podemos encontrar o protocolo IP versão 4 em todos os *hosts* ligados a uma rede. Sem ele seria impossível realizar qualquer tipo de comunicação ou troca de dados entre dois ou mais dispositivos conectados.

Esta versão 4 foi, e está sendo, utilizada por muito anos, porém, com o crescimento demasiado da Internet e má utilização deste protocolo, o mesmo alcançou o seu limite quanto à alocação de endereço para *hosts* dentro das redes, ou seja, dentro de pouco tempo não seria mais possível a inserção de nenhum novo *host* dentro da Internet. Assim, podemos concluir que este protocolo chegou ao seu limite.

Como a estrutura da Internet (redes) não para de crescer e a cada dia que passa novos dispositivos são conectados à rede, surgiu a necessidade de realizar o desenvolvimento de um novo protocolo, o qual viesse a suprir a necessidade de alocação de novos *hosts*.

Este novo protocolo foi denominado de protocolo IP versão 6, e o mesmo trouxe a possibilidade de crescimento praticamente infinito para as redes existentes.

Desde seu surgimento, o processo de migração da versão 4 para a versão 6 tem sido efetuado. Este processo tem acontecido de forma gradual, para que todos os provedores de serviço (provedores de Internet) e os provedores de conteúdo (portais) tenham plena condição de realizar as alterações necessárias sem que seus serviços ou clientes venham a sofrer por falta de conectividade ou informação.

Este processo de migração já vem acontecendo há alguns anos, porém, atualmente nem 10% de todo o conteúdo existente na Internet opera na versão 6 deste protocolo. Esta dupla pilha de protocolos será utilizada até que todos os serviços e conteúdos estejam 100% em versão 6. Somente neste momento o protocolo versão 4 será descontinuado.

7.1 | IPv4

O protocolo IP versão 4 foi o protocolo que deu origem à comunicação e interligação das redes existentes. Sua atuação acontece em cima de cada datagrama ou pacote transferido na rede. É graças ao protocolo IP que as informações conseguem alcançar o seu destino final.

Dessa maneira, um pacote IPv4 é composto por um cabeçalho e os seus dados, como pode ser observado na Figura 54. O cabeçalho é responsável pelas informações para realizar o direcionamento e entrega do pacote de forma segura e confiável, e os dados, ou carga útil do pacote, são compostos simplesmente pelas informações que o usuário deseja transmitir.

FIGURA 54 - CABEÇALHO IPV4

Versão	Comprimento do Cabeçalho	Tipo de Serviço	Comprimento do Datagrama
Identificador		Flags	Deslocamento de Fragmentação
Tempo de Vida	Protocolo	Bits para verificação da Integridade do Cabeçalho	
Endereço IP da Fonte			
Endereço IP do Destino			
Opções			
Dados			

FONTE: O autor

Como pode ser observado na imagem anterior, o pacote IPv4 possui vários parâmetros que fazem com que o mesmo possa vir a trafegar entre diferentes redes sem grandes problemas. Iremos explicar cada campo deste protocolo.

- Número da versão → o número da versão é responsável por identificar qual a versão de protocolo que está sendo utilizada por este pacote, IPv4 ou IPv6.
- Comprimento do cabeçalho → o comprimento do cabeçalho é responsável por determinar em que parte do pacote termina o cabeçalho e iniciam os dados. Isso acontece porque um pacote IPv4 pode ter seu tamanho variado, podendo vir a ter mais informações no cabeçalho ou menos, e assim, a posição dos dados dentro pacote pode variar, isso, é claro, quando nos referimos aos *bits* que estão sendo trafegados.
- Tipo de Serviço → estes *bits* foram incluídos no cabeçalho do protocolo IP versão 4, para poder diferenciar os diferentes tipos de pacotes IP que estão circulando dentro da rede. Dessa maneira, é possível dar prioridade para um determinado tipo de pacote que está circulando dentro da rede. Um exemplo muito simples de compreender esta aplicação é a questão dos pacotes de voz sobre IP, onde os mesmos não devem possuir nenhum tipo de atraso e assim precisam ter prioridade dentro da rede em relação aos outros pacotes.
- Comprimento do datagrama → o comprimento do datagrama nada mais é do que o tamanho total do pacote, ou seja, levando em consideração que todo o cabeçalho do pacote deve possuir no máximo 16 *bits* e o tamanho máximo de um pacote é de 65.535 *bytes*, porém, em praticamente 100% das redes existentes atualmente, os datagramas não são maiores que 1.500 *bytes*, pois os equipamentos que normalmente realizam a conversão das redes não suportariam pacotes superiores a este valor de 1.500 *bytes*.

- Identificador, *flags*, deslocamento de fragmentação → estes três campos estão diretamente ligados à fragmentação do pacote, sendo assim, é este campo que determina o tamanho máximo que um pacote pode ter para realizar a transmissão de dados dentro da rede. Caso o dado gerado ou transmitido seja maior que o meio possa carregar, o pacote é fragmentado, ou seja, dividido em outros pacotes para que assim possa vir a alcançar o seu destino. Esta informação fragmentada será remontada e interpretada pelo destino. No protocolo IPv4, esta fragmentação (divisão) pode vir a acontecer em roteadores, caso um determinado pedaço do caminho a ser utilizado seja menor que as outras partes envolvidas. Este processo de fragmentação dentro do roteador garante a entrega confiável do pacote. Caso o mesmo não fosse realizado, o pacote seria descartado, pois não seria possível enviar um pacote de informação com um tamanho superior ao meio em que o mesmo será inserido.
- Tempo de vida → este campo foi inserido dentro dos pacotes como uma forma de segurança para que os pacotes perdidos não fiquem circulando dentro da rede, consumindo processamento de transmissão dos equipamentos envolvidos. Dessa forma, ao gerar um pacote, o *host* em questão define um TTL (*time-to-live*) para este pacote; o mesmo, ao passar por um roteador, sofre uma decrementação do valor, assim, quando o mesmo chegar a 0, o pacote é descartado pelo roteador, não permitindo que o mesmo fique circulando dentro da rede, congestionando o meio. Este TTL normalmente tem seu valor aproximadamente de 30, assim, o mesmo pode passar por 30 roteadores até alcançar o seu destino.
- Protocolo → o campo protocolo não é utilizado durante a transmissão, e sim ao chegar ao seu destino final. Este campo é responsável por determinar qual tipo de protocolo está sendo utilizado pela camada de transporte para realizar a transmissão dos dados. Lembrando que os principais protocolos de transmissão utilizados pela camada de transporte são o TCP e o UDP.
- Soma de verificação de cabeçalho → este item do cabeçalho é responsável por auxiliar os roteadores na detecção de erros nos *bits* recebidos. Seu funcionamento é bem simples. Ele realiza uma soma de todos os *bits* existentes dentro do pacote. Considerando que a cada dois *bits* seja um número, a soma total de todos os *bits* é inserida dentro do pacote neste campo. Ao ser trafegado dentro da rede, o pacote é analisado por diferentes roteadores e *hosts*, com a intenção de direcionar o pacote para seu destino correto, porém, durante esse processo, cada nó da rede realiza a soma de todos os *bits* existentes dentro do pacote, da mesma forma que o remetente fez. Realizando a soma dos *bits*, cada nó pode realizar uma validação dos dados, comparando a soma existente dentro do cabeçalho com a soma alcançada por ele em sua verificação. Caso os números sejam idênticos, o pacote não sofreu nenhum tipo de alteração binária durante seu deslocamento, caso contrário, o mesmo foi modificado propositalmente ou accidentalmente, mas em ambos os casos o pacote é descartado, pois não está mais íntegro e, assim, não atende às especificações de segurança e qualidade exigidas pelo protocolo em questão.

- Endereços IP de fonte e de destino → quando uma fonte cria um pacote, insere seu endereço IP no campo de endereço de fonte IP e insere o endereço do destino final no campo de endereço destinatário IP. Muitas vezes o endereço do destinatário é encontrado através de uma consulta de DNS, o qual já foi estudado anteriormente.
- Opções → este campo permite que um cabeçalho IP seja ampliado, acrescendo outras informações que o desenvolvedor acha importante. Esse campo é muito pouco utilizado.
- Dados → neste campo são carregadas as informações propriamente ditas, ou seja, os dados que serão transmitidos e recebidos pela rede. Como vimos anteriormente, os dados não são trafegados de forma inteira, e sim fragmentados, divididos a quantidade de vezes que for necessária, lembrando que cada pacote dentro da rede possui um tamanho máximo, tamanho o qual irá determinar a quantidade de pacotes que cada informação gerará.

7.1.1 Endereçamento IPv4

Como vimos até aqui, dentro de uma rede de computadores, cada dispositivo, ativo de rede para se comunicar com outro ativo e realizar o encaminhamento dos pacotes ou mesmo gerar pacotes, obrigatoriamente necessita possuir um IP.

O endereço IP é responsável por realizar a sincronização entre os *hosts*, no sentido de que ambos estejam alocados próximos no sentido lógico da rede para que assim possam vir a se comunicar.

Sendo assim, cada ativo de rede deve possuir uma interface de rede, lógica ou física. Esta interface de rede é a fronteira entre o *host* em si e a camada de rede, e é ela que realizará toda a transferência do dado gerado pelo *host* em questão para o meio físico onde o mesmo está conectado.

Sendo o endereçamento algo tão fundamental para as redes de computadores, daremos maior atenção a ele.

Kurose (2010, p. 247) explica o endereçamento IPv4 da seguinte forma:

“Cada endereço IP tem o comprimento de 32 bits (equivalente a 4 bytes). Portanto, há um total de 2^{32} endereços IP possíveis. Fazendo uma aproximação de 2^{10} por 10^3 , é fácil ver que há cerca de 4 bilhões de endereços IP possíveis. Esses endereços são escritos em notação decimal separada por pontos na qual cada byte do endereço é escrito em sua forma decimal e separado dos outros bytes do endereço por um ponto. Por exemplo, considere o endereço IP 193.32.216.9. O 193 é o número decimal equivalente aos primeiros 8 bits do endereço; o 32 é o decimal equivalente ao segundo conjunto de 8 bits do endereço e assim por diante. Por conseguinte, o endereço 193.32.216.9, em notação binária é 11000001 00100000 11011000 00001001”.

Sendo assim, cada interface de cada *host*, roteador ou qualquer outro ativo de rede deve possuir um endereço IP para que possa se comunicar com os demais equipamentos. Porém, para adicionar um IP a uma interface, o mesmo não pode ser feito de forma aleatória: é preciso respeitar a sub-rede em que o *host* está alocado.

Os endereços IP versão 4 são divididos em cinco categorias, listadas na imagem a seguir:

FIGURA 55 - CLASSES IPV4

Classe	32 Bits			Intervalo dos endereços de host
A	0	rede	host	1.0.0.0 - 127.255.255.255
B	10	rede	host	128.0.0.0 - 191.255.255.255
C	110	rede	host	192.0.0.0 - 223.255.255.255
D	1110	endereço multicast		224.0.0.0 - 239.255.255.255
E	1111	reservado para uso futuro		240.0.0.0 - 255.255.255.255

FONTE: Kurose (2010)

Essa alocação chegou a ser denominada de endereçamento de classes completo. Embora não seja mais usada, ainda são comuns referências a essa alocação na literatura.

Em resumo, podemos reconhecer a classe de um determinado endereço IP pelo seu primeiro conjunto de *bits*, como pode ser observado na imagem anterior. Assim, podemos resumir as classes da seguinte forma:

- Classe A --> Primeiro *bit* do primeiro octeto iniciando em 0
- Classe B --> Primeiros dois *bits* do primeiro octeto sendo 10
- Classe C --> Primeiros três *bits* do primeiro octeto sendo 110
- Classe D --> Primeiros quatro *bits* do primeiro octeto sendo 1110
- Classe E --> Primeiros quartos *bits* do primeiro octeto sendo 1111



Multicast é a entrega de informação para múltiplos destinatários usando a estratégia mais eficiente, onde as mensagens só passam por um *link* uma única vez e somente são duplicadas quando o *link* para os destinatários se divide em duas direções. Em comparação com o Multicast, a entrega simples ponto a ponto é chamada UNICAST, e a entrega para todos os pontos de uma rede chama-se Broadcast.

FONTE: Disponível em: <IPV6.br>. Acesso em: 7 abr. 2016.

A distribuição dos endereços IP é responsabilidade da ICANN (*Internet Corporation for Assigned Names and Numbers*), esta é a organização que realiza o gerenciamento dos endereços e classes de rede. Esta abordagem de um órgão mundial para gerir os recursos de numeração foi essencial para evitar possíveis conflitos de rede, já que não pode haver, dentro de uma rede, dois *hosts*/ativos coexistindo com o mesmo número de IP.

Assim, a ICANN realiza a delegação dos endereços IP para diversas autoridades regionais, como a LANIC na América Latina, e ela, por sua vez, designa os blocos de IPs aos provedores de acesso, que então repassam os endereços aos seus clientes.



LANIC - Latin American Network Information Center é a organização que gerencia dentro da América Latina os registros de nomes da Internet e os recursos de numeração.

Os endereços IP são hierárquicos, diferentemente dos endereços *Ethernet*. Cada endereço de 32 bits é composto de uma parte de rede de tamanho variável nos *bits* superiores e uma parte de *host* nos *bits* inferiores. A parte de rede tem o mesmo valor para todos os *hosts* em uma única rede. Isso significa que uma rede corresponde a um bloco contínuo de espaços de endereços IP. Este bloco de endereço fixo e comum a todos os *hosts* é denominado de prefixo.

Em geral, os endereços de rede são números de 32 bits escritos em notação decimal com pontos. Assim, a cada um dos quatro *bytes* é escrito em notação decimal, de 0 a 255.

Os prefixos são escritos dando menor endereço IP no bloco de endereços. O tamanho do prefixo é determinado pelo número de *bits* na parte de rede; os *bits* restantes fazem parte do campo de *hosts* e podem variar. Isso significa que o tamanho do endereço deve ser uma potência de dois. Por convenção, ele é escrito após o prefixo com uma barra seguida pelo tamanho em *bits* da máscara de rede.

A principal vantagem acrescida pela utilização de prefixos de rede é proporcionada aos roteadores, que podem efetuar o encaminhamento dos pacotes apenas baseado nos mesmos. A parte final, ou seja, a parte destinada aos *hosts*, não importa para os roteadores, pois todos os *hosts* que utilizam o mesmo prefixo obrigatoriamente estarão alocados juntos.

Assim, a máscara de rede, em resumo, é responsável por determinar a quantidade de *hosts* possíveis dentro da rede ou da sub-rede. É ela que descreve o início e o fim de uma rede. Desta forma, vamos estudar como calcular a máscara e o endereço IP para uma determinada rede.

Sempre ao realizar um cálculo de rede, possuiremos um endereço base para realizar o cálculo. Em nosso exemplo utilizaremos o endereço 192.168.0.2/24. Para tal cálculo, temos que levar em consideração o tamanho máximo de *bits*, ou seja, 32 *bits*. O primeiro cálculo que iremos realizar é a quantidade de *hosts* possíveis a serem alocados nesta rede.

Para realizar o cálculo de *hosts*, utilizaremos o valor total de *bits* possíveis 32 e descontaremos a quantidade fixa utilizada pela máscara 24, chegando ao valor 8. Este valor 8 representa a quantidade de *bits* que poderão ser alterados para a formação dos endereços dos *hosts*, lembrando que os 24 *bits* da máscara representam os *bits* do prefixo de rede e, dessa forma, os mesmos são fixos.

Tendo o valor de 8 *bits* para *hosts*, e lembrando que estamos trabalhando com números binários, onde as possibilidades são de 0 ou 1, realizaremos a operação 2^8 . O resultado dessa operação é o valor total de IPs, ou seja, temos 256 IPs dentro desta rede. Como descrito, encontramos a quantidade de IPs, não a quantidade de *hosts* possíveis, isso porque temos que descontar ainda dessa quantidade total de IPs o endereço de *broadcast* e o endereço de rede (que dá nome/identificação à rede) para, aí sim, chegarmos à quantidade de *hosts* possíveis. Realizando esta operação, chegamos a 254 *hosts* possíveis.

Agora que temos a quantidade de *hosts*, temos que encontrar o endereço de rede e o endereço de *broadcast* desta rede. Vamos iniciar com o endereço de rede: para tal cálculo, iniciaremos realizando a conversão do endereço de rede informado e da máscara de rede para binário, como é possível visualizar na Figura 56.

FIGURA 56 - CONVERSÃO ENDEREÇO IP E MÁSCARA DE REDE PARA BINÁRIO

IP = 11000000.10101000.00000000.00000010
192 . 168 . 0 . 2
Máscara de rede = 11111111.11111111.11111111.00000000
255 . 255 . 255 . 0

FONTE: O autor

O próximo passo é realizar uma operação de E entre o endereço de rede e a máscara de rede, realizando a comparação de *bit* a *bit*, onde valores iguais permanecem iguais e valores diferentes são convertidos para 0, como pode ser observado na Figura 57.

FIGURA 57 - OPERAÇÃO E ENTRE MÁSCARA DE REDE E ENDEREÇO IP

```
IP = 11000000.10101000.00000000.00000010
```

```
M= 11111111.11111111.11111111.00000000
```

```
E = 11000000.10101000.00000000.00000000
```

```
R = 192 . 168 . 0 . 0
```

FONTE: O autor

Assim, conseguimos chegar ao endereço de rede, que neste caso é 192.168.0.0, e agora iremos realizar o cálculo para encontrar o endereço de *broadcast* da rede. Para este cálculo também utilizaremos o endereço de rede fornecido, porém a máscara sofrerá uma inversão, ou seja, todos os *bits* 1 da máscara de rede passarão a ser 0 e os *bits* 0 passarão a ser 1.

Com o endereço de rede fornecido, faremos uma operação OR com a inversão da máscara de rede. Esta operação consiste em uma nova comparação *bit a bit* entre os dois endereços, porém, desta vez os *bits* diferentes serão transformados em 1 e os *bits* iguais permanecerão iguais, como pode ser observado na figura a seguir:

FIGURA 58 - OPERAÇÃO OR

```
IP = 11000000.10101000.00000000.00000010
```

```
IM= 00000000.00000000.00000000.11111111
```

```
OR = 11000000.10101000.00000000.11111111
```

```
B = 192 . 168 . 0 . 255
```

FONTE: O autor

Desta forma, encontramos o endereço de *broadcast* da rede, o qual é representado por 192.168.0.255. Com estes cálculos, encontramos o endereço de rede, *broadcast* da rede e a quantidade de endereços que podem vir a serem utilizados para ativos dentro da rede.



O *Broadcast* de uma rede é definido como um endereço de rede que realiza o transporte de informações a todos os *hosts* da rede. O endereço utilizado para *broadcast* é sempre o último endereço IP da rede. Este endereço também pode ser utilizado para mapeamento de rede entre outras funções.

7.1.2 Sub-redes

Levando em consideração tudo o que estudamos até aqui, lembramos que todo dispositivo ligado a uma rede obrigatoriamente possui um endereço, o qual está diretamente vinculado a uma rede ou sub-rede.

Uma sub-rede nada mais é do que uma rede que foi dividida diversas vezes, onde cada fragmento dessa divisão deu origem a uma nova rede, independentemente da quantidade de vezes em que a rede inicial foi dividida.

Este conceito de sub-redes surgiu com a necessidade de economizar os endereços de rede, onde é possível de uma rede fazer várias outras, e assim realizar a distribuição destas diferentes redes para diferentes locais sem que haja endereços IPs desperdiçados, ou seja, alocando uma rede inteira para um ou dois *hosts*. Dessa maneira, é possível realizar um dimensionamento correto baseado na quantidade de IPs necessários e criar uma sub-rede que venha atender à demanda correta, sem que haja uma grande sobra de IPs dentro dessa rede.

Quando possuímos uma rede e resolvemos realizar a sua subdivisão, a mesma não precisa de autorização da ICANN ou de qualquer outra organização, pois para elas o bloco ou rede continua igual, ou seja, a subdivisão da rede não muda nada no sentido de direcionamento de tráfego. Assim, as alterações somente terão efeito dentro da rede local, onde as subdivisões realmente terão o efeito programado, isolando o tráfego entre as redes criadas e não permitindo acesso direto entre as sub-redes, por mais que as mesmas estejam utilizando os mesmos meios físicos para realizar as transmissões dos seus dados.

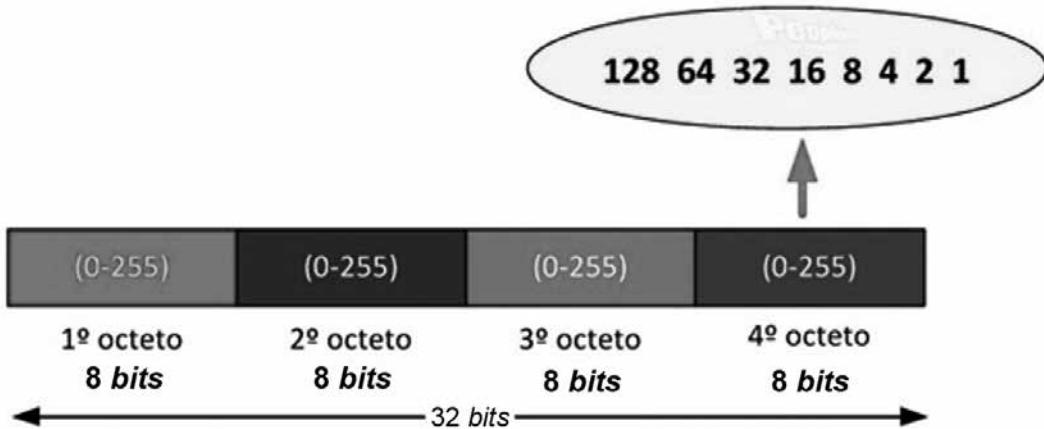
Para implementar a divisão em sub-redes é necessária a utilização de uma máscara de sub-rede, pois é ela que realiza a divisão entre o número de rede, mais sub-rede e o *host*. Estas máscaras de sub-rede também são escritas em notação decimal com pontos, com a inclusão de uma barra vertical seguida pelo número de *bits* na parte de rede mais sub-rede. Uma máscara de rede sub-rede pode ser escrita como 255.255.252.0 ou em uma anotação alternativa /22 para indicar que a máscara de sub-rede tem 22 *bits*, como já estudado.

Esta subdivisão de uma rede é de suma importância para um bom planejamento e estruturação de uma rede com a intenção de não desperdiçar endereços IP. Sendo assim, a subdivisão de uma rede acontece da seguinte forma: partindo da rede inicial 192.168.1.0/24, que, baseado no que estudamos até agora, sabemos possuir 256 endereços, sendo 254 disponíveis para *host*, pede-se para dividir esta rede em seis novas sub-redes que possam alocar 30 *hosts* em cada uma delas.

O primeiro passo para uma subdivisão é identificar se a rede principal suportaria esta nova rede. Para tanto, iremos verificar quantos endereços IP serão necessários para montar esta rede. Lembrando que toda nova rede terá um endereço de rede e um endereço de *broadcast*, dessa maneira, para cada nova rede serão gastos 32 endereços IP. Logo, $32 \times 6 = 192$, assim serão necessários 192 endereços. Como nossa rede principal suporta 254 endereços, a primeira premissa de disponibilidade de IPs é atendida pela rede principal.

Após a verificação de disponibilidade da rede principal, iremos realizar o cálculo de rede da nova máscara de rede. Dando prioridade à exigência a nível de PCs, vamos considerar o diagrama a seguir para ajudar na identificação de *bits*.

FIGURA 59 - OCTETOS DE ENDEREÇO IPV4



FONTE: Disponível em: <<http://informatica-da-cmc.blogspot.com.br/2013/01/redes-como-calcular-sub-redes-como.html>>. Acesso em: 10 jan. 2016.

Baseados na imagem, e sabendo que cada nova rede deve possuir ao menos 32 endereços IPs, sendo 30 para *hosts*, 1 para rede e 1 para *broadcast*, iremos identificar em qual das opções existentes na elipse amarela melhor se enquadra para nossa necessidade. Baseados nessa analogia, podemos alocar nossa rede de 32 IPs em três possibilidades: 128, 64 ou 32. Porém, pensando no conceito já abordado sobre realizar a melhor escolha economizando, ou melhor, não desperdiçando IPs, a melhor opção para nossa situação seria o 32. Logo, podemos afirmar que estas novas redes distam 32 endereços umas das outras.

Agora que já sabemos onde alocar nossa nova máscara de rede, iremos realizar o cálculo da mesma. Até então, nossa rede principal era composta por uma máscara de rede de 24 bits, ou seja, ocupando três dos quatro octetos possíveis. Como vamos subdividir esta rede, a nossa nova máscara passará a ocupar alguns bits do último octeto. Sendo assim, iremos somar os valores ocupados desse último octeto ao valor atual da máscara, e assim encontraremos nossa nova máscara de rede. Nossa máscara atual /24 é 255.255.255.0, porém, baseados na escolha do 32 efetuado acima, sabemos que em nosso último octeto utilizaremos três bits, ou seja, será marcado com bit 1 até o valor 32 da elipse amarela, desta maneira, $24 + 3 = 27$. Nossa nova máscara de rede é /27 ou 255.255.255.224 (lembrando que o 224 veio da soma de $128+64+32$).

Com a máscara de rede identificada e a quantidade de hosts em cada nova sub-rede, é possível agora identificar cada uma dessas sub-redes. Vale ressaltar que o valor 0 (zero) é contado como um endereço de rede. Dessa maneira, iremos montar nossa tabela com as redes partindo do endereço de rede e somando sempre 32 para identificar a próxima rede, também descontando 1 (um) do valor inicial da próxima rede para identificar o endereço de broadcast da rede anterior, como pode ser observado na tabela:

TABELA 3 - ENDEREÇOS DE REDE

ID	Endereço de sub-rede	Máscara	Endereços Válidos	Endereço de Broadcast
1	192.168.1.0	/27	192.168.1.1 - 192.168.1.30	192.168.1.31
2	192.168.1.32	/27	192.168.1.33 - 192.168.1.62	192.168.1.63
3	192.168.1.64	/27	192.168.1.65 - 192.168.1.94	192.168.1.95
4	192.168.1.96	/27	192.168.1.97 - 192.168.1.126	192.168.1.127
5	192.168.1.128	/27	192.168.1.129 - 192.168.1.158	192.168.1.159
6	192.168.1.160	/27	192.168.1.161 - 192.168.1.190	192.168.1.191
7	192.168.1.192	/27	192.168.1.193 - 192.168.1.222	192.168.1.223
8	192.168.1.224	/27	192.168.1.225 - 192.168.1.254	192.168.1.255

FONTE: O autor

Baseados nesta tabela que construímos, podemos perceber que, além de atender à necessidade inicial que eram seis novas sub-redes, foi possível criar mais duas novas sub-redes, alcançando um total de oito sub-redes baseadas em nossa rede principal.

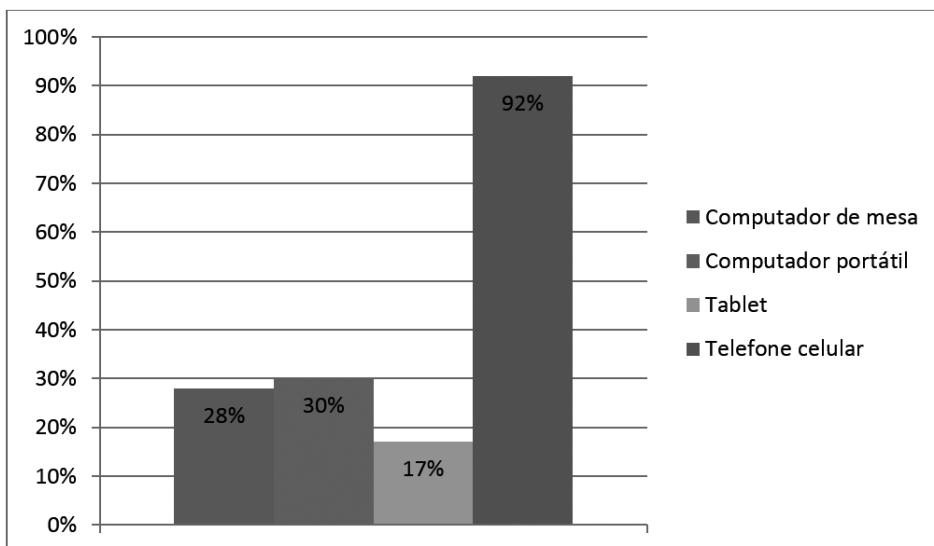


- Começar por preencher todas as linhas associadas ao endereço de sub-rede. Desta forma sabemos sempre que o endereço *broadcast* da linha anterior é esse **endereço-1**.
- Depois de saber o *broadcast* sabemos também que o último endereço válido é o endereço **broadcast -1**.
- O primeiro endereço de rede é sempre a soma de +1 ao endereço de sub-rede.

7.2 IPv6

Durante a década de 90 iniciou-se um esforço para desenvolver um novo protocolo de rede que viesse a substituir o IPv4. O principal motivo para esta evolução seria o fim de endereços do IPv4. Isso se deve ao fato do crescimento demasiado da utilização da Internet, como pode ser observado no Gráfico 1.

GRÁFICO 1 - DOMICÍLIOS QUE POSSUEM EQUIPAMENTOS NA INTERNET



FONTE: Disponível em: <<http://Registro.br>>. Acesso em: 1 mar. 2016.

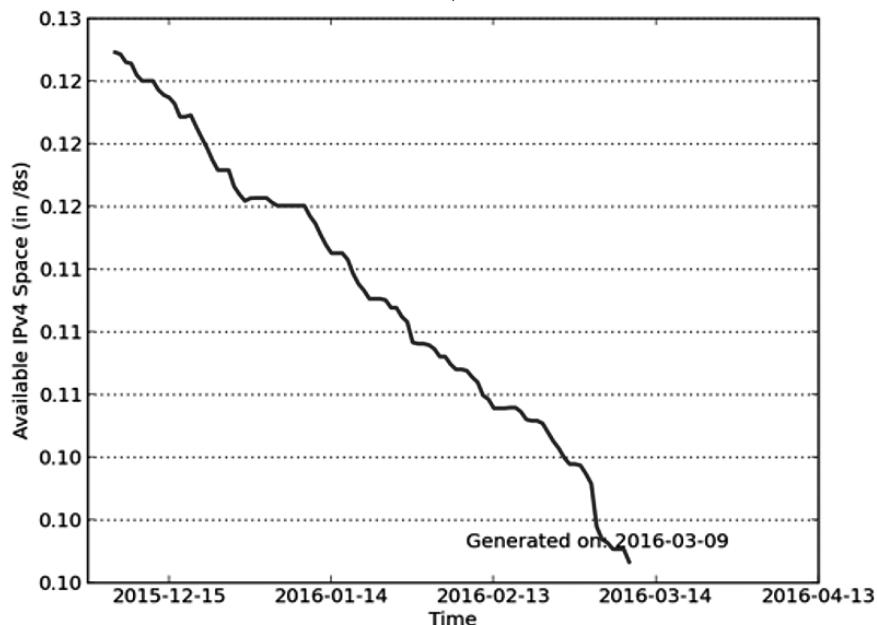
O gráfico demonstra em 2014 a utilização da Internet em dispositivos por residência no Brasil. É possível observar que ainda há muito o que crescer no sentido de infraestrutura e disponibilidade de serviços para os usuários.

Este crescimento foi o ponto-chave para o desenvolvimento dessa nova arquitetura de rede que visa sanar o problema de falta de endereços de rede. Caso nenhuma atitude fosse tomada, chegaria um determinado momento em que todos os endereços IP estariam ocupados e, assim, não seria possível a entrada de mais nenhum usuário na rede.

Este problema relacionado ao fim do IPv4 já vem atormentando os pesquisadores e desenvolvedores há muitos anos, tanto que várias estratégias foram desenvolvidas ao longo do tempo com a intenção de prolongar a vida do IPv4. Entre tais estratégias podemos destacar a utilização do NAT (mascaramento de conexão, que iremos estudar mais adiante), melhores políticas de distribuição de endereços, recuperação de blocos distribuídos a grandes empresas no início do surgimento da Internet, de maneira equivocada, como as principais ações adotadas.

Tais ações conseguiram prolongar a vida deste protocolo até os dias de hoje, porém, segundo o próprio Registro.br que é a entidade que administra os recursos de numeração no Brasil, esse prolongamento de vida tem data para o seu encerramento, sendo decretado pelos mais otimistas ao final de 2018. Tal esgotamento pode ser observado no Gráfico 2.

GRÁFICO 2 - QUANTIDADE DE ENDEREÇOS IPV4 DISPONÍVEIS



FONTE: Disponível em: <<http://Registro.br>>. Acesso em: 1 mar. 2016.

Para tanto, foi desenvolvido este novo protocolo de rede, denominado IPv6, como já citado anteriormente, e o mesmo já se encontra em funcionamento e em processo de substituição ao seu antecessor.

O protocolo IPv6 sofreu algumas alterações em relação ao protocolo IPv4, começando pela diferença básica no número de *bits* em sua composição, onde até então tínhamos 32 *bits* com a versão 4, com a versão 6 temos agora 128 *bits*, o que nos possibilita termos 340.282.366.920.938.463.463.74.607.431.768.211.456 de endereços IPs no total, ou seja, um número muito superior aos quatro bilhões de endereços do IPv4.

Além da grande quantidade de alocação de *hosts*, outra diferença entre os protocolos é o formato do seu datagrama, ou seja, no seu cabeçalho. O mesmo ficou muito mais enxuto, com a intenção de dar mais agilidade à transmissão dos dados e economizar processamentos dos ativos intermediários.

Esta nova abordagem no cabeçalho do IPv6 pode ser observada na Figura 60.

FIGURA 60 - CABEÇALHO IPV6

Versão (Version)	Classe de Tráfego (Traffic Class)	Identificador de Fluxo (Flow Label)				
Tamanho dos Dados (Payload Length)		Próximo Cabeçalho (Next Header)	Limite de Encaminhamento (Hop Limit)			
Endereço de Origem (Source Address)						
Endereço de Destino (Destination Address)						

FONTE: Kurose (2010, p. 248)

É fácil perceber as diferenças em relação ao cabeçalho do IPv4. Assim, vamos detalhar cada uma das funções existentes neste novo protocolo:

- Versão --> este campo é formado por quatro *bits* e identifica a versão do protocolo.
- Classe de tráfego --> este campo é formado por oito *bits* e tem funcionalidade similar ao campo "Tipo de Serviço do IPv4", ou seja, ele identifica os pacotes por classes de serviço ou prioridade.
- Identificador de fluxo --> campo formado por 20 *bits*, identifica pacotes do mesmo fluxo de comunicação. Idealmente esse campo é configurado pelo endereço de destino para separar os fluxos de cada uma das aplicações e assim os nós intermediários de rede podem utilizá-lo de forma agregada com os endereços de origem e destino para realização de tratamento específico dos pacotes.
- Tamanho dos dados --> campo formado por 16 *bits*, indica o tamanho, em *bytes*, apenas dos dados enviados junto ao cabeçalho. Ele vem para substituir o campo tamanho total do IPv4, que indicava o tamanho do cabeçalho mais o tamanho dos dados transmitidos. Contudo, o tamanho dos cabeçalhos de extensão também é somado nesse novo campo.

- Próximo cabeçalho --> este campo é formado por oito *bits*, e identifica o cabeçalho de extensão que segue o atual. Ele foi renomeado, este campo no protocolo IPv4 era denominado de protocolo, e assim deixou de carregar os valores de outros protocolos para indicar os tipos de cabeçalhos de extensão.
- Limite de encaminhamento --> esta parte do cabeçalho IPv6 é formada por oito *bits* e é decrementada a cada salto de roteamento, e indica o número máximo de roteadores pelos quais o pacote pode passar antes de descartado. Tem função similar ao campo de TTL do protocolo Ipv4.
- Endereço de Origem --> campo formado por 128 *bits* e indica o endereço de origem do pacote.
- Endereço de Destino --> campo também formado por 128 *bits* e indica o endereço de destino do pacote.

Como descrito, o IPv6 traz uma nova abordagem quando às informações adicionais a serem carregadas no seu cabeçalho. Essas informações são agrupadas em outro cabeçalho, denominado cabeçalho de extensão. Esta nova estrutura permite até seis cabeçalhos de extensão, sendo eles interligados e estruturados de maneira hierárquica.

Essa diminuição de campos no cabeçalho principal e a criação do cabeçalho de extensão no IPv6 tiveram como objetivo a diminuição de uso dos processadores dos roteadores e assim, consequentemente, o aumento de velocidade nas transferências de arquivos.

Isso vem a acontecer, pois quando um roteador recebe um determinado pacote que deve ser encaminhado para um *host* da rede, ele realiza a abertura do cabeçalho do pacote para identificar origem e destino e assim encaminhar o pacote da forma correta. Bem, no protocolo IPv4, o cabeçalho continha, além das informações de origem e destino, várias outras informações, tais como: tamanho, tipo de protocolo, entre outras. Porém, para o roteador, boa parte destas informações não é necessária, mas mesmo assim faziam parte do cabeçalho.

Sendo assim, os roteadores, antes de enviar tinham - e têm, pois este protocolo ainda está em produção - de processar todas estas informações mesmo que desnecessárias, ocupando assim muito do processador do mesmo e gerando congestionamento de rede. Pensando desta forma, o novo protocolo traz em seu cabeçalho principal somente informações pertinentes no que diz respeito ao encaminhamento dos dados.

Com este resumo de informações, o roteador não ocupa por tanto tempo o seu processador, pois está processando somente informações que realmente são importantes para o encaminhamento correto das informações, dando, desta maneira, mais agilidade e performance à rede em questão.

Outra importante alteração no protocolo IPv6 é em relação à fragmentação dos pacotes. Até então, um pacote, ao passar por um roteador, se necessário, era fragmentado de acordo com a capacidade do *link* onde seria inserido, desta maneira, o mesmo pacote poderia sofrer uma fragmentação ao sair do remetente,

outra ao passar por um roteador e mais outras vezes, se necessário, até chegar ao seu destino.



A fragmentação consiste em dividir uma determinada informação em pequenas partes para que a mesma possa vir a ser transmitida de um ponto da rede até outro. Esta fragmentação acontece na camada internet do modelo TCP/IP. Seu tamanho padrão em redes ethernet é de 1.500 bytes.

Este processo de fragmentação da informação também é um grande responsável pelo alto uso de processador dos roteadores e causador de congestionamento de rede.

Já no protocolo IPv6 isso não acontece, pois os roteadores não têm mais o dever de realizar a fragmentação correta do pacote. Com o protocolo IPv6 em produção, os roteadores têm somente a função de encaminhar o dado como o mesmo foi recebido, assim, a fragmentação fica sob responsabilidade do remetente da informação, então, se um pacote gerado e transmitido por um remetente, ao chegar em um roteador intermediário, não tiver condições de propagar esse pacote para o seu destinatário pois seu tamanho excede o tamanho do meio, o pacote em questão será devolvido ao remetente juntamente com o erro de tamanho excedido.

O remetente, ao receber a devolução do pacote juntamente com o erro de tamanho excedido, realizará a fragmentação do pacote novamente, agora com um tamanho menor que o anterior, e realizará o envio da informação novamente. Este processo pode ocorrer diversas vezes até que o tamanho do pacote esteja correto.

Esta nova política em relação à não fragmentação de pacotes por qualquer componente intermediário da rede faz com que todos os ativos não se ocupem com serviços que não são de sua responsabilidade.

7.2.1 Cálculo de rede com IPv6

A representação de um IPv6 divide o endereço em oito grupos de 16 bits, separando-os por ":" escritos com dígitos hexadecimais (0-F). Por exemplo:

2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1

"Na representação de um endereço IPv6 é permitido utilizar tanto caracteres maiúsculos quanto minúsculos. Além disso, as regras de abreviação podem ser aplicadas para facilitar a escrita de alguns endereços muito extensos"

(MOREIRAS, COREDEIRO, DOS SANTOS, HARANO, MORALES, GANZELLI, NAKAMURA, CARNIER, 2012, p. 42).

Dessa forma, é permitido omitir os zeros à esquerda de cada bloco de 16 *bits*, além de substituir uma sequência longa de zeros por "::", como pode ser observado no exemplo:

$2001:0DB8:0000:0000:130F:0000:0000:140B = 2001:DB8:0:0:130F::140B$ ou
 $2001:DB8::130F:0:0:140B$

Neste exemplo é possível perceber que a abreviação de um conjunto de zeros pode ser realizada uma única vez, porém não existe uma única forma para realizar tal operação, deixando a critério do usuário se o mesmo quer realizar a abreviação no início, meio ou no fim do endereço.

Outra representação importante é a dos prefixos de rede. Esta notação continua sendo escrita da mesma forma, composta pelo endereço IP/tamanho do prefixo.



Tamanho do prefixo é um valor decimal que especifica a quantidade de *bits* contíguos à esquerda do endereço que compreendem o prefixo.

FONTE: Disponível em: <<http://www.IPV6.br>>. Acesso em: 7 abr. 2016.

Dentro da estrutura de endereços do IPv6, existem três tipos de endereços definidos:

- *Unicast* --> este tipo de endereço identifica uma única interface, de modo que um pacote enviado a um endereço *unicast* é entregue a uma única interface;
- *Anycast* --> identifica um conjunto de interfaces. Um pacote encaminhado a um endereço *anycast* é entregue à interface pertencente a este conjunto mais próximo da origem. Este endereço é utilizado na comunicação de um para um de muitos;
- *Multicast* --> também identifica um conjunto de interfaces, porém, um pacote enviado a um endereço *multicast* é entregue a todas as interfaces associadas a esse endereço. Este formato é utilizado para comunicação de um para muitos.

O endereço IPv6 é constituído por uma estrutura hexadecimal, como já falamos anteriormente. Utilizaremos a tabela de conversão binário para hexadecimal para facilitar:

TABELA 4 - CONVERSÃO BINÁRIO PARA HEXADECIMAL

Quantidade de <i>bits</i>	Valor representativo
10	A
11	B
12	C
13	D
14	E
15	F

FONTE: O autor

Como já sabemos, um endereço IPv6 é composto de 128 *bits*, então, utilizaremos uma técnica denominada de EUI-64 para realizar a formação dos nossos endereços. Lembrando que o endereço IP é algo único, cada *host* deve possuir o seu endereço e o mesmo não pode se repetir dentro da rede.

Assim, baseado na grande quantidade de endereços IP disponíveis dentro do IPv6, adotaremos uma abordagem específica para garantir que nosso endereço IP não esteja sendo utilizado por nenhum outro *host*. Esta abordagem consiste em utilizar o endereço de MAC do *host* em questão como parte ativa do endereço IPv6. Mas como funciona isso?

É muito simples. Inicialmente precisamos identificar o endereço MAC do nosso *hardware*. Por exemplo:

5C:1D:E0:8C:E7:E7

Após a identificação do MAC, temos que identificar ou requerer um prefixo de rede, como, por exemplo:

2001:db8:ba1a:d0ce::64

Agora que temos a informações básicas, podemos dar continuidade à construção do nosso endereço de rede. Como podemos observar, nosso endereço de MAC é composto de 48 *bits*, dessa forma precisamos adicionar os dígitos hexadecimais FF-FE entre o terceiro e o quarto *byte* do endereço MAC (transformando no padrão EUI-64), como pode ser observado a seguir:

5C:1D:E0:FF:FE:8C:E7:E7

Caso o endereço de MAC a ser usado já fosse constituído por 64 *bits*, esta operação não seria necessária. Em seguida, iremos realizar a conversão para binário dos dois primeiros *bytes*. Observe:

TABELA 5 - CONVERSÃO BINÁRIA

	Conversão para binário			
Bytes	8	4	2	1
5	0	1	0	1
C	1	1	0	0

FONTE: O autor

Após realizar a conversão, temos o binário 01011100 para representar 5C. Em seguida, realizamos a substituição do sétimo *bit* mais à direita, o qual é chamado *bit U/L*. Essa substituição consiste em mudar o valor do *bit*, caso o mesmo seja 0, deve ser substituído por 1, caso seja 1 deve ser substituído por 0.

Complementa-se o *bit U/L*

$$\begin{aligned} 01011100 &\rightarrow 01011110 \\ 01011110 &\rightarrow 5E \end{aligned}$$

Após esta alteração dentro da estrutura do binário do endereço MAC, é possível montar o nosso endereço IP, que será:

2001:0DB8:BA1A:D0CE:5E1D:E0FF:FE8C:E7E7

Caso o endereço MAC já fosse constituído por 64 *bits*, não seria necessária a adição dos hexadecimais FF-FE, podendo ir diretamente para a alteração do *bit U/L*.

Como esta, existem outras técnicas de construção de endereços IPv6, porém esta baseada no formato EUI-64 tem sido a mais utilizada no momento.

O IPv6 é uma realidade e está cada vez mais presente dentro das redes de computadores. Nos próximos anos passaremos por grandes mudanças dentro das redes com a implantação deste novo protocolo de comunicação, o qual é inevitável para o bom andamento da internet e das redes. Sendo assim, serão grandes mudanças nas redes e no modo com que vemos e planejamos estes ambientes, exigindo maior dedicação e aprimoramento dos conhecimentos adquiridos.

O IPv6 é uma tecnologia já consolidada, porém várias estruturas e conceitos estão surgindo e se aperfeiçoando, muitos deles com a finalidade de realizar uma interligação entre IPv6 e IPv4, então é preciso se manter atualizado e buscar novas tendências tecnológicas para não ficar fora das novas redes de comunicação.

LEITURA COMPLEMENTAR

Vulnerabilidades do DNS

Vimos que o DNS é um componente fundamental da infraestrutura da Internet, com muitos serviços importantes - incluindo a *Web* e o *e-mail* - simplesmente incapazes de funcionar sem ele. Desta maneira, perguntamos: como o DNS pode ser atacado? O DNS é alvo esperando para ser atingido, pois causa dano à maioria das aplicações da internet junto com ele?

O primeiro tipo de ataque que vem à mente é o ataque inundação na largura de banda DDoS contra servidores DNS. Por exemplo, um atacante pode tentar enviar para cada servidor DNS raiz uma inundação de pacotes, fazendo com que a maioria das consultas DNS legítimas nunca seja respondida. Tal ataque DDoS em larga escala contra servidores DNS raiz aconteceu em 21 de outubro de 2002. Nesse ataque, os atacantes se aproveitavam de um *botnet* para enviar centenas de mensagens *ping* para cada um dos servidores DNS raiz. Felizmente, esse ataque em larga escala causou um dano mínimo, tendo um pequeno ou nenhum impacto sobre a experiência dos usuários com a Internet. Os atacantes obtiveram êxito ao direcionar centenas de pacotes aos servidores raiz. Mas muitos dos servidores DNS raiz foram protegidos por filtros de pacotes, configurados para sempre bloquear todas as mensagens *ping* ICMP encaminhadas aos servidores raiz. Desse modo, esses servidores protegidos foram poupanados e funcionaram normalmente. Além disso, a maioria dos servidores DNS locais oculta os endereços IP dos servidores de domínio de nível superior, permitindo que o processo de consulta ultrapasse frequentemente os servidores DNS raiz.

Um ataque DDoS potencialmente mais eficaz contra o DNS seria enviar uma inundação de consultas de DNS aos servidores de domínio de alto nível, por exemplo, para todos os servidores de domínio que lidam com o domínio .com. Seria mais difícil filtrar as consultas DNS direcionadas aos servidores DNS; e os servidores de domínio de alto nível não são ultrapassados tão facilmente quanto os servidores raiz. Mas a gravidade de tal ataque poderia ser parcialmente amenizada pelo *cache* dos servidores DNS locais.

O DNS poderia ser atacado potencialmente de outras maneiras. Em um ataque de homem no meio, o atacante intercepta consultas do hospedeiro e retorna respostas falsas. No ataque de envenenamento, o atacante envia respostas falsas a um servidor DNS, fazendo com que o servidor armazene os registros falsos em sua *cache*. Ambos os ataques podem ser utilizados, por exemplo, para redirecionar um usuário da *Web* inocente ao *site Web* do atacante. Esses ataques, entretanto, são difíceis de implementar, uma vez que requerem a interceptação de pacotes ou o estrangulamento de servidores.

Outro ataque DNS importante não é um ataque ao serviço DNS por si mesmo, mas, em vez disso, se aproveitar da infraestrutura do DNS para lançar um ataque DDoS contra um hospedeiro-alvo. Nesse ataque, o atacante envia consultas DNS para muitos servidores DNS autoritativos, com cada consulta tendo o endereço-fonte falsificado do hospedeiro-alvo. Os servidores DNS, então, enviam suas respostas diretamente para o hospedeiro-alvo. Se as consultas puderem ser realizadas de tal maneira que uma resposta seja muito maior do que uma consulta, então o atacante pode entupir o alvo sem ter que criar muito do seu próprio tráfego. Tais ataques de reflexão que exploram o DNS possuem um sucesso limitado até hoje.

Em resumo, não houve um ataque que tenha interrompido o serviço DNS com sucesso. Houve ataques refletores bem-sucedidos; entretanto, eles podem ser abordados por uma configuração apropriada de servidores DNS.

FONTE: KUROSE, J. F. **Redes de computadores e a internet**. 5. ed. São Paulo: Pearson, 2010.

RESUMO DO TÓPICO 2

Neste tópico você viu:

- A importância dos protocolos de rede para um ambiente computacional.
- Os modelos de referência OSI e TCP/IP, suas características e diferenças.
- A estrutura em camadas utilizada pelos modelos de referência e como acontece o tratamento da informação nestas camadas.
- Os principais protocolos utilizados em cada uma das camadas dos modelos de referência OSI e TCP/IP.
- Detalhamento do protocolo IPv4 e IPv6, suas características, funcionalidades e aplicabilidade.



- 1 Dentro da camada de aplicação existem diversos protocolos de rede, que são utilizados para a sincronização das aplicações. Cite três exemplos de protocolos de rede desta camada e explique para que servem.
- 2 Para realizar a comunicação entre diferentes arquiteturas de rede foram desenvolvidas regras para negociação de dados, estas regras foram denominadas de:
 - a) () Serviços
 - b) () Protocolos
 - c) () Arquitetura de rede
 - d) () TCP/IP
 - e) () Ethernet
- 3 Determine qual a máscara de rede para os seguintes IPs:
 - a) 192.168.50.50/24
 - b) 192.168.70.2/30
 - c) 10.0.0.4/8
 - d) 192.168.71.4/29
- 4 Dados os endereços a seguir, diga qual a máscara de rede, endereço de rede, número de hosts e endereço de broadcast para cada respectivo endereço.
 - a) 14.32.56.0/13
 - b) 192.168.1.56/24
 - c) 192.168.40.224/30
 - d) 177.16.1.90/16
 - e) 10.0.0.4/8
- 5 Comprima ao máximo possível os endereços de rede IPv6:
 - a) 2001:0db8:1200:0fe0:0000:0000:0003
 - b) 2001:0db8::ca5a:0000:2000
 - c) 2001:0db8:face:b00c:0000:0000:0100:00ab



Assista ao vídeo de
resolução da questão 4



1 INTRODUÇÃO

Todas as redes de computadores são formadas por um conjunto de ativos (equipamentos). Tais ativos devem ser alocados adequadamente baseados no seu funcionamento e topologia lógica utilizada na rede.

Na construção de uma rede se faz uso de diferentes equipamentos, alocados e configurados diferentemente uns dos outros, pois cada equipamento terá uma função específica dentro do ambiente onde está localizado.

Cada equipamento tem sua importância dentro da rede, o qual pode fazer com que a rede venha a ganhar performance e confiabilidade quando instalado de maneira adequada, como também pode gerar lentidão e indisponibilidade da rede quando alocado de maneira equivocada.

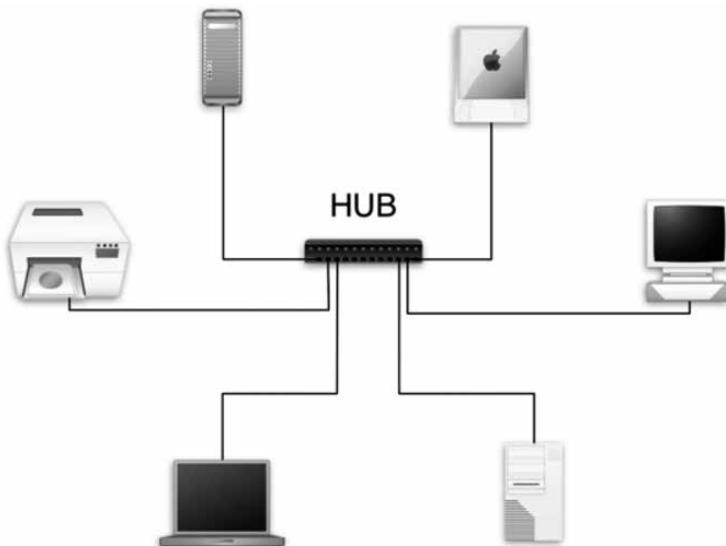
2 EQUIPAMENTOS DE REDE

Ao estruturarmos uma rede de computadores, vários ativos são utilizados para montar a estrutura lógica da mesma. Sendo assim, vamos estudar detalhadamente as principais funções e como aplicar os principais ativos dentro de uma rede.

2.1 *HUB*

O *HUB* é um equipamento muito comum e amplamente utilizado nas redes devido à sua fácil implantação e não necessidade de configuração. Sua principal funcionalidade é receber determinada informação em uma das suas portas e replicar as mesmas a todas as demais portas existentes a fim de entregar a informação a todos os *hosts* conectados, para dessa forma alcançar o destinatário do dado, como pode ser observado na imagem:

FIGURA 61 - UTILIZAÇÃO DO HUB



FONTE: Disponível em: <<https://maxipedro.wordpress.com/2010/06/17/equipamentos-de-interligacao-de-redes/>>. Acesso em: 7 abr. 2016.

As principais características do *HUB* estão diretamente ligadas à estrutura física, a qual determina boa parte do seu funcionamento e limitações. Podemos destacar:

- O *HUB* atua somente na camada física da rede, ou seja, ele não realiza nenhum tipo de tratamento nas informações que estão circulando por ele. O mesmo somente faz o encaminhamento do dado bruto recebido a todas às suas portas.
- Sua principal aplicabilidade refere-se à concentração de sinal, onde realizará o agrupamento e interligação dos dados.
- Serve como um amplificador de sinal para conexões de longa distância.
- Pode ser cascaneado, ou seja, existe a possibilidade de realizar a ligação de dois ou mais *hubs* interligados com a intenção de aumentar as portas de rede existentes no ambiente, sem que haja necessidade de qualquer tipo de configuração.
- Como atua somente na camada física, não possui nenhum tipo de controle de congestionamento ou de erros.
- Possui uma estrutura de barramento no seu interior, dessa forma, não realiza mais de uma transmissão de dados ao mesmo tempo. Assim, quando um *host* que está ligado ao *HUB* está realizando uma transmissão de dados, todos os outros dispositivos não podem realizar; caso dois *hosts* venham a transmitir dados ao mesmo tempo, os pacotes irão colidir, fazendo com que nenhum dos dois *hosts* envolvidos no processo tenha êxito em sua transmissão de informação.
- Os *hubs*, em sua grande maioria, utilizam o cabo UTP (par trançado) como meio físico para realizar suas transmissões de dados.

Desta maneira, podemos elencar o hub como um dos primeiros ativos utilizados nas redes de computadores. Isso se deve ao seu baixo custo de aquisição

e implantação, sendo desnecessário qualquer tipo de conhecimento técnico para sua instalação.

2.2 SWITCH

Podemos dizer que um *switch* atua como um concentrador de rede da mesma forma que o *hub*, o qual estudamos há pouco. Porém, seu funcionamento lógico difere do *hub*.

Até então, sabíamos que o *hub* tem seu funcionamento atuando como um barramento, já o *switch* utiliza uma estrutura mais parecida com um ponto a ponto. Isso acontece pois o mesmo não realiza a replicação de dados de forma direta para todas as interfaces de rede e, sim, realiza o chaveamento das interfaces. Com este chaveamento, cada porta receberá somente os dados que têm como destino o *host* que está ligado a ela.

Este chaveamento das interfaces acontece através da montagem de uma tabela interna do *switch* com todos os MACs *Address* dos dispositivos conectados a ele. Assim, ao receber um determinado pacote, o mesmo tem seu cabeçalho processado, onde constam os endereços de origem e destino dessa informação. Baseado nesses endereços, o *switch* realiza o encaminhamento da informação para a interface correta, a qual entrega o dado ao seu destinatário.



MAC Address ou endereço de MAC (Media Access Control) é o endereço físico associado à interface de rede existente dentro de cada dispositivo. Este endereço é único, não existindo, assim, dois adaptadores de rede com o mesmo número.

Graças a esta estrutura é possível atingir um maior desempenho de rede, diminuindo assim o *broadcast* entre as interfaces e, consequentemente, diminuindo a ocupação do meio físico para transmissões de dados desnecessários.

Desta maneira, o *switch* é um *hardware* que atua na camada 2 (enlace) do modelo OSI, já realizando um tratamento das informações e não mais só replicação de dados. Podemos destacar como principais funcionalidades de um *switch*:

- São equipamentos que podem utilizar diferentes meios físicos para a transmissão de dados, entre eles: cabos UTP e fibras ópticas.
- Não restringe as transmissões de dados, ou seja, pode realizar mais de uma transmissão de informação ao mesmo tempo, não limitando assim a um *host* por vez.

- Possibilitam a otimização de tráfego entre os segmentos de rede.

Atualmente no mercado existem dois modelos de *switch*, os denominados como gerenciáveis (Layer3) e os não gerenciáveis (Layer2). *Switches* não gerenciáveis ou L2, têm sua funcionalidade muito parecida com o *hub*, pois realizam somente a propagação da informação, lembrando que esta propagação obedece a algumas regras de funcionamento, como já descrito anteriormente, onde aceita-se mais de uma conexão de transmissão simultânea e existe uma tabela de MACs para alocar o dado na interface correta, evitando alguns problemas de rede. Este modelo apresenta um custo mais baixo, podendo assim ser aplicado com certa facilidade no lugar dos *hubs*.

Outro ponto importante a ser mencionado sobre os *switches* L2 é a não necessidade de configuração. Neste mesmo caso, não é necessário conhecimento técnico para realizar a instalação, pois basta ligar o equipamento em uma fonte de energia e conectar todos os cabos da rede a ele, mesma situação que acontece com os *hubs*.

Já o *switch* L3 ou gerenciável é um equipamento mais completo e robusto, desta forma seu custo é mais elevado, porém seu desempenho e performance oferecido à rede também é muito superior. Para manipular este tipo de *switch* é requerido um maior conhecimento técnico, pois o mesmo necessita ser configurado e ajustado para a rede em questão.

Neste tipo de equipamento é possível realizar diferentes tipos de configurações, adaptando-se às diferentes necessidades do ambiente. São equipamentos com uma capacidade de processamento elevado, o que permite a manipulação de múltiplos pacotes e grandes volumes de dados.

Estes *switches* categorizados como L3 podem ser acessados pelos usuários via *prompt* de comando ou *browser* (interface gráfica), tal escolha fica a critério do administrador de rede. Em ambas interfaces de configuração e gerenciamento é possível analisar o *status* de cada interface de rede (conectada, desconectada, velocidade de transmissão, tipo de negociação entre outras possibilidades), uso de memória e processador, versão do sistema operacional existente no equipamento, entre outras informações básicas sobre o seu funcionamento.

Consideramos estes equipamentos gerenciáveis, pois é possível realizar a manipulação das informações e a criação de determinadas regras de acesso. Podemos utilizar como exemplo de manipulação a utilização de VLAN's.

As VLAN's são redes virtuais criadas para priorizar algum determinado tráfego de rede, isolar algumas interfaces das demais ou para criação de túneis virtuais dentro de uma rede local. Assim, é possível realizar agrupamento de interfaces dentro de um *switch*, tal que as interfaces que não venham a fazer parte desse agrupamento não tenham acesso às informações que estão circulando dentro das interfaces que estão agrupadas (dentro da VLAN), isso, mesmo que todas as interfaces façam parte do mesmo equipamento físico.

Com esta estrutura de redes virtuais também é possível a criação de regras/políticas de priorização de tráfego, onde as informações que recebem o *tag*, ou marcação da VLAN, ao chegarem no *switch* terão prioridade sobre as demais.

Esta estrutura de redes virtuais (VLAN) pode ser implementada dentro do *switch* utilizando a estrutura de portas do próprio equipamento, onde tal rede pode estar vinculada a uma única porta ou a um grupo de portas. Pode ser vinculada a determinado endereço MAC, protocolo de comunicação ou ainda a uma TAG que está diretamente relacionada a um determinado fluxo de dados.

Outra funcionalidade muito importante utilizada dentro do *switch* L3 é o gerenciamento de sub-redes, ou seja, é possível utilizar um equipamento desse porte para realizar o isolamento entre duas redes distintas e através dele realizar a negociação de pacotes para que ambas as redes possam vir a trocar informação sem que haja um contato direto entre elas ou um NAT entre as interfaces. Nesta situação, ambas as redes podem trocar informações diretamente buscando um *host name* ou o próprio endereço IP do *host* para acessar seus dados.

Esta utilização de gerenciamento de sub-redes com um *switch* permite uma economia de equipamento e infraestrutura, pois acaba por minimizar o *broadcast* existente dentro das redes, já que não permite que a sujeira gerada por uma determinada rede acabe por utilizar outra rede para se propagar, e assim, causar lentidão e congestionamento de dados dentro da estrutura.

Podemos concluir que um *switch* tem grande importância dentro de uma rede. Sendo gerenciável ou não, agrega muito ao ambiente computacional em questão, pois aumenta a segurança, disponibilidade e agilidade do meio.

2.3 ROTEADOR

A Internet é um aglomerado de redes de computadores todas interligadas. Os roteadores são os responsáveis por realizar toda a organização desta grande rede. Sem eles a Internet não poderia existir, ou melhor, nenhum tipo de negociação de dados entre redes distintas seria viável.

A função do roteador é realizar a interligação das redes e realizar o encaminhamento das informações para suas redes de destino corretas. Porém, como isso funciona na prática? De certa forma, o funcionamento de um roteador é muito simples e similar a um *switch* L3, porém com um poder computacional muitas vezes maior, para poder gerir uma quantidade de informação muitas vezes maior do que as do *switch*.

Na prática, um roteador possui várias interfaces de rede, tal quantidade irá variar de acordo com a aplicabilidade do equipamento. Cada interface de rede estará interligada a uma rede distinta e possuiará uma configuração de rede

(IP e Máscara). Estas configurações de rede serão responsáveis por realizar a comunicação do roteador com a rede em que o mesmo está conectado.

Porém, além da configuração de rede para encaminhar as informações, os roteadores precisam de *gateways*, ou seja, caso uma determinada informação chegue até ele, buscando algum endereço IP que não pertença a nenhum *range* de rede à qual uma de suas interfaces esteja alocada, o mesmo precisa encaminhar esta informação para outro equipamento, para que assim a mesma possa vir a ser entregue.

Para realizar este encaminhamento de dados foram desenvolvidos protocolos de roteamento: uma estrutura lógica que pode ser estática ou dinâmica e que repassa as informações para os roteadores da rede de como devem proceder quando não possuem um IP local para entregar o dado. Essa estrutura de rotas nada mais é do que *gateways*, os mesmos *gateways* utilizados por *desktops*, celulares, *notebooks* e outros dispositivos conectados à rede.



Os *gateways* padrão desempenham um papel importante na rede TCP/IP. Eles fornecem uma rota padrão para os *hosts* TCP/IP usarem durante a comunicação com outros *hosts* em redes remotas.

A única diferença de um *gateway* padrão de um micro para as rotas existentes nos roteadores é a quantidade de *gateways*, em outras palavras, destinos. Em um computador temos normalmente uma rota única, descrevendo que toda a informação gerada por ele, e que tenha como destino um IP fora do *range* local de rede, deve ser enviada para um determinado IP da rede local que será responsável por dar continuidade no tratamento da informação.

Quando tratamos de roteadores, podemos ter uma rota única e similar às rotas dos computadores, como já mencionamos. Esta estrutura é muito utilizada em *modems* ADLS e roteadores *Wireless*. Nestes casos, ambos os equipamentos irão direcionar o tráfego para um único local.

Ao contrário destes equipamentos, os roteadores possuem várias rotas para vários destinos diferentes. Da mesma forma que configuramos as interfaces de rede dos computadores em modo automático (DHCP) ou estático, podemos configurar a estrutura de rotas dos roteadores, porém, nesse caso, usamos nomenclaturas diferentes: descrevemos como rotas estáticas e rotas dinâmicas ou autônomas.

Ao utilizar a estrutura de rotas estáticas, é responsabilidade do administrador de rede realizar a configuração das rotas, lembrando que não estamos falando da configuração de rede das interfaces (IP e MÁSCARA), e sim da forma como

as informações serão encaminhadas. Assim, o administrador terá que conhecer todos os destinos possíveis da sua rede, para que desta forma possa cadastrar em seu equipamento todas as rotas para alcançar os seus destinos. Simplificando, podemos dizer que o administrador de rede deve ensinar a seu equipamento os caminhos para chegar aos destinos que seus usuários querem alcançar.

Muitas vezes estes destinos estão alocados fisicamente e logicamente distantes da origem, o que faz com que esta informação venha a passar por vários roteadores até alcançar o seu destino final. Assim, cada roteador deve conhecer o melhor caminho para levar a informação até seu ponto final e devolvê-la à origem. Caso uma dessas rotas ou caminhos esteja configurada de maneira errada, apontando um caminho diferente tanto para alcançar o destino quanto para devolver a informação ao remetente, o pacote com os dados será perdido, pois um dos sentidos da informação é inválido.

Podemos observar na imagem que segue um exemplo de uma rota padrão criada de forma estática.

FIGURA 62 - ROTA ESTÁTICA

Rotas ativas:				
Endereço de rede		Máscara	Ender. gateway	Interface
0.0.0.0		0.0.0.0	192.168.64.254	192.168.64.111

FONTE: O autor

Esta estrutura com rotas estáticas pode ser uma estratégia muito interessante quando estamos tratando de pequenas redes, onde as rotas a serem gerenciadas são poucas e não existe nenhum tipo de estrutura em anel ou *backup*. Quando a rede possui um anel ou alguma forma de *backup*, não se recomenda a utilização da estrutura estática, pois ao haver qualquer problema, surgindo a necessidade de utilização do anel ou do *link* de *backup*, será necessário alterar a configuração dos roteadores envolvidos, mostrando aos mesmos como alcançar novamente a rede que perdeu comunicação com o seu *link* principal.

Ao tratarmos de uma rede maior, mais complexa, a melhor alternativa para gerenciar o encaminhamento das informações são os protocolos de roteamento. Dessa maneira, construiremos uma rede dinâmica (autônoma), a qual irá aprender os melhores caminhos existentes para os destinos sem que haja necessidade de qualquer alteração de configuração pelo administrador de redes.

Esta estrutura de rede trabalha de modo que todos os equipamentos envolvidos realizem anúncios, ou seja, comuniquem para os roteadores parceiros (equipamentos que estão ligados de forma direta um no outro) quais as redes existentes em sua tabela interna. Desse modo, seus parceiros acabam por conhecer estas redes e aprendem que quando chegar qualquer informação até eles buscando estas redes, o mesmo deve encaminhar estes pacotes para este determinado roteador.

Da mesma forma que um roteador anuncia as redes que ele gerencia ou possui, ele repassa para seus parceiros todas as rotas e caminhos que ele venha a conhecer, fazendo com que todos os equipamentos conectados na rede conheçam todos os caminhos para todos os destinos, criando assim uma grande rede de comunicação.

Esta estrutura dinâmica trabalha juntamente com um monitor de comunicação. Este monitor tem por responsabilidade checar de tempo em tempo a disponibilidade de comunicação do *link* utilizado. Ao contrário da estrutura de rotas estáticas, esta topologia é amplamente utilizada em rede em anel e com uma interface de *backup*, pois com este monitor de comunicação, quando o mesmo detecta que um dos *links* está fora do ar, o que deixaria parte da rede fora, o mesmo passa a realizar seus anúncios de redes e rotas através do *link* secundário.

Neste momento, os demais equipamentos ligados na rede passam a receber informações de alterações de rota, reprendendo o caminho para alcançar as redes que foram comprometidas com a interrupção deste *link* primário. Tudo isso sem que o administrador de rede tenha tido qualquer interferência no meio.

No momento em que o *link* primário é restabelecido, o monitor de comunicação percebe o *status* de conexão deste *link* e repassa uma nova informação para todos os seus parceiros recalcularem as rotas para que possam vir novamente a utilizar este *link* primário.

Segue uma lista de rotas criadas por um protocolo de rede dinâmica:

FIGURA 63 - ROTAS DINÂMICAS

Destino	Máscara de rede	Gateway	Interface	Métrica	Protocolo
10.57.76.0	255.255.255.0	10.57.76.1	Local Area C...	1	Local
10.57.76.1	255.255.255.255	127.0.0.1	Loopback	1	Local
10.255.255.255	255.255.255.255	10.57.76.1	Local Area C...	1	Local
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.45.0	255.255.255.0	192.168.45.1	Local Area C...	1	Local
192.168.45.1	255.255.255.255	127.0.0.1	Loopback	1	Local
224.0.0.0	224.0.0.0	192.168.45.1	Local Area C...	1	Local
224.0.0.0	224.0.0.0	10.57.76.1	Local Area C...	1	Local
255.255.255.255	255.255.255.255	192.168.45.1	Local Area C...	1	Local
255.255.255.255	255.255.255.255	10.57.76.1	Local Area C...	1	Local

FONTE: O autor

Dentre os protocolos de roteamento dinâmicos podemos citar o BGP, o OSPF e RIP, os quais estudaremos mais adiante.

Podemos descrever que os roteadores são ferramentas insubstituíveis para as redes de computadores e de forma geral para a Internet. Em redes de pequeno porte, onde um único *range* de rede contempla todo o ambiente, o roteador fica restrito à realização do NAT (mascaramento dos endereços locais). Já em redes

maiores, ou até mesmo quando tratamos da Internet, eles são o coração de toda essa estrutura. Sem eles, como já mencionamos, não seria possível realizar qualquer tipo de conexão entre redes distintas.

LEITURA COMPLEMENTAR

Virtualização

Falar em virtualização: é inevitável que a maioria das pessoas a associem à ideia de vários sistemas operacionais rodando na mesma máquina. Esse é, na verdade, um dos diversos tipos de virtualização: a de *hardware*. Se por um lado ela não é a única, por outro é, certamente, a mais perceptível.

O presente artigo contempla os aspectos triviais da virtualização, com noções conceituais, aplicações práticas e sua forma de interação com o usuário final.

A VIRTUALIZAÇÃO EM SI

Para entender perfeitamente o conceito da tecnologia, deve-se traçar um paralelo entre o que é real e o que é virtual. Seguindo essa linha de raciocínio, algo real teria características físicas, concretas; já o virtual está associado àquilo que é simulado, abstrato. Dessa forma, a virtualização pode ser definida como a criação de um ambiente virtual que simula um ambiente real, propiciando a utilização de diversos sistemas e aplicativos sem a necessidade de acesso físico à máquina na qual estão hospedados.

Isso acaba reduzindo a relação de dependência que os recursos de computação exercem entre si, pois possibilita, por exemplo, a dissociação entre um aplicativo e o sistema operacional que ele utiliza (já imaginou acessar o Microsoft Word através do Linux?).

E qual é a vantagem?

Prioritariamente, econômica. Com a iminente crise ambiental global (principal fomentadora da TI verde) e a crescente necessidade de diminuir o desperdício de recursos (incluída aí a energia elétrica), não há nada mais natural que o surgimento de alternativas para otimizar o uso de tais recursos.

Agora pense em um computador no qual opere um servidor de *e-mails*: mesmo que o disco rígido seja plenamente utilizado, não se pode dizer o mesmo sobre sua capacidade de processamento: enquanto ela pode chegar ao ápice em horários de pico (como às 15h), também pode se aproximar da ociosidade durante a madrugada. E se essa “sobra” fosse usada para gerar relatórios, aproveitando melhor o tempo e processamento livres? Na teoria, surtiria a tão desejada economia de recursos; na prática, isso é obtido através da virtualização.

OS TIPOS DE VIRTUALIZAÇÃO

Virtualização de *Hardware*

Como mencionado no começo da matéria, a virtualização de *hardware* consiste em rodar vários sistemas operacionais na mesma máquina. Isso é possível com o uso de programas específicos, que geram máquinas virtuais (*Virtual Machines*, ou VMs): estas emulam os componentes físicos de um PC, possibilitando que um sistema operacional diferente seja instalado em cada uma delas.

Há duas grandes vantagens na adoção dessa tecnologia: uma voltada a usuários, outra a servidores. No caso dos primeiros, o trunfo consiste em eliminar a incompatibilidade entre aplicativos e sistemas operacionais; pense em um usuário cujo PC tenha o Windows Vista instalado, mas que deseje rodar um aplicativo que só é compatível com o Windows XP. Isso é possível com a criação, nesse PC, de uma VM que rode o WinXP: depois disso, basta instalar o aplicativo nessa VM e executá-lo normalmente (como se fosse um computador dentro de outro).

Quanto aos servidores, sua virtualização permite que, ao invés de se ter diversos subservidores (que utilizam apenas uma porcentagem dos recursos das máquinas em que estão hospedados), os processos sejam distribuídos de forma equânime entre um número menor de computadores (que, com isso, chegam mais próximos do aproveitamento total de sua capacidade). Isso reduz a quantidade de mão de obra técnica, o espaço para alocar as máquinas e o gasto com eletricidade necessários; tudo isso incorre em economia.

Virtualização da Apresentação

A maioria dos programas disponíveis no mercado funciona no mesmo local em que se encontra a instalação. Isso pode parecer óbvio para usuários tradicionais, mas tal barreira foi quebrada com o uso da Virtualização da Apresentação: trata-se do acesso a um ambiente computacional sem a necessidade de estar em contato físico com ele. Isso propicia, entre outras coisas, a utilização de um sistema operacional completo (bem como de seus aplicativos) de qualquer local do planeta, como se estivessem instalados no seu PC. O conceito é bem parecido com o de acesso remoto, com a diferença de que vários usuários podem se beneficiar do mesmo sistema simultaneamente (sem interferir uns aos outros).

Virtualização de Aplicativos

Cada aplicativo depende do sistema operacional para uma variedade de serviços, como alocação de memória ou gerenciamento de *drivers*. Resolver incompatibilidades entre determinado programa e o sistema operacional instalado na máquina é fácil, podendo ser feito uso de qualquer um dos dois tipos de virtualização já citados (*hardware* e apresentação). Mas e quando o conflito é entre dois aplicativos distintos? Pode ser que cada um deles requeira, por exemplo, uma versão diferente de uma mesma DLL.

Isso é resolvido através da virtualização de aplicativos. A técnica consiste em ter uma única cópia de determinado aplicativo, instalada em um servidor virtual; usuários que desejarem ter acesso a tal aplicativo podem fazê-lo diretamente, sem a necessidade de que ele também esteja instalado na máquina física. A partir daí o programa pode ser executado normalmente, já que as características específicas de cada aplicativo (seus *drivers*, entradas no registro, DLLs e afins) são compiladas e baixadas diretamente para o PC do usuário, através da geração de um aplicativo virtual que fica à parte.

A VIRTUALIZAÇÃO NO FUTURO

A virtualização está chegando com o vento em popa – suas vantagens econômicas são atrativas demais para serem resistidas. A adoção de tecnologias como a computação em nuvens só corrobora para seu inevitável progresso. Será que daqui a alguns anos poderemos acessar nossos PCs de qualquer lugar do planeta? Só o tempo dirá.

FONTE: Disponível em: <<http://www.tecmundo.com.br/web/1624-o-que-e-virtualizacao-.htm->>. Acesso em: 15 mar. 2016.

RESUMO DO TÓPICO 3

Neste tópico você viu:

- A importância dos equipamentos de rede e o dimensionamento correto dos mesmos, de formar a suprir a necessidade do ambiente.
- Os principais comutadores utilizados nas redes de computadores, suas diferenças e características.
- Os diversos tipos de *switches* e suas aplicações.
- A aplicabilidade dos roteadores dentro das redes e suas diferenças para os demais comutadores de rede.

AUTOATIVIDADE



1 Quando uma rede de uma grande empresa possui várias sub-redes independentes (por exemplo, para vários departamentos), essas sub-redes podem ser associadas a diferentes VLAN's e interconectadas utilizando um comutador (*switch*) de nível 3.

PORQUE

Os comutadores de nível 3 realizam o encaminhamento IP, o que permite a interconexão de estações de duas VLAN's distintas.

Assinale a alternativa CORRETA:

- a) () As duas afirmações são verdadeiras, e a segunda justifica a primeira.
- b) () As duas afirmações são verdadeiras, e a segunda não justifica a primeira.
- c) () A primeira afirmação é verdadeira, e a segunda é falsa.
- d) () A primeira afirmação é falsa e a segunda é verdadeira.
- e) () As duas afirmações são falsas.

2 Um *HUB* tem seu funcionamento comparado a qual topologia de rede?

- a) () Anel
- b) () Hibrida
- c) () Barramento
- d) () Garfo
- e) () Compartilhada

3 Relacione os equipamentos com suas funções.

- (1) *Switch* () Replica as informações para todos os *hosts* conectados.
- (2) Roteador () Realiza o encaminhamento do pacote, escolhendo o melhor caminho de rede.
- (3) *Hub* () Realiza a replicação dos dados somente para o segmento ou interface de rede adequado.



Assista ao vídeo de
resolução da questão 3



UNIDADE 3

REDES LANS, WANS, REDES SEM FIO E SEU GERENCIAMENTO

OBJETIVOS DE APRENDIZAGEM

Esta unidade tem por objetivos:

- conceituar e definir a estrutura de uma rede LAN;
- conhecer no que consiste uma rede WAN;
- explorar o funcionamento e parâmetros de segurança de uma rede Wireless;
- demonstrar estratégias de gerenciamento de redes.

PLANO DE ESTUDOS

Esta unidade está dividida em quatro tópicos. No final de cada um deles você encontrará atividades visando à compreensão dos conteúdos apresentados.

TÓPICO 1 – CONCEITO DE REDES LAN

TÓPICO 2 – CONCEITO DE REDES WAN

TÓPICO 3 – CONCEITOS DE REDES WIRELESS

TÓPICO 4 – NOÇÕES DE GERENCIAMENTO DE REDES



Assista ao vídeo
desta unidade.



CONCEITO DE REDES LAN

1 INTRODUÇÃO

As redes de computadores são classificadas de acordo com a sua localização. Uma rede LAN consiste em uma rede local, onde o gestor da rede possui autonomia total sobre todos os ativos de redes existentes dentro desse ambiente.

Dessa maneira, o administrador da rede pode realizar qualquer tipo de alteração dentro do ambiente no sentido lógico e físico sem depender de ninguém.

2 REDES LAN

As redes locais, popularmente conhecidas como LAN's, são redes privadas e com uma abrangência reduzida, contemplando residências, empresas, universidades entre outros. São pequenas redes, com a capacidade de alocação de *hosts* reduzida e limitada.

Estas redes são normalmente utilizadas para conectar dispositivos locais, tais como computadores, dispositivos portáteis, estações de trabalho, entre outros dispositivos que venham a possuir uma interface de rede.

As principais características de uma rede LAN, que a diferencia de outras topologias de rede, são o seu tamanho, topologia e suas tecnologias de transmissão.

As LANs têm um tamanho bem restrito e, dessa forma, muitas vezes é possível identificar problemas no ambiente com antecedência, prevenindo assim futuros incômodos com indisponibilidade da rede.

No sentido de sua tecnologia, as LANs muitas vezes apresentam uma agregação de tecnologias. No seu surgimento e até pouco tempo atrás, sua constituição era quase que 100% formada de par metálico, o conhecido cabo UTP (cabo de rede). Com esta estrutura, as LANs possuem uma velocidade de transmissão de 10 a 100 Mbps. Atualmente, dificilmente encontra-se uma rede local com velocidade inferior a 100 Mbps, porém, são facilmente encontradas redes com uma velocidade superior aos 100 Mbps, algo na casa do Gbps.

Nem só de cabo UTP se constitui uma LAN; hoje, com a forte tendência de mobilidade, muitas redes locais, além do cabeamento de rede, apresentam ou disponibilizam conexões do tipo *WI-FI* para seus colaboradores e até visitantes. Esta nova tecnologia tem sido aplicada com grande eficiência dentro das organizações e residências.

Vale salientar que, ao aplicar uma estrutura sem fio dentro de uma LAN, alguns cuidados com segurança devem ser tomados. Assim, é preciso uma atenção especial a esses ativos e a esta LAN, pois com uma rede sem fio não é possível determinar de forma eficiente o alcance que nossa rede terá. Desta forma, muitas vezes estamos colocando em risco toda a estrutura de rede das organizações, pois estamos realizando um prolongamento da rede da organização para fora dos seus domínios.

Com este prolongamento, a rede pode ficar suscetível a ataques externos, o que não acontecia com a rede cabeada, a qual ficava somente sob os domínios da organização. Não estamos dizendo que uma rede cabeada não possa vir a sofrer algum tipo de ataque externo, porém é muito mais difícil acontecer um ataque externo à rede interna.

Outros meios de transmissão, como fibras ópticas, também têm se popularizado dentro das redes locais. O meio de transmissão escolhido irá sempre variar de acordo com o valor a ser investido no ambiente e o volume de tráfego. Somente assim é possível realizar um dimensionamento correto da estrutura a ser utilizada no ambiente no sentido de eficiência máxima em troca de dados.

Como descrito anteriormente, para realizar a construção de uma rede é necessário conhecer a criticidade do ambiente, ou seja, conhecer os pontos fundamentais para a organização, os quais não podem sofrer com a indisponibilidade da rede e o volume de dados que cada equipamento irá gerar. Conhecendo o ambiente detalhadamente é possível realizar um projeto de rede que atenda às necessidades da organização.

Este projeto de rede deve contemplar os meios de transmissão, como já mencionado, porém deve definir também a melhor topologia lógica para a organização.

Nesse sentido, podemos optar por uma topologia em anel, caso a organização possua algum ponto interno muito crítico e não possa ficar sem comunicação. Nesta situação uma rede em anel garantirá uma redundância de forma autônoma para o ambiente, onde, caso haja uma falha no *link* principal, o *link* secundário assumirá a transmissão dos dados sem que os usuários percebam.

Em outro ponto da organização, onde o ambiente não é considerado tão crítico e com isso pode vir a ter um SLA maior, pode-se estruturar uma rede em formato estrela, onde haverá um concentrador central e todos os ativos desse ambiente estarão ligados diretamente a ele. Nesta situação, caso haja uma falha nesse concentrador, todos os ativos ligados a ele ficarão sem conectividade.

Analisando a estrutura da organização baseada em seus setores, por exemplo, é possível realizar uma topologia em árvore, ou seja, com uma hierarquia de concentradores. Isso significa um concentrador ligado após o outro e com os ativos ligados nos concentradores. Com esta abordagem, havendo uma falha em um dos concentradores, boa parte da rede ficará inoperante.

Ou, ainda, é possível estruturar uma rede composta por várias abordagens de rede, onde possa haver pontos construídos em anel, outros em árvore, por exemplo, e todas as estruturas interligadas. Quando encontramos este ambiente nos referimos a ele como uma estrutura híbrida, ou seja, composta por várias topologias de rede ao mesmo tempo.

Essa estrutura híbrida é muito utilizada, pois dentro de uma mesma organização sempre haverá diversos tipos de cenário, onde serão necessárias, em alguns pontos, maior segurança e disponibilidade de serviços, enquanto outros serão mais tolerantes e pacientes a falhas.

Assim, sempre que formos avaliar uma rede local (LAN) quanto à sua topologia de rede, deve-se levar em consideração algum ponto de referência, pois na grande maioria dos casos encontraremos diferentes tipos de topologias agrupadas, formando uma estrutura híbrida, como já mencionado. Porém, em casos isolados é possível identificar alguma topologia específica dentro do ambiente e, assim, é necessário desconsiderar o todo e se focar no local especificado.

Em resumo, uma rede local será composta de diferentes tecnologias para a transmissão de seus dados e sua arquitetura lógica também será composta por diferentes abordagens. Desta maneira, é possível contemplar um índice de disponibilidade e confiabilidade para rede elevado, garantindo a satisfação do usuário final, perante o que ele espera do ambiente.

3 ETHERNET

A *Ethernet* surgiu na década de 1970 e, desde então, vem evoluindo e crescendo, consolidando sua posição no mercado como principal padrão utilizado para redes de alta velocidade.

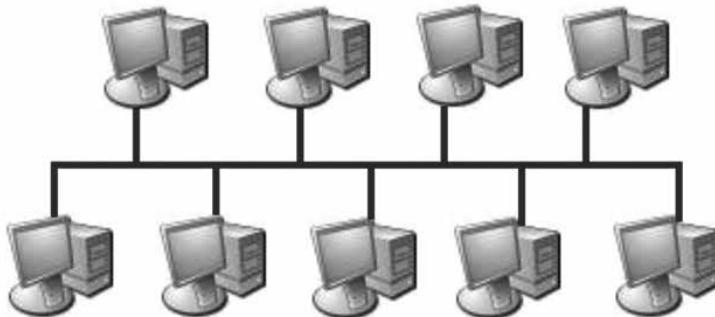
Seu surgimento aconteceu no Havaí, na University of Hawaii, onde a necessidade de comunicação entre as ilhas era algo fundamental. Para tanto, lançar cabos sob o oceano para realizar esta comunicação era inviável. Dessa maneira, a solução encontrada foi a utilização de rádios de baixa frequência para realizar essa comunicação.

Cada terminal de usuário continha um rádio, o qual era responsável por realizar a transmissão e recepção dos dados entre os pontos, esta pequena rede ficou conhecida como *ALOHANET*.

Durante este mesmo período, Bob Metcalfe e David Boggs tomaram conhecimento deste projeto executado no Havaí e foram conhecê-lo. Com base no que aprenderam durante sua estada no Havaí, ao voltarem para seu trabalho na Xerox, onde estava sendo desenvolvido o primeiro projeto de computador pessoal, foi projetada e implantada a primeira rede local, isso em 1976, rede esta que foi denominada de *Ethernet*.

A *Ethernet* foi uma evolução da *ALOHANET*, seu funcionamento acontecia da seguinte forma: todos os comutadores ligados à rede tinham de ficar com um estado de escuta, acompanhando o meio para, assim, identificar quando o mesmo ficará disponível. Quando o mesmo estará sem utilização, o comutador alterava seu estado de escuta para transmissão e realizava a transmissão dos seus dados; ao finalizar a transmissão, o mesmo voltará para o seu estado de escuta. Seu formato era similar a uma rede em formato de barramento, como pode ser observado na Figura 64.

FIGURA 64 - ARQUITETURA DA ETHERNET ORIGINAL



FONTE: Disponível em: <<http://.culturamix.com>>. Acesso em: 10 abr. 2016.

Essa estrutura de rede da Xerox foi também bem-sucedida, e em 1978, juntamente com a Intel, foi desenvolvido um novo padrão *Ethernet* de 10 Mbps. Este novo padrão possuía uma capacidade de transmissão de dados muito superior às 2,48 Mbps da estrutura antiga. Desde então, a *Ethernet* não parou de evoluir, surgindo novas versões com capacidade de transmissão de 100 Mbps, 1.000 Mbps.

Esta primeira topologia de barramento definida pelo padrão *Ethernet* foi utilizada até a metade da década de 1990. Após este período, as estruturas de rede deixaram de utilizar a ideia de barramento para incorporar um *hub* (repetidor) em sua estrutura. Baseada nesta alteração, a topologia lógica das redes sofreu uma mudança, passando a utilizar o formato de estrela, onde todos os *hosts* estão interligados diretamente a um único concentrador. Com esta topologia, os dados passam a ser transmitidos dentro da rede através do *broadcast*.

Esta topologia de rede, tendo o *hub* como concentrador, foi utilizada até o início do ano 2000, onde o padrão *Ethernet* vem a sofrer mais uma grande evolução. Neste período a topologia de rede em estrela permanece, porém o concentrador principal é alterado. Substituindo o *hub* por um comutador (*switch*). Esta alteração

fez com que as estruturas *Ethernet* se tornassem mais confiáveis e rápidas, pois problemas como colisão e erros voltados ao encaminhamento das informações foram solucionados.

A *Ethernet* não é único padrão de LAN, existem outros padrões, tais como *Token*, *ATM* e *Frame Relay*, porém é o mais utilizado e disseminado no mercado, pois apresenta um menor custo e facilidade para implantação. Este padrão *Ethernet* ficou conhecido também como 802.3

Juntamente com a *Ethernet*, os conceitos de *half* e *full duplex* surgem no mercado. Estes conceitos estão relacionados com transmissões de dados. As transmissões em *half duplex* têm como base o conceito utilizado nas redes em barramento, onde o *host* não pode receber e transmitir dados ao mesmo tempo. Já quando tratamos de uma rede *full duplex*, o *host* possui a capacidade de recepção e transmissão de dados simultâneos.

Segundo Kurose (2010, p.345):

A *Ethernet* usa transmissão em banda-base, isto é, adaptador envia um sinal digital diretamente ao canal *broadcast*. A placa de interface não desloca o sinal para outra banda de frequência, como é feito nos sistemas ADSL e de modem a cabo. Muitas tecnologias *Ethernet* também usam a codificação Manchester. Com esta codificação, cada bit contém uma transição; um 1 tem uma transição de cima para baixo, ao passo que um 0 tem uma transição de baixo para cima. A razão para o uso da codificação Manchester é que os relógios nos adaptadores remetentes e receptores não estão perfeitamente sincronizados. Ao concluir uma transição no meio de cada bit, o hospedeiro receptor pode sincronizar seu relógio com o relógio do hospedeiro remetente. Tão logo o relógio do adaptador receptor esteja sincronizado, o receptor pode delinear cada bit e determinar se é um 1 ou um 0. A codificação Manchester é mais uma operação de camada física do que de camada de enlace.

3.1 CSMA/CD: PROTOCOLO DE ACESSO MÚLTIPLO DA ETHERNET

Ao utilizarmos concentradores de rede que não podem ser classificados como comutadores como é o caso do *hub*, as LAN's acabam por se tornar verdadeiras redes de *broadcast*. Isso acontece, pois quando um adaptador envia um quadro de informação, todo os demais adaptadores de rede ligados ao *hub* recebem o quadro.

Para tanto, é necessário o emprego de um protocolo específico de acesso múltiplo dentro da rede, este protocolo é denominado de CSMA/CD (CSMA with Collision Avoidance – CSMA com abstenção de colisão). Este protocolo realiza verificação de canal físico e lógico antes de realizar qualquer tipo de transmissão.

Assim, Kurose (2010, p. 345) descreve as características desse protocolo da seguinte maneira:

- Um adaptador pode começar a transmitir a qualquer tempo, ou seja, não há noção de compartilhamento de tempo.
- Um adaptador nunca transmite um quadro quando percebe que algum outro adaptador está transmitindo, ou seja, ele usa detecção de portadora.
- Um adaptador que está transmitindo aborta sua transmissão quando percebe que algum outro adaptador está transmitindo, ou seja, usa detecção de colisão.
- Antes de tentar retransmissão, um adaptador espera um período de tempo aleatório que é caracteristicamente pequeno em comparação com o tempo de transmissão de um quadro.

Dessa maneira, o CSMA/CD garante um maior desempenho às redes LAN's, garantindo maior confiabilidade e agilidade aos serviços. Quando um *host* dentro da rede possui um quadro a ser enviado, e ninguém mais dentro do ambiente possui dados a serem transmitidos, o *host* em questão pode fazer uso total de velocidade de transmissão que a rede possui (10 Mbps, 100 Mbps ou 1 Gbps). Porém, se outros *hosts* tiverem quadros a serem transmitidos, esta velocidade é reduzida.

Assim, definimos a eficiência da *Ethernet* como parte do tempo final gasto durante a transmissão dos quadros no canal, sem colisões e erros de comunicação entre os nós ativos da rede.

Dessa forma, se pensarmos que até então as redes eram baseadas em estruturas de barramento, onde o controle de acesso ao meio era realizado de maneira muito superficial, o protocolo CDMA/CD surge com a intenção de criar normas em um mundo desordenado, aumentando a confiabilidade do meio, resolvendo os problemas de erros e colisões de maneira satisfatória, dando maior agilidade e performance às estruturas já existentes e recém-construídas.

3.2 SERVIÇOS ORIENTADOS E NÃO ORIENTADOS A CONEXÕES

O padrão *Ethernet* fornece serviços para outras camadas. Estes serviços podem ser caracterizados por sua confiabilidade. Assim, alguns serviços são confiáveis, pois nunca perdem dados, ou seja, é implementado para que o receptor confirme o recebimento de cada mensagem, para que desta forma o transmissor tenha certeza de que o dado foi entregue corretamente, enquanto outros não realizam essa confirmação de recebimento, deixando a critério do destinatário o tratamento das falhas de comunicação que podem vir a ocorrer.

Nos serviços sem conexão, os pacotes são inseridos individualmente na rede e roteados de forma independente uns dos outros. Nesse formato, os pacotes não recebem nenhum tipo de marcação ou um caminho determinado. Dessa maneira, cada pacote pode fazer um caminho diferente de outro dentro da

rede para alcançar o mesmo destino. Assim, os pacotes podem vir a chegar ao destino de forma desordenada e fora de um contexto. Dentro destes modelos de serviço temos duas variações: a primeira seria o serviço não confiável, quando o destinatário recebe o pacote e o encaminha para uma verificação de CRC, onde o mesmo é analisado e, independente do resultado, na análise não é gerado nenhum retorno para a origem do pacote; já na segunda possibilidade, quando existe uma confiabilidade do serviço, o pacote é analisado em busca de CRC's, caso sejam encontrados erros no pacote e o mesmo esteja utilizando o protocolo de transporte TCP, então será gerado um retorno à origem solicitando o mesmo pacote.



CRC (sigla da expressão inglesa *Cyclical Redundancy Check* e que em português é traduzida por Verificação de Redundância Cíclica) consiste num número criado por um cálculo matemático no computador fonte de um pacote de dados. Quando o pacote chega a seu destino, o cálculo é refeito. Se os resultados forem os mesmos, isso indica que os dados no pacote permaneceram estáveis. No caso do cálculo no destino diferir do cálculo na fonte, tal significa que os dados foram alterados durante a transmissão. Neste caso, a rotina CRC sinaliza o computador fonte para retransmitir os dados.

FONTE: Disponível em: <<http://knoow.net/ciencinformtelec/informatica/crc-cyclical-redundancy-check/>>. Acesso em: 10 abr. 2016.

Os serviços orientados à conexão estabelecem uma conexão direta entre origem e destino. Dessa forma, todos os pacotes gerados ao destino para o qual foi estabelecida a conexão utilizaram o mesmo caminho de rede para chegar até o destinatário. Como parte da configuração da conexão, este caminho fica armazenado nas tabelas internas dos roteadores para que não haja troca de rotas. Ao finalizar a conexão, depois do envio dos dados, a conexão é encerrada e a rota definida é excluída.

Nos serviços orientados à conexão, a confirmação de entrega também pode não acontecer, porém a ordem de envio e recebimento é respeitada e questões voltadas a congestionamentos são tratadas, devido ao estabelecimento da conexão entre origem e destino. Outras informações sobre congestionamento serão abordadas mais adiante neste caderno.

Na Figura 65 pode-se observar exemplos práticos de aplicações e quais são os tipos de conexões utilizadas:

FIGURA 65 - EXEMPLO DE SERVIÇOS

Serviço	Exemplo
Fluxo de mensagens confiáveis	Sequência de páginas
Fluxo de <i>bytes</i> confiáveis	Download de filme
Conexão não confiável	VOIP
Datagrama não confiável	Lixo de correio eletrônico
Datagrama confirmado	Mensagem de texto
Solicitação/resposta	Consulta a banco de dados

FONTE: Adaptado de <<https://sites.google.com/site/estudandoredes/capitulo-01---introducao/1-3-software-de-rede/1-3-3-servicos-orientados-a-conexoes-e-servicos-sem-conexoes>>. Acesso em 10 abr. 2016.

RESUMO DO TÓPICO 1

Neste tópico você viu que:

- As LAN's são redes de computadores que possuem um alcance reduzido e uma quantidade de *hosts* limitada. Normalmente são restritas a pequenos locais, empresas e residências.
- Pode-se considerar uma rede LAN sempre que o gestor ou administrador de rede tenha acesso e possua gerência sobre os equipamentos que compõem a rede.
- Ao analisar e categorizar uma rede de computadores é preciso levar em consideração de que ponto estamos analisando a rede, pois uma LAN para determinado usuário pode vir a ser uma WAN para outro, tudo irá depender de que ponto estamos analisando, como já mencionado.
- As redes LAN's estão por todas as partes e se fazem presentes em nosso dia a dia constantemente.
- O padrão *Ethernet* surgiu há muito tempo e vem evoluindo constantemente, trazendo maior velocidade para as redes e integridade aos dados.
- A maneira com que os dados são transferidos dentro da rede pode variar de acordo com a aplicação que está sendo executada e, assim, as características e o formato desse deslocamento podem mudar.

AUTOATIVIDADE



Vamos praticar o que estudamos até agora!

1 As redes locais de computadores são também conhecidas como:

- a) () LANs
- b) () MANs
- c) () WANs
- d) () ATMs
- e) () CRCs

2 Qual conceito define melhor uma rede de computadores?

- a) () Consiste em interligar pelo menos cinco computadores conectados entre si de modo a poderem compartilhar seus serviços.
- b) () Consiste de dois ou mais computadores conectados entre si de modo a poderem compartilhar serviços.
- c) () Consiste de dois ou mais computadores conectados diretamente entre si.
- d) () Consiste de cinco ou mais computadores conectados entre si.
- e) () Consiste de um computador com vários dispositivos de interface humana.

3 O que é uma LAN e quais suas características?

4 Qual a principal diferença entre a comunicação sem conexão e a comunicação orientada à conexão?



Assista ao vídeo de
resolução da questão 4



CONCEITO DE REDES WAN

1 INTRODUÇÃO

Uma rede WAN consiste em uma rede externa à rede local, ou seja, o que estiver fora do alcance da rede local de forma direta e o gestor da rede não possuir gerência, é considerado como uma rede WAN.

As redes WAN's são constituídas a partir de uma interligação de várias outras redes. Pensando dessa forma, o que vai categorizar se uma rede é LAN ou WAN é a possibilidade de gerência de determinado equipamento dentro da rede, e a localização do usuário em relação a esta rede.

2 REDE WAN

Uma rede de computadores que possui uma grande abrangência e sua distribuição é geograficamente distribuída, é denominada de WAN (*Wide Area Network*).

Sua formação consiste em vários *hosts* (máquinas finais de usuários) e muitos nós, ou seja, vários roteadores espalhados por todos os pontos de cobertura desta rede. Assim, é possível realizar o encaminhamento dos pacotes de informações de forma correta e muitas vezes autônoma dentro desta super-rede.

Esta grande rede denominada de WAN, na verdade, é formada pela interligação de várias sub-redes distintas, as quais são interligadas umas às outras através dos roteadores de borda. Estes são equipamentos robustos que realizam a separação de diferentes blocos ou *ranges* de rede, e são capazes de processar inúmeros pacotes de dados simultaneamente. Desta forma, acabam por realizar a interligação de endereços de rede, que até o momento não poderiam trocar qualquer tipo de informações, devido às máscaras de redes distintas que impossibilitam a comunicação direta entre os *hosts*.

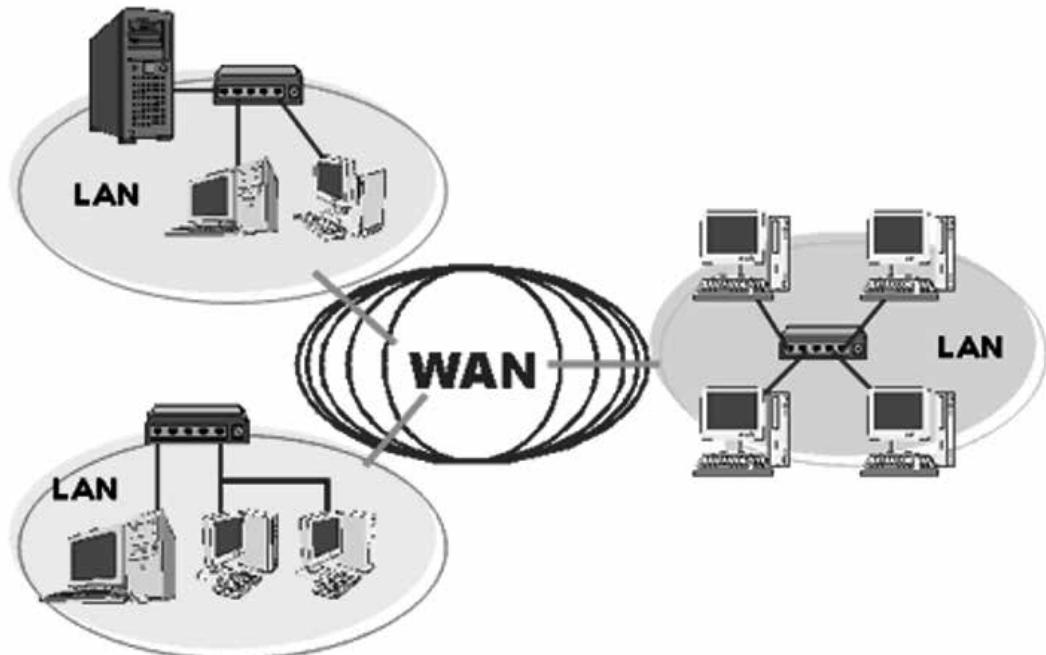
Desta maneira, a função destas sub-redes é realizar a conexão ponto a ponto entre diferentes ativos de rede e, assim, realizar o transporte das informações de um local até o seu destino final. Estas redes, normalmente, são administradas pelas operadoras de telecomunicações de cada região, e interconectadasumas às outras para realizar o trânsito destes dados gerados a partir dos *hosts* conectados nestas operadoras.

Segundo Tanenbaum (2003),

Na maioria das redes geograficamente distribuídas, a sub-rede consiste em dois componentes distintos: linhas de transmissão e elementos de comutação. As linhas de transmissão transportam os bits entre as máquinas. Elas podem ser formadas por fio de cobre, fibras ópticas ou mesmo enlaces de rádio. Os elementos de comutação são computadores especializados que conectam três ou mais linhas de transmissão. Quando os dados chegam a uma linha de entrada, o elemento de comutação deve escolher uma linha de saída para encaminhá-los, estes elementos no passado receberam diversos nomes, porém o mais utilizado até hoje é roteador.

Um exemplo de uma rede WAN pode ser observado na Figura 66:

FIGURA 66 - REDE WAN



FONTE: Disponível em: <<https://10infrhcpaulo.wordpress.com/2012/12/11/wan/>>. Acesso em: 3 abr. 2016.

3 QoS (QUALITY OF SERVICE - QUALIDADE DE SERVIÇO)

A qualidade de serviço ou QoS tem por objetivo melhorar o desempenho das aplicações dentro das redes fazendo uso de funções específicas, tais como MPLS, *Frame Relay*, métodos que iremos estudar mais adiante neste caderno.

A principal estratégia do QoS dentro das redes é tratar as aplicações com a atenção que elas merecem. Para isso, o QoS define regras e estratégias para atender todas as necessidades das aplicações. Para tanto, é realizada reserva de banda, criados índices de prioridade, realizando o controle do *jitter* (variação de atraso do pacote) e controlando a latência entre os pontos que estão realizando a troca das informações, tudo isso visando criar o melhor ambiente possível para a aplicação.

Os pacotes dentro das redes de computadores seguem um determinado caminho para alcançar o seu destino, esse caminho ou direção que os dados estão realizando é denominado de fluxo.

Este fluxo de dados é dado pela confiabilidade, retardo, flutuação e largura de banda oferecida. Quando estes quesitos são tratados de forma homogênea, temos então o QoS (*quality of service* – qualidade de serviço) exigido pelas aplicações.

Assim, cada aplicação possui características básicas que devem ser respeitadas para sua perfeita execução, como pode ser observado na tabela:

TABELA 6 - A RIGIDEZ DOS REQUISITOS DE QUALIDADE DE SERVIÇO

Aplicação	Confiabilidade	Retardo	Flutuação	Largura de banda
Correio Eletrônico	Alta	Baixa	Baixa	Baixa
Transferência de arquivos	Alta	Baixa	Baixa	Média
Acesso à Web	Alta	Média	Baixa	Média
Login Remoto	Alta	Média	Média	Baixa
Áudio por demanda	Baixa	Baixa	Alta	Alta
Vídeo por demanda	Baixa	Baixa	Alta	Alta
Telefonia	Baixa	Alta	Alta	Baixa
Videoconferência	Baixa	Alta	Alta	Alta

FONTE: Tanenbaum (2003, p. 423)

A Cisco (2006) define QoS como:

Serviço de rede melhor e mais previsível, fornecendo largura de banda dedicada, *jitter* controlado e latência, e perda de características melhoradas. QoS atinge esses objetivos fornecendo ferramentas para gerenciar o congestionamento da rede, formação de rede tráfego,

utilizando de maneira ampla áreas de *links* de forma mais eficiente, e definindo políticas de tráfego em toda a rede. QoS oferece serviços de rede inteligente que, quando corretamente aplicados, ajudam a fornecer desempenho consistente e previsível. (CISCO SYSTEMS, 2006, p. 3).

Podemos dizer então que o QoS é um conjunto de regras que irão determinar quais recursos ficaram reservados e disponíveis dentro da rede para determinada aplicação.

Para realizar a aplicação de QoS, temos dois princípios básicos:

- Serviços integrados (*Intserv*): têm o objetivo de garantir a qualidade de serviço fim a fim. Tal garantia acontece através da reserva de recursos. Para tanto, utilize-se o protocolo RSVP (*Resource Reservation Protocol*) para determinar o que a aplicação necessita para sua execução, e assim definir os parâmetros adequados de QoS, visando à eliminação do congestionamento de rede.
- Serviços diferenciados (*Diffserv*): realizam o tratamento das solicitações baseados em classes, manipulando as classes de diferentes maneiras dentro das redes. A *Diffserv* tem como objetivo realizar o QoS em grandes redes como a Internet, para tanto trata as necessidades requisitadas como garantia de banda, por exemplo, de forma ponto a ponto. Neste formato, quando um pacote chega em um roteador intermediário, o mesmo é interpretado e tenta realizar a negociação de QoS. Caso a negociação não seja bem-sucedida, os parâmetros de QoS são ignorados pelo roteador e o dado segue sua transmissão de forma normal, sem qualquer garantia.

O QoS torna-se realmente eficiente quando é possível determinar seu funcionamento em todos os ativos de rede, pois temos a garantia do seu funcionamento. Quando aplicamos o QoS aos pacotes que possuem como destino a Internet, onde não se tem jurisdição sobre todos os ativos de rede, a sua usabilidade fica comprometida e à mercê das configurações ativas em cada roteador.

4 MPLS (*Multi-Protocol Label Switching*)

O MPLS é uma tecnologia de encaminhamento de pacotes baseada no rótulo de cada pacote que está circulando no meio. Este rótulo não fica vinculado ao endereço IP, pois o pacote recebe esta marcação assim que entra na rede. Sendo assim, podemos dizer que o MPLS atua entre as camadas 2 e 3 do modelo de referência OSI.

O principal objetivo do MPLS dentro da rede é fazer com que o transporte dos pacotes seja mais rápido e eficiente. O desenvolvimento da sua tecnologia fez com que funções como o QoS e VPN fossem mais aproveitadas.

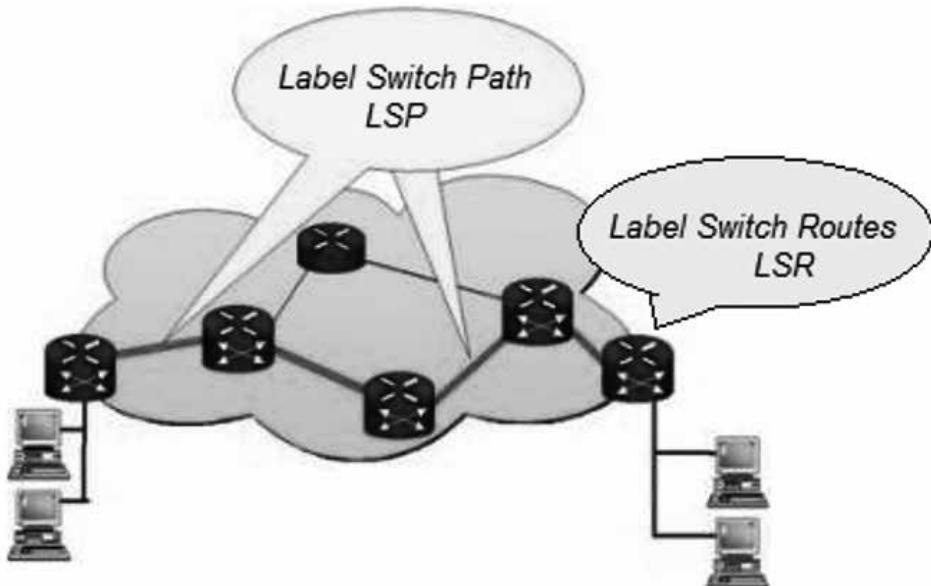
O MPLS permite uma maior otimização da rede, reduzindo problemas com atraso e perda de pacotes, aumentando a taxa de transmissão.

Como já mencionado, o funcionamento do MPLS é baseado em rótulos ou marcação dos pacotes. De modo geral, dentro das redes, os pacotes, ao passarem por um roteador, têm o seu cabeçalho analisado; baseado nesta análise, o roteador determina qual o melhor caminho para que o pacote alcance o seu destino. Este processo, muitas vezes, acaba por gerar atrasos e congestionamento nas redes, pois o cabeçalho de um pacote é composto por diversos campos, os quais consomem muito o processador dos roteadores para realizar a sua análise.

Dessa maneira, o MPLS propõe uma nova ideia de encaminhamento de dados. Esta proposta consiste em etiquetar todos os pacotes que estejam utilizando o MPLS. Neste momento, o pacote é associado às entidades de encaminhamento tanto de origem quanto de destino, as chamadas FEC (*Forwarding Equivalence Class*). Após esta associação, o pacote entra na rede MPLS.

Quando um pacote chegar ao roteador, não será necessário realizar toda análise do cabeçalho. Neste momento, roteador de rótulos (*Label Switch Router - LSR*) irá trocar o rótulo do pacote, inserindo um novo índice, ou seja, removendo o rótulo de entrada por um de saída que levará o pacote até o próximo roteador. Este processo acontecerá até o pacote chegar ao último roteador LSR. Neste momento, o rótulo é removido por completo e o pacote entregue ao destinatário. Observe:

FIGURA 67 - ESTRUTURA MPLS



FONTE: Adaptado de <http://www.gta.ufrj.br/grad/01_2/mpls/mpls.htm>. Acesso em: 8 abr. 2016.

Dentre as principais vantagens da utilização do MPLS, podemos destacar:

- A não necessidade de leitura do cabeçalho dos pacotes, o que acarreta em uma diminuição de uso do processador dos roteadores, que leva a maior agilidade nas transmissões dos pacotes, evitando assim possíveis congestionamentos de rede.

Isso acontece porque o pacote é processado somente nas extremidades da rede, deixando os demais equipamentos folgados no que se refere a processamento de dados.

- Engenharia de tráfego, que possibilita escolher como as informações serão encaminhadas na rede, permitindo assim habilitar serviços como QoS, priorizando determinados tipos de dados e controlando o fluxo das informações.

Por suas características, o MPLS tornou-se de suma importância para as operadoras de telecomunicações, garantindo maior sobrevida aos ativos de rede e aumentando de certa forma a capacidade de transmissão dos seus enlaces.

RESUMO DO TÓPICO 2

Neste tópico você viu que:

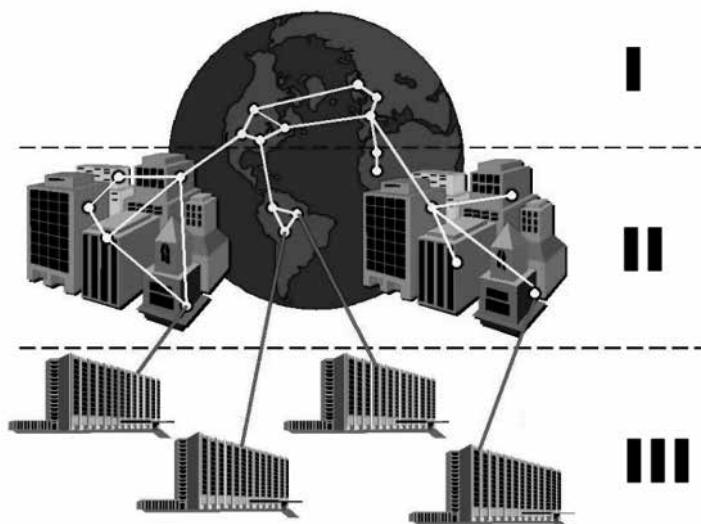
- O conceito de rede WAN consiste em uma interligação de várias redes distintas para, juntas, darem origem a uma única rede, popularmente conhecida como Internet.
- Toda a rede que está localizada fora dos domínios da rede local é considerada uma rede WAN, do ponto de vista do usuário que está localizado dentro da rede local.
- A categorização de uma rede sempre dependerá do ponto de vista de onde está sendo realizada a análise.
- O MPLS é uma estrutura de rede muito utilizada em provedores de telecomunicações, pela sua facilidade de implementação e o ganho de performance dado à rede através de sua aplicabilidade.
- Aplicando o MPLS dentro da rede, outras funcionalidades podem ser agregadas ao ambiente para diminuir o uso de processamento desnecessário por parte dos roteadores, ganhando em vida útil dos ativos de rede.
- O QoS é uma importante funcionalidade, que pode ser aplicada à rede com a intenção de melhorar os serviços oferecidos por ela e assim fazer com que as aplicações trabalhem de forma correta.
- Com o QoS habilitado dentro da rede, todas as aplicações podem ter seus requisitos mínimos de funcionamento respeitados, garantindo o seu melhor funcionamento.

AUTOATIVIDADE



Prezado(a) acadêmico (a), vamos testar seus conhecimentos?

- 1 São constituídas pela interconexão de múltiplas redes menores e sistemas computacionais dentro de grandes áreas geográficas e, dada a sua dimensão, as tecnologias usadas para a transmissão dos dados são as mais diversas:
 - a) CAN
 - b) MAN
 - c) WAN
 - d) RAN
 - e) LAN
- 2 Defina o significado de LAN e WAN e compare suas características, mostrando suas diferenças e suas semelhanças.
- 3 Baseando-se na imagem abaixo, qual a classificação das redes I, II e III?



FONTE: Adaptado de Marcio Henrique (2014)

- a) () LAN - WAN - SAN
- b) () MAN - WAN - LAN
- c) () WAN - MAN - LAN
- d) () WAN - LAN - PAN
- e) () WAN - MAN - CAN



Assista ao vídeo de
resolução da questão 2



- 4 Em uma rede, uma sequência de pacotes desde uma origem até um destino é chamada fluxo. As necessidades de cada fluxo podem ser caracterizadas por quatro parâmetros principais que juntos definem a QoS (*Quality of Service* – qualidade de serviço) que o fluxo exige.

Os parâmetros citados são:

- a) () velocidade de transmissão, paridade, roteamento e flutuação.
- b) () confidencialidade, retardo, flutuação e largura de banda.
- c) () confidencialidade, irretratabilidade, retardo e largura de banda.
- d) () retardo, usabilidade, flutuação e velocidade de transmissão.
- e) () volatilidade, velocidade de transmissão, retardo e flutuação.

CONCEITOS DE REDES WIRELESS

1 INTRODUÇÃO

As redes sem fio nos últimos anos passaram a se tornar cada vez mais comuns. Em qualquer local é possível encontrar um sinal de Wi-fi sendo disponibilizado. Esta estrutura de rede trouxe versatilidade aos ambientes, pois tornou possíveis e reais questões como a mobilidade dentro dos ambientes corporativos e residências.

Porém, junto com grandes benefícios, este conceito de rede trouxe algumas preocupações quanto à segurança desta estrutura de rede. Isso porque com esta nova abordagem não é possível realizar uma delimitação precisa do alcance da rede, acabando assim por deixar a rede em questão suscetível a ataques.

2 CONCEITOS

As redes sem fio tiveram seu início na Universidade do Havaí em 1971. Seu desenvolvimento teve por objetivo realizar a conexão entre as quatro ilhas sem utilizar cabos telefônicos. Porém, sua popularização só veio a se concretizar nos anos 80, quando a ideia de compartilhar arquivos entre dispositivos começou a se tornar mais comum, deixando de ser algo utilizado somente por grandes corporações.

As primeiras redes sem fio não faziam uso de rádios transmissores e receptores de frequências de rádio, mas de infravermelho. Este conceito de transmissão de dados foi logo descartado, pois como o infravermelho não tem a capacidade de transportar obstáculos, seu alcance no sentido de propagação de dados acabou por ser o seu limitador para a difusão dessa tecnologia.

As ondas de rádio somente passaram a ganhar destaque nas redes sem fio a partir dos anos 90, quando os processadores dos dispositivos passaram a ser rápidos o suficiente para gerenciar a transmissão e recepção de dados utilizando essas ondas eletromagnéticas.

Esta nova tecnologia de transmissão de dados se tornou algo revolucionário, porém seu alto custo e diversos problemas de incompatibilidade entre diferentes fabricantes vieram a causar grandes obstáculos e dúvidas quanto à eficiência dessa topologia de rede.

Somente por volta de 1997 surge um novo padrão para transmissão de dados, utilizando ondas eletromagnéticas: o padrão IEEE 802.11. Esta nova abordagem tinha capacidade de realizar transmissões de dados com uma velocidade máxima de 2 *megabits* por segundo.

Em 1999 o IEEE veio por finalizar o padrão 802.11b de 2,4 GHz, e assim, consequentemente, aumentando a velocidade de transmissão de dados para 11 Mbps.

Após o lançamento e início da difusão dessa tecnologia no mercado, outros fabricantes de *hardware*, como Apple, desenvolveram a sua própria tecnologia para transmissão de dados sem fio e, assim, lançaram no mercado dispositivos evoluídos dessa tecnologia. Então surgiu o padrão 802.11a, padrão o qual deixava de utilizar 2.4 GHz como frequência para transmissão de dados e passava a utilizar o 5GHz. Esta nova abordagem permitia realizar transmissões de dados com velocidade máxima de 54 Mbps.

Assim, em 2002 surgiu outro padrão para transmissão de dado, o então 802.11g. Este novo padrão volta a fazer utilização da frequência de 2.4 GHz, e fornece compatibilidade com qualquer tipo de *hardware*. Esta nova abordagem de redes permite a transmissão de dados com uma velocidade máxima de 54 Mbps, igualando à velocidade dos dispositivos já existentes no mercado, porém com um custo-benefício muito mais acessível que seu concorrente e com muito menos problemas de compatibilidade.

Nos últimos anos, o padrão 802.11a vem evoluindo consideravelmente, permitindo transmissões de dados em alta performance, rompendo assim a barreira dos *gigabits*, porém sua aplicabilidade acabou se tornando muito restrita, principalmente devido ao custo e sua cobertura. Quando falamos no sentido de alcance, este padrão, por utilizar uma frequência mais alta (5 GHz), acaba por possuir uma abrangência de sinal muito mais restrita que outras frequências, o que muitas vezes impossibilita a sua utilização para determinadas situações.

Para tanto, surge o padrão 802.11n, o qual continua a utilizar a frequência de 2.4 GHz como frequência de transmissão, porém utiliza uma banda de propagação mais elevada, deixando o 20 MHz utilizado pelos outros padrões até o momento e passa a utilizar 40 MHz como banda de propagação. Esta alteração em sua estrutura garantiu a sua ampla cobertura em nível de sinal, pois sua frequência de sinal continuou a mesma e fez aumentar sua taxa de transferência de dados, deixando os 54 Mbps para alcançar velocidades máximas de 600 Mbps.

Esta tecnologia 802.11n, porém, só pode ser utilizada por dispositivos que já possuem esse padrão. Dispositivos que ainda não o possuem acabam por utilizar

o seu padrão 802.11b ou 802.11g no momento da sua conexão, o qual acabará por limitar a sua taxa de transmissão. No entanto, sua compatibilidade com os outros padrões acaba por se tornar um grande diferencial para a tecnologia, o que assim garante sua popularização e eficiência no mercado.

3 HARDWARE SEM FIO

Para construirmos uma rede sem fio são necessários somente dois tipos de *hardware*, um ponto de acesso central e um adaptador de rede sem fio. Os pontos de acesso são dispositivos totalmente independentes e atuam como um concentrador ou *hub* na rede sem fio. **Os adaptadores de rede são vinculados aos dispositivos finais, ou seja, aos computadores ou dispositivos portáteis que o usuário final irá utilizar para conectar-se à rede em questão.**

Para realizar a conexão entre estes dois tipos de dispositivos, ambos devem possuir antenas para realizar a transmissão e recepção do sinal em questão. Muitos dos dispositivos aqui relatados já possuem suas antenas embutidas, as quais realizam a ampliação da capacidade de transmissão e recepção do sinal. Em outros casos, é possível realizar a substituição destas antenas com ideia de aumento de abrangência do sinal do equipamento.

Cada antena incorporada ao equipamento tem a capacidade de realizar o aumento da propagação de sinal do mesmo, porém, de nada adianta colocar uma antena de grande capacidade em um equipamento que tem baixa potência de propagação. Desta forma, antena e potência de transmissão do ponto de acesso ou mesmo do receptor devem ser equivalentes, para que o alcance almejado com alteração do *hardware* padrão seja alcançado.

Os pontos de acesso das redes sem fio possuem uma derivação no seu funcionamento, o qual acaba, em alguns casos, sendo responsável por alguns problemas de encaminhamento de dados ou falhas em roteamento de informações. Esta disposição pode ser da seguinte maneira: *gateway*, *bridge* ou repetidor.

Os dispositivos, ao assumirem a configuração de *gateway* dentro de uma rede, passam a ser o concentrador principal do ambiente. São eles que irão realizar o direcionamento da informação e a separação dos ambientes. Nesta disposição, o *hardware* em questão irá receber o sinal de comunicação externo pela interface WAN, as demais portas de rede e a interface wireless do roteador estarão agrupadas e formarão, desta maneira, o ambiente LAN.

Este agrupamento das interfaces receberá um único endereço IP, o qual será obviamente de uma *range* de rede diferente do IP utilizado na interface WAN deste mesmo roteador. Neste ambiente LAN é possível iniciar um servidor DCHP para realizar a distribuição das configurações de rede para os demais dispositivos de rede do ambiente.

Com esta abordagem, será criada uma barreira entre as duas redes, onde todas as informações geradas dentro da LAN terão livre acesso à rede WAN, porém toda informação gerada inicialmente pela WAN não terá acesso livre para LAN. Este acesso somente será possível se regras de *firewall* forem criadas, ou liberações de determinadas portas forem feitas, juntamente com o encaminhamento dos pacotes gerados.

Esta configuração em modo *gateway* traz o benefício de barrar todo o *broadcast* dentro da rede e inter-rede, porém seu grande problema é a adição de um salto a mais dentro da rede e sua gerência, pois sempre que houver necessidade de algum acesso remoto a qualquer *host* dentro desta rede, será necessária a intervenção no equipamento para realizar a liberação da porta ou serviço.

Quando a escolha por uma configuração em modo *bridge* acontecer, o roteador cria um único *range* de portas, ou seja, ele realiza um agrupamento de todas as portas de rede que o mesmo possui, juntamente com a interface *wireless*. Neste modelo, o equipamento terá seu funcionamento similar a um *HUB*, onde o mesmo terá um endereço IP pertencente ao *range* de rede local para seu possível gerenciamento. O serviço de DHCP ficará desativado e, desta maneira, este equipamento não contará como um salto de rede, pois não realiza a troca de prefixos de rede.

Em modo *bridge*, toda a informação recebida pelo equipamento será propagada em todas as suas portas de rede, dessa forma, todos que estiverem ligados por conexões cabeadas ou *wireless* a esse equipamento farão parte da mesma rede, recebendo qualquer tipo de informação.

A grande vantagem desse método de configuração é a sua simplicidade em nível de gerência e economia na quantidade de saltos dentro da rede. Por outro lado, seu grande problema é a propagação de *broadcast* da rede, que acaba por consumir os *hardwares* envolvidos e os meios de comunicação em questão, diminuindo a performance da rede.

Quando a opção feita é pelo modo repetidor, neste caso é necessário possuir dois ou mais roteadores, os quais estarão interligados pelas suas interfaces *wireless*, as quais, além de realizar a integração entre os equipamentos, farão a propagação de sinal para os demais dispositivos realizarem as conexões. Esta topologia de rede é muito utilizada em locais onde não é possível o lançamento de cabeamento de rede ou o mesmo acaba por se tornar inviável.

Nestas situações o modo repetidor é uma opção a ser levada em consideração. Com esta abordagem, os equipamentos *wireless* podem trabalhar de forma homogênea, ou seja, todos como o mesmo SSID (nome visível da rede) e com a mesma senha, caso seja opção definida. Porém, é possível que os equipamentos estejam em modo repetidor, mas suas configurações de SSID e senha sejam diferentes do equipamento anterior que está realizando a integração com a rede cabeada.

Com a abordagem de repetidor, ganha-se e muito em alcance para as redes sem fio, pois é possível o cascamenteamento de muitos roteadores até que o alcance da rede esteja a contento. Porém, a grande desvantagem dessa estrutura, além de grande mão de obra de configuração, é a questão do *broadcast* envolvido, pois ao trabalharmos em modo repetidor, os equipamentos devem estar em *bridge*, ou seja, totalmente transparentes entre si para que assim haja a sincronização. Assim, todos os anúncios de rede e demais serviços são propagados para todos os ativos de rede, gerando grande volume de informação sem necessidade.

Outro grande problema enfrentado por esta estrutura é a baixa taxa de transferência, pois cada interface, além de ser responsável pela sincronização com o *host* posterior, precisa gerir as conexões sem fio dos *hosts* que estão ligados a ele diretamente, o que acaba consumindo grande quantidade de processamento e memória do dispositivo. Assim, consequentemente, a performance de transferência tende a cair, sem mencionarmos que uma rede toda em modo repetidor acaba por se tornar algo muito frágil, pois basta um equipamento falhar para que toda a rede ou boa parte dela venha a ficar sem comunicação, diminuindo assim a confiabilidade do ambiente.

Abaixo é possível visualizar a Tabela 7, com ativos de redes sem fio e suas aplicabilidades:

TABELA 7 - VISÃO GERAL SOBRE HARDWARE SEM FIO PARA PEQUENOS ESCRITÓRIOS E RESIDÊNCIAS

<i>Dispositivos</i>	<i>Forma de conexão</i>	<i>Função</i>	<i>Armadilhas</i>
Ponto de acesso ou <i>gateway</i> sem fio	Sua conexão Internet, normalmente via rede <i>Ethernet</i>	Atua como o <i>hub</i> para sua rede sem fio, compartilha sua conexão Internet com outros computadores conectados por meio da rede cabeada convencional ou sem fio, conecta dispositivos em rede via dispositivos sem fio.	Em geral, projetado para o mundo do Windows, os usuários Apple e Unix/Linux podem ter dificuldades, protocolos não Windows/IP não necessariamente suportados.
Adaptador de rede sem fio	Seu computador	Possibilita que um computador ou outros equipamentos se conectem a um ponto de acesso sem fio.	Tipos menos comuns exigem <i>drives</i>
Antena	Um ponto de acesso ou adaptador de rede sem fio	Estende o alcance da rede sem fio; normalmente embutida.	Frequentemente desajeitada.

Concentrador do tipo ponte (<i>bridge</i>) sem fio	Sua rede <i>Ethernet</i>	Permite conectar redes cabeadas convencionais por meio de tecnologia sem fio ou fazer uma ponte entre uma rede cabeada convencional e uma rede sem fio existente.	Algumas pontes querem uma unidade para cada rede.
Extensor de rede sem fio	Sua rede sem fio	Estende o intervalo da rede sem fio, pois ele aumenta o alcance da rede	O <i>throughput</i> é reduzido porque um único rádio precisa receber e retransmitir cada pacote.

FONTE: Adaptado de *Kit do Iniciante em Redes Sem Fio* (2005)

4 SEGURANÇA EM REDES SEM FIO

Atualmente a segurança das informações tem se tornado um assunto constante dentro dos meios de comunicação e das organizações. Isto se deve ao valor agregado que cada informação possui dentro de uma organização. Dessa maneira, é dever do administrador de rede ou de quem estiver gerenciando os serviços de TI garantir a integridade, disponibilidade e confiabilidade da rede para que, assim, as informações que estejam circulando por ela consequentemente tenham um grau de confiabilidade elevado.

Sendo assim, ao tratarmos de uma rede sem fio, este desafio quanto à segurança se torna mais difícil, pois como não é possível determinar precisamente o alcance de uma rede que usa ondas eletromagnéticas como meio de propagação de dados, precisamos nos cercar de algumas formas para garantir, ou melhor, minimizar possíveis tentativas de ataques e invasões a estas redes.

Para garantir a segurança das informações em um ambiente deste tipo, algumas abordagens são essenciais e básicas para garantir o mínimo de segurança no ambiente em questão.

Estas abordagens são configurações simples que todos os dispositivos utilizados como pontos de acesso oferecem a quem os configura. As possibilidades são: controle de acesso por endereço físico, criptografia e ocultação de SSID.

4.1 SEGURANÇA POR ENDEREÇO FÍSICO

O endereço físico ou endereço MAC, como pode ser observado na figura a seguir, é uma forma adotada de segurança por muitos responsáveis, porém ela sozinha não pode ser considerada muito eficiente, já que deixa uma grande vulnerabilidade dentro da rede.

FIGURA 68 - ENDEREÇO MAC

Adaptador Ethernet Conexão local:	
Estado da mídia.	: mídia desconectada
Sufixo DNS específico de conexão.	:
Descrição.	: NIC Fast Ethernet PCI-E Realtek
Família RTL8102E/RTL8103E (NDIS 6.20)	
Endereço Físico.	: 00-1E-EC-8A-D4-83
DHCP Habilidado.	: Sim
Configuração Automática Habilitada.	: Sim

FONTE: O autor

O endereço MAC aqui mencionado é um endereço existente em cada *hardware*, computadores ou qualquer outro dispositivo utilizado, como placas *wireless*, roteadores, entre outros. Este endereço é atribuído ao dispositivo pelo próprio fabricante do mesmo. O endereço MAC é formado por letras e números e sua constituição é controlada pela IEEE (*Institute of Electrical and Electronics Engineers*), o qual determina a composição e padronização dos endereços para cada fabricante de *hardware*.

Com esta padronização é possível perceber e reconhecer um determinado dispositivo somente pelo seu endereço MAC, pois o prefixo do endereço será semelhante a outros *hardwares* desenvolvidos por este determinado fabricante.

Assim, sabendo que cada *hardware* existente possui um número específico e inigualável, é possível criar um controle de conexões baseado nesses endereços.

Desta forma, para adicionar o controle de MAC à nossa rede, basta realizar o cadastro de todos os endereços que terão permissão para conectar-se na rede dentro do nosso ponto de acesso. Assim, ao tentar estabelecer uma conexão entre cliente e ponto de acesso, será conferido se o endereço do *hardware* solicitante está cadastrado na tabela de *hosts* válidos dentro do roteador, caso esteja, sua conexão é permitida, caso contrário a conexão não é estabelecida.

Esta abordagem como forma de segurança não pode ser considerada uma das mais seguras, pois muitas vezes a origem das conexões pode vir a ser forjada, ou seja, alterado endereço IP de origem no pacote para se fazer passar por um endereço válido. Como estamos tratando de uma rede sem fio, é possível a utilização de ferramentas de captura de pacotes, as quais já capturariam os endereços de MAC da origem e do destino de cada pacote. Dessa forma, um possível invasor já teria em mãos um endereço físico válido para estabelecer a comunicação entre cliente e ponto de acesso.

Como todo dispositivo tem seu endereço, o qual é inserido via *software* pelo fabricante dentro do *hardware*, é possível pelo mesmo processo realizar a alteração deste endereço e, assim, com um endereço válido em mãos e a possibilidade de alteração do seu endereço de forma simples, um possível atacante conseguiria se fazer passar por outro usuário da rede alterando seu MAC e assim conseguindo acesso.

Porém, não é possível realizar duas conexões simultâneas partindo do mesmo MAC de origem. Neste caso, um usuário teria que se desconectar para que outro venha a estabelecer a sua comunicação, no entanto, o atacante mais cedo ou mais tarde conseguiria esta conexão com certa facilidade, demonstrando assim a fragilidade dessa topologia de rede quando trabalha de forma isolada das demais estruturas de segurança.

Mesmo possuindo esta fragilidade, a segurança baseada em endereço MAC é muito utilizada e de certa forma muito eficiente, pois para fazer uso desta técnica descrita acima, o possível invasor deve ter conhecimento técnico e compreender o funcionamento das redes sem fio e suas estruturas de segurança. Assim, esta topologia de segurança pode muito bem ser utilizada em vários ambientes sem maiores problemas, e mesmo com sua fragilidade conseguirá manter um nível de segurança relativamente satisfatório, desde que o ambiente em questão não seja de alta criticidade.

4.2 SEGURANÇA POR CRIPTOGRAFIA

As redes sem fio, por darem a possibilidade de mobilidade aos usuários, passaram a ser grandes alvos de ataques, com finalidade de utilização de recursos do ambiente ou capturar e furtar informações importantes da organização ou mesmo da pessoa física em questão. Como estudado anteriormente, a segurança baseada em endereço MAC, por si só, não oferece altíssimo nível de segurança.

Assim, o protocolo 802.11, no seu surgimento agregou a possibilidade de cifração dos dados. Essa cifração consiste na utilização de um algoritmo baseado numa chave predefinida para realizar o embaralhamento das informações (RUFINO, 2011).

Desta forma, o protocolo inicialmente desenvolvido e utilizado para esta cifração foi o WEP, o qual é totalmente disseminado em todos os equipamentos de ponto de acesso e clientes.

O protocolo WEP é um protocolo que utiliza algoritmos simétricos; portanto, existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o concentrador, com o objetivo de cifrar e decifrar as mensagens trafegadas (RUFINO, 2011).

Desta maneira, o usuário deve conhecer a chave para realizar a conexão. Após o estabelecimento da mesma, esta chave utilizada para estabelecer a conexão entre os pontos sofre uma operação matemática e é subdividida em outras quatro chaves. Destas quatro chaves geradas, uma delas é escolhida pela conexão para realizar a cifragem dos dados durante a sua transmissão e, assim, garantir segurança das informações trafegadas.

O método de criptografia WEP foi utilizado por um longo período, porém foi constatado que o mesmo apresenta muitas vulnerabilidades e, assim, acaba por se tornar um algoritmo frágil, sendo possível realizar, por exemplo, métodos de engenharia reversa para realizar a decifragem dos dados, ou até mesmo ser capaz de interceptar informações transmitidas e, assim, baseado em processo de comparação e força bruta, vir a descobrir a senha de estabelecimento de conexão, tornando a senha que antes era sigilosa em algo comum.

Tendo em vista os problemas de segurança do protocolo WEP, foi divulgado e disponibilizado um novo protocolo de criptografia para as conexões sem fio, o qual foi denominado de WPA.

Este novo protocolo obteve avanços consideráveis, na sua combinação de algoritmos e temporalidade das chaves utilizadas por ele, para envio e recebimento de dados, garantindo assim maior confiabilidade no seu funcionamento.

Segundo Rufino (2015, p. 37), em seu livro:

Os protocolos para cifrar as informações podem ser de dois tipos: um voltado para pequenas redes e de uso doméstico, onde existirá uma chave compartilhada previamente (*Pre-shared*, ou WPA-PSK), conhecida como máster, que será responsável pelo reconhecimento do equipamento pelo concentrador; o outro é conhecido como infraestrutura, que exigirá, ao menos, a figura de um servidor de autenticação (RADIUS), portanto um equipamento adicional. Poderá, ainda, necessitar de uma infraestrutura de chaves públicas, caso utilize certificados digitais para promover a autenticação do usuário.

Outra novidade que o WPA tem incorporado dentro da sua estrutura é o surgimento do protocolo de criptografia TKIP (*Temporal Key Integrity Protocol*), o qual é responsável pela gerência das chaves temporárias utilizadas pelos equipamentos para realizar a comunicação entre os dispositivos envolvidos. Seu grande diferencial em relação ao seu antecessor, o WEP, é a não utilização de uma chave estática para troca de dados, neste caso, a chave utilizada para cifrar os dados é trocada constantemente, sendo possível, assim, manter o segredo da autenticação.

Quando nos referimos à troca de chaves, não estamos realizando a troca da senha de autenticação e, sim, a troca das chaves geradas randomicamente pelos dispositivos sem fio, chaves as quais são geradas a partir do segredo escolhido pelo usuário. Esta troca de chaves é feita de maneira automática pelos dispositivos interconectados, sem que o usuário perceba ou tenha que realizar qualquer interação.

O protocolo WPA foi uma grande revolução em se tratando de autenticação e segurança da informação em redes sem fio, porém, mesmo fazendo utilização de grandes estratégias, o mesmo também apresenta falhas e vulnerabilidades, as quais não são tão perceptíveis quanto as existentes no seu irmão, o protocolo WEP. Mesmo sendo pequenas falhas, devem ser tratadas para minimizar possíveis impactos negativos na rede em questão.

Baseado nessas vulnerabilidades que apareceram ao longo do tempo, o protocolo WPA evoluiu e transformou-se no WPA2, o qual teve incorporado a seus métodos de autenticação o CCMP. O qual faz uso do algoritmo AES para realizar a cifragem dos dados na forma de blocos (128 bits), deixando de realizar o processo *byte a byte*.

Esta nova abordagem é o processo mais seguro atualmente para realizar a criptografia de dados. No entanto, esta abordagem possui um pequeno problema em relação à maior utilização de processador do equipamento, que acaba por ter uma pequena diminuição de performance. Porém, este problema só vem a acontecer em equipamentos mais antigos, que não foram desenvolvidos propriamente para a utilização desses algoritmos. Equipamentos novos que suportam essa tecnologia não apresentam este problema, pois seu processador já foi dimensionado corretamente.

4.3 SEGURANÇA POR OCULTAÇÃO DE SSID

A segurança baseada em ocultação do SSID (*Service Set Identifier*) consiste no princípio básico de esconder uma rede, para que tenha conexão somente quem saiba da sua existência. Nessa estratégia, o SSID, ou nome da rede, fica invisível para os usuários. Por mais que se tente *scanner* para encontrar uma determinada rede, seu nome não irá aparecer como uma possível rede a se conectar. Dependendo do *software* utilizado para realizar o *scan* em busca de alguma rede, o sinal mostrando que existe uma rede sem fio no local pode até vir a aparecer, porém, seu nome para estabelecer a comunicação, não.

A utilização desta abordagem não é muito utilizada e também não oferece um alto nível de segurança ao ambiente quando é utilizada isoladamente, pois existem outros métodos para estabelecer comunicação com um dispositivo, como pelo MAC, sem que seja necessário saber o seu SSID. É uma forma eficiente para enganar usuários mais leigos quanto à existência de uma rede no ambiente.

Sua configuração para a utilização é bastante simples, basta que o usuário, no momento da configuração de seu equipamento, marque a opção de obscuridade ou desabilite o *Broadcast* do SSID, como pode ser observado na figura a seguir:

FIGURA 69 - OCULTAÇÃO DE SSID

Configurações Wireless Avançadas

Estas configurações são para usuários avançados que possuem conhecimentos sobre WLAN. Estas configurações não devem ser alteradas a menos que você saiba os efeitos que elas causarão no seu AP.

Região de Domínio:	FCC(1-11)
Tipo de Autenticação:	<input type="radio"/> Sistema Aberto <input type="radio"/> Chave Compartilhada <input checked="" type="radio"/> Automático
Fragmento de Entrada:	2346 (256-2346)
Entrada RTS:	2347 (0-2347)
Intervalo de Aviso:	100 (20-1024 ms)
Tempo Inativo:	30000 (101-60480000 10ms)
Ack Esgotado:	0 (0-255 µs)
Taxa de Dados:	Auto
Tipo de Introdução:	<input checked="" type="radio"/> Introdução Longa <input type="radio"/> Introdução Curta
SSID Broadcast:	<input checked="" type="radio"/> Habilido <input type="radio"/> Desabilitado
Proteção 802.11g:	<input checked="" type="radio"/> Habilido <input type="radio"/> Desabilitado
WMM:	<input type="radio"/> Habilido <input checked="" type="radio"/> Desabilitado
Potência de Saída de RF (Wireless):	<input checked="" type="radio"/> 100% <input type="radio"/> 50% <input type="radio"/> 25% <input type="radio"/> 10% <input type="radio"/> 5%
Modo Turbo:	<input type="radio"/> Automático <input type="radio"/> Sempre <input checked="" type="radio"/> Desligado
Atenção: O modo Turbo requer compatibilidade com equipamentos Realtek.	
Watchdog:	<input type="radio"/> Habilido <input checked="" type="radio"/> Desabilitado
Tempo do Watchdog:	1 (1-60 minutos)

Fonte: O autor

Utilizando esta simples técnica, somente os usuários que conhecerem o nome, ou SSID desta rede, poderão estabelecer a comunicação de forma eficiente, ou seja, a conexão entre cliente e ponto de acesso deverá ser realizada de forma manual. Após a realização da paridade entre os dois dispositivos, tais configurações realizadas ficarão gravadas no *host* para futuras conexões.

Sendo assim, imaginando uma estratégia de segurança para um ambiente baseado em rede sem fio, podemos tomar como precaução a ocultação do SSID, com o uso de uma chave de autenticação utilizando de preferência o modelo WPA e, quem sabe, um controle de MAC habilitado, pois desta forma um possível atacante terá que identificar a rede, realizar um clone de MAC e realizar a quebra da chave criptografada, garantindo assim um alto nível de confiabilidade para a rede.

Porém, ao incorporar vários itens de segurança ao ambiente, devemos levar em consideração o volume de informações que este ambiente irá possuir. Quanto mais parâmetros para garantir a segurança forem incorporados ao ambiente, mais será exigido dos dispositivos (ponto de acesso), o que pode vir a causar certa lentidão na rede e desconforto para o usuário. Este terá vários procedimentos para conseguir êxito em sua conexão e maior mão de obra existirá para o administrador dessa rede, pois o mesmo terá que cadastrar todo e qualquer dispositivo que poderá a vir necessitar acesso à rede.

Assim, ao planejarmos qualquer estrutura de segurança, é necessário levar em consideração o ambiente onde será aplicada esta estrutura, imaginando o volume de dados que irá circular, a criticidade do ambiente, no sentido de quais informações irão circular e o conhecimento técnico dos usuários para lidar com os parâmetros de segurança implantados.

Em muitos casos, uma simples criptografia ou chave para conectar-se à rede já é o suficiente para o ambiente, pois o mesmo não possui um nível crítico em suas informações e ativos, permitindo assim ser mais maleável quanto à segurança deste ambiente.

Porém, em outros ambientes onde segurança é algo fundamental para o meio, onde as informações que circulam dentro desta rede são de alta confidencialidade, é necessária a implantação de uma estrutura de segurança mais complexa, contemplando uma criptografia e outros parâmetros, como autenticação por MAC, ocultação de SSID, ou até mesmo alguma outra forma de autenticação.

Desta forma será possível elevar o nível de segurança da informação no ambiente, com a ideia de garantir a identificação do usuário dentro da rede, e o *hardware* que está sendo utilizado para realizar a conexão.

LEITURA COMPLEMENTAR

Criptografia

Forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet.

À primeira vista ela até pode parecer complicada, mas para usufruir dos benefícios que proporciona, você não precisa estudá-la profundamente e nem ser nenhum matemático experiente. Atualmente, a criptografia já está integrada ou pode ser facilmente adicionada à grande maioria dos sistemas operacionais e aplicativos, e para usá-la, muitas vezes, basta a realização de algumas configurações ou cliques de *mouse*.

Por meio do uso da criptografia você pode:

- proteger os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas e a sua declaração de Imposto de Renda;
- criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- proteger seus *backups* contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
- proteger as comunicações realizadas pela Internet, como os *e-mails* enviados/recebidos e as transações bancárias e comerciais realizadas.

Criptografia de chave simétrica e de chaves assimétricas

De acordo com o tipo de chave usada, os métodos criptográficos podem ser subdivididos em duas grandes categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

- Criptografia de chave simétrica: também chamada de criptografia de chave secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados. Em casos nos quais a informação é codificada e decodificada por uma mesma pessoa não há necessidade de compartilhamento da chave secreta. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave). Exemplos de métodos criptográficos que usam chave simétrica são: AES, *Blowfish*, RC4, 3DES e IDEA.
- Criptografia de chaves assimétricas: também conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não repúdio. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um *smartcard* ou um *token*. Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ECC e *Diffie-Hellman*.

A criptografia de chave simétrica, quando comparada com a de chaves assimétricas, é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento é mais rápido. Todavia, quando usada para o compartilhamento de informações, se torna complexa e pouco escalável, em virtude da:

- necessidade de um canal de comunicação seguro para promover o compartilhamento da chave secreta entre as partes (o que na Internet pode ser bastante complicado) e;
- dificuldade de gerenciamento de grandes quantidades de chaves (imagine quantas chaves secretas seriam necessárias para você se comunicar com todos os seus amigos).

A criptografia de chaves assimétricas, apesar de possuir um processamento mais lento que a de chave simétrica, resolve estes problemas visto que facilita o gerenciamento (pois não requer que se mantenha uma chave secreta com cada um que desejar se comunicar) e dispensa a necessidade de um canal de comunicação seguro para o compartilhamento de chaves.

Para aproveitar as vantagens de cada um destes métodos, o ideal é o uso combinado de ambos, onde a criptografia de chave simétrica é usada para a codificação da informação e a criptografia de chaves assimétricas é utilizada para o compartilhamento da chave secreta (neste caso, também chamada de chave de sessão). Este uso combinado é o que é utilizado pelos navegadores Web e programas leitores de *e-mails*. Exemplos de uso deste método combinado são: SSL, PGP e S/MIME.

Assinatura digital

A assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada.

A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isto. A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

Para contornar a baixa eficiência característica da criptografia de chaves assimétricas, a codificação é feita sobre o *hash* e não sobre o conteúdo em si, pois é mais rápido codificar o *hash* (que possui tamanho fixo e reduzido) do que a informação toda.

FONTE: Disponível em: <<http://cartilha.cert.br/criptografia/>>. Acesso em 06 abr. 2016.

RESUMO DO TÓPICO 3

Neste tópico você viu que:

- As redes sem fio trouxeram muita mobilidade para as redes, permitindo conexões móveis dentro da organização ou residência, por exemplo.
- A implantação das redes sem fio, em sua maioria, é bastante simples graças aos equipamentos oferecidos que possuem uma interface gráfica de configuração muito amigável, sendo fácil o seu entendimento.
- Com esta nova topologia de rede, algumas preocupações com segurança da informação vieram à tona. Tais preocupações são justificáveis, pois com uma rede sem fio não existe a possibilidade de delimitação específica da área de cobertura da rede, fazendo com que ela acabe por sair das dependências da organização ou residência, se tornando alvo fácil para possíveis invasões.
- As principais formas de segurança de rede sem fio mais acessíveis aos usuários são: criptografia, controle de acesso por MAC e ocultação de rede.
- Os parâmetros de segurança oferecidos pelos comutadores de rede sem fio não garantem a segurança totalmente, porém, resolvem pequenos problemas quanto a conexões indevidas.
- Para atingir um índice de segurança elevado em uma rede sem fio é necessário realizar uma mescla de várias tecnologias voltadas para segurança de redes.
- Desenvolver uma estratégia de segurança é algo fundamental para proteger uma rede.
- Monitorar e auditar as premissas de segurança da rede periodicamente é algo de suma importância para garantir a segurança da informação.

AUTOATIVIDADE



Prezado(a) acadêmico(a), vamos praticar!

- 1 Que tipo de rede sem fio possui uma taxa de transferência de dados de até 11 Mbps, que é suficiente para a maioria das redes residenciais com acesso à Internet por cabo de banda larga ou por DSL, e opera na faixa de frequência de 2,4 GHz?
 - a) () a.
 - b) () b.
 - c) () g.
 - d) () j.
 - e) () n.
- 2 Qual é o padrão definido pela IEEE para as redes sem fio?
 - a) () 802.3
 - b) () 802.5
 - c) () 802.9
 - d) () 802.11
 - e) () 802.6
- 3 Qual equipamento deve ser utilizado para ligar computadores (ou *notebooks*) com placas de rede sem fio em uma rede cabeada?
 - a) () *Hub*
 - b) () Ponte
 - c) () Roteador
 - d) () *Access Point*
 - e) () *Switch*
- 4 Qual dos seguintes não é um protocolo de criptografia utilizado nas redes sem fio?
 - a) () WEP
 - b) () TCP
 - c) () WPA
 - d) () WEP - TKIP
 - e) () WPA2

NOÇÕES DE GERENCIAMENTO DE REDES

1 INTRODUÇÃO

Por se tratar de uma estrutura complexa, as redes de computadores necessitam de um acompanhamento constante, para assim minimizar problemas com indisponibilidade, lentidão e gargalos na rede.

Este acompanhamento de rede é conhecido como gerenciamento de rede. Ele consiste em realizar o acompanhamento de todos os ativos existentes dentro do ambiente, conhecendo suas características técnicas, funcionalidades, aplicabilidade e performance.

Além dos *hardwares* e *softwares* existentes dentro da rede, é tarefa do gerenciamento de rede compreender e conhecer todos os tipos de informações que circulam dentro da sua rede, e, consequentemente, reconhecer o volume total de dados que circula em seu ambiente, seus horários de maior utilização, para que desta forma se possa realizar um dimensionamento correto dos componentes que formam a sua rede com a intenção de prevenir possíveis problemas.

Em resumo, o gerenciamento de rede consiste em acompanhar todas as estruturas de rede para que se possa agir preventivamente para evitar interrupções na rede.

2 VISÃO GERAL

Uma rede de computadores consiste na junção de *hardware*, como computadores, roteadores e outros dispositivos físicos, e *softwares* interagindo entre si, dando origem aos enlaces. Porém, não podemos esquecer dos protocolos, já mencionados anteriormente, existentes dentro dos *softwares*, que fazem com que toda essa desordem de informação seja compreendida e traduzida ao usuário final.

Essa junção de componentes dá origem às redes de computadores. Pensando dessa forma, quanto mais componentes envolvidos em nosso ambiente, maior é a amplitude e magnitude da rede existente. Assim, a probabilidade de problemas ou falhas dentro desse ambiente acaba se tornando algo preocupante, preocupação esta que acaba por desencadear a necessidade da existência de um profissional altamente qualificado e capaz de entender a complexidade do ambiente para tratar e monitorar o mesmo, visando evitar possíveis problemas iminentes e futuros trazidos por uma parada não programada nos meios de comunicação. Esta demanda fez surgir o administrador de redes.

A primeira intervenção de um administrador de rede foi vista durante a década de 80, quando as redes de computadores davam os seus primeiros passos. Esta primeira rede de computadores, que ficou conhecida na história como ARPANET, foi desenvolvida e construída baseada em experimentos. Dessa maneira, não existia nenhum *expert* no assunto, e o mesmo foi caracterizado por diversos problemas e falhas, sendo que o mais grave aconteceu no dia 27 de outubro de 1981, quando a rede em questão deixou de funcionar.

Este momento foi crucial para o surgimento do conceito de administração de redes, pois até aquele momento, nenhum componente, *software* ou *hardware* era controlado ou acompanhado. Assim, o período de interrupção do serviço acabou sendo longo, pois não foi possível realizar um diagnóstico rápido do que havia acontecido. Somente horas depois que o problema em questão (um erro de comunicação entre protocolos de rede) foi encontrado, pôde ser tratado e resolvido pelos profissionais envolvidos.

Assim, foi definido que um administrador de rede tem por dever monitorar, administrar e controlar cada componente existente dentro do seu ambiente computacional, com a intenção de prever incidentes e minimizar possíveis interrupções de serviço.

Um administrador de rede deve ter em mente que o seu trabalho de gestão impacta diretamente no cotidiano de todas as pessoas que o cercam, pois caso seu trabalho não seja realizado de maneira eficiente, vários pontos de rede (nós) podem ficar sem comunicação e assim vários usuários perderão sua conectividade. Quando levamos esse pensamento ao meio corporativo, a associação se torna mais fácil, pois uma empresa sem conectividade nos dias atuais ficará totalmente incomunicável, elevando consideravelmente os índices negativos da organização.

Baseado neste cenário de suma criticidade em que um administrador de rede vive, de acordo com Kurose (2010), a ISSO (*International Organization for Standardization*) desenvolveu um modelo de gerenciamento de rede que consiste em:

- Gerenciamento de Desempenho → Possui a função de medir, quantificar, informar, analisar e controlar o desempenho principalmente de enlaces, como, por exemplo roteador e terminal.

- Gerenciamento de Falhas → Registra, detecta e reage às condições de falhas na rede. Realiza o tratamento imediato das falhas que surgem na rede.
- Gerenciamento de Configuração → Permite que o administrador conheça todo os dispositivos da sua rede e quais suas configurações de *hardware* e *software*.
- Gerenciamento de Contabilização → Registra e controla o acesso de usuários e dispositivos aos recursos da rede. Trabalhando, por exemplo, com quotas de utilização, cobrança por utilização.
- Gerenciamento de Segurança → Controla o acesso aos recursos da rede conforme uma política definida.

Desta maneira, percebe-se que cada ativo existente dentro de uma rede é de suma importância para o bom desempenho da rede como um todo. Assim, cada nó deve ser devidamente acompanhado e monitorado.

O administrador de rede deve conhecer a fundo cada *hardware* envolvido no seu ambiente, sua capacidade, seus benefícios e também suas deficiências e limitações para, assim, realizar o dimensionamento correto de cada equipamento envolvido na sua rede de comunicação.

Para auxiliar o administrador de rede em suas tarefas, existem diversas ferramentas de redes, porém, as ferramentas não irão realizar o trabalho do administrador. Elas servem de base para a tomada de decisões e ações dentro de um determinado ambiente que está sendo monitorado. As ferramentas sozinhas não resolvem os problemas de falhas ou interrupções de serviços. Um conjunto de ferramentas ajuda, e muito, um administrador, mas o mesmo deve saber como e onde aplicá-las para alcançar os índices máximos de eficiência e eficácia no seu ambiente computacional.

3 SOFTWARES DE GERENCIAMENTO

Como já visto nesta unidade, os *softwares* de gestão de rede, sozinhos, não são a solução para todos os problemas de redes de computadores existentes, sem mencionar que a grande maioria destes *softwares* de gestão possui um alto custo de implantação. Este custo elevado se deve a três fatores:

- *Hardware*
- *Software*
- Treinamento

O custo de implantação ao adquirir uma determinada ferramenta de rede ou um conjunto de ferramentas deve ser justificado, ou seja, devem ser demonstrados os benefícios que tal pacote de ferramentas irá trazer ao seu ambiente.

Para tanto é necessário justificar tais investimentos, esclarecendo que os mesmos são capazes de minimizar e até prevenir possíveis interrupções na rede, ou de terminal, não deixando funcionários ociosos, ou deixando de entregar algum tipo de mercadoria, ou algum cliente sem atendimento. Tais fatos que podem acarretar grandes prejuízos financeiros e mercadológicos para a empresa.

Este dimensionamento deve ser feito baseado no lucro obtido por hora pela empresa e comparado com os possíveis problemas e falhas que cada equipamento parado dentro da rede pode vir a causar, além do seu prazo para reparo.

Os *softwares* de gerenciamento de rede são subdivididos em passivo e ativo quanto aos seus procedimentos de reconhecimento de ambiente. Os *softwares* passivos são ferramentas que realizam somente o monitoramento da infraestrutura a partir de uma configuração de ambiente e *hosts* pré-configurados pelo usuário, ou seja, ele não possui a capacidade de reconhecimento do que está ao seu redor.

Já as ferramentas que são consideradas como ativas não necessitam necessariamente que o usuário ou administrador informe os *hosts* existentes dentro do ambiente. Ele por si só realiza um mapeamento, identificando todos os dispositivos e, consequentemente, todos os serviços de rede oferecidos por cada *host*, para que possa vir a monitorar cada um deles de forma correta, e desta maneira, os relatórios possam ser mais precisos possíveis.

Essa *idCrase* => identificação de rede automatizada é popularmente conhecida como descoberta de rede. Não necessariamente ao realizar uma descoberta de rede os *hosts* irão ser alocados de maneira correta em relação ao seu local físico, pois muitas vezes o *software* não consegue realizar o mapeamento lógico correto em relação às sub-redes existentes ou, até mesmo, aos *hubs* ou *switches* que realizam as interações entre *hosts* e redes. Dessa maneira, essa descoberta de rede pode gerar alguns transtornos para o usuário em nível organizacional no seu sistema de gerenciamento.

O monitoramento realizado dentro de uma rede consiste na observação das informações coletadas pelas ferramentas de gerenciamento. Estas informações podem ser divididas em três categorias:

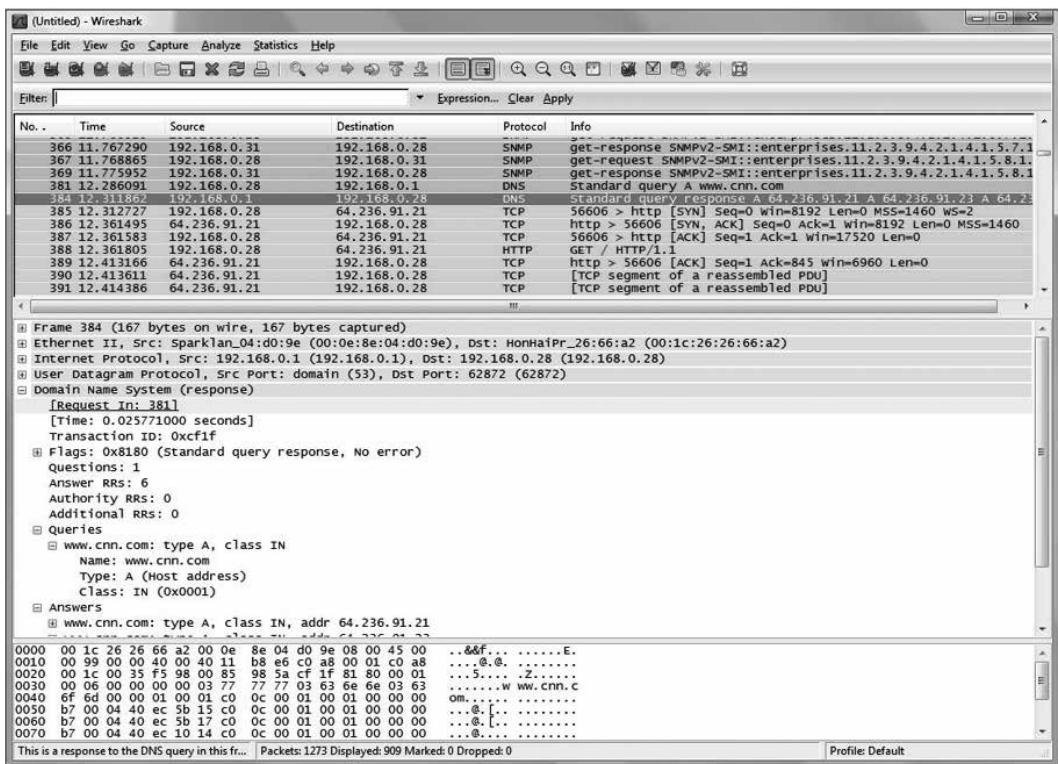
- Informações Estáticas → caracterizam os elementos na atual configuração, como o número e identificação das portas em um roteador;
- Informações Dinâmicas → relacionadas aos eventos na rede, como a transmissão de um pacote;
- Informações Estatísticas → podem ser derivadas de informações dinâmicas como a média de pacotes transmitidos por unidade de tempo em um determinado sistema.

As ferramentas de gerenciamento de rede têm evoluído com o passar dos anos, e cada ferramenta se especializou em uma determinada área de gerência. Sendo assim, elas foram classificadas da seguinte maneira:

- Analisadores de protocolos
- Geradores de gráficos
- Gerenciamento de falhas
- Gerenciamento de configuração
- Gerenciamento de segurança

Os analisadores de protocolos são ferramentas que observam o tráfego de informação dentro da rede em que estes *softwares* estão conectados. Ao utilizar aplicações desse tipo, a interface de rede do dispositivo passa a capturar todos os pacotes que estão circulando dentro da rede. Desta maneira, todos os pacotes válidos ou *broadcast* existentes dentro do meio físico de comunicação serão interceptados por esse *host* e analisados pela aplicação. Como pode ser observado na Figura 70.

FIGURA 70 - WIRESHARK



FONTE: O autor

Na imagem é possível perceber todos os pacotes que estão circulando dentro da rede. A própria aplicação já realiza um pré-agrupamento dos dados baseado no seu protocolo de comunicação, com a finalidade de auxiliar o administrador de rede no momento da interpretação dos dados colhidos pela ferramenta.

Essa manipulação de dados é popularmente conhecida como “escovar *bits*”, pois o administrador está colhendo pacotes dentro da rede, os quais são formados somente por *bits* e, dessa maneira, precisa tratar os dados colhidos para que os mesmos venham a ser úteis.

Ao utilizar um analisador de protocolos, o administrador pode medir seu tráfego de rede médio, para que seus usuários estão utilizando a rede, quais *hosts* estão realizando maior movimentação de informações no momento, entre outras funcionalidades. Baseado nestas informações é possível tomar decisões administrativas com a intenção de expansão de rede, bloqueios de conteúdo e formas de garantir a segurança da informação, por exemplo.

Estes analisadores são importantes ferramentas de gestão, pois através delas o administrador de rede tem total conhecimento do que está acontecendo dentro de sua rede e a partir daí pode tomar decisões para correções de problemas e ações preventivas para antecipar e minimizar possíveis problemas futuros.

Um analisador de protocolos somente pode ser utilizado se o mesmo estiver conectado diretamente à rede que se deseja *sniffar* (capturar os pacotes), não é possível realizar qualquer forma de captura sem que o *host* que irá colher os dados esteja fisicamente na mesma rede dos demais *hosts* envolvidos no processo.

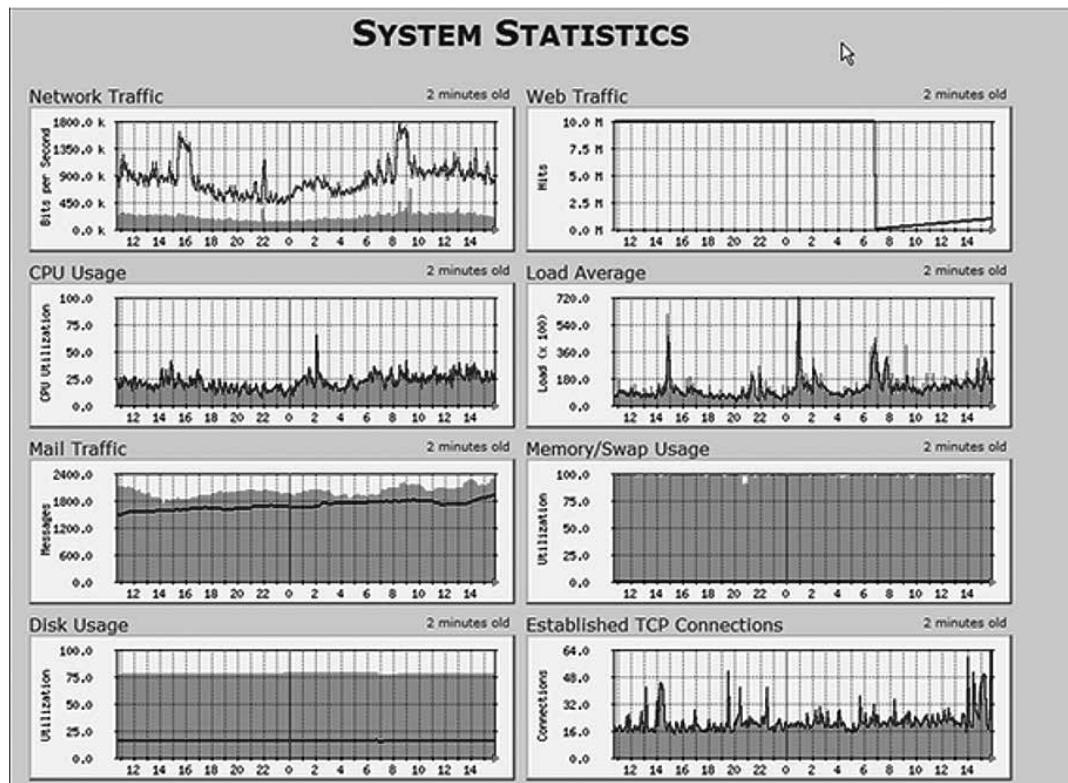
Um *software* bastante usado é o *Wireshark*, mas existem outras ferramentas similares, como TCPDUMP e IPTRAF, entre outras. A maioria destas ferramentas está disponível para *download* de forma gratuita.

Geradores de gráficos ou analisadores de tráfego são ferramentas baseadas em coletas de dados (tráfego de informação), então, para fazer uso de uma destas ferramentas é necessário possuir algum *software* que realize a captura das informações e armazene estes dados em arquivos de texto, os chamados *logs*.

Os *logs* são muito comuns, a grande maioria das aplicações existentes no mercado tem como forma de segurança a criação destes *logs*, que nada mais são do que um espaço ou um arquivo onde a aplicação armazena tudo o que está acontecendo durante o seu funcionamento, desde problemas internos com a aplicação até movimentações e ações realizadas pelo usuário da aplicação.

Os geradores de gráfico são ferramentas que irão colher as informações destes *logs* das aplicações e criará um modelo de apresentação para estas informações, como é possível ver na Figura 71.

FIGURA 71 - MRTG



FONTE: O autor

A imagem é um exemplo prático de uma aplicação geradora de gráfico. Neste exemplo foi utilizado o *software* MRTG, que realiza o monitoramento das interfaces de rede e do processador para montar seus gráficos, e, assim, ajudar o administrador de rede a entender como estão os seus *hosts* de rede em cada momento do dia.

Outro exemplo de aplicação deste tipo é o SARG, como pode ser observado na figura:

FIGURA 72 - SARG

Squid User Access Report									
Period: 2009May19-2009May19									
Sort: BYTES, reverse									
Topuser									
Topsites									
Sites & Users									
Downloads									
Denied									
NUM	USERID	CONNECT	BYTES	% BYTES	IN-CACHE-OUT	ELAPSED TIME	MILISEC	%TIME	
1	bilao	5.95K	149.79M	35.36%	5.09%	94.91%	03:54:12	14.052.500	24.17%
2	zezinho	2.14K	139.28M	32.88%	0.17%	99.83%	02:51:09	10.269.369	17.67%
3	192.168.0.4	1.49K	28.92M	6.83%	3.17%	96.83%	00:34:06	2.046.091	3.52%
4	marconi	1.70K	24.42M	5.77%	0.76%	99.24%	01:09:36	4.176.805	7.19%
5	leon	2.43K	15.67M	3.70%	8.70%	91.30%	02:11:48	7.908.609	13.61%
6	wallace	1.45K	14.15M	3.34%	1.96%	98.04%	01:01:20	3.680.183	6.33%
7	laercio	2.19K	14.00M	3.31%	11.96%	88.04%	02:11:00	7.860.662	13.52%
8	renato	1.99K	11.89M	2.81%	2.06%	97.94%	00:50:37	3.037.098	5.22%
9	bebe	776	7.07M	1.67%	9.91%	90.09%	00:34:21	2.061.239	3.55%
10	joelma	309	6.42M	1.52%	0.02%	99.98%	00:13:39	819.041	1.41%
11	drecio	568	3.99M	0.94%	8.80%	91.20%	00:11:25	685.607	1.18%
12	angel-guga	79	3.00M	0.71%	0.02%	99.98%	00:07:27	447.675	0.77%
13	mida	35	2.85M	0.67%	0.03%	99.97%	00:05:43	343.154	0.59%
14	zeca	34	1.09M	0.26%	0.00%	100.00%	00:01:14	74.820	0.13%
15	fofa	279	992.42K	0.23%	4.76%	95.24%	00:11:05	665.745	1.15%
TOTAL		21.45K	423.58M		3.22%	96.78%	16:08:48	58.128.598	
AVERAGE		1.43K	28.23M				01:04:35	3.875.239	

FONTE: O autor

O SARG é uma aplicação utilizada em conjunto com ferramentas de PROXY. Ele é responsável por criar os relatórios de acessos de volume de dados que estão circulando pelo Proxy. Porém, o SARG sozinho não faz nada, para que ele opere de forma correta, a aplicação de Proxy precisa estar em perfeito funcionamento e armazenando as informações coletadas no *log* da aplicação. Somente depois da alimentação do *log* é que o SARG entra em ação.



O Proxy é um computador que funciona como intermediário entre um navegador da Web (como o Internet Explorer) e a Internet. Os servidores proxy ajudam a melhorar o desempenho na Web armazenando uma cópia das páginas da Web utilizadas com mais frequência. Quando um navegador solicita uma página que está armazenada na coleção do servidor proxy (o cache), ela é disponibilizada pelo servidor proxy, o que é mais rápido do que acessar a Web. Os servidores proxy também ajudam a melhorar a segurança, porque filtram alguns tipos de conteúdo da Web e softwares mal-intencionados.

FONTE: <http://windows.microsoft.com/pt-br/windows-vista/what-is-a-proxy-server>.
Acessado em 07.abr 2016

Neste momento a aplicação geradora de gráficos acessa o arquivo de *logs* da aplicação parceira e monta a sua base de dados para gerar seus gráficos. Todo esse processo é realizado sem efetuar nenhuma alteração no arquivo de *logs* da aplicação principal. Este modelo de ferramenta tem por finalidade demonstrar em um formato mais amigável o que está acontecendo com a rede durante determinado período.

Todos os gráficos podem ser gerados de acordo com a preferência do gestor de rede, ou seja, tendo um tempo de atualização maior ou menor de acordo com a criticidade do ambiente em questão.

Caso o administrador prefira manipular o arquivo de *logs* ele mesmo, sem a interação com um grafador, também é possível, porém a interpretação das informações se torna algo muito trabalhoso. Isso porque encontraremos nos *logs* somente linhas de texto, e, certamente, no momento de apresentação dos dados para outras pessoas envolvidas no processo de gerência, será muito mais complexa a explicação do que está acontecendo no ambiente.

As ferramentas de gerência de falhas são muito parecidas com as ferramentas geradoras de gráficos, pois elas também vêm a trabalhar baseadas nos *logs* das aplicações. A diferença, neste caso, é que os *logs* analisados pelas ferramentas de gerência de falhas são os *logs* de funcionamento das aplicações e não os *logs* de utilização da aplicação ou das informações que esta aplicação está manipulando.

Estas ferramentas tratam com os *logs* que todos os softwares possuem, que são seus arquivos e registros de funcionamento. Estes registros são armazenados localmente ou remotamente conforme configuração realizada pelo administrador da aplicação. Estes registros armazenam todo o funcionamento e anomalias dentro das aplicações, dessa maneira estas ferramentas de gerência de falhas fazem o trabalho de interpretar estas informações geradas pelas aplicações e transformá-las em alertas ou alarmes para que o gestor possa identificar o problema o mais rapidamente possível, e assim tomar as atitudes para resolução do mesmo.

O gerenciamento de falhas não possui somente a função de mostrar as falhas que causaram a interrupção em uma determinada aplicação, mas também devem ter um caráter preventivo, ou seja, gerar alarmes baseados em pequenas anomalias no sistema com a finalidade de prevenir problemas e assim ser um agente minimizador de impacto dentro do ambiente computacional em que está inserido.

Prevenir problemas acaba se tornando sua função mais importante, pois assim é possível evitar interrupções nas aplicações e serviços prestados pelo ambiente computacional envolvido, como ilustrado pela Figura 73:

FIGURA 73 - SYSLOG

The screenshot shows the Syslog Watcher application interface. The main window displays a table of log messages with columns: Received, Source IP, Facility, Severity, Tag, and Message. A message in the table is highlighted, showing the timestamp (03/20/2008 19:25:03), source IP (192.168.1.1), facility (user-level), severity (Info), tag (kernel), and message content ("NET: Registered pro..."). The left panel contains a sidebar with various logs and a detailed view of the selected message, including its source IP (192.168.1.35) and host name (MECOM). The bottom status bar indicates "Status: Listening" and "Vendor Pack: Active".

Received	Source IP	Facility	Severity	Tag	Message
03/20/2008 19:25:03	192.168.1.1	user-level	Info	kernel	Initializing IPsec netli...
03/20/2008 19:25:03	192.168.1.1	user-level	Debug	syslog	tftpd
03/20/2008 19:25:03	192.168.1.1	user-level	Info	kernel	TCP: Hash tables co...
03/20/2008 19:25:03	192.168.1.1	user-level	Debug	syslog	bftpd
03/20/2008 19:25:03	192.168.1.1	user-level	Info	kernel	IP: routing cache has...
03/20/2008 19:25:03	192.168.1.1	user-level	Debug	kernel	PCI: Setting latency t...
03/20/2008 19:25:03	192.168.1.1	user-level	Info	kernel	NET: Registered prot...
03/20/2008 19:25:03	192.168.1.1	user-level	Debug	syslog	sntp -s time.window...
03/20/2008 19:25:03	192.168.1.1	user-level	Info	kernel	NET: Registered prot...
03/20/2008 19:25:03	192.168.1.1	user-level	Info	kernel	PPP generic driver ve...
03/20/2008 19:25:03	192.168.1.1	user-level	Info	kernel	Initializing Cryptogra...
03/20/2008 19:25:03	192.168.1.1	user-level	Info	kernel	NET: Registered pro...
03/20/2008 19:25:03	192.168.1.1	user-level	Info	kernel	Memory: 13948K/160...
03/20/2008 19:25:03	192.168.1.1	user-level	Notice	kernel	Ebttables v2.0 register...
03/20/2008 19:25:03	192.168.1.1	user-level	Critical	kernel	ADSL G.992 channel ...
03/20/2008 19:25:03	192.168.1.1	user-level	Critical	kernel	ADSL G.992 started
03/20/2008 19:25:03	192.168.1.1	user-level	Critical	kernel	ADSL G.994 training
03/20/2008 19:24:22	192.168.1.1	user-level	Debug	syslog	kill -9 521

FONTE: O autor

Atualmente no mercado existem muitas ferramentas com estas funcionalidades, tais como: SYSLOG, SYSMON, Nedi, MON e SNIPS.

O gerenciamento de configuração tem por objetivo facilitar a vida do administrador de rede na gestão das configurações efetuadas em cada ativo de rede. Estas aplicações agregam aos ativos interfaces gráficas de fácil manipulação para realizar suas configurações, deixando de lado os *promptps* de comando utilizados ainda hoje por muitos gestores.

Outro ponto fundamental destas aplicações é a sua possibilidade de integração com outras aplicações, com a intenção de agilizar o processo de configuração e restauração de serviços danificados. Esta recuperação é baseada em arquivos de *backup* efetuados pela ferramenta anteriormente citada com a intenção de poupar tempo em momentos de alta criticidade, onde o ambiente computacional está parado devido a um erro de configuração efetuado na rede, ou até mesmo uma falha de um ativo, onde o mesmo está sendo substituído e precisa ser totalmente reconfigurado.

O gerenciamento de configuração também agrupa a ideia de padronização de configurações em um mesmo ambiente, para tanto, o administrador de rede deve ter amplo conhecimento de seus ativos, para que possa vir a utilizar o melhor de cada um em seu ambiente computacional. Uma aplicação de gestão de configuração irá ajudar, porém não realizará as configurações de forma automática ou dirá qual a melhor estratégia para cada ambiente. Sendo assim, parte do administrador a iniciativa de definir a melhor abordagem para cada local e a disposição desses *hardwares* dentro do ambiente.

Somente com uma boa gestão é que a aplicação trará bons resultados ao ambiente. Sem conhecimento adquirido sobre o porquê de cada ativo e suas funcionalidades do ambiente, a aplicação não responderá de forma esperada.

Atualmente existem diversas ferramentas de gestão de configuração no mercado, muitas delas pagas e outras sem custo de implantação. Destacam-se: WEBMIN, CACIC, IPPLAN, METCHE, entre outras.

Na figura a seguir pode-se ver uma imagem do WEBMIN, onde é possível observar sua complexidade e a gama de ferramentas e possibilidades de gestão que o mesmo oferece:

FIGURA 74 - WEBMIN



FONTE: O autor

O WEBMIN é uma das ferramentas mais importantes no sentido de gestão de configuração para ambientes Linux. Através dessa porta de comunicação criada pela ferramenta é possível realizar a gestão completa do *hardware* que dá suporte ao sistema operacional, configurar todo o sistema operacional e, consequentemente, todas as aplicações existentes dentro dessa máquina. Em resumo, é uma ferramenta de suma importância para acompanhar o bom andamento da máquina em questão e que traz uma grande facilidade para o administrador de rede no momento de qualquer ajuste ou nova configuração no ambiente.

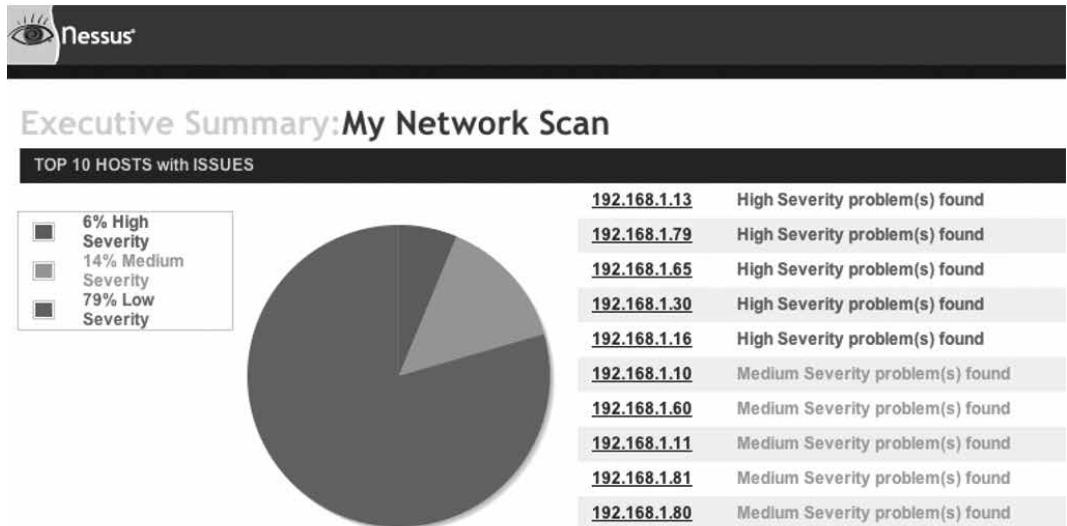
O gerenciamento de segurança é um conjunto de aplicações que visa trazer aos administradores de rede formas eficientes de proteção e de auditoria dos seus sistemas computacionais.

Nos dias atuais, a segurança vem se tornando algo fundamental para qualquer meio computacional, então a rede de computadores precisa de uma atenção muito especial, pois é ela que dará sustentabilidade a todos os outros serviços existentes. Se a rede não oferecer um mínimo de segurança, todo o ambiente computacional estará comprometido, mesmo tendo uma aplicação (sistema) eficiente, pois a informação estará vulnerável sempre que entrar em contato com a rede, e todos os *hosts* estarão expostos, pois estarão interconectados.

Assim, a gerência de segurança visa identificar e corrigir problemas existentes no meio computacional da organização e prever possíveis problemas. Podemos citar o NMAP, NESSUS e SNORT como exemplos de ferramentas

destinadas à gerência de segurança. Na figura a seguir é possível observar o NESSUS, uma importante ferramenta de identificação de vulnerabilidades.

FIGURA 75 - NESSUS



FONTE: O autor

Através destas aplicações destinadas à gerência de segurança é possível realizar varreduras nos sistemas existentes dentro da organização identificando portas de comunicações expostas, as quais poderiam vir a se tornar uma forma de invasão ao ambiente, além de sistemas e versões de sistemas utilizados pela organização. Mas por que identificar os sistemas ou versões dos sistemas utilizados é algo tão importante? É através desta identificação que um possível invasor dará início ao seu trabalho, identificando os sistemas computacionais que estão em operação e suas versões. É possível realizar outras varreduras buscando as falhas ou *bugs* existentes dentro destas aplicações e, assim, um possível invasor acaba por encontrar um alvo fácil para seus ataques.

Do mesmo jeito que estas ferramentas podem e são utilizadas para disseminar o mal dentro das redes de computadores, ou seja, com a intenção de invadir sistemas, elas também são utilizadas para garantir e aumentar cada vez mais a segurança dos ambientes. O processo é o mesmo utilizado por um atacante, porém os problemas ou fragilidades encontradas no ambiente serão catalogadas e corrigidas para que nenhuma pessoa venha a explorar essas vulnerabilidades encontradas no ambiente.

Ninguém está livre de falhas de sistema ou qualquer outra eventualidade dentro de um ambiente computacional. Quando se fala em segurança é algo que sempre demanda muito cuidado e atenção por parte dos usuários e do administrador de redes. Estas ferramentas servem como uma forma de auditoria para a organização, para levantar as fragilidades dos sistemas e do ambiente, porém não realizam o reparo de forma autônoma. É preciso que o gestor de rede

entenda o ambiente e, baseado nas fragilidades identificadas, desenvolva políticas e estratégias para correção dos problemas. Só assim as ferramentas serão úteis, caso contrário elas não passarão de aplicações comuns.

Um bom administrador de redes deve estar cercado de boas aplicações para facilitar o seu trabalho e lhe dar mais agilidade nas identificações dos problemas e soluções, mas cabe lembrar que o conhecimento e estratégias partem do gestor e não das aplicações, tornando-as parte da engrenagem na administração da rede e não a máquina como um todo. Um administrador de rede sobrevive sem aplicações para lhe auxiliar, porém uma rede não sobrevive somente com aplicações de gestão sem um gerente.

4 MONITORAMENTO E CONTROLE

O monitoramento e controle de recursos dentro das redes de computadores é algo importantíssimo para o meio computacional. Dessa maneira, pode-se conceituar estes itens como:

Monitorar → Analisar, registrar e observar as principais operações quando se faz o monitoramento de qualquer coisa. Saber como determinado equipamento se comporta em determinadas situações e, o mais importante, saber o que acompanhar. O gerente deve ter bem esclarecido quais as suas metas quanto ao acompanhamento da rede, saber quais seus pontos críticos e quais são as informações e equipamentos ou protocolos mais importantes para o andamento normal da sua estrutura.

Controle → Agir, modificar e decidir. Neste momento o gerente deve tomar as decisões e executá-las, com o intuito de recuperar os serviços danificados ou até mesmo realizar as janelas de manutenção preventivas de equipamentos e *softwares*.

5 PROTOCOLOS DE GERENCIAMENTO

Vimos até o momento o que é e para que serve a ideia de administração de redes. Agora, vamos entender como este sistema funciona e quais as melhores formas de coletar dados dentro destes ambientes.

No capítulo anterior estudamos os conceitos de protocolos de rede, onde um protocolo são as regras ou normas para estabelecer uma comunicação entre dois ou mais *hosts* dentro de uma rede. Na gestão das redes de computadores também existem dois protocolos que se destacam como formas muito eficientes para monitoramento e controle do ambiente. Estes dois protocolos são o SNMP e ICMP.

5.1 SNMP

O protocolo de rede denominado de SNMP (*Simple Network Management Protocol*) surgiu durante a década de 80 e foi desenvolvido pela IETF (*Internet Engineering Task Force*) com o objetivo de disponibilizar uma forma simples e prática de realizar o gerenciamento e controle dos ativos de redes.

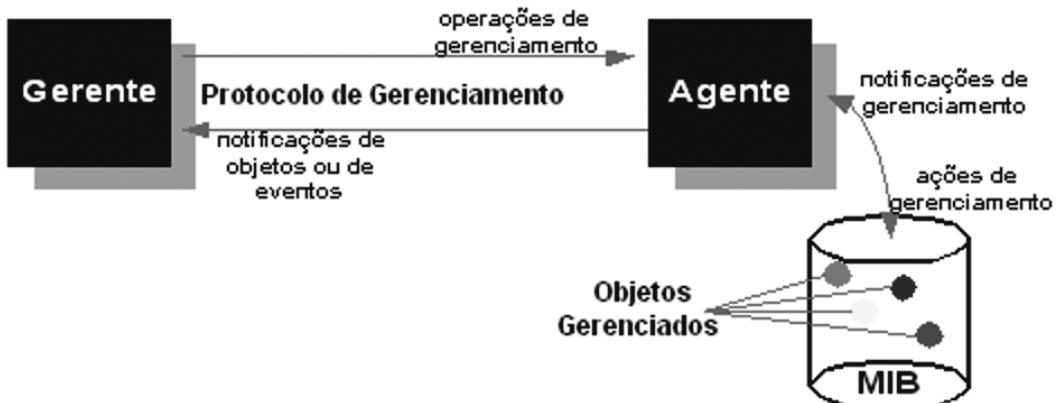
Somente em 1988 o SNMP foi publicado e disseminado no mercado. Este protocolo prevê um conjunto de operações simples que acabam por permitir o gerenciamento por completo de qualquer ativo de rede que suporte o mesmo. Desta forma, é possível acompanhar e controlar, por exemplo, a negociação de uma interface de rede, o volume de tráfego que está passando pela interface de rede, o uso de um processador ou memória, e assim por diante. Este protocolo de monitoramento abriu um leque enorme de possibilidades quando se refere à gerência dos ativos e seus desempenhos.

Em resumo, a utilização do SNMP e seu aprimoramento têm por finalidade alcançar a utilização máxima da rede, ou seja, fazer com que cada equipamento envolvido no ambiente computacional alcance o seu máximo em performance e eficiência para que, assim, possa-se tirar de cada equipamento o seu melhor.

O funcionamento do SNMP é baseado em agente e gerente, onde o agente fica localizado no *host* que será monitorado e o gerente no local onde estará funcionando a aplicação de monitoramento do ativo.

O agente é formado pela MIB (*Management Information Base*), a qual é composta por objetos, como pode ser observado na Figura 76:

FIGURA 76 - FUNCIONAMENTO DO SNMP



FONTE: Disponível em: <<http://aldembergmarinho.blogspot.com.br>>. Acesso em: 10 jan. 2016.

Os objetos que compõem a MIB são os componentes que serão monitorados dentro do agente. Interfaces de rede, processador e HD, por exemplo, são objetos ou partes de um agente que geram informações sobre os seus *status* de funcionamento e condições para que as mesmas sejam reportadas aos gerentes.

A MIB é a construção de uma base de dados dos objetos. Desta maneira, toda a informação colhida dos objetos fica armazenada nesta grande base de informações que é a MIB, à espera de uma solicitação por parte do gerente sobre determinado objeto. Esta memória de armazenamento ou base de dados não é segura nem estática, pois caso o dispositivo em questão seja reiniciado, por exemplo, todos os dados colhidos até o momento serão perdidos. Todos os objetos geram informações constantemente, e estas informações dentro da MIB também são sobrepostas, não havendo possibilidade de recuperação de algum determinado dado anterior. Lembrando que qualquer recuperação de informação de um determinado período só pode ser realizada pela aplicação de gerência, pois a mesma cria suas bases de informações, não voltando assim na MIB para buscar informações passadas.

Esta base de informação que é a MIB, segundo Comer (2005, p. 407) pode ser dividida em três categorias:

- MIB II → fornece informações gerais sobre um determinado equipamento. Ex.: estado da interface, quantidade de pacotes transmitidos, entre outras.
- MIB Experimental → são aquelas em que os equipamentos estão em desenvolvimento ou teste. Elas fornecem informações mais específicas sobre os meios de transmissão e equipamentos empregados.
- MIB privada → é possível desligar interface, saber sobre colisões de pacotes e até reiniciar os equipamentos.

Tendo um agente instalado dentro de um dispositivo, o gerente que deve estar localizado no *hardware* fará o monitoramento da rede junto à aplicação, irá realizar uma solicitação de determinada informação sobre o dispositivo em questão. Esta solicitação e a resposta por parte do dispositivo utilizam o protocolo de transmissão de rede UDP, que é utilizado por dois motivos básicos, sendo o primeiro sua grande velocidade para transmissão de dados dentro de uma rede de comunicação; e outro ponto fundamental, a sua propriedade de utilização em *real time*, ou seja, caso haja qualquer problema durante determinada transmissão de algum dado e o mesmo não tenha alcançado o seu destino, o mesmo é ignorado pelo gerente, que passa a receber o dado seguinte. Esta propriedade faz com que o usuário não perceba que determinado pacote de informação foi perdido ou aplicação venha a falhar por falta desta informação.

Assim, ao receber uma solicitação de informação por parte do gerente, o agente localizado dentro do *host* que está sendo acompanhado interpreta esta solicitação, identificando o que foi pedido pelo gerente e busca em sua MIB a informação. Caso ela ainda não esteja armazenada, talvez por não ter sido ainda

solicitada, o agente aciona o seu objeto que dará início à transmissão dos dados para a MIB. Esta retorna ao agente o dado que será encaminhado pelo agente para o gerente localizado no *host* de monitoramento. Ao chegar no gerente, essa informação é então repassada para a aplicação que a solicitou, a qual realiza o tratamento do dado coletado e transforma o mesmo em algo palpável para o usuário final que está trabalhando com a aplicação.

Para realizar a comunicação entre gerente e agente, ambos precisam comunicar-se de maneira eficiente dentro da rede, ou seja, estarem na mesma faixa de rede ou em redes diferentes, porém que possam trocar informações entre si. Após a localização do *host* que será monitorado, ou seja, conhecer o endereço de IP do mesmo, basta realizar a sincronização das comunidades entre os dois dispositivos.

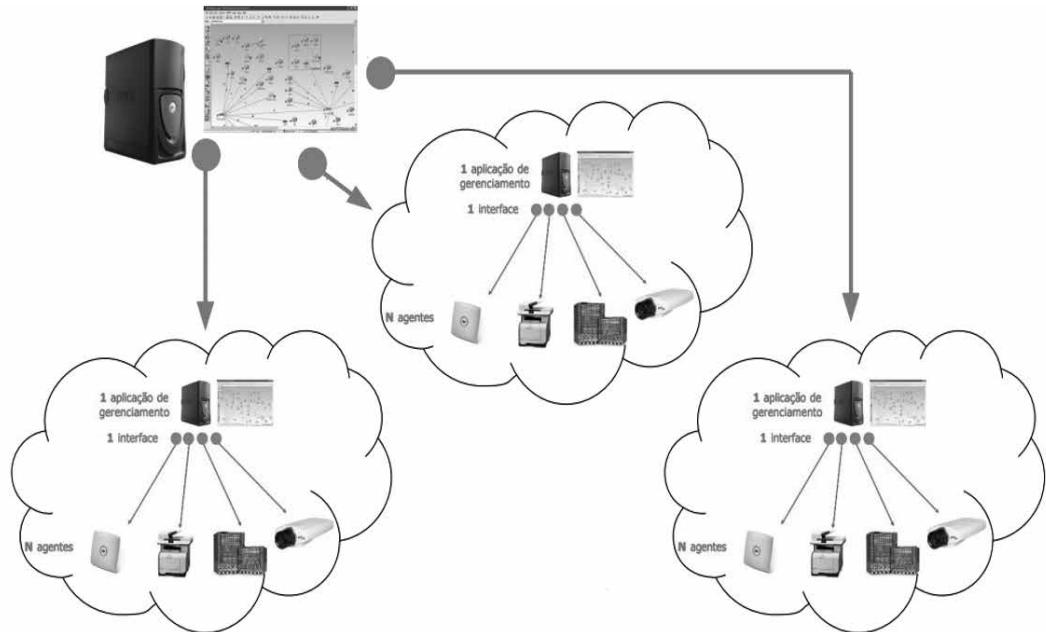
O SNMP utiliza para sua sincronização, desde o seu início, premissa de comunidade, ou seja, é necessário definir em ambos os lados o mesmo nome de comunidade. Esta nada mais é do que um grupo de trabalho escolhido pelo usuário para realizar a comunicação.

Olhando para este protocolo de forma bem superficial, suas primeiras versões possuíam grandes problemas voltados para a segurança das informações transmitidas, pois qualquer pessoal que identificasse um *host* e viesse a conhecer a comunidade de comunicação poderia colher dados do mesmo.

Pensando nesta fragilidade o SNMP evolui para versão 2 e nos últimos anos para a versão 3. Até então, nesta primeira versão era possível somente colher dados de um dispositivo sabendo a comunidade e seu endereço de rede. Na versão 2 deste mesmo protocolo foram criados os privilégios para as conexões entre agente e gerente, ou seja, já era possível definir se determinado endereço de rede poderia se conectar ao agente e se este determinado endereço teria permissão para consultar dados, ou consultar e alterar informações.

Outra evolução vinda na versão 2 foi a descentralização do gerenciamento dos dados. A partir deste momento, a ideia de múltiplos gerentes dentro de uma rede realizando o monitoramento do ambiente passou a ser algo comum. Nesta situação, existe um gerente geral que realiza a comunicação com seus subgerentes, os quais fazem a comunicação final com os agentes, como é possível observar na figura:

FIGURA 77 - SNMP, DESCENTRALIZAÇÃO DOS GERENTES



FONTE: Adaptado de <<http://snmp.com>>. – Acesso em 31 jan. 2016.

Porém, com o passar dos anos e com a evolução das conexões, percebeu-se que garantir a segurança de uma determinada informação baseada em endereços de conexões não era mais eficiente, pois ataques baseados em pacotes forjados começaram a ser cada vez mais comuns. A partir de então foi desenvolvida a versão 3 desse protocolo. Esta nova versão agrupa a questão de autenticação dos usuários para realizar o sincronismo entre agente e gerente, e passa a realizar a transmissão das informações de forma criptografada. Esta criptografia de dados tornou-se necessária, pois outra forma de ataque de captura de informações em trânsito passou a se popularizar, e assim o protocolo, por tratar de informações de suma importância para as organizações, deve adotar políticas mais eficientes ao se tratar da integridade dos dados que estão sendo transmitidos.

As mensagens utilizadas no protocolo SNMP para a comunicação entre agente e gerente não possuem campos fixos e por isso são construídas de trás para frente. A mensagem possui três principais partes, segundo Kurose (2010, p. 560): *version, community, SNMP PDU*.

- Versão do SNMP → tanto o gerente como o agente devem utilizar a mesma versão. Mensagens contendo versões diferentes são descartadas.
- Comunidade ou *community* → é utilizada para permitir acesso do gerente às MIB's.
- SNMP PDU → é o protocolo, ou seja, formato de comunicação entre agente e gerente, o protocolo utilizado entre ambos. Lembrando que este protocolo de sincronização não tem nenhum vínculo com o protocolo UDP utilizado para a transmissão dos dados, em resumo, um realiza a comunicação e o outro a transmissão.

A estrutura de gerenciamento do SNMP ou a SMI (*Structure of Management Information – SMI*) é a linguagem usada para definir as informações de gerenciamento que residem em uma unidade gerenciadora de rede. Essa linguagem é necessária para garantir a sintaxe e semântica dos dados, para que os mesmos não entrem em ambiguidade. A SMI define a linguagem de comunicação.

É através da SMI que se identificam os tipos de dados colhidos e o *status* e semântica de um objeto gerenciado.

O SNMP possui duas operações básicas (*SET* e *GET*) e suas derivações (*GET-NEXT*, *TRAP*) para realizar a comunicação com o *host* que está sendo monitorado e, assim, realizar a coleta dos dados e possíveis alterações de configuração no *host* em questão. Estas operações possuem derivações, segundo Comer (2005, p. 410), as quais são:

- A operação *SET* é utilizada para alterar o valor da variável. O agente solicita que o agente faça uma alteração no valor da variável;
- A operação *GET* é utilizada para ler o valor da variável. O gerente solicita que o agente obtenha o valor da variável;
- A operação *GET-NEXT* é utilizada para ler o valor da próxima variável. O gerente fornece o nome de uma variável e o cliente obtém o valor e o nome da próxima variável. Também é utilizado para obter valores e nomes de variáveis de uma tabela de tamanho desconhecido;
- A operação *TRAP* é utilizada para comunicar um evento. O agente comunica o gerente o acontecimento de um evento, previamente determinado. São sete tipos básicos de *TRAP* determinados:
 - o *coldStart* → a entidade que a envia foi reinicializada, indicando que a configuração do agente ou a implementação pode ter sido alterada;
 - o *warmStart* → a entidade que a envia foi reinicializada, porém a configuração do agente e a implementação não foram alteradas;
 - o *linkDown* → o enlace de comunicação foi interrompido;
 - o *linkUp* → o enlace de comunicação foi estabelecido;
 - o *authenticationFailure* → o agente recebeu uma mensagem SNMP do gerente que não foi autenticada;
 - o *egpneighborLoss* → uma EGP parou;
 - o *enterpriseSpecific* → indica a ocorrência de uma operação *TRAP* não básica.
 - o *get-response-->* obtém uma possível resposta de erro para as operações anteriores.



O EGP é um protocolo que informa a um dispositivo de rede IP como alcançar outras redes IP. Ele não informa a rota completa para a outra rede, mas ela permite que um dispositivo saiba em que direção a rede existe.

Operações de notificação de qualquer agente para o gerente no protocolo SNMP são:

- *get e set* → padronização dos protocolos
- *inform* → permite comunicação entre gerentes em nível de hierarquia.
- *Report* → reporta falhas dentro do agente ou gerente.

O grande problema do protocolo SNMP quando se trata de grandes redes é a questão do volume de informação gerada por ele. Mesmo utilizando um protocolo de transmissão de alta performance, o mesmo pode vir a comprometer determinados serviços ou *hosts* dentro da rede, pela quantidade de solicitações que terá que responder para sanar os pedidos do gerente, e isso em determinadas situações pode vir a ser um problema, consumindo o *host* ou serviço ao ponto de tirá-lo do ar.

Desta forma, devem ser muito bem avaliados os *hosts* ou serviços que serão monitorados fazendo uso deste protocolo de monitoramento, para que assim seja possível colher informações pertinentes de cada *host* sem comprometer o seu funcionamento.

5.2 ICMP

O ICMP (*Internet Control Message Protocol*) foi desenvolvido para ser um protocolo de controle, sendo que opera no nível 3 do modelo OSI. Este protocolo não é utilizado para realizar a transmissão de dados como os protocolos TCP e UDP que ocupam a camada 4 do modelo OSI. A finalidade do ICMP é realizar a comunicação de informações entre os ativos de rede, onde sua principal função é efetuar a comunicação de erros destas mensagens entre os *hosts* envolvidos.

Um exemplo dessa comunicação de erros entre *hosts* acontece ao tentar realizar uma conexão de TELNET, por exemplo, em determinado equipamento. Quando essa conexão recebe o retorno de *host* de destino inacessível, refere-se à falta de comunicação entre os dois pontos remotos e o ICMP reporta a origem da conexão do erro de falta de conectividade com uma mensagem.

Estas mensagens de erros do ICMP nunca serão geradas a partir de outra mensagem de erro, ou a partir de um endereço de broadcast. Para gerar uma mensagem de erro de comunicação, sempre deve haver alguma solicitação de algum *host* válido para outro, caso contrário não poderá existir qualquer tipo de mensagem de retorno.

O ICMP, além de transmitir os erros entre *hosts* de uma rede, serve para realizar o encaminhamento de pacotes dentro das redes. Esta função normalmente não é utilizada por máquinas clientes dentro das redes, e sim pelos roteadores que realizam o direcionamento dos pacotes entre si. Nesta situação, o ICMP é utilizado entre estes roteadores para calcular o melhor caminho, seja ele o mais curto, o mais

eficiente para a entrega dos pacotes. É através deste cálculo, que pode ser realizado de algumas formas, tais quais número de saltos na rede, custo de transmissão ou até mesmo capacidade de transmissão, que os pacotes irão se deslocar dentro da rede. Caso ocorra qualquer problema com alguma dessas linhas de comunicação, o ICMP detectará o problema e mandará uma mensagem de redirecionamento para cada roteador, para que, assim, cada equipamento envolvido no deslocamento do pacote possa vir a se reconfigurar em função da perda da linha de comunicação e passe a encaminhar seus dados por outra linha.

Existem diferentes tipos de ICMP, como pode ser observado na Tabela 8:

TABELA 8 - TIPOS DE ICMP

Tipos	Código	Descrição
0	0	Resposta de eco (par ping)
3	0	Rede de destino inalcançável
3	1	Hospedeiro de destino inalcançável
3	2	Protocolo de destino inalcançável
3	6	Rede de destino desconhecida
3	7	Hospedeiro de destino desconhecido
4	0	Redução de fonte (diminuição de velocidade de transmissão), controle de congestionamento
8	0	Solicitação de eco
9	0	Anúncio de roteador
10	0	Descoberta do roteador
11	0	TTL expirado
12	0	Cabeçalho IP inválido

FONTE: Disponível em: <<http://iana.org>>. Acesso em: 10 fev. 2016.

Além de ser um importante parâmetro para as tratativas de erros dentro das redes, o ICMP também é utilizado para reconhecimento de serviço e identificação de atividades do *host* dentro do ambiente, ou seja, verificar se os *hosts* em questão estão respondendo às possíveis requisições. Para tal funcionalidade é utilizada uma solicitação de ECO, nesta solicitação o *host* que recebeu o ECO deve retornar um pacote com uma resposta para a origem do pedido.

Esta funcionalidade é muito utilizada para verificar se servidores de DNS estão respondendo corretamente. Para fazer uso dessa função foi desenvolvida uma aplicação que ficou muito conhecida e até hoje é muito utilizada dentro da área de gestão de redes, o PING.

Através do PING é possível enviar uma solicitação ao *host* e analisar o seu tempo de resposta e se existe ou não alguma anomalia na rede que poderia ocasionar qualquer falha de transmissão.

Este tempo de resposta do pacote é o tempo decorrido do envio da informação de uma origem até sua chegada no destino e retorno para origem. Quanto menor esse tempo for, mais eficiente é a rede em questão. Desta forma, pode-se realizar um pequeno diagnóstico rápido dentro de uma rede fazendo uso desta aplicação e analisando os dados que o ICMP retornou a ela.

Porém, ao enviarmos uma solicitação de ECO para um dispositivo, o mesmo pode não estar conectado ou simplesmente recusar esta solicitação. Caso haja uma recusa do mesmo, deve ser observado que tipos de serviços estão em funcionamento neste *host*, pois serviços que dependem da identificação de máquina poderão não funcionar caso o ICMP esteja bloqueado no *host*.

Caso o pacote enviado não encontre o *host* de destino, o ICMP possui um dispositivo de segurança para garantir que o pacote seja encerrado ou morto e o remetente receba uma mensagem de erro, notificando que a informação não foi entregue ao destino, pois o *host* não foi encontrado. Este dispositivo é denominado de TTL (*Time to Live*), foi criado com a simples função de garantir que um pacote de informação não fique em *loop* eterno dentro da rede atrás de um *host* que possivelmente não exista mais ou está impossibilitado de receber informações.

Este TTL é carregado em cada pacote e seu valor pode variar em cada sistema operacional, porém, por padrão, a grande maioria dos sistemas cria os pacotes com um TTL de 64 *hops*. Desta forma, sempre que este pacote passar por um roteador, servidor ou qualquer outro dispositivo de rede que possa ser considerado como um salto, uma troca de rede, este TTL é decrementado em uma unidade. Ao chegar em zero, o pacote é descartado e o equipamento que realizar o descarte do pacote envia uma mensagem de erro para a origem do pacote informando que tempo expirou em trânsito.



Aos serem transmitidos através de uma rede de computadores, os pacotes passam por vários roteadores diferentes. Cada roteador consulta sua tabela de endereços e envia o pacote para o roteador que está conectado diretamente a ele e esteja mais próximo do destino do pacote. Assim, sempre que o pacote sai de um roteador e chega até outro, temos um *HOP*. Sendo assim, sabendo a quantidade de roteadores que o pacote passa para alcançar o seu destino, identificamos a quantidade de *HOPS* ou saltos que o pacote dá até o seu destino final.

Outra aplicação que ficou muito conhecida e utilizada na gerência de redes e que tem seu funcionamento baseado no ICMP é o *traceroute*. Esta aplicação compatível com diferentes sistemas operacionais tem por finalidade identificar os saltos por onde o pacote deve passar até a chegada ao seu destino final. Dessa maneira, é possível identificar possíveis falhas de transmissões em enlaces

específicos dentro da rede, ou até mesmo refazer o direcionamento das informações para que deixem de utilizar este meio de transmissão que está comprometido e passem a utilizar uma nova linha de comunicação mais eficiente para o momento, como pode ser observado na Figura 78.

FIGURA 78 - TRACEROUTE

```

C:\>tracert mediacollege.com
Tracing route to mediacollege.com [66.246.3.197]
over a maximum of 30 hops:
1 <10 ms <10 ms <10 ms 192.168.1.1
2 240 ms 421 ms 78 ms 219-88-164-1.jetstream.xtra.co.nz [219.88.164.1]
3 20 ms 30 ms 38 ms 210.55.205.123
4 * * * Request timed out.
5 30 ns 30 ns 48 ms 202.50.245.197
6 30 ns 40 ns 48 ms g2-0-3.tkb3.global-gateway.net.nz [202.37.245.140]
7 30 ns 30 ns 48 ms so-1-2-1-0.akbr3.global-gateway.net.nz [202.50.116.161]
8 160 ns 161 ns 160 ms p1-3.sjbr1.global-gateway.net.nz [202.50.116.178]
9 160 ns 171 ns 160 ms so-1-3-0-0.paby3.global-gateway.net.nz [202.37.245.230]
10 160 ns 161 ns 170 ms pao1-br1-g2-1-101.gnaps.net [198.32.176.165]
11 180 ns 181 ns 180 ms lax1-br1-p2-1.gnaps.net [199.232.44.5]
12 170 ns 170 ns 171 ms lax1-br1-ge-0-1-0.gnaps.net [199.232.44.50]
13 240 ns 241 ns 240 ms nyc-n20-ge2-2-0.gnaps.net [199.232.44.21]
14 240 ns 251 ns 250 ms ash-n20-ge1-0-0.gnaps.net [199.232.131.36]
15 241 ns 240 ns 250 ms 0503.ge-0-0-0.gbr1.ash.nac.net [202.99.39.152]
16 251 ns 260 ns 250 ms 0.so-2-2-0.gbr2.nvr.nac.net [209.123.11.29]
17 250 ns 260 ns 261 ms 0.so-0-3-0.gbr1.oct.nac.net [209.123.11.233]
18 250 ns 260 ns 261 ms 209.123.182.243
19 250 ns 260 ns 261 ms sol.yourhost.co.nz [66.246.3.197]

Trace complete.
C:\>

```

FONTE: O autor

Assim sendo, o ICMP é um importante protocolo de comunicação, e aliado às aplicações como PING e *traceroute*, torna-se uma importante ferramenta para a gerência de rede.

É através destas funcionalidades que muitas aplicações de monitoramento realizam as suas operações de controle dos ativos da rede. Através de um teste simples utilizando o PING é possível diagnosticar um problema de rede, seja ele uma interrupção total no serviço ou simplesmente algum *delay* ou falhas nas transmissões dos pacotes que acarretariam uma lentidão dentro da rede.

Muitos administradores de rede/servidores optam por bloquear este protocolo em seus ativos, pois ao mesmo tempo em que o ICMP é uma importante ferramenta de diagnóstico e transmissão e dados, ele pode ser utilizado para possíveis ataques e interrupções de serviços causados por *hackers*.

Estas interrupções são popularmente conhecidas como ataques de negação de serviço ou ataques DOS (*Denial of Service*) e DDOS (*Distributed Denial of Service*). Este formato de ataque é caracterizado por uma quantidade gigantesca de solicitações de ECO a um ativo de rede. O ativo em questão irá responder ou tentará responder cada uma destas solicitações. Ao chegar a determinado ponto em que o *host* não tem mais capacidade de responder a tantas requisições ou

até mesmo para de receber estas requisições, pois seu *link* de comunicação ficou totalmente comprometido, neste momento o serviço oferecido por este *hardware* fica temporariamente fora do ar.

Nesta situação, assim que as requisições cessarem, o serviço voltará ao seu funcionamento correto. Por este motivo, muitos administradores de rede optam por bloquear totalmente alguns tipos de ICMP, ou adotam políticas com intenção de evitar múltiplas solicitações de ECO partindo do mesmo *host*. Com esta abordagem é possível minimizar possíveis ataques de negação de serviço.

Caso a escolha seja bloquear alguns tipos de ICMP, é preciso tomar muito cuidado para não vir a bloquear nenhum tipo de ICMP que suas aplicações base necessitem para seu pleno funcionamento.

Desta forma, ao gerenciar qualquer ativo ou simplesmente ao fazer qualquer diagnóstico dentro da rede, devemos levar em conta todas as informações colhidas através deste importante protocolo e realizar um planejamento efetivo para garantir a segurança das informações e a eficiência da rede em que se está operando.

6 INTERLIGAÇÃO DE REDES

Da mesma forma como os computadores podem se conectar uns aos outros, as redes também podem se conectar. Se uma coleção de redes de computadores é conectada uma à outra, temos o que se denomina uma rede de redes, formalmente conhecida como inter-rede. Assim, uma inter-rede é uma coleção de redes interconectadas, denominadas de sub-redes. Os dispositivos conectados a uma sub-rede são chamados de nós terminais, e os dispositivos que interconectam as sub-redes são denominados nós intermediários. Uma inter-rede pode conectar redes locais e conexões de longa distância.

O termo inter-rede é frequentemente usado na forma abreviada em inglês: internet. Assim, em um sentido mais geral, uma internet nada mais é que uma coleção de redes interconectadas. Usando como nome próprio e, portanto, com inicial maiúscula, o termo Internet refere-se à maior inter-rede do mundo, composta de centenas de milhares de redes interconectadas e à qual se associa uma certa cultura. De fato, podemos considerar a Internet uma inter-rede de longa distância. A internet também é uma série de redes que dão suporte ao mesmo protocolo que é o TCP/IP. Assim, a internet é uma coleção de redes de computadores que se apoiam em um conjunto específico de padrões de rede, o qual descreve como os computadores pertencentes a diferentes redes se comunicam uns com os outros. A internet possibilita que redes individuais e autônomas funcionem e tenham a aparência de uma grande rede única.

O conceito de interligar redes distintas surgiu com a necessidade de alojar grandes quantidades de *hosts* no mesmo ambiente, porém a necessidade da criação

de uma única rede não seria viável, pois acarretaria em uma grande dificuldade para a sua gestão e um volume de *broadcast* interno muito alto, o qual poderia vir a comprometer o desenho da rede em questão.

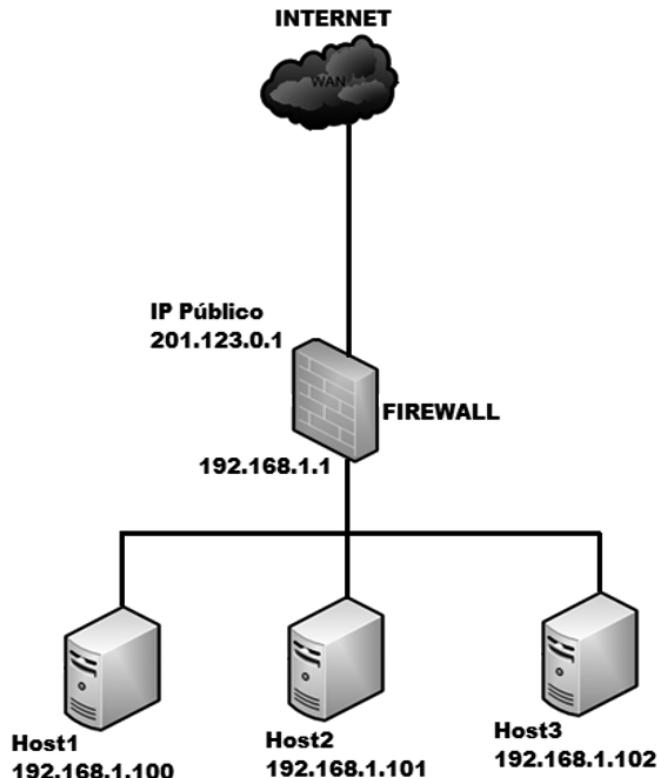
Dessa maneira, a criação de redes distintas surgiu para facilitar a administração das redes, aumentar a segurança de determinados serviços que não deveriam ficar acessíveis a todos e aumentar a performance das redes.

Este isolamento de tráfego de informação pode ser realizado através do NAT (*Network Address Translation*) ou do roteamento de rede.

O NAT, ou mascaramento, é uma técnica muito utilizada em redes de computadores. Seu surgimento foi atribuído ao esgotamento dos endereços de redes do protocolo TCP/IP na versão 4. Através desta técnica é possível atribuir um único endereço de rede para várias máquinas, ou seja, todos ativos de rede que estão localizados após o NAT irão compartilhar o mesmo endereço de rede para realizar a comunicação inter-rede.

Esta técnica consiste em criar uma barreira entre duas redes distintas, onde esta barreira tenha conectividade com as duas redes onde está ligada, porém ambas as redes não possuem um contato direto entre elas, como pode ser observado na Figura 79:

FIGURA 79 - NAT (NETWORK ADDRESS TRANSLATION)



FONTE: O autor

Nesta abordagem, os dispositivos que estão localizados na rede existente após o NAT (dentro da LAN) possuem acesso livre à rede existente antes do NAT, ou seja, a chamada WAN. Os equipamentos que estão localizados na WAN não possuem acesso direto aos dispositivos existentes após o NAT, pois os mesmos estão localizados em uma rede diferente da rede WAN e com restrições quanto ao fluxo da informação.

Como já descrito anteriormente, esta técnica tem o intuito de proteger uma rede LAN de acessos diretos dos dispositivos que estão localizadas dentro da rede WAN e, ainda, realizar uma grande economia de IP's dentro da rede WAN.

Esta economia de IP's, a qual motivou a criação dessa arquitetura de rede, tem por finalidade a possibilidade da utilização da mesma rede LAN em diferentes pontos da rede WAN sem que os dispositivos entrem em conflito. Isto é possível, pois o NAT estabelece um mascaramento da conexão onde somente a interface do NAT que está ligado diretamente à rede WAN, e que possui um IP válido, será responsável por enviar e receber as informações.

Desta maneira, sempre que um dispositivo localizado dentro da rede LAN realizar qualquer solicitação de dados ou for enviar algum pacote para fora da rede, este pacote obrigatoriamente deve passar pelo NAT, o qual é *gateway* local desta rede. Ao passar por este concentrador o cabeçalho do pacote é modificado, recebendo como endereço de origem não mais o endereço local do dispositivo que gerou o mesmo, e sim o endereço IP da interface do NAT que está conectado à rede WAN.

Mesmo tendo seu cabeçalho modificado, o endereço IP real da origem ainda continua contido no pacote, pois quando o destinatário desta informação devolver o pacote à interface WAN do NAT, deve ser capaz de remontar o pacote com o endereço original do remetente para que assim seja possível devolver o pacote ao IP de direito.

Caso algum dispositivo localizado dentro da rede WAN deseje estabelecer uma conexão com algum dispositivo da rede LAN, o NAT irá bloquear qualquer tipo de conexão, a menos que se estabeleçam regras de acesso por serviços. Assim, é possível direcionar determinada porta de comunicação para dentro da rede local, sem um acesso direto.

Neste processo de direcionamento, a solicitação de serviço vem vinculada à interface WAN do NAT, ou seja, a origem da informação deve buscar pelo IP da interface WAN do NAT e uma porta específica de comunicação. Ao receber esta solicitação, a interface externa consultará a tabela de direcionamento de dados existente dentro de si próprio e assim realizará o encaminhamento do dado para o IP localizado dentro da rede LAN.

Com a vinda do protocolo TCP/IP versão 6, a utilização desta arquitetura de rede tende a diminuir, pois questões relacionadas à economia de IP's não serão mais relevantes, porém, é uma estrutura que garante certa segurança à rede onde está localizada e facilita a gestão dos serviços e aplicações existentes dentro da rede local.

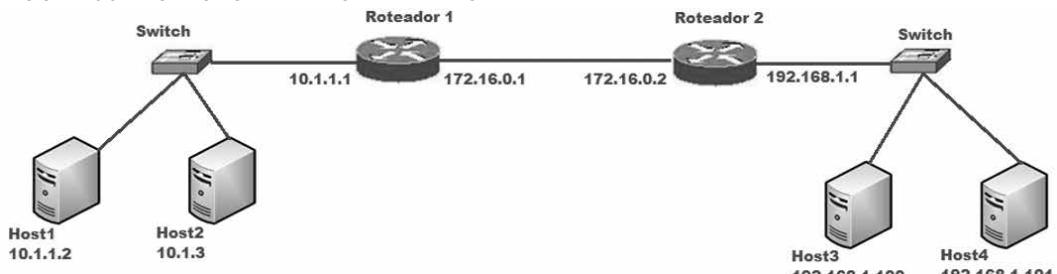
A grande e única desvantagem desta arquitetura se refere ao fato de que todos os serviços localizados na LAN, para que estejam acessíveis na WAN, devem estar liberados no NAT, caso contrário seu acesso ficará totalmente comprometido. Consequentemente, ao realizar a construção de várias tabelas de liberações e restrições nos concentradores NAT, os mesmos demandam de *hardware* relativamente forte, para assim suprir as necessidades de encaminhamento e gestão das informações.

Já o roteamento de rede consiste neste mesmo isolamento de redes, com o mesmo intuito de diminuir o *broadcast* dentro das redes, porém a ideia de economia de IP's já não é mais tão importante.

O conceito de roteamento diz respeito a determinar o caminho que um pacote de dados toma ao viajar entre os nós de origem e de destino. O roteamento é efetuado usualmente por unidades de *hardware* dedicadas e especiais, chamadas roteadores.

Nesta abordagem de rede, as redes WAN e LAN possuem acesso direto uma à outra, sem a necessidade de redirecionamento de dados. Isto é possível, pois os concentradores destas redes (os roteadores) possuem conectividade para ambas as redes, como acontece no NAT. No entanto, neste caso não ocorre o mascaramento da conexão, ou seja, as redes, mesmo sendo distintas através destes concentradores, podem realizar a troca de informações entre si. Observe a figura:

FIGURA 80 - ESTRUTURA DE ROTEAMENTO



FONTE: O autor

Para realizar esta troca de informações de forma direta, os roteadores fazem o direcionamento do dado, desta maneira, sempre que uma requisição de informação chegar até ele, o mesmo tratará o pacote e fará a leitura do seu destino e direcionará o mesmo para o local correto dentro da rede. Assim, as redes, mesmo sendo distintas, passam a trocar informações de forma direta com ajuda dos roteadores, porém sem enfrentar possíveis problemas básicos de rede, tais como *broadcast* excessivo ou um conflito de IP.

Ao utilizar a ideia de roteamento de rede, pode-se optar por duas formas de utilização dessas técnicas: as rotas estáticas ou rotas dinâmicas.

Primeiramente, deve-se ter bem claro o conceito de rotas para um roteador. Este conceito refere-se ao encaminhamento de pacotes, lembrando que uma rede é composta por vários ativos e *ranges* de redes. Para que um pacote alcance seu destino em uma rede diferente do seu bloco de origem é responsabilidade dos roteadores, baseados em suas tabelas de rotas, realizar o encaminhamento, ou seja, apontar para que direção o pacote deve seguir para alcançar o seu destino final.

Identificado o seu caminho, o pacote de dados é transmitido para o próximo salto dentro da rede ou até mesmo para o seu destino final. Sem essas tabelas que descrevem por onde cada informação deve passar, ou por cada nó de rede que o dado deve trafegar para chegar ao destino, não seria possível a comunicação entre redes distintas.

Essas tabelas de rotas funcionam como guias dos pacotes dentro das redes de comunicação. Dessa forma, estas tabelas devem estar sempre atualizadas e indicando o melhor caminho para o pacote. Estas tabelas podem ser, como já mencionado anteriormente, dinâmicas ou estáticas.

Quando tratamos estas tabelas de rotas de forma estática, é dever do administrador construir as mesmas e realizar as atualizações sempre que necessário. Dessa forma, o administrador de rede deve acessar cada roteador (concentrador entre duas redes) e realizar o apontamento da rede, ou seja, realizar a criação da rota, descrevendo que para alcançar determinada rede a informação deve ser direcionada para determinado IP (o qual pode estar atribuído a uma máquina ou a outro roteador), o qual se responsabilizará pelo tratamento desse pacote. O administrador de rede deve construir essa tabela em todos os roteadores da sua rede, mostrando a todos eles como alcançar todas as redes existentes no ambiente.

Uma comunicação em rede de computadores, como já vimos, é composta por envio e confirmação de recebimento de dados, dessa maneira, ao criar todas as rotas de encaminhamento de dados, é necessário criar as rotas reversas, ou seja, os roteadores devem saber enviar a informação para o ponto à frente, porém devem saber também devolver a informação para sua origem.

Esta estrutura de tabelas estáticas é muito utilizada em redes de pequeno porte, onde a quantidade de redes existentes no ambiente é pequena e a quantidade de ativos de rede também é reduzida. Quando passamos para uma topologia com muitos *ranges* de rede e uma grande quantidade de ativos no ambiente computacional, essa estrutura de tabelas estáticas se torna inviável, pois sempre que houver qualquer alteração na rede ou o surgimento de uma nova rede, o administrador terá que reconfigurar manualmente todos os ativos da rede, fazendo com que o mesmo perca muito tempo.

Outro problema que é enfrentado ao utilizar esta estrutura estática é quanto às falhas de comunicação entre redes por motivos de falhas em ativos, ou até mesmo perda de comunicação entre dois concentradores.

Com esta abordagem, mesmo que existam *links* de comunicação entre roteadores, a comunicação irá ser interrompida, pois não é possível duas rotas para o mesmo destino coexistirem utilizando caminhos diferentes. Sendo assim, sempre que houver uma falha de comunicação e for necessário utilizar outra via de comunicação, o administrador de rede terá que passar nos ativos de redes afetados e realizar a sua reconfiguração, para que assim os pacotes sejam direcionados para este novo caminho.

Ao restabelecer a comunicação no *link* principal, o administrador deve reconfigurar novamente os ativos para que os pacotes voltem a realizar a transmissão de dados por este caminho. Dessa maneira, percebe-se que esta estrutura estática acaba por se tornar muito dependente do administrador de rede, pois diante de qualquer alteração ou anomalia no ambiente, os equipamentos necessitam ser reconfigurados para esta nova abordagem, o que acaba demandando muito tempo e muitas interrupções de rede em momentos críticos.

A estrutura de rotas dinâmicas tem uma grande vantagem, pois seu funcionamento básico quanto ao encaminhamento dos pacotes, orientando e mostrando o caminho, é o mesmo das rotas estáticas, porém sua administração e construção é muito mais simples e ágil.

Para utilizar esta estrutura de rotas dinâmicas é necessária a utilização de um protocolo específico de roteamento, tais como: BGP, OSFP, RIP, IGRP, entre outros.

O protocolo de roteamento escolhido pelo administrador tem por finalidade realizar a comunicação entre os roteadores envolvidos. A base de funcionamento de todos os protocolos descritos acima é muito semelhante, só difere na forma de escolha e monitoramento das rotas. Em resumo, o funcionamento de todos os protocolos é muito parecido.

Até então o administrador de rede deveria, ao construir sua rede, acessar todos os roteadores em questão e adicionar de forma manual todas as rotas, ou caminhos, para alcançar todas as redes. Com esta nova abordagem, utilizando rotas dinâmicas, não é mais necessário este tipo de serviço. Para tanto, basta que seja definido um protocolo de roteamento para realizar a comunicação entre os equipamentos em questão, e adicionar em cada um deles suas interfaces de rede e ativar o anúncio de rede, onde cada roteador irá propagar para o roteador mais próximo quais redes o mesmo administra, e assim todos os roteadores irão conhecer todos os caminhos para todos os destinos, pois cada roteador irá propagar sua configuração e as demais configurações recebidas por ele a partir da comunicação com outros roteadores.

Estes anúncios são realizados pelos *links* de comunicação que cada roteador possui. Baseado no protocolo escolhido, ele terá uma forma peculiar de avaliar a qualidade, estabilidade e performance de cada *link* conectado a ele, e assim acaba

por definir prioridades para cada *link*. Esta forma de avaliar a eficiência de um *link* pode ser baseada na quantidade de nós para alcançar determinado destino, latência dos *links*, capacidade de transmissão dos *links*, entre outras possibilidades.

Quando utilizamos esta abordagem de rede, em um mesmo roteador pode haver dados que para alcançar determinado destino acabem por utilizar o *link* 1, por exemplo, e, para alcançar outro destino, utilizem o *link* 2. Isso se deve ao fato da avaliação do protocolo de roteamento ter escolhido determinado *link* para esta situação baseado em algum critério predeterminado, o qual lhe dará maior eficiência na transmissão dos dados em questão.

Havendo qualquer modificação ou aumento de rede, o equipamento afetado irá anunciar para todos os outros equipamentos que estão conectados a nova alteração efetuada dentro da rede, fazendo com que todos recebam esta modificação e, assim, acabem corrigindo as suas configurações.

Além dessa grande praticidade em nível de administração e gerência dos equipamentos, outra grande vantagem desta estrutura dinâmica é sua autossuficiência em correção de erros.

Ao utilizarmos um protocolo de roteamento dinâmico, o mesmo executa por si só um monitoramento das suas linhas de comunicação com os outros roteadores ligados na rede. Dessa forma, ao perceber qualquer interrupção ou alteração de performance de uma dessas linhas de comunicação, o protocolo de gerência destas rotas automaticamente desabilita este *link* de comunicação e acaba por desviar todo o fluxo de informação para outro *link*, sem qualquer parada no sistema ou interação com o administrador de redes. Assim, a disponibilidade de um serviço de rede se torna muito maior, minimizando possíveis problemas com falhas de ativos ou *link* de comunicação entre redes distintas.

É possível perceber que separação ou fragmentação de uma rede em outras redes menores é um importante mecanismo no momento da gestão das redes em um ambiente computacional. Além de facilitar a identificação dos *hosts*, é possível minimizar e isolar problemas referentes a conflitos de IP's dentro da rede, segurança das informações que estão circulando e disponíveis na rede, gerenciar e controlar os recursos existentes dentro das redes, tais como compartilhamentos, internet, entre outros acessos.

Para tanto, é necessário identificar a necessidade de cada ambiente para assim poder construir a melhor estrutura lógica para o mesmo, utilizando uma técnica de roteamento, NAT ou até mesmo fazendo uma mescla das estruturas para que, assim, seja possível alcançar um alto índice de satisfação, segurança e confiabilidade para a rede em questão.

LEITURA COMPLEMENTAR

Por que monitorar uma rede

O monitoramento de redes é uma das prioridades da TI da sua empresa?

Os profissionais de TI sabem que até mesmo os equipamentos de última geração e os *softwares* mais atualizados não garantem sistemas imunes a erros. Por isso, qualquer sistema crítico para um negócio deve ser monitorado constantemente para evitar interrupções que prejudiquem sua utilização pelos usuários.

Hoje veremos como as redes, que garantem a troca de informações entre os computadores da sua empresa, também exigem um acompanhamento de perto da equipe de TI para que possam ter um bom desempenho. Descubra a importância do monitoramento de redes!

Sempre por dentro

Quando uma empresa monitora sua rede, os funcionários responsáveis pelos processos de TI serão informados sobre possíveis falhas por meio de alertas de *e-mail* pré-programados. Isso faz com que a equipe fique sempre por dentro do desempenho a partir de qualquer lugar, podendo atuar de forma mais ágil, caso algum problema ocorra.

Imagine que a rede da empresa apresenta alguma falha no fim da noite. Caso a infraestrutura seja monitorada, um profissional poderá solucionar o problema imediatamente, de forma remota, antes mesmo que os funcionários começem a trabalhar no dia seguinte.

Agilizando correções

O monitoramento da rede também torna a correção dos problemas mais rápida. Isso acontece porque as soluções para esse fim já mostram qual dispositivo pode estar causando a falha, reduzindo o tempo necessário para identificá-los e solucioná-los.

Identificando tendências

A rede de uma empresa pode apresentar diversos problemas de forma isolada ao longo dos anos e, caso eles não sejam analisados com cuidado, algumas tendências importantes podem passar despercebidas pela equipe de TI.

Com uma ferramenta do monitoramento, os profissionais são capazes de identificar padrões nas falhas e, consequentemente, entender como está a saúde da rede para definir ações de melhoria.

Planejando com calma

Se algum equipamento começa a apresentar problemas constantes, prejudicando as tarefas, isso significa que sua empresa já perdeu o momento adequado para substituí-lo.

Quando a equipe de TI monitora a rede, no entanto, será possível programar manutenções periódicas ou investimentos em novos equipamentos para prevenir problemas em *hubs*, roteadores, *modems* ou outros pontos da infraestrutura. Isso evita que a rede opere no limite de sua capacidade por muito tempo, permitindo que a empresa planeje os investimentos com mais tranquilidade e sem grandes impactos no orçamento.

Facilitando a visualização

Quando a equipe de TI precisa explicar alguma questão técnica à alta gestão da empresa, são grandes as chances de que ocorram ruídos na comunicação. Por isso, monitorar a rede com ferramentas voltadas para esse fim pode facilitar a visualização do desempenho do sistema e seus pontos críticos, o que favorece a tomada de decisão não somente da equipe de TI, como também dos proprietários do negócio.

Com tudo isso, é possível perceber que o monitoramento de redes ajuda a tornar o trabalho da equipe de TI mais estratégico, criando soluções para os desafios tecnológicos antes mesmo que eles se apresentem.

Ferramenta para gerenciar e monitorar redes

Para gerenciar e analisar todos os dados trafegados na rede as organizações precisam se valer de soluções que apoiem a gestão de TI, fornecendo formas de visualização destes dados.

FONTE: Disponível em: <<http://www.opservices.com.br/qual-importancia-monitoramento-de-redes>>. Acesso em: 12 mar. 2016.

RESUMO DO TÓPICO 4

Neste tópico você viu que:

- O gerenciamento de redes tornou-se uma atividade necessária para alcançar a máxima eficiência das redes existentes.
- Esta atividade consiste em realizar um monitoramento e acompanhamento de cada ativo de rede existente no ambiente. Desta forma é possível prever acontecimentos e agir antes que os mesmos venham a interromper o funcionamento da rede.
- Para realizar o gerenciamento de redes são utilizados protocolos específicos, entre os quais podem se destacar o SNMP e o ICMP.
- Estes protocolos são utilizados por ferramentas (*softwares*) que irão realizar o acompanhamento da rede.
- As ferramentas de gerenciamento de redes podem ser classificadas em: analisadores de protocolos, geradores de gráficos, gerenciamento de falhas, gerenciamento de configuração e gerenciamento de segurança.
- Existem algumas formas de realizar a interligação de redes, ou seja, fazer com que duas ou mais redes distintas tenham capacidade de realizar a troca de informações sem que ambas necessitem estar ligadas diretamente.
- Entre as estratégias utilizadas para realizar a interligação de redes destaca-se o NAT (*Network Address Translation*), o roteamento estático e o roteamento dinâmico.
- Ao realizarmos a interligação das redes com roteamento, seja ele estático ou dinâmico, os *hosts* possuem livre acesso a ambos os sentidos da rede, podendo trocar dados de forma direta, ou seja, buscando o endereço IP do *host*.
- Ao utilizarmos o NAT como técnica de interligação de rede, os *hosts* alocados dentro da LAN do NAT têm acesso de forma direta aos *hosts* alocados na WAN do NAT, porém o caminho inverso não é permitido, tendo acesso somente através da liberação de serviços dentro do NAT.
- Em ambos os casos a interligação das redes funcionará e garantirá a troca de informação entre os *hosts* envolvidos, trazendo maior segurança para as redes, maior facilidade de gestão e aumentando a performance das mesmas.

AUTOATIVIDADE



Vamos praticar!

- 1 Qual o protocolo da camada de transporte que é utilizado pelo protocolo de gerenciamento de redes SNMP para realizar a coleta dos dados em seus agentes?
 - a) () TCP
 - b) () UDP
 - c) () POP
 - d) () HTTP
 - e) () FTP
- 2 Para que servem as portas de comunicação?
- 3 Com o esgotamento dos endereços de rede IPv4 foram desenvolvidas várias técnicas para dar sobrevida ao mesmo. O NAT (*Network Address Translation*) foi uma das mais importantes, sendo assim, descreva no que consiste essa técnica e no que ela se difere das técnicas de roteamento.
- 4 As redes de computadores são muito complexas, pois são formadas por *hardwares* e *softwares*, todos interligados e trabalhando de maneira homogênea. Assim, cite quais são as três principais funções do administrador em relação à sua rede.



Assista ao vídeo de
resolução da questão 3



REFERÊNCIAS

ALMEIDA, Y. L. **Evolução das Redes de Transporte**: Packet Transport Networks e MPLS-TP. Teleco, São José dos Campos, agosto 2011. Disponível em: <<http://Evolucao das Redes de Transporte:PacketTransportNetworks e MPLS-TP>>. Acesso em: 5 mar. 2016.

AMARAL, A. F. F. **Redes de computadores**. Colatina: Instituto Federal do Espírito Santo, 2012.

BARRET, D; KING, T. **Redes de computadores**. Rio de Janeiro: LTC, 2010.

Camadas TCP/IP. Disponível em: <<https://jbgsm.wordpress.com/2010/05/31/camadas-tcpip/>>. Acesso em: 10 fev. 2016.

CERT.BR. Disponível em: <<http://cert.br>>. Acesso em: 20 fev. 2016.

COMER, D. E. **Interligação em redes com TCP/IP**. 7. ed. Rio de Janeiro: Elsevier, 1999.

CISCO SYSTEMS. Implementing Cisco Quality of Service volume 1-2 version 2.2, EUA, 2006.

Conceitos de MPLS. Disponível em: <http://ix.br/pttforum/8/doc/10-introducao_ao_mpls.pdf>. Acesso em: 8 abr. 2016.

Criptografia - Segurança da Informação. Disponível em: <<http://cartilha.cert.br/criptografia/>>. Acesso em: 6 abr. 2016.

DANTAS, M. **Redes de comunicação e computadores**: abordagem quantitativa. Florianópolis: Visual Books, 2010.

DANTAS, M. **Tecnologias de redes de comunicação e computadores**. Rio de Janeiro: Axcel Books, 2002.

ENGST, A. C. **Kit do iniciante em redes sem fio**. 2. ed. São Paulo: Pearson Makron Books, 2005.

Equipamentos de rede. Disponível em: <http://support.ricoh.com/bb_v1oi/pub_e/oi_view/0001043/0001043279/view/fax/int/0121.htm>. Acesso em: 20 fev. 2016.

GALLO, M. A. **Comunicação entre computadores e tecnologias de redes**. São Paulo: Thomson, 2003.

GHODDOSI, N. Fundamentos de redes e comunicação de dados. 2. ed. Indaial: Uniasselvi, 2009.

IANA. Disponível em: <<http://iana.org>>. Acesso em: 15 jan. 2016.

Introdução à MPLS – Disponível em: <http://ix.br/pttforum/8/doc/10-introducao_ao_mpls.pdf>. Acesso em 8 abr. 2016.

IPV6. Disponível em: <http://ipv6.br>. Acesso em: 20 fev. 2016.

KUROSE, J. F. Redes de computadores e a Internet. 5. ed. São Paulo: Pearson, 2010.

LATZKE, C. A; GROSS, J. C. Infraestrutura de redes de computadores. Indaial: Uniasselvi, 2013.

MENDES, D. R. Redes de computadores: teoria e prática. São Paulo: Novatec, 2007.

MIB SNMP - Disponível em: <<http://aldembergmarinho.blogspot.com.br/>>. Acesso em: 10 jan. 2016.

Modelo de Referência. Disponível em: <<http://professorgilberson.blogspot.com.br/2010/02/modelo-de-referencia-osi.html>>. Acesso em: 10 fev. 2016.

MORAES, A. F. Redes de computadores. São Paulo: Érica, 2014.

MOREIRAS, A. M.; COREDEIRO E. S.; DOS SANTOS R. R.; HARANO A. Y; MORALES, E. B.; GANZELLI, H. S.; NAKAMURA, T. J.; CARNIER E. B. IPV6. Disponível em: <<http://ipv6.br/media/arquivo/ipv6/file/64/livro-lab-ipv6-nicbr.pdf>>. Acesso em: 1 abr. 2016.

MPLS CISCO. Disponível em: <<http://www.cisco.com.br>>. Acesso em: 8 abr. 2016.

MPLS. Disponível em: <http://www.gta.ufrj.br/grad/01_2/mpls/mpls.htm>. Acesso em 8 abr. 2016.

PINHEIRO, J. M. S. Guia completo de cabeamento de redes. Rio de Janeiro: Campus, 2003.

PROXY. Disponível em <<http://windows.microsoft.com/pt-br/windows-vista/what-is-a-proxy-server>>. Acesso em: 04 abr. 2016.

QoS. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialqosotm/pagina_3.asp> Acesso em: 8 abr. 2016.

Rede WAN. Disponível em:<<https://10infrpcpaulo.wordpress.com/2012/12/11/wan/>>. Acesso em: 3 abr. 2016.

ROSS, J. Redes de computadores. Rio de Janeiro: Almeida e Porto, 2008.

RUFINO, N. M. O: **Segurança em redes sem fio.** 3. ed. São Paulo: Novatec, 2011.

Serviços de rede. Disponível em: <<https://danielteofilo.wordpress.com/2010/01/31/servico-orientado-a-conexao-e-servico-nao-orientado-a-conexao/>>. Acesso em: 10 abr. 2016.

SNMP. Disponível em: <<http://snmp.com>>. Acesso em: 31 jan. 2016.

SOARES, L. F. G; LEMOS, G; COLCHER, S. Redes de Computadores: das LANs, MANs e WANs às redes ATM. 2. ed. Rio de Janeiro: Campus, 1995.

SOUSA, L. B. Projetos e implementação de redes: fundamentos, arquiteturas, soluções e planejamento. 3. ed. São Paulo: Érica, 2013.

SOUSA, L. B. Protocolos e serviços de redes. São Paulo: Érica, 2014.

TANENBAUM, A. S. Redes de computadores. 2. ed. Rio de Janeiro: Campus, 1994.

TANENBAUM, A. S. Redes de computadores. 8. ed. Rio de Janeiro: Elsevier, 2003.

TORRES, G. Redes de computadores: curso completo. Rio de Janeiro: Axcel Books, 2001.

ANOTAÇÕES

