REDES DE COMPUTADORES

AUTORES
Ricardo Tombesi Macedo
Roberto Franciscatto
Guilherme Bernardino da Cunha
Cristiano Bertolini

LICENCIATURA EM COMPUTAÇÃO

REDES DE COMPUTADORES

AUTORES
Ricardo Tombesi Macedo
Roberto Franciscatto
Guilherme Bernardino da Cunha
Cristiano Bertolini

1ª Edição
UAB/NTE/UFSM

UNIVERSIDADE FEDERAL DE SANTA MARIA

Santa Maria | RS
2018

Este caderno foi elaborado pelo Núcleo de Tecnologia Educacional da Universidade Federal de Santa Maria para os cursos da UAB.

NÚCLEO DE TECNOLOGIA EDUCACIONAL

DIRETOR DO NTE
Paulo Roberto Colusso

ELABORAÇÃO DO CONTEÚDO
Ricardo Tombesi Macedo, Roberto Franciscatto
Guilherme Bernardino da Cunha, Cristiano Bertolini

REVISÃO LINGUÍSTICA
Camila Marchesan Cargnelutti
Maurício Sena

APOIO PEDAGÓGICO
Carmen Eloísa Berlote Brenner
Caroline da Silva dos Santos
Keila de Oliveira Urrutia

EQUIPE DE DESIGN
Carlo Pozzobon de Moraes – Ilustrações
Juliana Facco Segalla – Diagramação
Matheus Tanuri Pascotini – Capa e Ilustrações
Raquel Bottino Pivetta – Diagramação

PROJETO GRÁFICO
Ana Letícia Oliveira do Amaral

R314 Redes de computadores [recurso eletrônico] / Ricardo Tombesi Macedo ... [et al.]. – 1. ed. – Santa Maria, RS : UFSM, NTE, 2018.
1 e-book

Este caderno foi elaborado pelo Núcleo de Tecnologia Educacional da Universidade Federal de Santa Maria para os cursos da UAB
Acima do título: Licenciatura em computação
ISBN 978-85-8341-225-0

1. Computadores – Redes 2. Internet I Macedo, Ricardo Tombesi II. Universidade Aberta do Brasil III. Universidade Federal de Santa Maria. Núcleo de Tecnologia Educacional

CDU 004.7

Ficha catalográfica elaborada por Alenir Goularte - CRB-10/990
Biblioteca Central da UFSM

Ministério da **Educação**

CAPES UNIVERSIDADE ABERTA DO BRASIL Universidade Federal de Santa Maria 1960 PROGRAD NÚCLEO DE TECNOLOGIA EDUCACIONAL

APRESENTAÇÃO

Prezados alunos, sejam bem-vindos à disciplina de Redes de Computadores! Provavelmente você já ouviu muitas vezes sobre as redes de computadores, mas talvez este assunto pode parecer um pouco vago e distante do seu cotidiano. Entretanto, com uma pequena reflexão você verá que as redes de computadores estão estritamente presentes no nosso dia-a-dia. Em algum momento você já pensou na quantidade de sistemas computacionais que as pessoas utilizam diariamente? Provavelmente você conhece alguém que está frequentemente conectado em sistemas de troca de mensagens instantâneas, redes sociais ou até mesmo que verifica com alta frequência sua conta bancária por meio de aplicativos instalados em um *smartphone*. Todas estas tecnologias foram construídas para operarem sob redes de computadores. Agora imagine um cenário hipotético onde estas redes simplesmente desaparecessem. Diante desta situação provavelmente existiria uma situação de caos em nossa sociedade, visto que além dos meros usuários destes sistemas, também existem diversas grandes corporações que dependem das redes de computadores para gerenciar dados sobre a sua cadeia de produção. Pensando sobre cenários desta magnitude, podemos concluir que nossa sociedade depende fortemente das redes de computadores. Esta disciplina aborda os aspectos teóricos das redes de computadores e sua empregabilidade em infraestruturas para educação a distância. O conteúdo desta disciplina foi dividido em seis unidades.

A Unidade 1 proporciona uma visão geral das redes de computadores, contextualizando os principais conceitos, esclarecendo onde as redes são usadas, seus principais benefícios, seu processo evolutivo e diferenciando as redes de comunicação de dados e teleprocessamento.

A Unidade 2 descreve de forma breve a evolução dos computadores, iniciando pelos primeiros dispositivos criados pela humanidade para executar operações matemáticas, passando rapidamente pelos computadores mecânicos, destacando o avanço tecnológico advindo com o surgimento dos computadores digitais e pautando as principais contribuições tecnológicas dos circuitos integrados.

A Unidade 3 aborda a forma como as arquiteturas de redes são organizadas em camadas, apresentando o modelo de referência OSI e a pilha de protocolos TCP/IP, a qual é empregada como padrão de fato. Além disso, esta unidade apresenta uma comparação entre o modelo OSI e TCP/IP, bem como descreve uma crítica para cada modelo.

A Unidade 4 ensina as diferenças entre os conceitos Internet e Web, focando nos diferentes protocolos da camada de aplicação.

A Unidade 5 compreende as técnicas de segurança e gerenciamento de redes, onde são detalhados, como por exemplo, as políticas de segurança, as contas e senhas de usuários, os métodos de criptografia existentes e as cópias de segurança.

A Unidade 6 encerra a disciplina ao detalhar as infraestruturas para educação a distância.

ENTENDA OS ÍCONES

ATENÇÃO: faz uma chamada ao leitor sobre um assunto, abordado no texto, que merece destaque pela relevância.

INTERATIVIDADE: aponta recursos disponíveis na internet (sites, vídeos, jogos, artigos, objetos de aprendizagem) que auxiliam na compreensão do conteúdo da disciplina.

SAIBA MAIS: traz sugestões de conhecimentos relacionados ao tema abordado, facilitando a aprendizagem do aluno.

TERMO DO GLOSSÁRIO: indica definição mais detalhada de um termo, palavra ou expressão utilizada no texto.

SUMÁRIO

1

VISÃO GERAL DAS REDES DE COMPUTADORES

INTRODUÇÃO

Ao analisarmos os séculos anteriores, percebe-se que a tecnologia desempenhou um papel fundamental em cada século, determinando a principal forma de produção em cada período. Os sistemas mecânicos predominaram no século XVIII. As máquinas a vapor representaram a principal inovação do século XIX. No século XX, os principais avanços foram relacionados com a aquisição, processamento e disseminação de informações. Dentre as mais notáveis tecnologias deste século pode-se mencionar o rádio, a televisão, os computadores, as redes de computadores e a Internet.

O surgimento das redes de computadores mudou a forma como os sistemas computacionais eram organizados. Inicialmente, os sistemas computacionais eram organizados tendo como base um único computador responsável por executar todo o processamento e armazenamento necessários. Este modelo foi massivamente empregado quando o custo dos computadores era expressivamente alto, dificultado a aquisição de uma grande quantidade destas máquinas por organização. Com o avanço da tecnologia, os computadores começaram a ser construídos com componentes mais potentes, menores e mais baratos, facilitando a popularização destes equipamentos. Em decorrência deste fato, as empresas e a população em geral puderam adquirir mais computadores. Este cenário propiciou uma forma diferente de organizar os sistemas computacionais, passando do modelo centralizado em um único computador para um sistema computacional organizado com diversos computadores.

Essa nova forma de pensar os sistemas computacionais abriu as portas para uma nova área, as redes de computadores. Neste momento, era evidente os benefícios da adoção de um único computador para realizar tarefas consideradas onerosas para os seres humanos, tais como a execução de cálculos complexos e o armazenamento de uma vasta quantidade de informação. Se apenas um computador pode gerar muitos benefícios, imagine se vários deles pudessem se comunicar e operar de maneira cooperativa? Pensando dessa forma podemos afirmar que o princípio por trás da criação das redes de computadores foi possibilitar a interconexão entre diversos computadores a fim de trocar dados e explorar os benefícios provenientes.

Esta unidade está organizada como segue. Primeiramente, entenderemos o contexto que motivou a larga adoção das redes de computadores. Em seguida, abordaremos os principais usos das tecnologias em redes e os seus benefícios gerados. Na sequência, estudaremos a evolução das redes de computadores e finalizaremos a unidade ao diferenciar o conceito de redes de comunicação das redes de teleprocessamento.

1.1
UMA BREVE CONTEXTUALIZAÇÃO

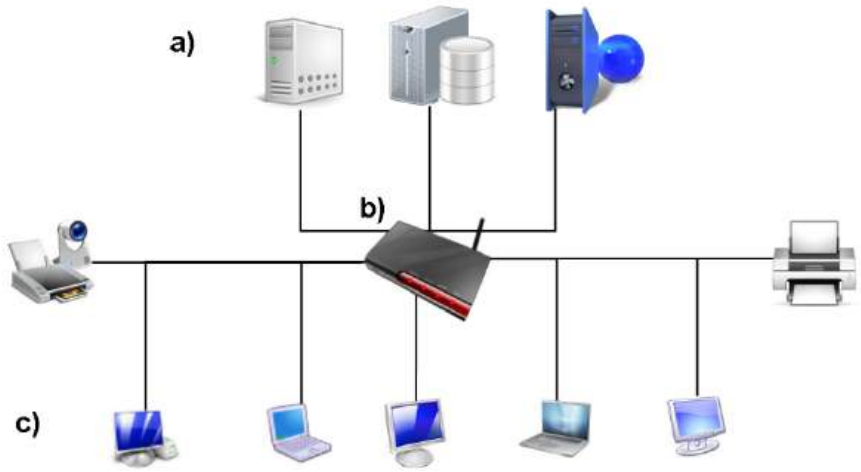
Nos dias atuais, seria praticamente impossível para nossa sociedade sobreviver sem o suporte das redes de computadores. A cada dia que passa, mais pessoas adquirem dispositivos capazes de se conectar à Internet para usufruir dos mais variados tipos de serviços oferecidos através da rede, tais como serviços de correio eletrônico (e-mail), redes sociais ou serviços de mensagens instantâneas. Estes serviços foram cuidadosamente projetados para potencializar a execução das atividades cotidianas das pessoas de forma a minimizar os ônus envolvidos nas atividades e melhorar significativamente a sua eficácia. Lembrando que ônus neste contexto diz respeito ao custo ou a sobrecarga envolvida em uma tarefa, e eficácia retrata a qualidade do resultado da atividade realizada. Por exemplo, ao comparar o ônus e eficácia do correio tradicional com o correio eletrônico, podemos claramente identificar vantagens do correio eletrônico em relação ao seu concorrente ao verificar o tempo de entrega da mensagem e o custo de envio. Devido aos benefícios proporcionados pelos serviços oferecidos por meio de redes de computadores, a nossa sociedade se tornou e está se tornando cada vez mais dependente destas redes.

Apesar das pessoas usarem diariamente os serviços oferecidos por meio das redes de computadores e da mesma forma adotarem um vocabulário muitas vezes repleto de termos técnicos para se referirem a estes serviços, a maioria delas desconhecem o significado real destes termos. Por exemplo, você já se perguntou o que realmente significa uma rede de computadores? O que seria um endereço IP? Ou, ainda, poderia explicar a definição do termo protocolo de rede? Existe uma grande probabilidade de você já ter usado ou em algum momento ter escutado algum destes termos, mas de fato não conseguir explicar de forma simples o seu significado. Devido a este fato, primeiramente definir alguns termos básicos para melhor compreender os assuntos aqui abordados.

Os dispositivos de uma rede de computadores podem ser computadores, *smartphones*, *smart TVs*, câmeras de segurança, ou dispositivos responsáveis pela comutação de dados. Estes dispositivos são autônomos, pois podem executar tarefas de maneira independente dos demais. A troca de dados compreende em um dos principais objetivos da criação da rede de computadores, sendo que estes dados podem variar desde um pequeno arquivo no formato TXT com um número de telefone até uma grande quantidade de *streamings* de vídeo transmitidas durante uma videoconferência. Para efetivamente transmitir os dados, todos os dispositivos devem ser configurados com uma mesma tecnologia, determinando, assim, um padrão seguido por todos os dispositivos. A Figura 1 apresenta um exemplo de uma rede de computadores.

TERMO DO GLOSSÁRIO: uma rede de computadores consiste em um conjunto de dispositivos autônomos e interconectados com a finalidade de trocar dados por meio de uma única tecnologia.

FIGURA 1 – Exemplo de uma rede de computadores



FONTE: Autores.

A Figura 1 ilustra uma rede de computadores formada por três principais dispositivos, sendo eles identificados com as letras *a*, *b* e *c*. Os dispositivos localizados na parte superior da figura identificados com a letra a consistem nos servidores. Os servidores compreendem os dispositivos de uma rede responsáveis por prestar algum tipo de serviço na rede. A principal característica dos servidores consiste em uma capacidade de processamento e de armazenamento superior aos demais, sendo essas capacidades ajustadas aos requisitos dos serviços oferecidos. Além disso, os servidores compreendem em dispositivos geralmente dedicados apenas à prestação dos serviços na rede, sendo por usuários especialistas responsáveis por sua manutenção e configuração. Os dispositivos interessados em usufruir destes serviços consistem nos clientes e são ilustrados na parte inferior da figura, sendo identificados com a letra c. Os clientes geralmente possuem um poder de processamento e armazenamento inferior aos dos servidores e são normalmente utilizados por usuários leigos. O elemento central da figura consiste em um roteador, cuja função consiste na interconexão entre os demais dispositivos da rede. Ao longo deste material serão fornecidas mais informações específicas sobre estes dispositivos e suas funcionalidades, mas, para o momento, basta obtermos uma visão mais generalista sobre cada tipo de dispositivo. Os elementos localizados nas extremidades direita e esquerda do centro da figura consistem em impressoras capazes de serem acessadas pelos demais dispositivos. Como existem conexões entre todos os dispositivos ilustrados, todos eles estão aptos a trocar informações ao utilizar uma mesma tecnologia.

Uma vez que compreendemos a definição de uma rede de computadores, podemos nos concentrar na segunda questão: *O que seria um endereço IP?* A fim de

responder este questionamento de maneira direta e sem aprofundar nas diversas especificidades existentes, precisamos compreender a necessidade de identificar os dispositivos existentes em uma rede de computadores. Como as redes de computadores possibilitam a troca de dados, surge a necessidade inerente de diferenciar os dispositivos e utilizar estratégias capazes especificar o emissor e receptor de uma mensagem. O emissor compreende o dispositivo com a necessidade de enviar dados, enquanto o receptor consiste no dispositivo que receberá os dados. A estratégia empregada para diferenciar os diversos dispositivos de uma rede de computadores consiste no endereçamento. Por meio desta estratégia torna-se possível atribuir identificadores únicos para cada dispositivo. Estes identificadores consistem em endereços. Ao longo deste material mais informações serão apresentadas sobre o endereçamento em redes de computadores.

ATENÇÃO: neste momento, podemos responder este questionamento afirmando que o endereço IP compreende em um tipo de endereço responsável por diferenciar dispositivos em uma rede de computadores.

A resposta do terceiro e último questionamento está estritamente relacionada com a definição do conceito de um protocolo de uma rede de computadores. Como uma rede de computadores pode ser composta por diferentes dispositivos em termos de funcionalidade, capacidade e fabricante, podemos facilmente identificar a necessidade de padronizar a forma como ocorre a interação entre esses dispositivos. Essa necessidade não existe apenas no contexto das redes de computadores, nós como seres humanos também seguimos de maneira quase inconsciente regras que determinam um padrão de interação em nossas relações. Por exemplo, quando recebemos uma chamada telefônica, intuitivamente seguimos um conjunto de regras para estabelecer uma comunicação. Primeiramente, levantamos o telefone do gancho e ficamos escutando a espera de uma mensagem de “alô”. Assim que recebemos essa mensagem, geralmente repetimos essa mensagem e, após esse procedimento, ambas as partes estão cientes que podem trocar informações. Esse comportamento compreende um conjunto de regras para nos comunicarmos através do telefone. Os computadores também precisam de regras para determinar como os dispositivos devem se comunicar, no entanto, essas regras precisam ser detalhadas de maneira muito precisa em forma de uma linguagem compreensível para eles.

ATENÇÃO: esclarecendo a necessidade de regras claras para estabelecer a comunicação, podemos responder ao terceiro questionamento afirmando que um protocolo de rede compreende um conjunto de regras que devem ser seguidas pelos dispositivos a fim de estabelecer a comunicação por meio de uma rede de computadores.

Através desta breve contextualização, talvez você tenha percebido que as pessoas utilizam termos técnicos estritamente relacionados com a área de redes de computadores no seu dia-a-dia sem compreender de fato o seu significado. Além dos termos aqui apresentados, existem muitos outros que poderiam ser mencionados. Como profissionais da área da informática, precisamos dominar esses conceitos e conhecer as diferentes classificações de estratégias relacionadas com as redes de computadores.

1.2
USO DAS REDES DE COMPUTADORES

As redes de computadores são empregadas para potencializar diversas atividades cotidianas das pessoas. Esta seção apresenta um panorama das principais áreas em que as redes de computadores são utilizadas. Os subitens abaixo abordam as finalidades comerciais e as finalidades domésticas, além de abordar a necessidade de mobilidade.

Finalidades Comerciais

O advento das redes de computadores proporcionou a exploração de novos nichos de mercado, pois as mesmas possibilitaram solucionar desafios existentes no modelo tradicional de comércio. Antes do surgimento das tecnologias em redes, um dos modelos mais empregados em transações comerciais se baseava na dependência de um local físico para atender os clientes e disponibilizar os produtos e/ou serviços. Com o surgimento das redes de computadores, muitos empresários visionários identificaram a oportunidade de quebrar este paradigma. As tecnologias de redes possibilitaram a flexibilização em relação à dependência de um local físico. Por meio desta inovação as empresas poderiam, por exemplo, oferecer seus produtos e serviços através da rede, proporcionando um gerenciamento mais eficiente dos produtos em estoque e aumentando a disponibilidade de atendimento aos clientes. A identificação deste potencial contribuiu para investimentos consideráveis para criação de uma infraestrutura de rede em escala global capaz de disponibilizar plataformas de comércio eletrônico.

ATENÇÃO: além do comércio eletrônico, as redes de computadores também geraram benefícios em relação ao compartilhamento de recursos e à comunicação entre funcionários.

Os recursos disponíveis em uma rede de computadores podem ser classificados como físicos e lógicos. Os recursos físicos compreendem os dispositivos de armazenamento, impressoras e unidades de processamento, ou seja, tudo o que pode ser tocado pelo ser humano. Os recursos lógicos consistem em tudo aquilo que não pode ser tocado, como, por exemplo, os dados e os programas disponíveis nos computadores.

A capacidade de compartilhamento de recursos por meio de uma rede representa um impacto positivo muito relevante. A aquisição de recursos físicos resulta em custos financeiros para as empresas. Alguns recursos físicos podem ter um custo financeiro moderado, como, por exemplo, uma impressora. Todavia, recursos físicos tais como um sistema de armazenamento de dados de alta capacidade possui um alto custo financeiro, agravando a situação. Como as instituições

comerciais são concebidas visando o lucro, as despesas financeiras tendem a ser minimizadas. O surgimento das redes de computadores possibilitou a criação de estratégias para minimizar as despesas com recursos físicos ao possibilitar o seu compartilhamento. Seguindo esta abordagem, as empresas poderiam adquirir, por exemplo, uma impressora e compartilhá-la para todos seus funcionários. Com o compartilhamento de recursos físicos, as redes de computadores possibilitam a minimização de custos financeiros, representando um importante ponto positivo para sua adoção nas empresas.

O compartilhamento de recursos lógicos resultou em benefícios ainda mais significativos para as empresas. As informações compreendem em um dos ativos mais importantes para as empresas. A carteira de clientes, os registros fiscais, as estratégias de negócio e os dados de movimentação de estoque de uma empresa consistem em informações vitais para uma empresa. A digitalização destes dados e armazenamento em um computador possibilita a manipulação destas informações de modo mais eficiente, potencializado a forma como elas são gerenciadas. O advento das redes de computadores permitiu que diferentes computadores compartilhassem esses dados, possibilitando uma sincronização entre as diferentes entidades responsáveis por manipular estes dados. Por exemplo, através do compartilhamento das informações de estoque, sempre que a entidade de um sistema responsável por efetuar uma venda, automaticamente o saldo atual do produto será atualizado para as demais entidades envolvidas no sistema.

As redes de computadores também potencializaram a forma como os funcionários se comunicam. Algumas empresas desempenham partes de suas atividades ou até mesmo serviços com base na dependência da comunicação de um funcionário com uma base de operação. Por exemplo, uma empresa com uma frota de caminhões necessita da comunicação dos motoristas com uma base de operações capazes de solucionar eventuais problemas durante suas viagens. O mesmo ocorre com empresas prestadoras de serviços técnicos de atendimento a domicílio, pois o técnico geralmente opera no exterior da empresa e necessita interagir com uma base de operações para obter informações sobre os clientes a serem atendidos e para finalizar ordens de serviço. Considerando o contexto das redes de computadores, muitos serviços e tecnologias de comunicação foram desenvolvidos, tais como o serviço de correio eletrônico e a voz sob IP (VoIP).

ATENÇÃO: estes serviços e tecnologias são comumente utilizados para possibilitar a comunicação entre a base de operação e os funcionários que desempenham tarefas externas das empresas com um baixo custo financeiro utilizando como base as redes de computadores.

Finalidades Domésticas

Muitas atividades domésticas também foram aprimoradas com o surgimento das redes de computadores. Os principais tipos de aplicações e serviços responsáveis por essa mudança podem ser organizadas em cinco categorias, sendo elas: *(i)*

aplicações baseadas na interação entre pessoas e uma base de dados remota; *(ii)* serviços construídos para possibilitar a comunicação entre pessoas; *(iii)* comércio eletrônico; *(iv)* aplicações de entretenimento; e *(v)* serviços para Internet das Coisas. Cada uma destas categorias será detalhada na sequência.

A principal característica das aplicações baseadas na interação entre pessoas e uma base de dados remota consiste na concentração de uma grande quantidade de dados disponibilizados por meio de servidores em uma rede de computadores. Um exemplo clássico deste tipo de aplicação consiste nas bibliotecas virtuais. Dentre estas bibliotecas, vale a pena mencionar o papel do portal de periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Este portal consiste em uma biblioteca virtual que disponibiliza o acesso às mais notáveis produções científicas internacionais, inclusive da área da Computação. Outro exemplo de aplicação largamente utilizada consiste na *Netflix*. Por meio deste serviço, os usuários podem acessar um vasto acervo de vídeos, tais como filmes, séries e documentários, através de *smartphones*, *smart TVs*, computadores ou *tablets*.

ATENÇÃO: neste caso, existe o papel de um agente humano com interesses de realizar operações de consultas nestes dados e interagem com os servidores para alcançar este objetivo.

A segunda classe de aplicações com fins domésticos possibilitam a comunicação entre pessoas. O objetivo deste tipo de aplicação consiste em promover a interação entre pessoas. Esta categoria pode ser subdividida em redes sociais, mensagens instantâneas e edição colaborativa de textos. As redes sociais permitem que seus usuários criem perfis e estabeleçam relações sociais com os demais usuários, como, por exemplo, o *Facebook*. Os serviços de mensagens instantâneas possibilitam que usuários mantenham uma rede de contatos para trocar mensagens. Muitos destes serviços oferecem não apenas a possibilidade do envio de mensagens de texto, mas também suportam o envio de conteúdos multimídia, tais como, áudio, vídeo e imagens ou chamadas de voz ou vídeo. A ferramenta *Skype* e o aplicativo *Whatsapp* consistem em uma das aplicações mais utilizadas desta categoria. Os serviços de edição de textos colaborativos potencializam a criação de um texto com diversos autores. Uma das aplicações que implementa este conceito consiste nas *wikis*. Dentre as *wikis* existentes, a *Wikipédia* ocupa uma posição de destaque ao prover uma enciclopédia livre criada e editada por diversos usuários ao redor do mundo.

As aplicações de comércio eletrônico possibilitaram a democratização na compra de produtos para usuários da Internet. Antes do surgimento desta classe de aplicações, as pessoas dependiam fortemente da visita física das lojas que vendiam os produtos do seu interesse. Com o comércio eletrônico, essa dependência foi eliminada, facilitando a aquisição e o pagamento de produtos por meio da infraestrutura da Internet. Como resultado, os usuários da Internet também tiveram acesso a um número muito maior de opções e produtos. Além disso, tornou-se fácil comparar os preços dos produtos praticados no mercado local dos usuários com aqueles oferecidos por lojas de diferentes regiões geográficas, possibilitando o pagamento de um preço mais justo pelos produtos. O Mercado Livre e o eBay constituem bons exemplos de serviços da classe de comércio eletrônico.

A forma como as pessoas desempenham atividades de lazer foi aprimorada com o advento de aplicações voltadas ao entretenimento. As atividades de lazer mais praticadas por meio da Internet consistem nos jogos on-line, em assistir vídeos e escutar músicas. Jogos com suporte para múltiplos jogares conectados em diferentes regiões geográficas foram criados para explorar mundos virtuais criados com objetivos de entretenimento. Alguns destes jogos contam com plataformas auxiliares para possibilitar a interação entre seus usuários por meio de chats e chamadas de áudio. Escutar músicas e assistir filmes também se tornaram atividades de laser dos usuários em ambientes domésticos. Neste sentido, a forma de acesso ao conteúdo de áudio e vídeo evoluiu ao longo dos anos. Nos primórdios da Internet, o aplicativo Napster foi criado para possibilitar o compartilhamento de músicas ao empregar um modelo descentralizado de armazenamento. Este modelo possibilitava aos usuários enviar e compartilhar músicas ao mesmo tempo, sem a presença de um servidor centralizado. O nome deste modelo consiste em *Peer-to-Peer* (P2P) ou *Par-a-Par* e será explicado com mais detalhes no decorrer deste material. Apesar dos benefícios proporcionados aos usuários, o Napster infringia os direitos autorais das músicas e foi judicialmente encerrado. Atualmente, o serviço *Spotify* possibilita a criação de *playlists* de músicas e muitos outros recursos sem infringir os diretos autorais das músicas ao pagar royalties aos autores. A *Netflix* também emprega estratégias semelhantes ao disponibilizar filmes por meio da sua plataforma.

INTERATIVIDADE: um vídeo sobre as redes P2P pode ser encontrado em: https://www.youtube.com/watch?v=QHGeWtmFOj4

A última classe de serviços e aplicações para usuários domésticos são projetados adotando o conceito de Internet das Coisas. Este novo conceito, também conhecido pela sigla IoT (do inglês, *Internet of Things*), surgiu como resultado de pesquisas no campo de redes sem fio modernas e assume que em um futuro próximo estaremos rodeados por uma larga quantidades de objetos (coisas) equipadas com interfaces de comunicação sem fio e unidades de processamento para melhorar a forma como são utilizadas. Essas coisas poderiam ser máquinas de lavar, cadeiras e até mesmo um lápis. Estes serviços poderiam prestar, por exemplo, serviços relacionados com os cuidados com a saúde das pessoas de uma casa ao coletar sinais vitais de um morador por intermédio de sensores localizados em sua camiseta, enquanto o mesmo assiste televisão. Apesar de que este cenário pareça um pouco assunto dos filmes de ficção científica, existe um esforço considerável da indústria para alcançarmos essa realidade em um futuro próximo. Podemos levemente perceber esse esforço ao observar que cada vez mais dispositivos dentro das nossas casas já possuem unidades de processamento e interfaces de comunicação sem fio, como por exemplo, as televisões e os *smartphones*.

ATENÇÃO: partindo deste princípio, novos serviços seriam concebidos explorando a conectividade entre estes objetos para potencializar diversas atividades cotidianas.

Mobilidade

Os usuários dos sistemas construídos para operar sob as redes de computadores geralmente permanecem interessados em acessar seus dispositivos para executar as mais variadas atividades. Como resultado, a indústria constantemente provê e aprimora dispositivos e tecnologias para comunicação sem fio. Ao usar este arcabouço de soluções, os usuários poderiam manter-se em movimento enquanto realizavam atividades de computação, abrindo portas para uma nova área relacionada com a área de redes de computadores, a mobilidade.

Essa nova área despertou a atenção do mercado das redes celulares e da indústria militar. Muitas empresas de telefonia celular se interessaram em atuar como provedores de uma infraestrutura capaz de servir usuários móveis, ao explorar a infraestrutura de antenas já existentes e até então usadas apenas para comunicação de tráfego de áudio de ligações. Entrando nesse novo nicho de mercado, as antenas poderiam incluir a prestação de serviços de dados com objetivos de aumentar suas receitas. As tecnologias tais como 3G, 4G e 5G surgiram como soluções para suprir essa demanda e atualmente estão presentes no cotidiano de grande parte das pessoas.

A indústria militar também demostrou grande interesse no conceito de mobilidade. Um tema largamente pesquisado neste contexto consiste na criação de redes de sensores sem fio. A ideia central desta abordagem compreende a criação de uma infraestrutura de rede de comunicação sem fio, onde existem diversos sensores capazes de coletar informações sobre um ambiente e armazenar os resultados em uma base de dados. Podemos imaginar os benefícios de uma rede como essa ao supor a aplicação de uma rede de sensores em uma área onde manobras militares são executadas e as informações coletadas sobre essa área fossem atualizadas em tempo real. Essas informações poderiam ser utilizadas na tomada de decisões antes da execução de manobras militares, podendo compreender uma vantagem tecnológica significativa.

Além destes dois exemplos, as redes de computadores sem fio também agregam benefícios para usuários de aplicações domésticas e comerciais. O mesmo acontece em relação às aplicações comerciais. Todavia, o mercado da mobilidade também abriu novas oportunidades para que empresários visionários aumentassem seus lucros. Muitas empresas conseguiram explorar particularidades específicas da mobilidade para prestar novos tipos de serviços para os usuários. Por exemplo, a empresa desenvolvedora do aplicativo Uber vem lucrando ao oferecer um serviço de transporte semelhante ao prestado pelo taxis, mas com um preço mais acessível e muitas vezes mais eficiente.

ATENÇÃO: a mobilidade potencializa as aplicações domésticas, permitindo que os benefícios mencionados na Seção 1.2.1 pudessem ser alcançados mesmo quando os usuários estivessem em trânsito.

A prestação de serviços para usuários móveis vem despertando o interesse de muitos segmentos e esperam-se muitas novidades neste setor para os próximos anos. O setor de telefonia celular e a indústria militar são exemplos de segmen-

tos com alto interesse em aplicações móveis. Estima-se que nos próximos anos venham a se consolidar outras tecnologias construídas com base na mobilidade, como por exemplo o Google Glass. Este novo dispositivo se parece com um óculos tradicional, mas agrega uma pequena tela acima do campo de visão para possibilitar a interação com rotas de mapas, opções de música, realizar chamadas de vídeo ou tirar fotos e compartilhar e acessar conteúdos disponíveis na Internet.

1.3
EVOLUÇÃO DAS REDES DE COMPUTADORES

As redes de computadores como conhecemos hoje surgiram como consequência de uma série de melhorias implantadas ao longo do tempo que caracterizam seu processo evolutivo. Os momentos mais relevantes da evolução das redes de computadores podem ser classificados em função das seguintes décadas: 1950 e 1960, 1970, 1980, 1990 e anos 2000.

Primórdios da Internet

Antes da criação do conceito das redes de computadores, algumas tecnologias foram desenvolvidas favorecendo o surgimento deste conceito. Estas tecnologias consistiram no teleimpressor, a *Mondothèque* e no modem. Os principais componentes destas máquinas consistiam em um teclado, um transmissor, um receptor, uma fita e uma impressora. Os teleimpressores evoluíram do sistema de telégrafos. A Figura 2 apresenta este dispositivo sendo utilizado durante a Segunda Guerra Mundial pelas forças aliadas contra o eixo.

TERMO DO GLOSSÁRIO: os teleimpressores consistem em máquinas eletromecânicas capazes de transmitir e receber mensagens de texto para impressão.

FIGURA 2 – Teleimpressores Sendo Utilizados Durante a Segunda Guerra Mundial

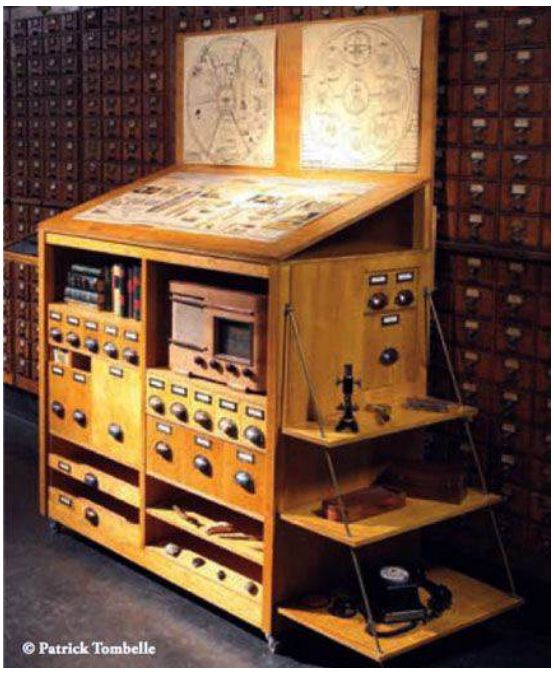
FONTE: Computer History. Disponível em: <http://www.computerhistory.org/timeline/networking-the-web/>

Os teleimpressores possuíam dois modos de operação, local e remoto. No modo local, o aparelho se comportava como uma máquina de escrever com funções adicionais para ler dados de uma fita. O modo remoto englobava as mesmas funcionalidades do modo local, com a adição das funções de impressão e enviar mensagens para impressão. Para implementar o modo remoto, estas máquinas empregavam os componentes transmissor e receptor para se comunicar usando diversos canais de comunicação em configurações ponto-a-ponto ou multiponto por meio de uma rede de comutação Telex. Inicialmente, a rede Telex foi desenvolvida para trocar mensagens militares, mas acabou servindo propósitos comerciais e persistiram até os anos 2000 em alguns países.

SAIBA MAIS: a rede Telex consistiu em uma rede criada para dar suporte aos teleimpressores, sendo muito parecida com as redes de telefonia convencional, mas transportavam apenas mensagens de texto.

A *Mondothéque* surgiu como resultado do pesquisador belga Paul Otlet em alcançar o objetivo de coletar, organizar e compartilhar todo o conhecimento do mundo. Este invento se relaciona com o conceito das redes de computadores, pois era idealizado que as pessoas teriam uma *Mondothèque* em suas casas como uma estação de trabalho conectada com uma biblioteca universal. Otlet iniciou seus esforços para criar um mecanismo de busca no início dos anos 1900, chegando a construir um catálogo com dezesseis milhões de dados, compreendendo fotos, documentos, microfilmes, entre outros. A Figura 3 apresenta uma réplica da *Mondothèque*.

FIGURA 3 – Réplica de uma "*Mondothèque*", uma estação multimídia domiciliar



FONTE: Computer History. Disponível em: http://www.computerhistory.org/timeline/networking-the-web/

Para reunir todo o conhecimento do mundo, Otlet idealizou uma "Cidade Mundial" ou "Cité Mondiale" que constituiria em uma exposição universal responsável por reunir todas as principais instituições do mundo. A responsabilidade da Cidade Mundial seria de transmitir conhecimentos para o resto do mundo e promover a cooperação universal. Vários arquitetos colaboraram para a criação desta cidade, contribuindo com diversos projetos e modelos. Além disso, muitos empresários bem-sucedidos investiram quantias consideráveis de recursos para consolidar o projeto, como foi o caso do empresário norte-americano Andrew Carnegie, também conhecido como o rei do aço. No entanto, Otlet morreu em 1944, seu projeto foi fechado e as fontes de financiamento foram perdidas.

Os fundamentos por trás da criação do modem surgiram em 1949 e descreviam como as informações poderiam ser representadas em um formato capaz de possibilitar a sua transmissão através de meios físicos. As principais funções de um modem consistem em modular dados digitais em sons e desmodularizar sons recebidos em dados digitais. Os modens estavam em ação nos serviços de teleimpressores desde os anos 1920. Cada teleimpressor deveria estar fisicamente conectado com um modem operando a 110 bits por segundo (bps), usando interfaces de conexão seria RS-232. Os modens possibilitavam estabelecer conexões remotas entre os teleimpressores, mas até este momento, não existiam computadores envolvidos.

SAIBA MAIS: o nome do dispositivo foi criado em função destas funções (*MODulation* + *DEModulation* = MODEM).

Com o passar do tempo, surgiu a necessidade das forças aéreas norte-americanas transmitirem centenas de imagens de radar para os centros de comando durante a Guerra Fria. Visando contornar esta necessidade, os pesquisadores da época se basearam na utilização do modem sistema telefônico. Em 1949, o Centro de Pesquisa das Forças Aéreas de Cambridge (*Air Force Cambridge Research Force* – AFCRC) desenvolveu um dispositivo para transmitir sinais de radar, modular dados digitais em sons e desmodularizar sons recebidos em dados digitais. A primeira aplicação deste dispositivo para computadores aconteceu em 1953 para servir aos propósitos do sistema SAGE, o qual detalharemos na sequência. A comercialização do modem para fins de aplicação em computadores aconteceu em 1958 pela companhia telefônica Bell. A Figura 4 apresenta o modem AT&T Circa de 1958. Os modens desempenharam um papel muito importante no rápido crescimento da Internet, sendo empregados em conexões dial-up, as quais possibilitavam a conexão de um computador à Internet por meio da infraestrutura das redes telefônicas.

ATENÇÃO: a estratégia de negócio da Bell consistia em permitir que os computadores utilizassem as linhas de voz dedicadas ao sistema telefônico, assim aumentaria a cobertura das linhas de comunicação para os computadores com um custo menor do que os telégrafos dedicados.

FIGURA 4 – Modem AT&T Circa de 1958

FONTE: Computer History. Disponível em: http://www.computerhistory.org/timeline/networking-the-web/

O sistema SAGE (*Semi-Automatic Ground Enviroement*) foi desenvolvido pela IBM para detectar bombardeiros russos durante a Guerra Fria. Este sistema foi pioneiro na exploração do emprego de computadores em rede. Ao todo, o sistema contava com vinte e três centros de computação distribuídos na América do Norte, os quais se comunicavam em tempo real com estações de radares e aeronaves de contra-ataque para reagir contra eventuais situações de ameaça. O sistema operou entre as décadas de 1950 e 1980. A Figura 5 mostra um usuário operando o sistema SAGE.

FIGURA 5 – SAGE: Primeiro Sistema de Defesa Aéreo em Rede

FONTE: Computer History. Disponível em: http://www.computerhistory.org/timeline/networking-the-web/

Um operador do sistema SAGE interagia com um console, um dispositivo sensível à luz semelhante a uma arma e um computador. A tela do console consistia em um tubo CRT semelhante aos dos primeiros computadores pessoais. O tubo possuía uma máscara alfanumérica no caminho de feixe de elétrons para representar a trajetória de um objeto no radar. Esta funcionalidade foi construída com processos eletrônicos complexos, mas se mostrou apto para atingir seus objetivos. O operador possuía um teclado para inserir dados e uma espécie de arma sensível a luz desenvolvida para reconhecer informações posicionais de um objeto e inseri-los no computador. Por meio da manipulação dos componentes do sistema, um operador identificava objetos em movimentos e inseria dados em um sistema computacional capaz de manipular estes dados e sinalizar operações de controle relacionadas com a proteção do espaço aéreo norte americano.

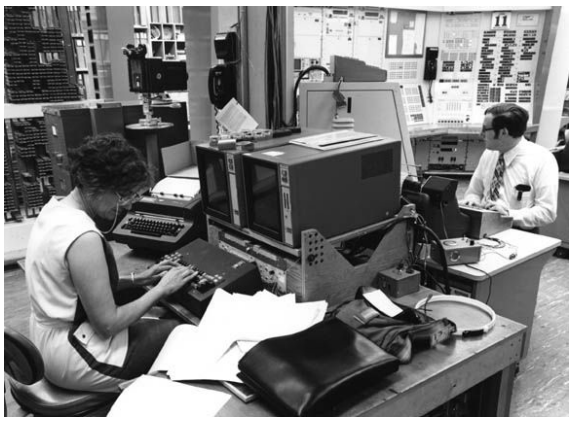
ATENÇÃO: a interconexão neste sistema era implementada por meio de radares posicionados até aproximadamente quarenta quilômetros de distância.

Anos 1960

Durante a década de sessenta, alguns acontecimentos chave contribuíram significativamente para o surgimento das redes de computados como conhecemos hoje. Dentre estes acontecimentos, podemos mencionar o surgimento do conceito de redes de computadores, avanços na comunicação via satélite, o surgimento do primeiro padrão universal para permitir a troca de dados entre máquinas fabricadas por diferentes empresas, a criação da primeira rede de computadores, a ARPANET, e a conexão dos primeiros computadores nesta rede. O advento do conceito de redes de computadores ocorreu em meados de 1962, sendo atribuído sua autoria ao cientista da computação e psicólogo Joseph Carl Robnett Licklider, conhecido simplesmente como J. C. R. ou Lick para seus familiares. Em outubro de 1962, 'Lick' se tornou um dos pesquisadores líderes do programa de pesquisa computacional ARPA (*Advanced Research Projects Agency*) do Departamento de Defesa dos Estados Unidos da América. A Figura 6 mostra J. C. R. Licklider trabalhando na estação de trabalho TX-2 enquanto rodava experimentos relacionados com o projeto de programas gráficos assistidos por computador.

ATENÇÃO: este conceito foi expresso, primeiramente, em memorandos escritos por J. C. R. Licklider ao descrever uma rede intergaláctica, onde cada indivíduo do globo estaria interconectado e poderia acessar programas e dados em qualquer sítio, independente da sua localização.

FIGURA 6 – Computador TX-2 no MIT



FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/196os/

Os anos 60 também foram marcados por avanços relacionados com a comunicação entre satélites. Em 1963, o satélite SYNCOM (*SYNchronous COMmunication satellite*), ou satélite de comunicação síncrona, foi lançado pela agência espacial NASA (*National Aeronautics and Space Administration*). A Figura 7 mostra o satélite SYNCOM em construção. Ainda em 1963, um comitê formado por membros da indústria e do governo criou o padrão ASCII (*American Standard Code for Information Interchange*). Este padrão possibilita que máquinas produzidas por diferentes fabricantes troquem dados. Por meio dele, cento e vinte e oito *strings* únicas de sete bits são usadas para descrever o alfabeto inglês, numerais arábicos, pontuações, símbolos e caracteres com funções especiais. Em 1968, o maior supercomputador do seu tempo foi construído pela NASA, o ILLIAC IV. Esta máquina foi construída com mais de mil transistores em sua memória RAM. A Figura 8 mostra o supercomputador ILLIAC IV.

TERMO DO GLOSSÁRIO: O ASCII consistiu no primeiro padrão universal para codificação de caracteres produzido para computadores.

FIGURA 7 – Satélite SYNCOM em Construção

FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/196os/

FIGURA 8 – ILLIAC IV: Maior Supercomputador da década de 60

FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/1960s/

A combinação dos esforços pelo grupo ARPA em conjunto com o advento do conceito da comutação por pacotes, resultou na criação ARPANET. Inicialmente, os pesquisadores da ARPA idealizaram a criação de uma rede de computadores com base na infraestrutura das redes telefônicas e seguindo o mesmo padrão de comutação de dados. Esse modelo de comutação, também conhecido como comutação por circuito, adotava como princípio a alocação exclusiva dos recursos dos dispositivos da rede de interconexão para realizar a troca de dados entre um emissor e um receptor. Em 1966, Donald Davies, apresentou o conceito da comutação por pacotes, resolvendo este problema. O princípio deste novo modelo de comutação consistia em quebrar a informação em várias partes pequenas, chamadas pacotes. Cada pacote seria enviado de um emissor para um receptor através de uma rede de dispositivos intermediários e medidas de controle da garantia destes pacotes seriam empregadas. Em 1967, os pesquisadores da ARPA empregaram o conceito da comutação por pacotes em seu protótipo de rede, a ARPANET. Com a implementação deste conceito, a velocidade da ARPANET foi melhorada de 2.4 Kbps para 50 Kbps. Como consequência, o projeto do modem da década de 50 foi vastamente aprimorado para implementar este conceito e possibilitar a troca de pacotes por meio das redes telefônicas.

ATENÇÃO: a ARPANET consistiu na primeira rede de computadores totalmente funcional de larga escala e hoje é considerada a avó da Internet atual.

A grande desvantagem deste modelo consistia no desperdício dos recursos da rede entre os dispositivos comunicantes, visto que somente após o término de uma conexão outra poderia ser estabelecida.

Neste momento surgiu o primeiro comutador de pacotes, o qual foi denominado de IMP (*Interface Message Processor*). A Figura 9 mostra a parte externa deste dispositivo. Sempre que um computador conectado na ARPANET enviava um pacote para um determinado destino, o IMP era responsável por encontrar a melhor rota entre o emissor e receptor considerando a rede intermediária de computadores entre eles. Por implementar a função de roteamento de pacotes, isto é, encontrar a melhor rota entre um emissor e um receptor, afirma-se que o IMP consistiu no primeiro roteador criado. Além disso, pode-se dizer que o IMP atuava como

um *gateway*, ou seja, uma máquina híbrida entre as redes de cada domínio. Para conectar o computador e o MPI, era utilizado uma interface serial especial. O primeiro IMP foi construído em 1969 em Massachusetts. Internamente, o IMP possuía um minicomputador Honeywell 516, capaz de armazenar doze mil palavras de memória. A Figura 10 apresenta a parte interna deste dispositivo.

TERMO DO GLOSSÁRIO: O IMP consistia em uma grande caixa de estrutura metálica responsável por prover uma interface entre os computadores e a ARPANET e foi o primeiro comutador de pacotes.

Neste momento, a ARPANET já possuía os principais componentes para ser implementada. O conceito da comutação por pacotes havia se apresentado como uma alternativa viável para resolver os problemas da comutação por circuitos e o IMP possibilitava a função de comutação de pacotes na prática. Para testar o funcionamento da ARPANET e de fato implementá-la, foram selecionados quatro nós, ou seja, os quatro primeiros computadores da rede a serem interconectados. A Figura 11 apresenta o diagrama criado em 1969 mostrando a interconexão entre estes nós.

ATENÇÃO: os quatro nós escolhidos estavam fisicamente localizados na Universidade da Califórnia em Los Angeles (*University of California*, Los Angeles - UCLA), o Instituto de Pesquisa de Stanford (*Stanford Research Institute* - SRI), a Universidade da Califórnia em Santa Bárbara (*University of California, Santa Barbara* - UCSB) e a Escola de Computação da Universidade de Utah.

FIGURA 9 – Parte externa do MPI, o Primeiro Comutador de Pacotes

FONTE: Computer History. Disponível em: http://www.computerhistory.org/revolution/networking/19/407/2086

FIGURA 10 – Parte interna do MPI, o Primeiro Comutador de Pacotes

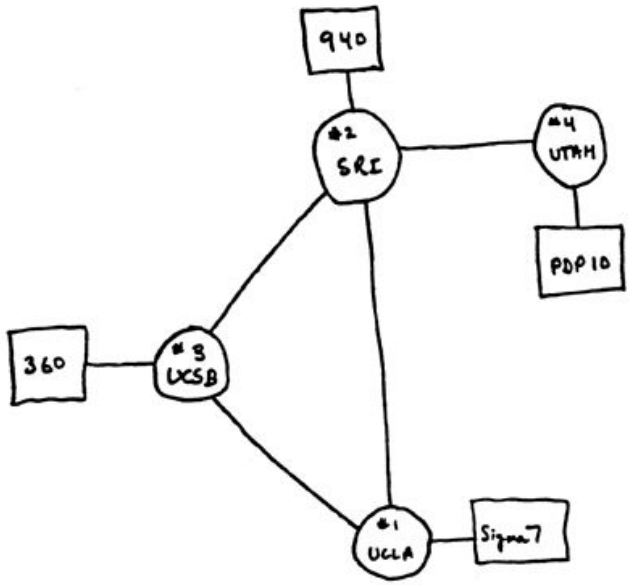
FONTE: Computer History. Disponível em: http://www.computerhistory.org/revolution/networking/19/407/2086

Em alguns dos primeiros nós da ARPANET foram realizadas pesquisas relacionadas com o aprimoramento da rede. Na UCLA, o pesquisador Leonard Kleinrock estabeleceu o Centro de Mensuração de Redes, o qual foi responsável por registrar o primeiro log de uma mensagem enviada através da ARPANET por meio de um IMP datada em 29 de Outubro de 1969. Além disso, esta instituição iniciou o desenvolvimento do NCP (*Network Control Protocol*). Com o passar do tempo, o NCP foi substituído pelo protocolo TCP/IP, mas isso será explicado no decorrer do material. O computador usado pela UCLA consistia no SDS Sigma 7, um computador de 32 bits desenvolvido para aplicações científicas. No SRI, o pesquisador Douglas Engelbart desenvolveu o NLS, o primeiro sistema a utilizar links de hipertexto, o mouse, monitor de vídeo e outros conceitos modernos da computação. A UCSB, por meio dos pesquisadores Glen Culler e Burton Fried, investigou métodos para apresentar funções matemáticas usando displays de armazenamento para tratar o problema da atualização dos dados da rede impressos em telas. O computador usado pela UCSB consistia em um IBM 360/75, um sistema de computador mainframe, equipado com um sistema operacional OS/MVT.

TERMO DO GLOSSÁRIO: O NCP consistiu no primeiro protocolo capaz de permitir aos usuários acessar/usar computadores remotos e transmitir arquivos entre dois computadores.

INTERATIVIDADE: um vídeo introdutório que explica o funcionamento da Internet e o papel do protocolo IP pode ser encontrado em https://www.youtube.com/watch?v=HNQDoqJoTC4

FIGURA 11 – Diagrama da ARPANET com Quatro Nós em 1969



FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/1960s/

Década de 1970

Os principais eventos em 1970 consistiram no surgimento do UNIX, na crescente adição de nós na ARPANET e nos aprimoramentos dos protocolos e das interfaces de conexão. Em 1970, os programadores Dennis Ritchie e Kenneth Thompson nos laboratórios da Bell finalizaram o desenvolvimento do Sistema Operacional (SO) UNIX. Este SO proporcionava as funcionalidades de tempo compartilhado e de gerenciamento de arquivos. Devido a estas características, o UNIX foi largamente utilizado, principalmente no meio científico. Ainda neste ano, foram adicionados nós à ARPANET em uma taxa de um nó por mês. Uma interface de rede de alta velocidade, capaz de transmitir 100 kbps entre o IMP e um computador PDP-6 foi desenvolvida por Bob Metcalfe. Esta interface operou por treze anos sem a intervenção humana. Em dezembro de 1970, a primeira versão do protocolo NCP foi implantada, permitindo a conexão ponto-a-ponto entre computadores na ARPANET.

ATENÇÃO: estas funcionalidades foram muito importantes para o desenvolvimento das redes de computadores, pois esse sistema possibilitava que um computador fosse acessado e utilizado por vários usuários simultaneamente.

O ano 1971 foi marcado pelo surgimento de um novo comutador de pacotes, novos protocolos e pelo crescimento do número de nós da rede. A empresa de tecnologia BBN (*Bolt, Beranek and Newman*) modificou o projeto do IMP para torná-lo mais simples e ser capaz de operar outras plataformas. Além disso, a BBN desenvolveu uma nova plataforma chamada TIP (*Terminal Interface Processor*), a

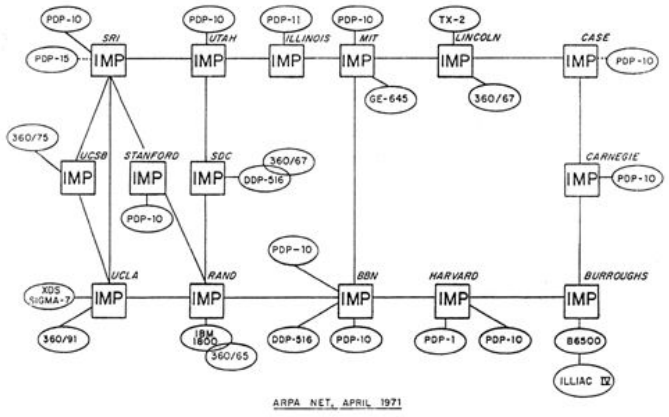
qual era capaz de suportar a entrada de múltiplos hosts ou terminais. A Figura 12 apresenta o TIP desenvolvido pela BBN. Os protocolos Telnet e FTP (*File Transfer Protocol*) foram desenvolvidos pelo *Network Working Group*, ou o Grupo de Trabalho de Redes. No início de 1971, a ARPANET possuía quatorze nós, no final deste mesmo ano havia dezenove computadores conectados à rede. A Figura 13 ilustra o mapa da rede neste ano, onde as elipses representam os computadores e os quadrados os comutadores.

ATENÇÃO: o Telnet possibilitava usuários a acessarem máquinas remotas conectadas na rede, enquanto que o FTP permitia a transferência de arquivos entre máquinas conectadas à ARPANET.

FIGURA 12 – Comutador de Pacotes TIP desenvolvido pela BBN

FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/1970s/

FIGURA 13 – Mapa da ARPANET em 1971



FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/1970s/

No final de 1971, existiam muitos pequenos projetos sendo desenvolvidos com o suporte da ARPANET. No entanto, o tráfego utilizado por estes projetos era ainda aquém da capacidade total da rede. Devido a este fato, os pesquisadores da ARPA identificaram a necessidade de estimular outros pesquisadores para atingir o conceito original de um ambiente colaborativo e interativo. Para colocar em prática esta ideia, os pesquisadores Larry Roberts e Bob Kahn decidiram coordenar uma demonstração pública da ARPANET durante a Conferência Internacional de Comunicação de Computadores, que seria realizada em Washington em outubro de 1972. Nessa demonstração, outros pesquisadores foram convidados a criar aplicações explorando o conceito original de colaboração e interatividade que deu origem à ARPANET. Como resultado, várias aplicações interessantes surgiram.

SAIBA MAIS: uma das demonstrações mais interessantes consistiu em uma conversação entre ELIZA, uma inteligência artificial de um psiquiatra localizada no MIT e PARRY, uma inteligência artificial desenvolvida e localizada em Stanford para se comportar como um paciente paranóico. Outras demonstrações interessantes consistiram em jogos de xadrez interativos e um simulador de controle de tráfego aéreo aprimorado.

Outros acontecimentos importantes aconteceram em 1972. Ray Tomlinson da empresa BBN escreveu o primeiro programa para enviar uma mensagem por meio de um correio eletrônico sob a ARPANET. O laboratório da Bell desenvolveu a linguagem C. Steve Wozniak, que mais tarde se tornaria um dos fundadores da *Apple Computers*, iniciou sua carreira desenvolvendo um dispositivo chamado de 'caixas azuis', um gerador de tons que possibilitava chamadas de longa distância ao burlar o equipamento de cobrança de tarifas da companhia telefônica. Além disso, a ARPANET cresceu mais dez nós durante os primeiros dez meses deste mesmo ano.

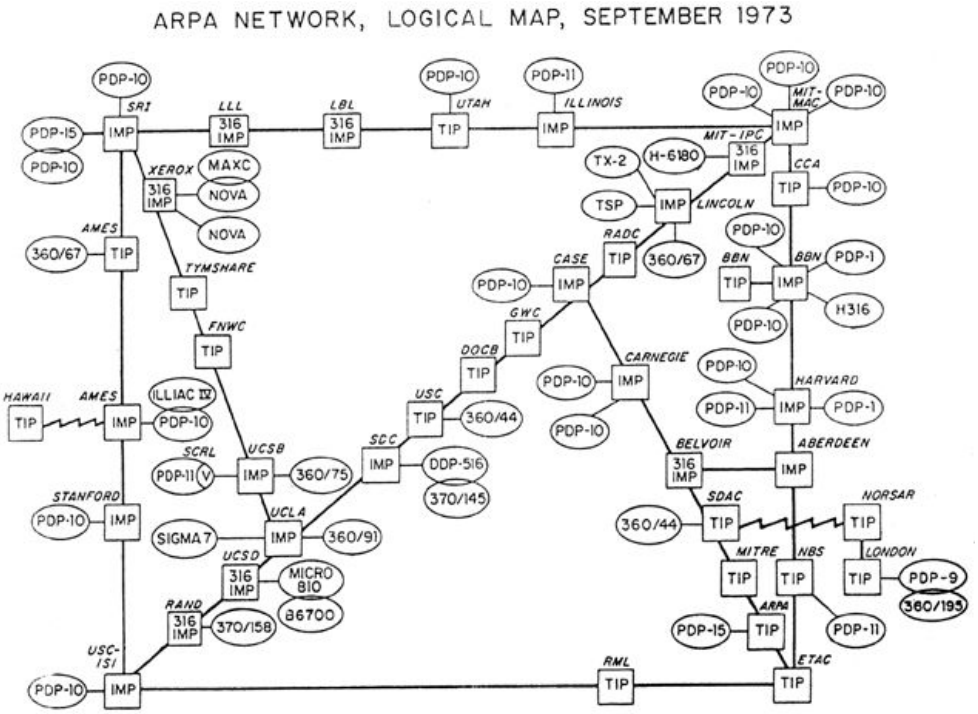
Em 1973, trinta instituições estavam conectadas à ARPANET e outras redes de computadores estavam operando na Europa. A Figura 14 apresenta o mapa da ARPANET em 1973. Pesquisas desenvolvidas na Universidade do Hawaii deram origem ao protocolo ALOHA, o qual servia como uma solução de controle de acesso ao meio. Estas pesquisas possibilitaram conectar as quatro ilhas do arquipélago do Hawaii por meio de enlaces sem fio, esta rede de computadores foi denominada ALOHANET. Conexões via satélite também foram criadas para conectar estações localizadas no Reino Unido e na Noruega. A rede francesa CYCLADES e a rede britânica NPL estavam começando a ser interconectadas, como apresenta a Figura 15. A união destas redes resultaria na rede EIN (*European Informatics Network*), ou Rede Europeia de Informática.

ATENÇÃO: neste momento, os usuários da rede compreendiam desde instituições industriais, corporações empresariais, tais como a BBN e a Xerox, e instituições governamentais, tais como a NASA e setores da força aérea norte americana.

Os principais eventos de 1974 consistiram na criação da rede NSF, o surgimento do protocolo TCP e a constatação de um grande volume de tráfego na ARPANET. A NSF (*National Science Foundation*) consistiu em uma iniciativa governamental nos Estados Unidos para incentivar as universidades a se conectarem às redes de computadores. Em 1974, a NSF possuía quase cento e vinte universidades. Em maio de 1974, Bob Kahn e Vint Cerf publicaram o artigo "*A Protocol for Packet Network Interconnection*" apresentando o protocolo TCP (*Transmission Control Protocol*). O governo norte americano financiou a implementação do TCP contratando três empresas para implementar este protocolo. Neste momento, o tráfego diário da ARPANET excedia três milhões de pacotes.

TERMO DO GLOSSÁRIO: O TCP provê confiabilidade e controle de erros em redes baseadas na comutação por pacotes.

FIGURA 14 – Mapa da ARPANET em 1973



FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/1970s/

FIGURA 15 – Rede Europeia de Informática em 1973

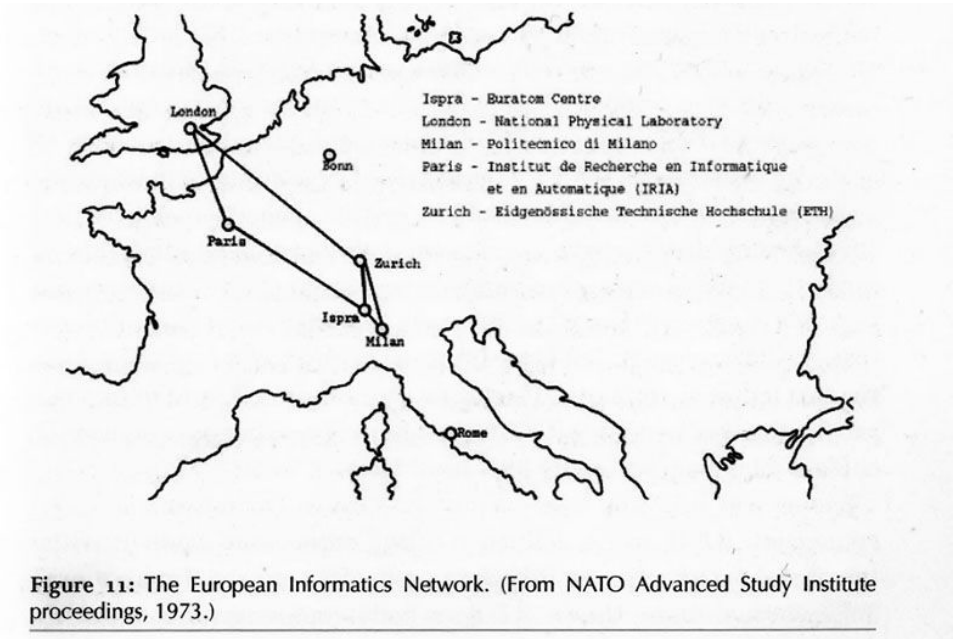


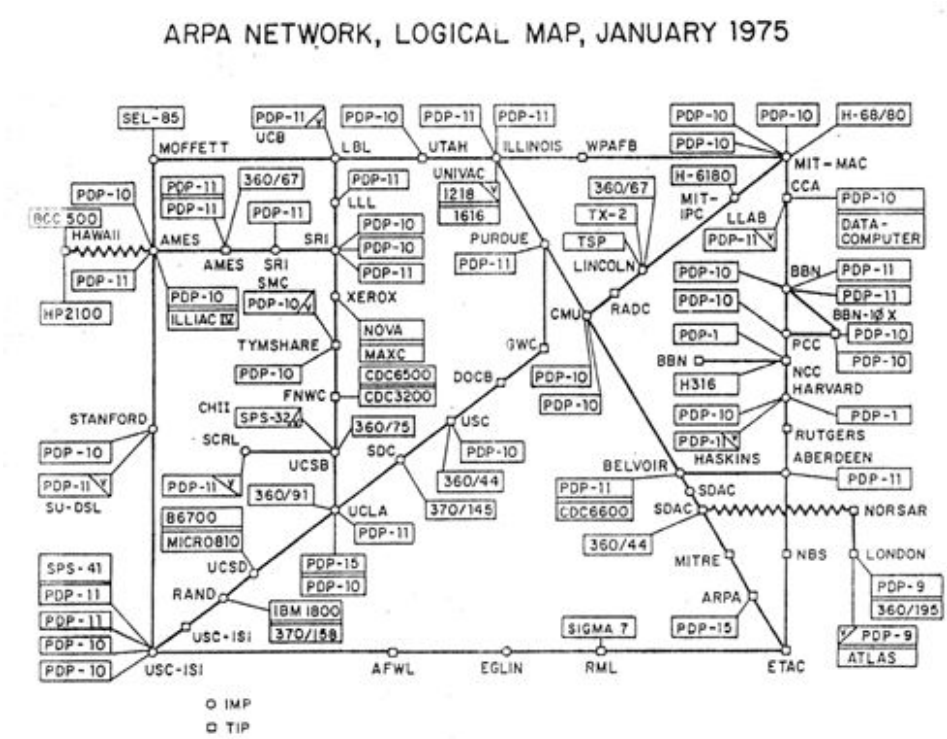
Figure 11: The European Informatics Network. (From NATO Advanced Study Institute proceedings, 1973.)

FONTE: Computer History. Disponível em: http://www.computerhistory.org/timeline/networking-the-web/

No ano de 1975, a ARPANET possuía 61 nós. A Figura 16 mostra o mapa da rede neste momento. Um grande avanço neste ano consistiu na iniciativa da BBN em liberar o código fonte dos softwares que operavam nos IMPs e TIPs, favorecendo a consolidação de um protocolo padrão para operar em diferentes redes de computadores. Como resultado da disponibilização do código fonte destes softwares, o Grupo de Trabalho de Redes proporcionou discussões sobre a implementação de melhorias nestes códigos por meio de listas de e-mail e por RFCs (*Request for Comments*).

TERMO DO GLOSSÁRIO: uma RFC consiste em um documento formal da IETF (*Internet Engineering Task Force ou Força Tarefa de Engenharia da Internet*) descrevendo o resultado do rascunho do comitê para que as partes interessadas possam revisar as ideias discutidas.

FIGURA 16 – Mapa da ARPANET em 1975



FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/1970s/

Entre 1976 e 1979 foi realizada uma série de avanços. Em 1976 os cientistas da Universidade da Califórnia Berkeley receberam o suporte da DARPA para incorporar os protocolos TCP/IP no UNIX. A DARPA consistia no departamento que até então mencionamos como ARPA. Este departamento foi reformulado para agregar a responsabilidade de defesa, em razão disto recebeu a letra 'D' de Defense em inglês. Note que o UNIX passou a operar com a pilha de protocolos TCP/IP e não apenas o protocolo TCP. Em 1977, a ARPANET foi conectada com a rede SATNET, possibilitando a troca de dados por satélites com o Colégio Universidade de Londres e os nós conectados na ARPANET. Nesse mesmo ano, a Universidade de Wisconsin nos Estados Unidos criou a rede THEORYNET para prover o serviço de e-mail para cerca de cem pesquisadores. Em 1978, começou a surgir muitos computadores de pequeno porte e capazes de se conectar à rede. Em 1979, a rede USENET iniciou uma série de algoritmos desenvolvidos por Steve Bellovin definindo os papéis de um cliente e um servidor na rede, onde o cliente envia requisições para um serviço disponibilizado por um servidor.

ATENÇÃO: a sigla TCP/IP consiste na combinação do protocolo TCP com o IP, sendo o primeiro responsável pelas medidas de controle dos pacotes e o segundo trata o endereçamento dos computadores.

Década de 1980

Durante a década de 80, muitos avanços foram realizados em relação à evolução das redes de computadores, compreendendo desde a proliferação de computadores pessoais, a interconexão das redes existentes e o surgimento da Web. Em 1980, a NFS patrocinou um workshop para revisar as estruturas de rede da época. Neste mesmo ano, a NFS concorda em gerenciar a rede CSNET por dois anos, depois disto as tarefas de administração da CSNET voltaria para o centro de pesquisa UCAR (*University Corporation for Atmospheric Research*), a qual era composta por mais de cinquenta instituições acadêmicas. Ainda em 1980, a IBM decide comercializar seu projeto de computador pessoal, o PC configurado com o sistema operacional DOS desenvolvido pela Microsoft.

ATENÇÃO: durante este período, o governo americano financiou a implantação dos protocolos TCP/IP na rede CSNET.

Em 1981, a rede CSNET possuía mais de duzentos computadores conectados. O grupo de trabalho da Internet tornou público a intenção de substituir o protocolo NCP pela pilha de protocolos TCP/IP. Surgiu o primeiro computador portátil, o Osborne. A Figura 17 apresenta o Osborne. Apesar de ser uma ideia visionária neste momento, o Osborne apresentava limitações que dificultavam a implantação do conceito de portabilidade. Por exemplo, o seu peso consistia em 10,8 quilogramas e não possuía uma bateria integrada, demandando que o dispositivo fosse conectado diretamente na rede elétrica. Ainda em 1981, a IBM começou a comercializar o PC conforme apresentado na Figura 18.

FIGURA 17 – Osborne, o Primeiro Computador Portátil

FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/1980s/

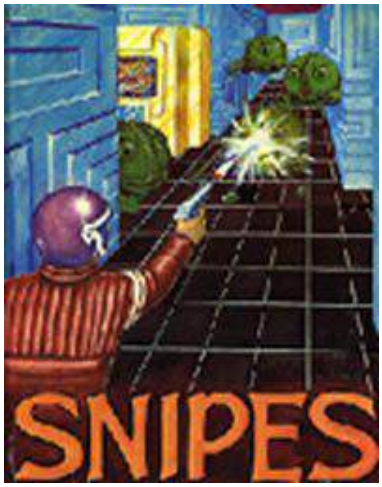
FIGURA 18 – Primeiro PC da IBM

FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/1980s/

Em 1982, começaram a surgir computadores clones do IBM PC. O jogo de ação Snipes surgiu neste mesmo ano, adotando como premissa a interconexão de PCs sob uma rede de computadores. A Figura 19 apresenta uma imagem publicitária deste jogo. Ainda neste ano surgiu a primeira interface de cabo coaxial para conectar um mainframe com um microcomputador. Também começou a existir esforços para discutir os padrões utilizados para definir como as arquiteturas de redes deveriam ser construídas. Até este momento, a pilha de protocolos TCP/IP prevalecia na maioria das redes. No entanto, muitos outros fabricantes possuíam seus próprios padrões proprietários, sendo incompatível com os demais. Por exemplo, uma empresa de fabricação de microcomputadores apenas seguiria os padrões de interconexão de rede, sobrando mais tempo para melhorar a usabilidade dos seus computadores. Para competir com o modelo TCP/IP, a ISO (I*nternational Organization for Standards*) apresentou o modelo de referência OSI (*Open Systems Interconnection*). No decorrer do material, estes dois modelos serão comparados e mais detalhes serão fornecidos. Como resultado desta competição, o modelo TCP/IP se consolidou como um padrão de fato, principalmente devido à grande adoção deste padrão por parte dos fabricantes e o modelo OSI permaneceu como uma diretriz a ser seguida, permanecendo como essencialmente teórica.

ATENÇÃO: a definição de um padrão a ser seguido por todos os fabricantes eliminaria esta incompatibilidade e exoneraria os fabricantes da tarefa de criar e manter seu próprio padrão, gerando a oportunidade das empresas se concentrarem apenas em serviços específicos alinhados com seu plano de negócio.

FIGURA 19 – Snipes – Jogo de Ação em Rede de 1982

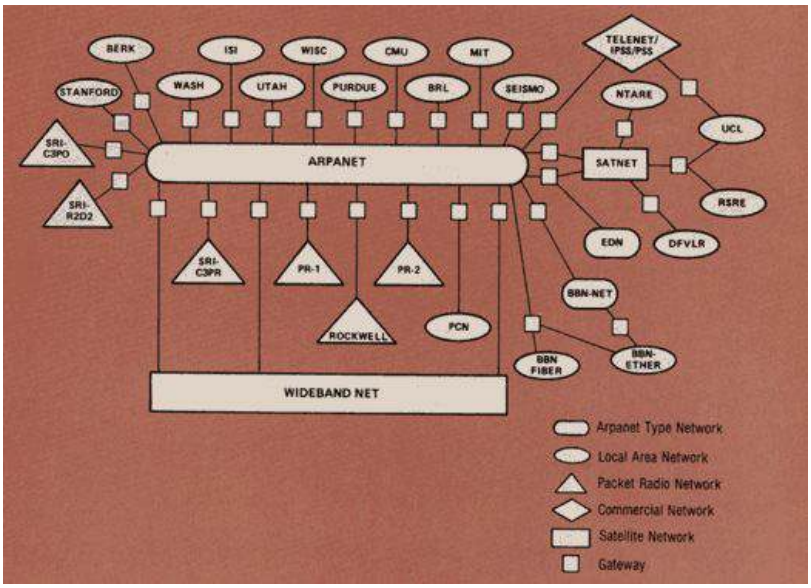


FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/1980s/

Em janeiro de 1983, a ARPANET padronizou o emprego da pilha de protocolos TCP/IP. Neste momento, a ARPANET agregava muitos sistemas de defesa de cunho militar e também diversos serviços e plataformas voltados para a pesquisa. Visando separar estas diferentes funções, a Agência de Comunicações de Defesa norte-americana decide dividir a ARPANET em duas diferentes redes, a ARPANET pública e MILNET, a qual concentraria somente parte da rede reservada para propósitos militares. A Figura 20 apresenta o mapa topográfico em 1983. Um problema existente nesta época consistia na forma como as pessoas identificavam os computadores nas redes. Nesse caso, a interação com os computadores por meio destes rótulos numéricos, se mostrou uma tarefa difícil à medida que muitos computadores foram adicionados à rede. Em novembro deste mesmo ano, os pesquisadores Jon Postel, Paul Mockapetris e Craig Partridge desenvolveram o serviço DNS (*Domain Name System*) para contornar este problema. Por meio deste serviço, cada endereço IP era associado com um nome, facilitando a interação entre pessoas e os computadores na rede. Em 1984, o DSN foi introduzido na Internet, dando origem aos domínios .gov, .edu, .org, .com e .mil. Em 1985, a Internet possuía dois mil computadores conectados.

ATENÇÃO: a forma utilizada consistia em usar apenas o endereço IP, ou seja, um rótulo numérico atribuído a cada computador da rede.

FIGURA 20 – Mapa Topográfico da Internet em 1983.

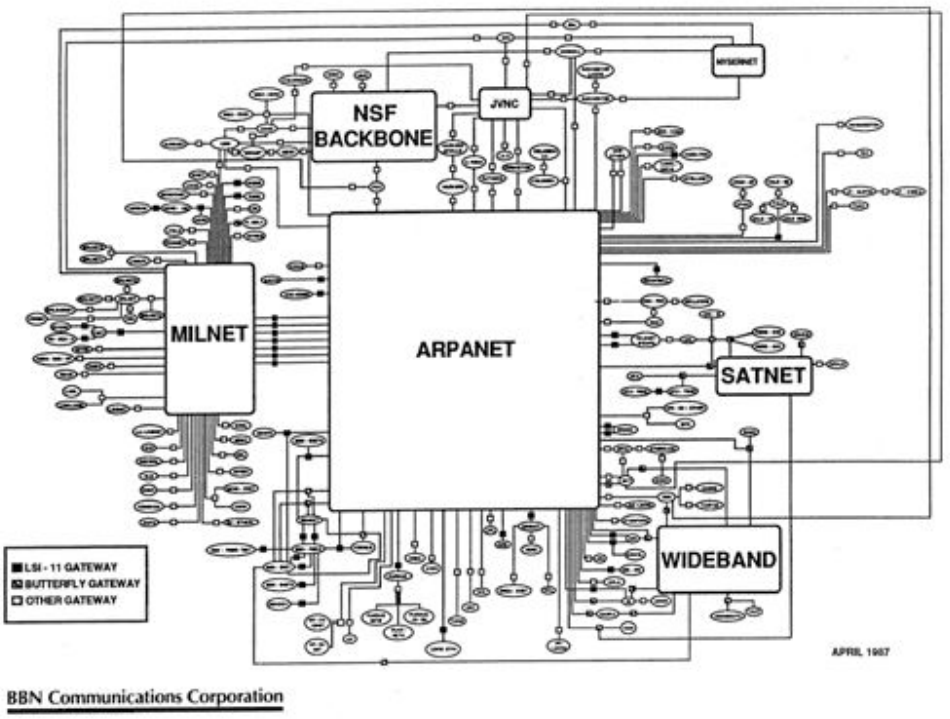


FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/1980s/

Em 1987, o gerenciamento de redes começou se tornar uma questão importante. Devido ao grande número de máquinas conectadas na Internet, se tornou evidente para muitos pesquisadores a necessidade de um protocolo capaz de implementar funções de gerenciamento dos computadores e dos serviços oferecidos por meio das redes. Visando contornar esta necessidade, surgiu o protocolo SNMP (*Simple Network Management Protocol*). Este protocolo permitiu identificar se um dispositivo estava conectado à rede e as condições de operação do mesmo. No fim de 1987, o número de computadores na Internet cresceu ainda mais, chegando a aproximadamente trinta mil. A Figura 21 apresenta o mapa da Internet em 1987. No Brasil, em 1988, a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp) e o Laboratório Nacional de Computação Científica (LNCC) se conectaram à rede Bitnet.

ATENÇÃO: O SNMP possibilitou o monitoramento de roteadores, comutadores, servidores, estações de trabalho, impressoras, entre outros.

FIGURA 21 – Mapa da Internet em 1987

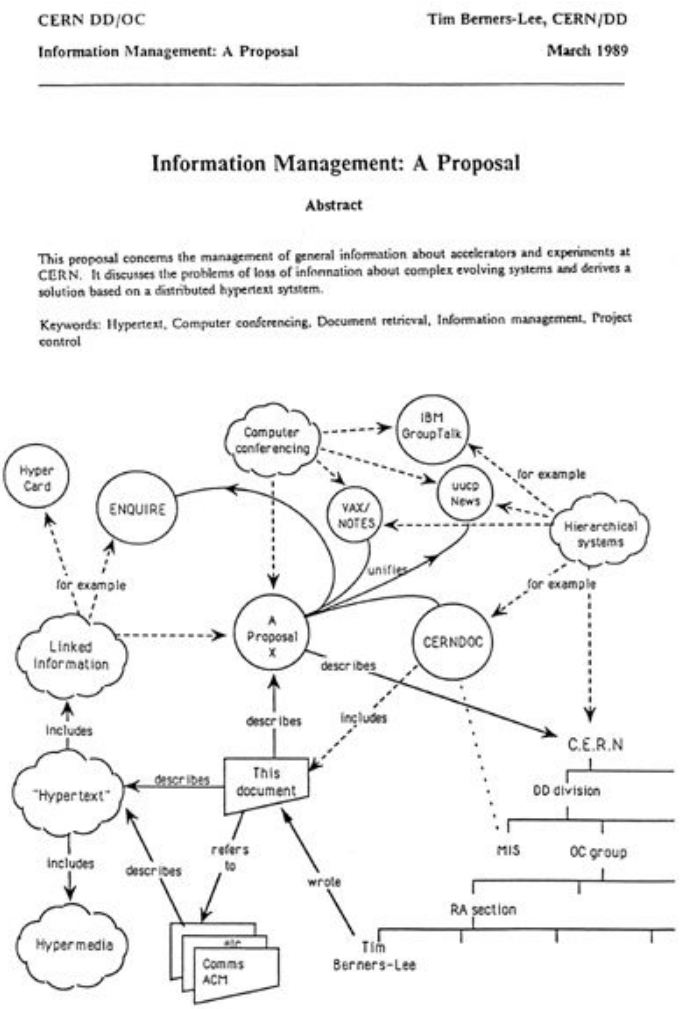


FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/1980s/

Em 1989, Austrália, Alemanha, Israel, Itália, Japão, México, Holanda, Nova Zelândia e o Reino Unido se juntam a Internet. A velocidade de operação da Internet também foi aprimorada, atingindo 100 Mbps. Outra revolução neste ano consistiu na criação da WWW (World Wide Web), ou simplesmente referenciado como Web. A Web consiste em um sistema de documentos hipermídia que emprega a Internet para realizar a interconexão destes documentos. O surgimento da Web gerou um grande impacto positivo na evolução da internet. A proposta de gerenciamento da informação que deu origem a Web foi publicada em março de 1989 e descrevia um sistema de informação mais elaborado. A Figura 22 apresenta a proposta inicial da Web criada por Tim Berners-Lee. No Brasil, neste mesmo ano, surgiu o projeto Rede Nacional de Pesquisa (RNP) financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) visando disseminar o uso de redes de computadores no país.

SAIBA MAIS: o criador da Web foi Tim Berners-Lee, um físico suíço do CERN (*Conseil Européen pourl la Recherche Nucléaire*).

FIGURA 22 – Diagrama de Berners-Lee descrevendo o hipertexto



CERN DD/OC — Tim Berners-Lee, CERN/DD

Information Management: A Proposal — March 1989

Information Management: A Proposal

Abstract

This proposal concerns the management of general information about accelerators and experiments at CERN. It discusses the problems of loss of information about complex evolving systems and derives a solution based on a distributed hypertext sytstem.

Keywords: Hypertext, Computer conferencing, Document retrieval, Information management, Project control

FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/1980s/

Década de 1990

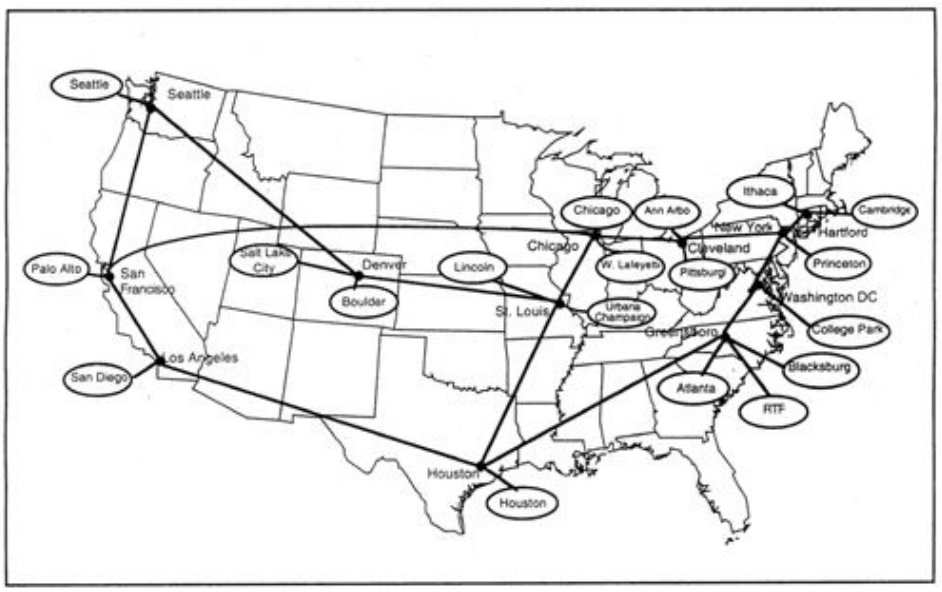
Em 1990, a ARPANET foi formalmente desativada. Em vinte anos, a rede cresceu de quatro para cerca de trezentos mil hosts. Vários países se conectaram na Internet, incluindo Argentina, Áustria, Bélgica, Brasil, Chile, Grécia, Índia, Irlanda, Coreia do Sul, Espanha e Suíça. Diversos mecanismos de busca surgiram, tal como o *ARCHIE* e *Gopher*. Várias instituições começaram a disponibilizar conteúdo on-line, tais como a Biblioteca Nacional Norte Americana de Medicina e a bolsa de valores Down Jones. Além disso, começaram a surgir relatos de eventos contra a segurança da informação. Ao todo, foram reportados cento e trinta eventos maliciosos, sendo doze deles identificados como ataques cibernéticos desencadeados por *worms*. Um *worm* é diferente de um vírus, pois o princípio do vírus consiste em infectar um programa previamente instalado no computador. Por outro lado, o *worm* compreende um programa completo e não precisa de um programa pré-existente para se propagar.

TERMO DO GLOSSÁRIO: um *worm* consiste em um programa capaz de se propagar automaticamente por meio das redes de computadores, ao enviar cópias de si mesmo entre os computadores da rede.

Ao desativar a ARPANET, o crescimento da rede continuou ocorrendo por meio da NSF. Para suportar esse crescimento, a infraestrutura de conexão da NSFNET foi aprimorada em 1991 de forma que seu *backbone* fosse atualizado para o padrão T3. O *backbone* normalmente é responsável pela interconexão entre cidades ou países. Ao utilizar o padrão T3, a Internet foi capaz de operar a taxas de transferências de dados de 44 Mbps. Em 1991, a NFSNET possuía um tráfego superior a um trilhão de bytes, ou dez bilhões de pacotes por mês. Esse tráfego era gerado pela interconexão de redes de cem países empregando seiscentos mil computadores e aproximadamente cinco mil redes. Em 1991 no Brasil, a RNP conectava quarenta instituições à Bitnet por meio da Fapesp e do LNCC.

TERMO DO GLOSSÁRIO: o termo *backbone* é largamente utilizado na área de redes de computadores e significa "espinha dorsal", sendo utilizado para identificar a rede principal pela qual os dados de todos os usuários da Internet passam.

FIGURA 23 – Backbone da NSFNet em 1992



FONTE: Computer History. Disponível em: http://www.computerhistory.org/internethistory/1990s/

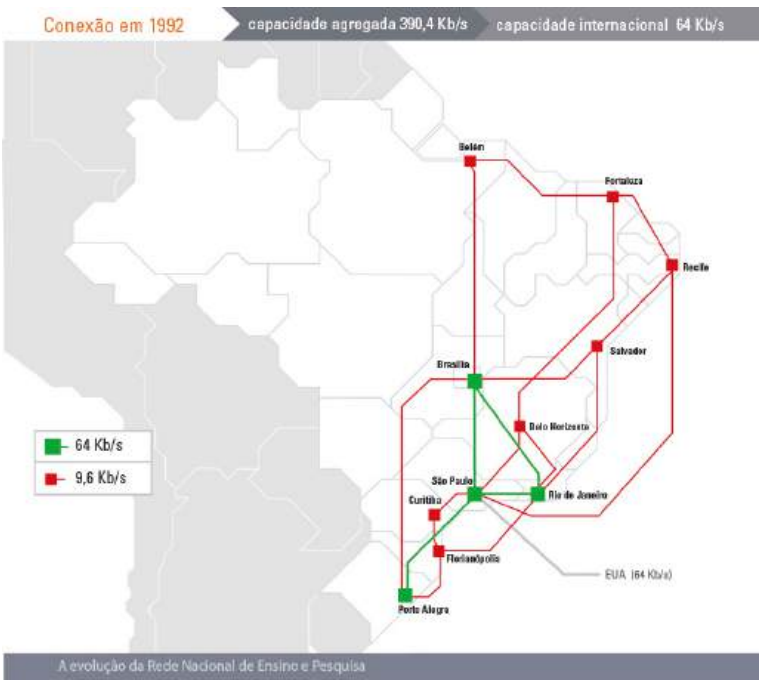
Os principais eventos que marcaram a evolução da 1992 consistiu no seu crescimento, na capacidade de transportar outros formatos de mídias e no surgimento do navegador Web Mosaic. A Figura 23 ilustra o *backbone* da NSFNET em 1992. Também consistiu no ano que a rede começou a transportar áudio e vídeo. Os alunos da Universidade de Illinois modificaram a proposta original do hipertexto de Tim

Berners-Lee e como resultado criaram o primeiro navegador com suporte a interface gráfica, o Mosaic. Como resultado da criação deste software, surgiu a empresa Netscape, responsável por comercializá-lo. Neste período foi iniciada a popularização da Web no mundo, ocasionando um crescimento ainda mais acelerado da Internet. Antes deste ano, o número de computadores na Internet duplicava a cada ano; após a popularização da Web, esse número duplicava a cada três meses.

ATENÇÃO: em 1992, o número de redes interconectadas excedeu o número de sete mil e quinhentas redes e o número de computadores ultrapassou o número de um milhão.

A Internet no Brasil também evoluiu significativamente na década de 90. Em 1992, a infraestrutura de conexão brasileira à Internet possuía dois tipos de enlaces, 64 Kb/s e 9,6 Kb/s. Os enlaces de 64 Kb/s abrangiam Porto Alegre, São Paulo, Rio de Janeiro e Brasília. Os enlaces de 9,6 Kb/s compreendiam Florianópolis, Curitiba, Belo Horizonte, Salvador, Recife, Fortaleza e Belém. A Figura 24 ilustra o mapa da Internet no Brasil em 1992. Apesar dos valores de 64 e 9,6 Kb/s parecem muito modestos atualmente quando comparado com a capacidade das nossas redes domésticas, naquele momento consistia na capacidade da rede de todo nosso território nacional.

FIGURA 24 – Mapa da Internet no Brasil em 1992



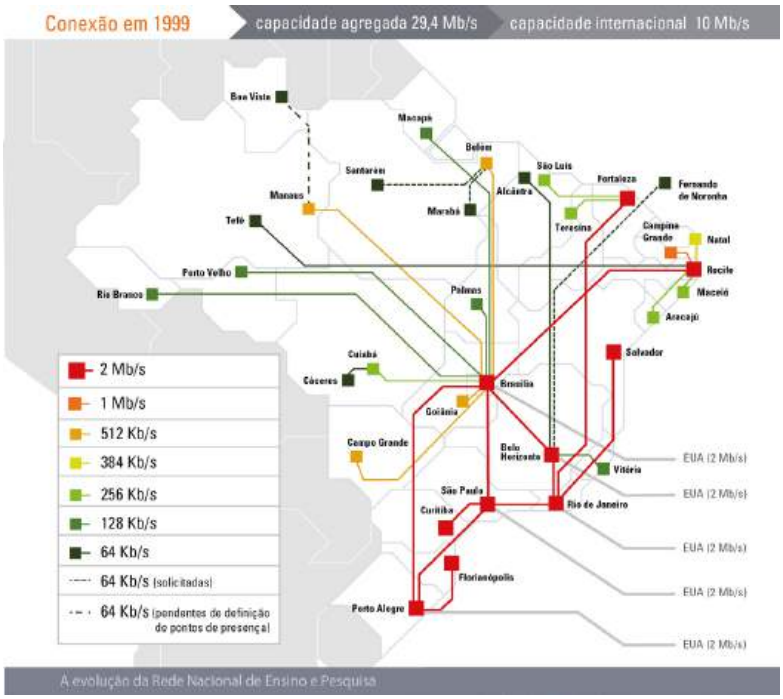
FONTE: Computer History. Disponível em: https://www.rnp.br/institucional/nossa-historia

Em 1995 a RNP sentiu uma pressão do setor de telecomunicações visando a comercialização da Internet em território nacional. Essa pressão tinha como objetivo tarifar o uso da Internet da mesma maneira como ocorria no sistema telefôni-

co e também existiu em outros lugares do mundo, tal como nos Estados Unidos. A Empresa Brasileira de Telecomunicações (Embratel) atuou como detentora do monopólio de serviços de redes de dados no Brasil. Entre os anos 1995 e 1998, a RNP prestou serviços de tráfego de dados comercial para prover uma alternativa à Embratel, a qual estava impedida por lei de exercer o monopólio. Todavia, em 1998 o Ministério da Educação criou o Programa Interministerial e uma das suas consequências consistiu em manter a RNP para atender as universidades e outras instituições governamentais. A RNP desempenhou e continua desempenhando um papel fundamental para manter e administrar a Internet no Brasil. A Figura 25 mostra o mapa da Internet no Brasil em 1999. Apesar de todo o crescimento da Internet, em 1995 existiam dezesseis milhões de usuários conectados à Internet, representando 0,4% da população mundial.

ATENÇÃO: em 1999, esse número cresceu significativamente, totalizando 248 milhões de usuários conectados, consistindo em 4,1% da população mundial.

FIGURA 25 – Mapa da Internet no Brasil 1999



FONTE: RNP. Disponível em: https://www.rnp.br/sites/default/files/media/1999-01.jpg

Na década de 90 foram desenvolvidas muitas empresas responsáveis por oferecer serviços importantes para operar sob a Internet, sendo que muitos deles operam até os dias atuais. Dentre as principais empresas, pode-se destacar a eBay, Hotmail, Google, Yahoo!, PayPal e Napster. A eBay surgiu em 1995 e possibilita a compra e venda de diversos itens na Internet em escala mundial. A Hotmail oferece um serviço de e-mail rodando no navegador e surgiu em 1996. A Google propôs em 1998 um mecanismo de busca na Web diferenciado e inovador, se destacando

ao propor um novo modelo de negócios. Através deste modelo, buscava-se obter lucro através das propagandas relacionadas com o interesse dos usuários e não através de anúncios estáticos como acontecia anteriormente. A Yahoo! surgiu em 1998 e concorria com a Google no mercado de pesquisas Web ao empregar o conceito de buscas por grupos de interesses. A PayPal foi criada para oferecer um sistema de pagamento na Internet. A Napster oferecia em 1999 um serviço descentralizado para possibilitar o download de músicas. No entanto, diferente das demais empresas até o momento que continuam em operação até os dias atuais, a Napster não está mais em funcionamento. O caso da Napster consistiu em um bom exemplo da necessidade de elencar novos tipos de preocupações que até então não tinham sido pautadas, mostrando a necessidade da criação de leis e regulamentações no ciberespaço.

SAIBA MAIS: a principal razão deste fato consistiu em uma intervenção legal, pois a empresa feria os diretos autorais dos artistas ao compartilhar suas músicas.

Anos 2000

O início dos anos 2000 foi marcado pelo evento conhecido como a bolha da Internet. Esse fenômeno ocasionou um crescimento dos valores das ações das novas empresas ligadas ao ramo da tecnologia da informação e comunicação operando com base na Internet. Os principais motivos para ocasionar estes investimentos relacionam-se à sua adoção em escala mundial em função do surgimento no navegador Web Mosaic. A bolha ocorreu entre 1997 e 2001, tendo seu ápice ocorrido em 10 de março de 2000. Devido a esta característica, alguns autores se referem a este evento como a bolha ".com", fazendo uma analogia à escolha dos investidores.

ATENÇÃO: durante este período, muitos investidores aplicaram grandes somas em qualquer empresa criada para prestar serviços através da Internet sem nenhuma avaliação, principalmente aquelas empresas que adotavam o sufixo ".com" em seu nome.

Todavia, essa sequência de investimentos sem uma avaliação chegou ao fim após impactar negativamente no mercado de ações. Os diversos investimentos realizados ajudaram muitas empresas bem estruturadas a se desenvolverem rapidamente, proporcionando um avanço tecnológico. Entretanto, nem todas as empresas que receberam esses investimentos eram cuidadosamente projetadas para se tornarem sustentáveis sem os investimentos que estavam sendo realizados. Uma empresa com essas características foi a Boo.com, a qual gastou cento e oitenta e oito milhões em apenas seis meses ao tentar criar uma loja de artigos de moda online global e depois faliu. Como consequência, muitas destas empresas fecharam, ocasionando um colapso no mercado financeiro. Por exemplo, em apenas seis dias, o Nasdaq perdeu quase 9%, caindo cerca de 5.050 em 10 de março de 2000 para 4.580 em 15 de março do mesmo ano. Apesar deste ponto negativo, a

bolha da Internet contribuiu para o crescimento do número de usuários na rede.

ATENÇÃO: no final de ano 2000, existiam trezentos e sessenta e um milhões de usuários, representando 5,8% da população mundial.

Em 2001, ocorreram sérios ataques contra usuários da Internet. Esses ataques foram desencadeados pelos *worms Code Red I, Code Red II e Nimda*. O *worm Code Red I* foi observado em 15 de julho de 2001 e explorava uma vulnerabilidade do servidor Web IIS da Microsoft. Este *worm* se disseminava na rede ao ocasionar um buffer overflow, ou seja, uma sobrecarga em um buffer de estrutura de armazenamento. O *Code Red II* operava de maneira similar ao seu antecessor e entrou em operação no dia 4 de agosto de 2001. A diferença entre essas duas versões de *worms* consistiu na função do ataque, pois o *Cod Red II* após a infecção, deixava uma *backdoor* do servidor Web IIS da Microsoft para possibilitar o acesso remoto e desencadear ataques de negação de serviço. Além disso, este worm empregava um método mais eficaz de disseminação na rede, pois usava uma técnica mais aprimorada para selecionar as próximas máquinas a infectar. Na primeira versão, a lista de máquinas a infectar era gerada de forma aleatória, podendo inclusive selecionar máquinas já infectadas previamente. Na segunda versão, esse método foi aprimorado para evitar essas situações. O *worm Nimda* surgiu em 18 de setembro de 2001 com o objetivo de infectar máquinas de usuários Windows 95, 98, NT e XP, bem como servidores NT e 2000. No seu pico máximo, este *worm* infectou cento e sessenta mil máquinas. Apesar de ter infectado um número menor de computadores, o *Nimda* utilizava uma abordagem mais agressiva do que o *Code Red*. A principal diferença na disseminação entre esses dois *worms* foi o tempo de disseminação; o *Nimda* foi identificado rapidamente e foi tratado em um pequeno espaço de tempo. Mesmo assim, gerou um grande impacto na Internet, motivando várias empresas a se desconectarem da rede para eliminar o *worm* da rede interna.

ATENÇÃO: o Code Red I começou a operar na rede no dia 13 de julho e até o dia 19 do mesmo mês infectou trezentos e cinquenta e nove mil computadores na Internet.

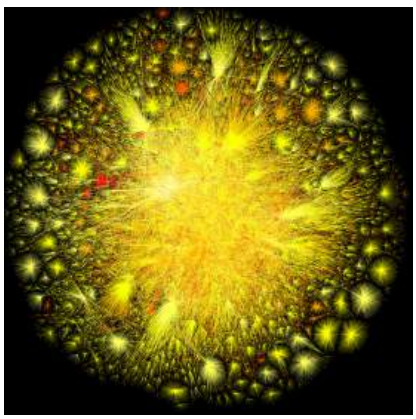
Durante a primeira década dos anos 2000 também houve um aumento significativo do número de dispositivos e existem estimativas para um crescimento ainda maior. A Figura 26 apresenta o mapa da Internet neste ano. Em 2010, esse número cresceu para um bilhão novecentos e setenta milhões de usuários, representando 28,8% das pessoas no planeta. A Figura 27 ilustra o mapa da Internet neste ano. Em 2015, esse número cresceu para três bilhões trezentos e sessenta e seis milhões, caracterizando 46,4% da população. O mapa da Internet neste ano é ilustrado na Figura 28. Em 2017, esse número aumentou para quatro bilhões cento e cinquenta e sete milhões de pessoas, ou seja, 54,4% das pessoas no planeta. Além disso, estima-se um crescimento ainda maior de dispositivos conectados com o surgimento do conceito da Internet das Coisas.

ATENÇÃO: no final de 2003, existiam setecentos e dezenove milhões de máquinas conectadas, representando 11,1% da população mundial.

FIGURA 26 – Mapa da Internet em 2003

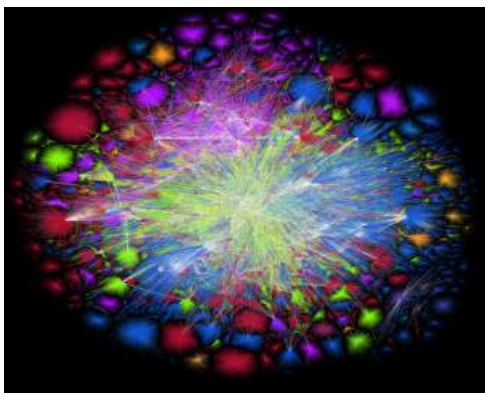
FONTE: The Opte Project. Disponível em: http://www.opte.org/the-internet/

FIGURA 27 – Mapa da Internet em 2010



FONTE: The Opte Project. Disponível em: http://www.opte.org/the-internet/

FIGURA 28 – Mapa da Internet em 2015



FONTE: The Opte Project. Disponível em: http://www.opte.org/the-internet/

Diversas organizações criadas para prestar serviços sob a Internet surgiram na primeira década dos anos 2000. Algumas das organizações mais importantes consistem na Wikipédia, Facebook, YouTube, Dropbox e Spotify. O Facebook surgiu em 2004 oferecendo serviços de rede social. O YouTube oferece serviços de compartilhamento de vídeos por meio da Internet, tendo surgido em 2005. O Dropbox surgiu em 2008 para proporcionar o armazenamento e sincronização dos dados dos computadores dos seus usuários em um ambiente distribuído de máquinas disponibilizado na Internet ao explorar o conceito de nuvens computacionais. O Spotify começou a operar em 2008 ao oferecer serviços de streaming de músicas. Em relação a este último serviço, pode se comparar seu objetivo com o Napster que surgiu em 1999 e foi fechado por infligir os direitos autorais dos artistas. A diferença entre o Napster e o Spotify consiste que este último paga royalties aos autores baseado na quantidade de vezes que suas músicas são ouvidas, enquanto que o primeiro apenas disponibilizava o arquivo digital da música, sem nenhuma preocupação com os diretos autorais.

1.4
REDES DE COMUNICAÇÃO E TELEPROCESSAMENTO

Os termos teleprocessamento e redes de comunicação estão relacionados com os tipos de tarefas em um sistema em rede. O sistema em rede compreende um conjunto de componentes geograficamente distribuídos e interconectados por meio de uma rede de computadores com o objetivo de prover um serviço. A essência do sistema de teleprocessamento consiste na transferência de sinais que apresentam os dados de um sistema computacional. Nesse contexto, podemos dizer que um sistema de teleprocessamento combina as funções de telecomunicações com o conceito de processamento.

TERMO DO GLOSSÁRIO: o teleprocessamento pode ser definido como um tipo de sistema em rede cuja principal característica consiste em enviar tarefas para serem executadas remotamente.

Usando essa definição, os primeiros sistemas de teleprocessamento construídos na década de sessenta contavam com dois principais tipos de componentes, um computador com alto poder de processamento e diversos terminais conectados a ele. Os usuários que acessam os terminais consistem em pessoas com conhecimento técnico moderado e com intenções nos serviços oferecidos pelo sistema em rede. O computador estaria logicamente centralizado na rede, assumindo a responsabilidade de receber, processar e responder as tarefas encaminhadas pelos terminais. Seguindo este modelo, o computador centralizado processa tarefas dos usuários, mas não é utilizado diretamente por eles. Para interagir com este componente, geralmente existe um usuário especialista, cujas atribuições consistem em configurar seu funcionamento e executar tarefas administrativas para mantê-lo em funcionamento. A principal vantagem deste primeiro tipo de sistema de teleprocessamento consistia na sua simplicidade e facilidade de implantação. Todavia, sua principal desvantagem consiste na presença de um ponto único de falha.

TERMO DO GLOSSÁRIO: os terminais consistem em estações de trabalho com baixo poder de processamento usadas pelos usuários do sistema.

ATENÇÃO: caso o computador centralizado venha a falhar por algum motivo, os serviços do sistema estarão indisponíveis para todos os seus usuários.

Visando contornar a presença do ponto único de falha dos primeiros sistemas de teleprocessamento surgiram os sistemas descentralizados. O princípio destes novos sistemas consistia em realizar o processamento de forma distribuída, ou seja, empregando um conjunto de computadores capazes de se coordenar para computar as tarefas. Seguindo este princípio, a ocorrência de uma falha em um computador não compromete a disponibilidade do serviço prestado, mas existe a necessidade de identificar as partes avariadas do sistema. Nestas situações, os sistemas de teleprocessamento geralmente empregavam mensagens de controle com a intenção de verificar a disponibilidade do sistema. Um exemplo deste tipo de sistema de teleprocessamento consiste na iniciativa do projeto SETI (*Search for Extraterrestrial Intelligence*), denominada de SETI@home. O projeto SETI possui o objetivo da busca constante por vida inteligente no espaço. Uma das principais abordagens deste projeto consiste em analisar sinais de rádio de baixa frequência captados por radiotelescópios em nosso planeta. O sistema SETI@home permite que usuários do mundo todo possam colaborar com a tarefa de processamento. Nesse caso, os usuários instalam um programa no seu computador e recebem uma carga de trabalho composta por sinais coletados que são processados em busca de padrões de comunicação não humana.

ATENÇÃO: apesar dos benefícios dos sistemas de teleprocessamento descentralizados, eles também apresentam desafios, sendo os principais deles relacionados com a alta complexidade de implementação e com os custos da comunicação à longa distância.

O conceito de redes de comunicação expande a definição de teleprocessamento. As redes de comunicação compreendem a transferência confiável da informação contida no sinal entre pontos distantes. Além disso, o conceito abrange funções como a detecção/correção de erros e protocolos de comunicação que não são exploradas no conceito de teleprocessamento. A essência deste conceito está na troca da informação e não de sinais, como ocorre no conceito de teleprocessamento. Cronologicamente, o conceito de redes de comunicação surgiu após o surgimento dos sistemas de teleprocessamento com o objetivo de prover o compartilhamento de recursos, o aumento da confiabilidade do sistema e a economia de recursos financeiros.

As redes de comunicação podem ser classificadas de acordo com o seu tipo de transmissão, escala, ou heurística de roteamento. Normalmente as heurísticas são usadas em situações que a execução de uma tarefa computacional retorna um tempo tão alto que se torna inaceitável. Nesses casos, torna-se aceitável obter uma solução boa em pouco tempo do que uma solução ótima em tempo não aceitável. O roteamento compreende no processo da escolha do melhor caminho pelo qual os dados deverão percorrer em uma rede. Assim, uma heurística de roteamento consiste em um processo para minimizar o tempo na tomada de decisão do caminho que uma informação deve percorrer na rede de computadores. Uma rede de comunicações pode usar dois tipos de heurísticas de roteamento, orientada a conexão e não orientada a conexão. Basicamente, a

principal diferença entre estes dois tipos consiste na forma como os dados são enviados. Na primeira delas os serviços estabelecem uma conexão explicita antes de enviar os dados, podendo empregar medidas de controle. A segunda abordagem apenas envia os dados sem empregar medidas de controle. No decorrer do material estes conceitos serão estudados com mais detalhes.

TERMO DO GLOSSÁRIO: uma heurística consiste em tipos de processos empregados em decisões não racionais com o objetivo de facilitar a tomada de decisão e realizá-la mais rapidamente, ao sacrificar parte da qualidade da decisão.

A escala da rede de comunicação diz respeito ao número de componentes envolvidos na troca de informação. Existem três principais tipos de escalas, as redes locais (LANS – *Local Area Network*), redes metropolitanas (MANS – *Metropolitan Area Network*) e redes geograficamente distribuídas (WANS – *Wide Area Network*). Nas LANS, os computadores estão em uma área pequena, como, por exemplo, dentro de uma residência ou em um escritório. Nas MANS, os computadores estão distribuídos em uma área do tamanho de uma cidade. As WANS possuem computadores distribuídos em uma área do tamanho de um país.

ATENÇÃO: a diferença entre as LANS, MANS e WANS consiste no tamanho do espaço físico onde os computadores comunicantes estão localizados.

O tipo de transmissão de uma rede de comunicação trata da forma como a informação é enviada para os componentes da rede de computadores. Existem três tipos de transmissão, ponto a ponto, *multicast* e *broadcast*. Na transmissão ponto a ponto, a informação parte de um transmissor para um receptor diretamente. Neste caso, dizemos que a comunicação ocorre de um para um, ou seja, existe um emissor vários receptores. Na transmissão *multicast*, um receptor envia uma informação para um grupo de receptores. Seguindo essa abordagem, existe um grupo de computadores previamente definido e cada membro do grupo possui a capacidade para enviar uma informação para os demais. Na comunicação *broadcast*, um receptor envia uma informação para todos os computadores da rede. Pode-se dizer que a comunicação *broadcast* consiste em uma comunicação de um transmissor para *n* receptores, sendo n o número total de computadores na rede.

ATIVIDADES DE REFLEXÃO OU FIXAÇÃO

1. Defina o conceito de redes de computadores.

2. Explique com suas palavras as motivações comerciais que incentivam o uso das redes de computadores.

3. Cite e explique como as redes de computadores podem ser utilizadas com finalidades domésticas.

4. Defina o conceito de mobilidade nas redes de computadores e como essa funcionalidade potencializa os serviços oferecidos por meio das redes de computadores.

5. Explique três acontecimentos que você considera mais os importantes dos primórdios da Internet.

6. Do seu ponto de vista, quais foram os três principais acontecimentos que ocorreram durante a década de 60 para consolidação da Internet?

7. Qual a função do protocolo NCP (*Network Control Protocol*) e qual foi o protocolo que veio a substituí-lo?

8. Explique a função de um modem em uma rede de computadores.

9. Defina o conceito de *backbone* e como ele se relaciona com as redes de computadores.

10. Explique os principais eventos que ocasionaram o surgimento da Internet que temos hoje tendo como ponto de partida o surgimento da ARPANET.

2

TOPOLOGIAS E MEIOS DE TRANSMISSÃO

INTRODUÇÃO

Talvez até esse momento você só tenha observado as redes de computadores como uma forma de acessar serviços e conteúdos remotamente, sem de fato refletir sobre como elas são organizadas fisicamente e quais os tipos de meios de transmissão envolvidos e suas respectivas características. O objetivo desta unidade consiste em detalhar as diferentes abordagens de organização física e lógicas das redes de computadores e apresentar os diferentes meios de transmissão que podem ser utilizados para interconectar os computadores.

Visando alcançar este objetivo, esta unidade está organizada em duas seções. A Seção 2.1 descreve as principais topologias das redes de computadores, sendo elas: a ponto a ponto, barramento, anel, estrela, malha, árvore e híbrida. Nela, estudaremos as topologias físicas e lógicas pelas quais uma rede de computadores pode ser organizada com o objetivo de distinguir as vantagens e desvantagens das principais topologias existentes.

A Seção 2.2 apresenta os meios de transmissão. Esta subunidade aborda os meios de transmissão guiados e não guiados. Dentre os meios de transmissão guiados, estudaremos o cabo coaxial, o cabo par trançado e o cabo de fibra óptica. Considerando a classe dos meios de transmissão não guiados, abordaremos a transmissão via rádio e a transmissão via satélite. Por meio do estudo desta subunidade você estará apto para identificar os pontos fortes e fracos de cada tipo de meio de transmissão e os cenários ideais para empregá-los em uma rede de computadores.

2.1
TOPOLOGIAS DE REDES DE COMPUTADORES

Esta subunidade aborda as diferentes topologias das redes de computadores. Existem dois tipos de topologias, física e lógica. A topologia física representa a disposição física dos componentes da rede de computadores e seus meios de comunicação. A topologia lógica compreende na descrição da comunicação dos nós da rede por meio dos meios de comunicação, ou seja, descreve principalmente no fluxo dos dados. Existem oito principais tipos de topologias utilizadas nas redes de computadores, sendo elas: a ponto a ponto, barramento, anel, estrela, malha, árvore e híbrida. As próximas subunidades abordam cada um destes tipos de topologias.

Ponto a Ponto

A topologia ponto a ponto consiste na forma mais básica de interconexões de computadores, onde um par de computadores são interligados diretamente através de um meio de transmissão. A Figura 29 ilustra a topologia ponto a ponto. Essa figura apresenta três pares de computadores interconectados diretamente.

FIGURA 29 – Ponto a Ponto

FONTE: Autores

A topologia ponto a ponto pode ser empregada apenas para prover a conectividade entre dois dispositivos ou em redes de comunicação par a par. Em algumas situações, pode ser interessante interligar dois dispositivos diretamente para trocar dados. Por exemplo, o sistema multimídia do seu carro poderia se conectar via Bluetooth com seu *smartphone* para permitir a execução de uma música em formato MP3 no sistema de som do carro. Além disso, essa topologia também pode ser usada para permitir a troca de dados entre pares de computadores não conectados à Internet por meio de um cabo *crossover*. Nessa configuração, são usados cabos de rede do tipo Cat5 ou Cat6 e a ligação dos pares internos do cabo par trançado são invertidos. Tanto no caso da conexão Bluetooth, quanto nas ligações com cabos *crossover*, a topologia ponto a ponto é empregada de forma física.

TERMO DO GLOSSÁRIO: este tipo de cabo, também conhecido como cabo de rede cruzado, consiste em uma configuração de um cabo de par trançado para permitir a troca de dados entre dois computadores.

Conexões lógicas da topologia ponto a ponto também podem ser muito úteis em redes de comunicação par a par. Este tipo de rede, também conhecidas como *Peer-to-Peer* (P2P), exploram a topologia lógica ponto a ponto para eliminar a estrutura centralizada do modelo cliente-servidor. A principal característica do modelo cliente-servidor compreende na existência de um computador com alto poder de processamento responsável por disponibilizar um serviço na rede para um conjunto de clientes. Este modelo assume a disponibilidade do servidor e a inexistência de ataques cibernéticos ou falhas de operação contra este componente. No entanto, as ameaças cibernéticas são um problema real e podem existir falhas no servidor em decorrência da falta de energia ou avarias de componentes internos. As redes P2P objetivam contornar este problema ao interconectar logicamente os pares. Seguindo neste modelo, cada nó da rede pode atuar como cliente ou servidor, ou seja, pode compartilhar ou adquirir conteúdo ao mesmo tempo. Nesse caso, mesmo que existam conexões físicas com topologias diferentes de ponto a ponto, a forma como os dados são trocados obedecem a topologia ponto a ponto.

Barramento

Nesta topologia existe um barramento físico de dados, no qual todos os computadores precisam se conectar para se comunicar. A Figura 30 ilustra a topologia barramento, na qual a linha central, onde todos os computadores estão conectados, representa o barramento. Esta topologia consiste em uma das mais utilizadas. Uma característica importante das redes que utilizam fisicamente esta topologia consiste na forma como os nós da rede recebem e enviam informações. Para enviar dados, primeiramente um computador precisa averiguar se o barramento está disponível, pois apenas uma mensagem pode ser transportada por vez. Quando esse nó consegue enviar uma mensagem, a mesma poderá ser escutada por todos os nós da rede, mesmo sendo endereçada a apenas um computador. Devido a esta característica, quando um computador recebe uma mensagem, a primeira operação executada consiste em verificar o endereço de entrega. Se a mensagem se destina a ele a mensagem é processada. Caso contrário, a mensagem é descartada, pois não existe a necessidade de encaminhamento para outros nós.

FIGURA 30 – Topologia em Barramento

FONTE: Autores

Devido às propriedades específicas de recebimento e envio de mensagens, as redes organizadas fisicamente em topologia barramento necessitam de mecanismos de controle de acesso ao meio e técnicas para evitar colisões de pacotes na rede. Esses mecanismos podem ser classificados em três grupos, acesso particionado, acesso aleatório e acesso ordenado.

TERMO DO GLOSSÁRIO: os protocolos de controle de acesso regulam a forma como o barramento é acessado pelos computadores.

Os protocolos de acesso particionado empregam técnicas para permitir que mais de uma mensagem sejam enviadas ao mesmo tempo no barramento ao variar a frequência, tempo ou empregando codificações. Exemplos de protocolos que implementam o acesso particionado consistem no FDMA (*Frequency Division Multiple Access*), TDMA (*Time Division Multiple Access*) e CDMA (*Code Division Multiple Access*). Uma limitação dos mecanismos de acesso particionado é a subutilização do barramento quando uma das partes envolvidas não possui dados para enviar.

Os protocolos de acesso aleatório contornam esse problema permitindo que um computador transmita dados sempre que necessário. Dentre estes protocolos pode-se citar o protocolo ALOHA e CSMA (*Carrier Sense Multiple Access*). Todavia, utilizando esses protocolos, surge o risco de colisões de pacotes. Esse evento ocorre sempre que dois ou mais computadores verificam ao mesmo tempo que o barramento está livre e enviam os dados simultaneamente. Nessa situação, os sinais elétricos que representam os dados se chocam no meio físico, impossibilitando sua transmissão.

Visando superar a colisão de pacotes, surgiram os protocolos de acesso ordenado. Nesse caso, definem uma ordem que os computadores devem utilizar o barramento. Exemplos de protocolo de acesso ordenado consistem no *Polling* e *Token*. Apesar de contornar o problema de conflito de pacotes no barramento, os protocolos de acesso ordenado também ocasionam a subutilização do barramento sempre que um componente responsável por transmitir não possui dados para enviar, assim como ocorre com os protocolos de acesso particionado.

As principais aplicações da topologia física de barramento consistem nas redes com cabos coaxiais, redes sem fio e redes de fibra óptica. As redes com cabos coaxiais eram vastamente usadas nos primórdios das redes de computados e possuíam um cabo único que percorria toda a extensão física da rede, representando o barramento. Sempre que havia a necessidade de inserir um novo computador na rede, esse cabo era cortado e um conector em formato de "T" era usado para conectar as pontas do cabo original com o novo computador. No caso das redes sem fio, o barramento consiste no ar. Em algumas configurações, as redes de fibra óptica também utilizam a topologia de barramento.

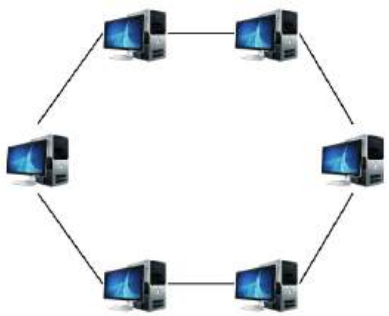
ATENÇÃO: apesar de ainda existirem algumas poucas redes deste tipo, essa tecnologia é considerada antiga.

Anel

Na topologia física anel, os computadores estão organizados em série, formando um circuito fechado. A Figura 31 ilustra seis computadores dispostos nesta topologia. Uma observação importante sobre a topologia anel, é que os computadores não estão necessariamente diretamente conectados, mas normalmente existem repetidores ligados por um meio físico, nos quais os computadores estão de fato conectados. Quando uma mensagem é envida na topologia anel, a mensagem circula na rede até chegar ao destino ou até voltar ao seu emissor. Devido a esta característica, uma vantagem da topologia anel consiste na facilidade de uma mensagem ser entregue a todos os demais computadores de uma rede.

ATENÇÃO: a função dos repetidores consiste em retransmitir os dados de uma origem para o destino em uma única direção de forma a diminuir possíveis efeitos da distorção e atenuação dos sinais transmitidos que representam os dados.

FIGURA 31 – Topologia em Anel



FONTE: Autores

Todavia, a topologia em anel também apresenta desvantagens em relação às falhas e ao atraso no processamento de dados. Os enlaces que interligam os dispositivos e os próprios dispositivos da rede não são imunes a falhas. Nessas situações, o funcionamento da topologia se torna comprometido, pois deixa de existir o circuito que interliga os computadores. Uma forma de contornar este problema consiste em utilizar um computador com a responsabilidade de monitorar os demais dispositivos da rede e gerar eventos sempre que eles deixarem de operar corretamente. Para implementar o monitoramento, este computador normalmente envia pacotes de teste para realizar tarefas de diagnóstico e tarefas de manutenção.

A topologia em anel também apresenta limitações quanto ao atraso no processamento de dados. A razão deste atraso surge em virtude das características do protocolo de controle de acesso ao meio utilizado em redes organizadas nesta topologia, o protocolo *Token Ring*. Assim, como ocorre na topologia em barramento, o controle de acesso ao meio se torna muito importante na topologia em anel para determinar qual estação pode transmitir em um dado instante para evitar a colisão de dados na rede. Para resolver este problema, a ideia básica do protocolo *Token Ring* consiste em utilizar um *token* que deve ser repassado sequencialmente entre

os computadores da rede. Todavia, caso exista um grande número de computadores na rede, o tempo de repassar o *token* na rede ocasiona um atraso nas estações que possuem dados a transmitir e precisam aguardar o recebimento do *token*.

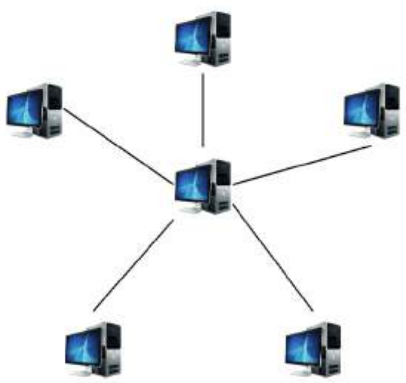
ATENÇÃO: o recebimento do token sinaliza que uma estação da rede pode transmitir seus dados. Seguindo essa abordagem, o protocolo elimina a ocorrência de colisões de pacotes.

Apesar dessas limitações, a topologia em anel atualmente é empregada em algumas configurações das redes de fibra óptica. Devido às suas propriedades físicas, as redes de fibra óptica possibilitam taxas de transferências muito mais altas do que os demais meios físicos. Inclusive, atualmente se desconhece a capacidade máxima obtida por meio deste meio de transmissão. Devido a esta característica, o emprego da topologia em anel em algumas situações compensa os atrasos de processamento do *token* ao reduzir o tempo de transmissão das mensagens no meio físico. No entanto, como a implantação de uma rede de fibra óptica implica em um alto custo financeiro, o emprego desse meio de transmissão ocorre somente em situações onde existe a necessidade de alto desempenho.

Estrela

Em uma rede de computadores organizada por meio de uma topologia estrela, toda a informação gerada pelas estações de trabalho deve passar por um nó central. O nó central se diferencia dos demais por possuir a inteligência para distribuir o tráfego de rede para os demais computadores da rede. Esse nó central se conecta com os demais computadores da rede por meio de uma conexão ponto a ponto. A Figura 32 ilustra seis computadores em rede organizados em uma topologia estrela. Nesta topologia, sempre que um computador deseja enviar pacotes para um determinado destino, esses dados deverão obrigatoriamente passar pelo nó central. Na sequência, o nó central possui informações como repassar as informações para os demais computadores da rede.

FIGURA 32 – Topologia em Estrela



FONTE: Autores

A topologia em estrela consiste em uma das topologias mais utilizadas atualmente. A maioria das redes LANs, seja de um escritório, uma casa ou uma universidade, possuem um conjunto de computadores que estão diretamente conectados a um roteador, *switch* ou *hub* para trocar dados. A diferença entre um roteador, *switch* e um *hub* consiste nas suas funcionalidades. Usando um *switch*, o pacote é recebido por uma porta e é encaminhado apenas para a porta em que se encontra o computador de destino. Enquanto que a função de um roteador consiste em processar o pacote e determinar sua rota, sempre que necessário. Além disso, muitos roteadores oferecem funcionalidades complementares, tais como o gerenciamento dos dispositivos das redes e da criação de redes virtuais. Apesar dessas diferenças, os *hubs*, *switches* e roteadores operam de maneira similar em uma topologia em estrela, interligando os dispositivos da rede e encaminhando o tráfego de uma origem para um destino. No caso das LANs, normalmente os roteadores, *switches* ou *hubs* também são conectados com um provedor de serviços de Internet, permitindo que os computadores da LAN possam acessar serviços disponibilizados na Internet.

ATENÇÃO: a função do *hub* consiste em receber um pacote por uma porta e encaminhá-lo por todas as demais portas.

Existem vantagens e desvantagens de empregar a topologia estrela. As principais vantagens consistem na facilidade de adicionar novos computadores, centralização do gerenciamento e a falha de um computador das bordas não afeta os demais computadores na rede. Como todos os computadores estão conectados no ponto central, a adição de um novo computador demanda apenas uma nova conexão ponto a ponto entre o novo computador e o dispositivo central. Como as tarefas de encaminhamento de pacotes são delegadas ao componente central, podemos dizer que estas tarefas estão centralizadas neste dispositivo e sempre houver a necessidade de executar algum procedimento de alteração, adição ou exclusão de regras de encaminhamento, basta apenas acessar o dispositivo central, não necessitando modificações em outros componentes da rede. Além disso, como todas os computadores posicionados nas extremidades da topologia apenas enviam e recebem os pacotes, caso ocorra uma falha nestes dispositivos, a rede continuará a operar sem problemas. Todavia, a desvantagem de organizar a rede por meio desta topologia consiste na possibilidade de falha do ponto central.

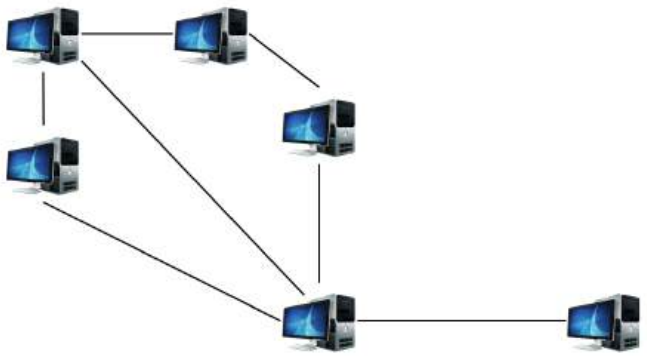
ATENÇÃO: nesse caso, a decisão de encaminhamento de pacotes estaria indisponível prejudicando o funcionamento da rede.

Malha

Uma rede de computadores organizada em topologia em malha possui duas propriedades principais, os dispositivos podem se comunicar entre si, desde que ambos estejam ao alcance um do outro. Usando essa organização, um dispositivo normalmente possui vários caminhos para acessar os demais dispositivos da

rede, gerando assim maior resiliência da rede em nível de falhas de enlaces. A Figura 33 ilustra uma rede de computadores organizada em malha.

FIGURA 33 – Malha



FONTE: Autores

Devido às características da topologia em malha, diz-se que a mesma consiste em uma rede *ad-hoc*, sendo normalmente empregada em redes sem fio. Em uma rede *ad-hoc*, cada nó opera como um roteador, recebendo um pacote e encontrando o melhor caminho dentro da rede para alcançar o destino. Como consequência desta propriedade, as redes *ad-hoc* possuem a habilidade de se auto-organizar, ou seja, caso aconteça uma falha em um dos nós da rede, a mesma continuará operando ao encontrar uma nova configuração para manter sua operacionalidade.

TERMO DO GLOSSÁRIO: o termo *ad-hoc* compreende em um tipo de rede que dispensa um ponto de controle em centralizado, antagonizando o conceito da topologia estrela.

A principal aplicação da organização física de computadores em malha, ocorre com em redes sem fio. Uma rede sem fio tradicional, normalmente possui um ponto de acesso central, onde todos os demais dispositivos se conectam para acessar a Internet, compreendendo em uma topologia em estrela. Como vimos anteriormente, essa forma de organização torna-se propensa a falhas no ponto de acesso central, prejudicando o funcionamento da rede. A razão do interesse em empregar a topologia em malha nas redes sem fio ocorre em razão da sua descentralização. Como a rede de computadores organizada em malha possibilita que todos os computadores da rede executem o procedimento de roteamento, o ponto de acesso central é eliminado, removendo também a existência de um ponto único de falhas.

Apesar da existência dos pontos fortes da topologia em malha, também existem problemas relacionados com esta forma de organização. Como consequência, a rede como um todo apresenta uma degradação de desempenho, podendo prejudicar a qualidade dos serviços oferecidos por meio dela. Outro problema com a utilização desta topologia consiste na perda de desempenho em função do número de saltos na rede. O termo salto aqui é utilizado para descrever a situação onde um determinado emissor não consegue acessar diretamente o receptor e necessita do repasse das informações por nós intermediários. Um salto, neste contexto, con-

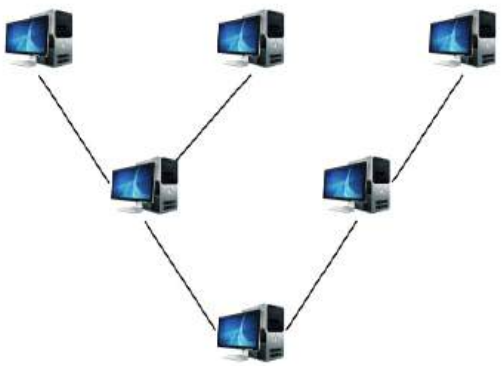
siste no evento que representa o repasse dos pacotes entre dois nós para alcançar o receptor. A realização de um salto na rede implica em um custo computacional e quanto mais saltos forem necessários, maior será o custo total da comunicação.

ATENÇÃO: o maior problema desta topologia consiste na existência de uma carga de processamento adicional (overhead) ocasionado pela implementação da função de roteamento em todos os nós da rede.

Árvore

Uma rede de computadores organizada fisicamente por meio da topologia em árvore possui uma estação central, onde todas as demais estações se conectam. Diferentemente da topologia estrela, que prevê a interligação apenas com um dispositivo centralizado, a topologia em árvore permite que as estações conectadas à estação central também se conectem com outras estações. Todavia, diferentemente da topologia em malha, a topologia em árvore não permite a existência de conexões fechando circuitos, ou seja, não existe a possibilidade de um pacote percorrer pelo menos três estações, de modo que o primeiro e o último computador sejam os mesmos. A Figura 34 ilustra uma topologia em árvore.

FIGURA 34 – Topologia em Árvore



FONTE: Autores

No caso da figura acima, o elemento central da árvore encontra-se na parte inferior. Este elemento geralmente é referenciado como raiz, ou primeiro da árvore. Logo após a raiz, encontram-se dois computadores, representando os ramos derivados da raiz, ou o segundo nível da árvore. Em seguida, os computadores posicionados nas extremidades da árvore consistem nas folhas, ou terceiro nível da árvore.

Essa topologia apresenta pontos positivos e negativos. Como por definição, esta representação não permite a existência de ciclos, elimina-se a possibilidade de um pacote permanecer em loop na rede, ocupando desnecessariamente os recursos de banda. Por outro lado, essa topologia apresenta uma fragilidade inerente a sua estrutura organizacional, no sentido que uma falha em algum enlace ou computador da rede ocasiona a fragmentação da rede, ou seja, existirão dois

grupos de computadores isolados que não poderão se comunicar. Devido a esta limitação, a organização física de computadores em uma rede normalmente não emprega a topologia em árvore.

ATENÇÃO: um dos principais pontos positivos consiste na facilidade de tomar decisões de roteamento de pacotes.

Uma das aplicações mais importantes da topologia em árvore consiste na representação lógica da rede de computadores para tomada de decisões de roteamento. Um dos algoritmos mais famosos que utilizam este conceito consiste no algoritmo de *Dijkstra*. Abordaremos superficialmente este algoritmo brevemente para exemplificar a importância da topologia em árvore. No algoritmo de *Dijkstra*, a rede de computadores é abstraída para uma estrutura denominada grafo. Por meio de um grafo, os vértices representam os computadores da rede e as arestas consistem nos enlaces que interligam os computadores. Além disso, o algoritmo atribui um valor inteiro em cada aresta para representar o custo da comunicação entre os nós que as interligam. Esse custo pode ser, por exemplo, a latência, a taxa de perda de pacotes ou a intensidade do sinal. Com base nessa estrutura, o algoritmo de *Dijkstra* realiza uma série de procedimentos para encontrar uma representação da rede em forma de árvore, capaz de mostrar o menor custo para conectar qualquer par de nós da rede de computadores. Essa representação comumente é empregada nas decisões de roteamento. Analisando este algoritmo, pode-se dizer que ele usa a topologia em árvore em uma representação lógica da rede, pois fisicamente os nós podem estar organizados em qualquer uma das topologias já estudadas até aqui.

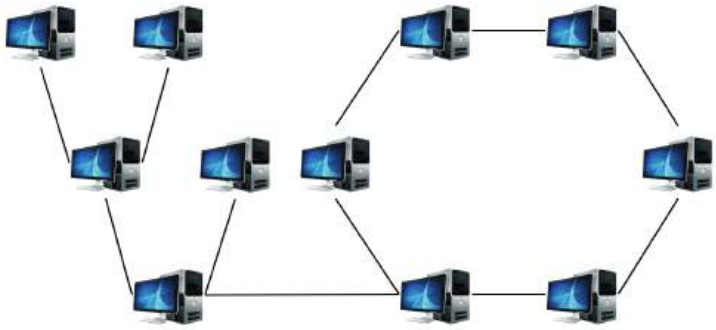
TERMO DO GLOSSÁRIO: um grafo consiste em um conjunto não vazio de vértices (pontos) e um conjunto de arestas (linhas).

INTERATIVIDADE: um vídeo sobre o funcionamento deste algoritmo pode ser encontrado em https://www.youtube.com/watch?v=ovkITlgyJ2s

Híbrida

A topologia híbrida em uma rede de computadores combina aspectos de duas ou mais topologias estudadas até o momento. Por exemplo, podemos ter uma topologia híbrida combinando a topologia anel com a topologia em árvore. A Figura 35 ilustra esse exemplo, onde no lado esquerdo temos computadores organizados em forma de árvore e no lado direito os computadores estão organizados em topologia anel. Entre essas topologias existe um enlace ligando ambas as topologias.

FIGURA 35 – Exemplo de Topologia Híbrida



FONTE: Autores

A topologia híbrida consiste na mais utilizada em grandes redes de computadores. Esse fato ocorre em função da interconexão das redes existentes para formação de redes de larga escala. A Internet consiste em um exemplo de uma rede de larga escala, pois como vimos na Unidade 1 deste material, essa rede surgiu por meio da agregação de vários tipos de redes. Devido a essa propriedade, cada rede interconectada possui suas próprias necessidades de interconexão, políticas de segurança e serviços oferecidos, ocasionando consequentemente em tipos de topologias específicas para atender essas necessidades. Logo, devido a estas características, existiam diferentes topologias interconectadas para formar a Internet.

2.2
TIPOS E MEIOS DE TRANSMISSÃO

Os meios de transmissão possibilitam que os dados codificados em sinais possam ser enviados de um receptor para um transmissor. Cada tipo meio de transmissão possui características únicas. Devido a este fato, conhecer bem as caraterísticas de cada meio de transmissão que pode ajudar na tomada de decisão sobre a escolha de qual utilizar para melhor alcançar as demandas de uma empresa ou instituição. Os meios de transmissão guiados consistem naqueles que podem ser manipulados durante sua instalação, como por exemplo um cabo coaxial ou cabo de par trançado. Enquanto que os meios de transmissão não guiados não apresentam essa característica, como por exemplo, a transmissão via rádio, ou via satélite. Nesta unidade estudaremos os meios de transmissão guiados e não guiados. Cada uma das seguintes subseções aborda um destes tipos de meios de transmissão.

ATENÇÃO: os meios de transmissão podem ser classificados como guiados e não guiados.

2.2.1 Meios de Transmissão Guiados

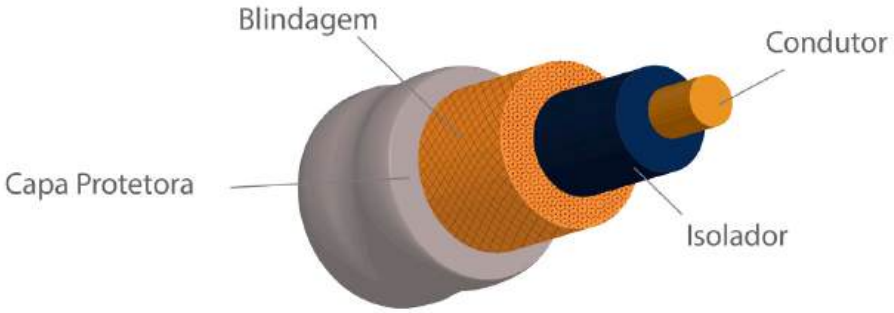
Os meios de transmissão guiados que serão abordados consistem no cabo coaxial, cabo par trançado e cabo de fibra óptica. Na sequência, abordaremos cada um destes meios de transmissão guiados.

Cabo Coaxial

As primeiras redes de computadores utilizavam o cabo coaxial para conectar os dispositivos da rede. Estes cabos foram utilizados nas redes de computadores até meados dos anos noventa. Os principais componentes de um cabo coaxial consistem na capa, na blindagem, no isolador e no condutor. A capa normalmente é fabricada em plástico e fica localizada na parte mais externa do cabo. A blindagem geralmente é construída com um material metálico. O isolador normalmente é fabricado com um material mais duro e está diretamente em contato com o condutor, cuja função consiste em transmitir os sinais elétricos que representam dados em uma rede de computadores. A Figura 36 ilustra como um cabo coaxial se parece internamente.

TERMO DO GLOSSÁRIO: o cabo coaxial possui um fio de cobre na parte central, protegido por um material isolante.

FIGURA 36 – Estrutura do Cabo Coaxial



FONTE: Adaptado de Oficina da Net. Disponível em: https://www.oficinadanet.com.br/post/10155-o-que-e-cabo-coaxial

Existem dois tipos de cabos coaxiais, o cabo coaxial fino (*thinnet*) e o cabo coaxial grosso (*thicknet*). O cabo coaxial fino, também conhecido como cabo coaxial 10Base2, possui um diâmetro de 4,7 milímetros e podem transmitir a uma distância máxima de 185 metros. O cabo coaxial grosso, muitas vezes referenciados como 10Base5, possui um diâmetro de 1,25 centímetros e podem transportar até 500 metros. Você pode ter notado que em ambas as nomenclaturas, aparece a palavra "Base". Este termo significa "banda base", denotando a distância máxima que o sinal pode percorrer em cada um dos cabos. Por exemplo, no caso do cabo 10Base2, a distância máxima teórica de transmissão consiste em 200 metros, todavia, em termos práticos, o máximo alcançado é 185 metros. O mesmo conceito é aplicado ao tipo de cabo coaxial 10Base5, o qual pode transmitir em termos práticos em até 500 metros de distância. Ambos os tipos de cabos coaxiais podem transmitir até 10 megabits por segundo.

ATENÇÃO: as redes que utilizavam estes cabos possuíam no máximo trinta computadores.

Existem três tipos principais de conectores de cabos coaxiais, o conector de cabo (*Bayonet Neill Concelman*) BNC, conector BNC em T e terminação BNC. A Figura 37 ilustra os três tipos de conectores de cabo coaxial. O conector de cabo BNC normalmente é fixado na extremidade do cabo, aparecendo no lado esquerdo da figura. O conector BNC T atua como interface com a placa de rede dos computadores, permitindo a conexão dos computadores à rede. A Figura 38 apresenta uma placa de rede compatível com um conector coaxial. Na Figura 37, o conector T encontra-se na parte central. A terminação BNC fica posicionada nas extremidades do cabo de uma rede em barramento visando absorver os sinais eletroestáticos.

ATENÇÃO: além disso, o conector BNC T também possibilita a continuidade do cabo coaxial principal.

FIGURA 37 – Conectores do Cabo Coaxial

FONTE: Autores

FIGURA 38 – Placa de Rede com Saída para Conector BNC

FONTE: Wikipédia. Disponível em: https://pt.wikipedia.org/wiki/BNC

As principais vantagens do cabo coaxial consistem na sua blindagem eficiente e na imunidade a ruído. A blindagem eficiente ocorre em virtude da utilização de três componentes para evitar o contato do condutor com o ambiente externo. Outra vantagem deste meio de transmissão consiste na ótima imunidade a ruído. Como consequência do ruído, as informações não podem ser reconhecidas no receptor. A principal razão da alta imunidade a ruído surge em função da grande quantidade de componentes que fazem a blindagem do cabo coaxial.

TERMO DO GLOSSÁRIO: um ruído consiste em uma interferência nos sinais propagados por meio do meio de transmissão, capaz distorcer os sinais transmitidos e consequentemente a informação que eles representam.

No entanto, o cabo coaxial também apresenta desvantagens. A principal desvantagem deste meio de transmissão consiste na dificuldade de instalação. Em virtude de sua rigidez, o cabo pode ser quebrado com facilidade no momento de fazer curvas acentuadas. Mesmo com essa desvantagem, os cabos coaxiais são empregados atualmente principalmente para transmitir sinais de televisão.

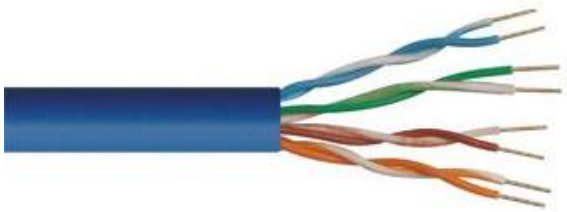
Cabo Par Trançado

O cabo par trançado é formado por uma capa externa que agrega um conjunto de pares de fios de cobres encapados e enrolados de forma helicoidal. A Figura 39

apresenta um cabo par trançado sem blindagem, onde pode-se perceber quatro pares de fios de cobre entrelaçados. Cada fio destes pares possui uma função específica. Para interpretar a informação recebida, o receptor se baseia na diferença de potência entre os dois níveis de tensão.

ATENÇÃO: um deles funciona como suporte de transporte dos sinais entre o transmissor e o receptor e o outro atua como referência.

FIGURA 39 – Exemplo de Cabo Par Trançado sem Blindagem



FONTE: Análise Informática. Disponível em: https://www.analiseinformatica.com.br/cabo-par-trancado-cat5e-4px24-100mhz-ftp-blindado-azul-furukawa-mt.html

Os cabos de par trançado podem pertencer a dois tipos, com ou sem blindagem. O cabo par trançado sem blindagem, normalmente referenciado como UTP (*Unshielded Twistead-Pair*), consiste no cabo de uso mais popular nas redes de computadores. A Figura 39 apresenta um exemplo de cabo UTP. O cabo par trançado blindado, também conhecido como STP (*Shielded Twistead-Pair*), possui uma blindagem eletromagnética metálica ou um revestimento em malha de cobre em cada par de fios isolados do cabo, proporcionando maior isolação e imunidade ao ruído. A Figura 40 ilustra um cabo par trançado blindado. No entanto, apesar dos benefícios do STP, o seu custo também é mais elevado.

FIGURA 40 – Cabo Par Trançado Blindado

FONTE: Medium. Disponível em: https://medium.com/@julydd/stp-vs-utp-which-one-is-better-96e6fc612afa

Outra forma de classificar os cabos de par trançado consiste na análise da categoria que eles pertencem. Existem sete categorias do cabo par trançado. A categoria 1 era empregada principalmente em instalações telefônicas e redes antigas, mas não é mais reconhecida pela Associação da Indústria de Telecomunicações (TIA). A categoria 2 era utiliza em redes em topologia em anel com suporte a *token*, mas assim como a categoria anterior, a segunda categoria não é mais reconhecida pela TIA. A categoria 3 consistiu no primeiro padrão projetado especialmente para redes de computadores e suporta a transmissão de sinais em uma frequência de até

16 mega-hertz (MHz) e continua em operação atualmente. A categoria 4 permite transmitir sinais a uma frequência de até 20 MHz e a uma taxa de dados de 20 Mbps. A categoria 5 é a mais utilizada e permite frequências de até 125 MHz. A categoria 6 em geral opera com frequência de 250 MHz, mas apenas em um alcance de 55 metros. Além disso, essa categoria apresenta maior poder para reduzir interferências e a perda de sinal. A categoria 7 permanece em desenvolvimento visando permitir a criação de redes capazes de transmitir 100 gigabits por segundo em cabos de 15 metros de alcance. A Tabela 1 compara as categorias de cabos de par trançados.

ATENÇÃO: a única exceção consiste na subcategoria CAT6a que permite um alcance de até 100 metros.

TABELA 1 - Comparação das Categorias de Cabos de Par Trançado

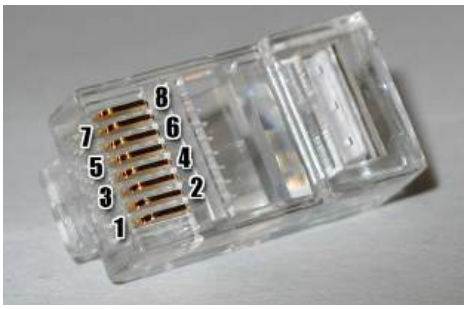
CATEGORIA	LARGURA DE BANDA	TAXA DE TRANSMISSÃO	TIPO DE SINAL	APLICAÇÃO
1	Muito baixa	< 100Kbps	Analógico	Telefone
2	<2 MHz	2 Mbps	Analógico/digital	Telefone/Dados
3	16 MHz	10 Mbps	Digital	LANs
4	20 MHz	20 Mbps	Digital	LANs
5	100 MHz	100 Mbps	Digital	LANs
6	200 MHz	200 Mbps	Digital	LANs
7	600 MHz	600 Mbps	Digital	LANs

FONTE: IFRN. Disponível em: http://www3.ifrn.edu.br/~macedofirmino/files/ensino/2012.1/redesI/redesI_meios_transmissao.pdf

O conector do cabo par trançado consiste no 8P8C, popularmente conhecido como RJ45. Os conectores 8P8C são frequentemente referenciados como conectores RJ45. A principal característica deste conector consiste na possibilidade de conexão de oito pinos. A Figura 41 apresenta um conector de cabo par trançado.

SAIBA MAIS: apesar da maioria das pessoas utilizarem essa terminologia, tecnicamente ela está incorreta, pois a interface mecânica e o esquema de instalação são diferentes no padrão de especificação do padrão. Mesmo existindo essa diferença técnica, provavelmente você sempre ouvirá as pessoas se referindo a este conector como RJ45 e no restante do material usaremos a terminologia popular a fim de não confundir os leitores já acostumados com essa definição.

FIGURA 41 – Conector Cabo Par Trançado



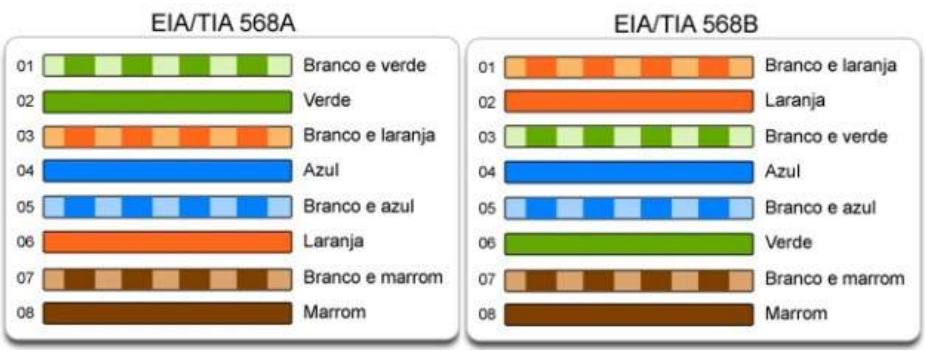
FONTE: Wikipédia. Disponível em: https://pt.wikipedia.org/wiki/8P8C

Existem dois principais tipos de ligação dos pares de fios do cabo par trançado nos conectores RJ45. Cada tipo de ligação resulta em um tipo de cabo para atender necessidades específicas, sendo eles o cabo reto e o cabo crossover. A principal característica deste tipo de cabo consiste em manter o mesmo padrão em ambas as pontas do conector. Existem dois padrões mais utilizados de combinação de pares a serem conectados no conector RJ45, sendo eles o EIA/TIA 568A e o EIA/TIA 568B. A Figura 42 ilustra o esquema de ligação de um cabo direto. Diferentemente do cabo direto, o cabo crossover permite interligar dois computadores diretamente, sem a necessidade de utilizar um hub, switch ou roteador. A característica mais marcante do cabo crossover consiste na inversão dos padrões em cada ponta do cabo, ou seja, pode-se utilizar em uma extremidade o padrão EIA/TIA 568A e na outra extremidade o padrão EIA/TIA 568B. A Figura 43 mostra a disposição dos fios do cabo par trançados com os conectores RJ45 em um cabo crossover.

ATENÇÃO: o cabo direto é empregado para interligar computadores com hubs, switches ou roteadores.

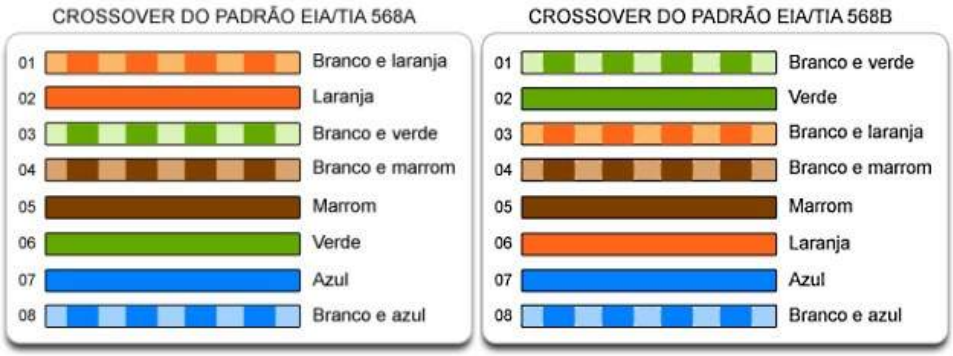
SAIBA MAIS: esse tipo de cabo se torna muito útil em situações que não existe uma infraestrutura de rede disponível e existe a necessidade de compartilhar uma grande quantidade de dados entre dois computadores.

FIGURA 42 – Ligação de um Cabo Direto



FONTE: TecMundo. Disponível em: https://www.tecmundo.com.br/manutencao-de-pcs/2187-manutencao-de-pcs-aprenda-a-crimpar-cabos-de-rede-video-.htm

FIGURA 43 – Ligação de um Cabo Crossover

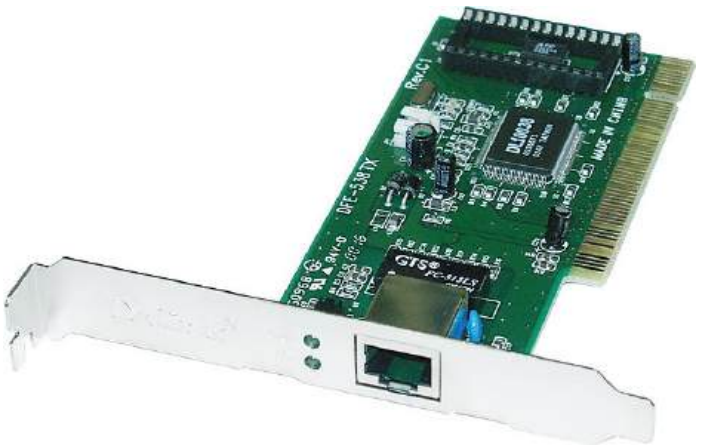


FONTE: TecMundo. Disponível em: https://www.tecmundo.com.br/manutencao-de-pcs/2187-manutencao-de-pcs-aprenda-a-crimpar-cabos-de-rede-video-.htm

Conhecendo os esquemas de ligação do cabo par trançado, basta analisarmos como os mesmos são conectados nos computadores. Para realizar esta função utilizam-se as placas de rede com suporte ao conector RJ45. A Figura 44 mostra uma placa de rede *off-board* capaz de suportar um conector RJ45. Algumas placas de rede podem estar integradas diretamente na placa mãe do computador. Nos referimos a este tipo de placa como *on-board*. Conhecendo agora estes dois termos, provavelmente você está se perguntando qual seria o mais indicado para você utilizar. Normalmente torna-se interessante utilizar uma placa mãe *off-board* pela facilidade de substituição de peças, pois no caso da queima de componentes de uma placa *on-board* geralmente implica na inutilização da placa como um todo.

ATENÇÃO: diz-se que essa placa de rede é off-board, pois ela pode ser acoplada na placa mãe em um slot apropriado para ela.

FIGURA 44 – Placa de Rede Cabo Par Trançado



FONTE: Ubuntu Iniciantes. Disponível em: http://www.ubuntuiniciantes.com.br/2016/09/comandos--para-gerenciar-sua-internet.html

A utilização do cabo par trançado apresenta vantagens e desvantagens. Dentre as desvantagens encontram-se o comprimento máximo sem perdas de 100 metros, a baixa imunidade a interferências externas (ruídos). Esta última desvantagem pode ser otimizada ao utilizar os cabos par trançados blindados, mas esta escolha resulta em um custo maior. Mesmo existindo desvantagens, este cabo ainda é muito utilizado nas redes LANs atualmente.

ATENÇÃO: as principais vantagens consistem na alta taxa de transferência de arquivos, no baixo custo de aquisição, na manutenção barata e na flexibilidade do cabo para passar por paredes.

Fibra Óptica

A fibra óptica consiste no meio de transmissão guiado mais avançado em termos de taxas de transmissão de dados por segundo. O princípio utilizado neste meio de transmissão consiste em transmitir pulsos de luz para representar bits. Como você já deve ter ouvido em algum momento, a velocidade da luz é uma das coisas mais rápidas que a humanidade conhece. Apesar dessa grandeza física ser muito impressionante, provavelmente em algum momento você escutou que até o momento a humanidade ainda não desenvolveu métodos muito aprimorados para dominar tecnologias que operam na velocidade da luz. Isso também ocorre com a transmissão de dados por meio da fibra óptica. Estima-se que o limite máximo de taxa de transmissão de dados por meio de uma fibra óptica pode ultrapassar a casa dos 50.000 Gbps (50 Tbps), algo surpreendente. No entanto, atualmente as tecnologias existentes nos permitem um limite prático de 100 Gbps, algo ainda muito aquém do potencial deste meio de transmissão. Como o limite alcançado ainda se torna muito interessante quando comparado com a taxa de transmissão por meio de fios de cobre e além disso existe um potencial muito grande a ser explorado, o investimento em fibra óptica se tornou muito promissor para as companhias responsáveis por prestar serviços de Internet e muito investimento vêm sendo realizado nessa área.

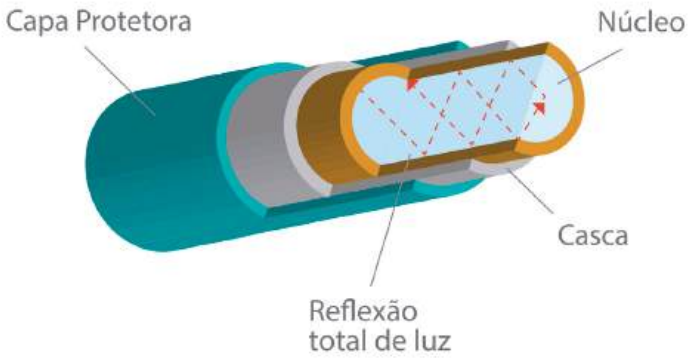
SAIBA MAIS: apenas por curiosidade, o seu valor exato da velocidade da luz é 299.792.458 metros por segundos ou 300.000 km/s.

Os cabos de fibra óptica se assemelham muito aos cabos coaxiais em termos de sua estrutura. A principal diferença entre eles encontra-se na utilização da malha metálica. Um cabo de fibra óptica compreende os seguintes componentes, uma capa protetora, uma casca ou revestimento interno e o núcleo. A Figura 45 ilustra a relação entre os componentes do cabo de fibra óptica. A capa protetora normalmente é construída com plástico, tal como no cabo coaxial e possui a função de realizar um isolamento externo inicial. A casca ou revestimento interno é

fabricada em vidro e oferece uma proteção adicional aquela proporcionada pela capa. O núcleo localizado no centro do cabo também é fabricado em vidro, sendo responsável por propagar os pulsos de luz que representam bits enviados.

ATENÇÃO: os cabos coaxiais possuem a malha metálica, enquanto que o cabo de fibra óptica não.

FIGURA 45 – Estrutura do Cabo de Fibra Óptica

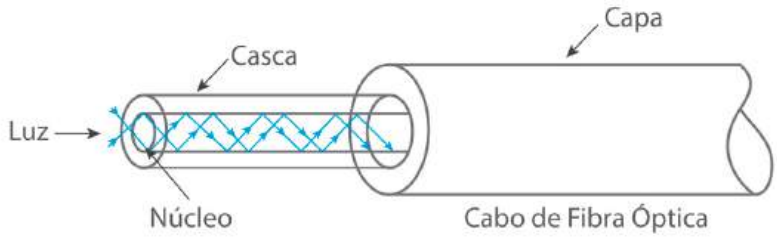


FONTE: Adaptado de Brasil Escola. Disponível em: https://brasilescola.uol.com.br/o-que-e/fisica/o-que-sao-fibras-opticas.htm

O diâmetro do núcleo de um cabo de fibra óptica varia de acordo com o modo como os raios de luz ricocheteiam em diferentes ângulos. Quando um raio de luz passa de um emissor para um receptor através da fibra, o raio é refratado (inclinado), como ilustrado na Figura 46, o núcleo da fibra. Esse processo envolve a definição de ângulos que determinam como o sinal ricocheteia nas extremidades da fibra até alcançar o destino. A forma como esse ângulo é definido nos ajuda a classificar os modos de transmissão na fibra óptica e refletirá no diâmetro do núcleo. Ao todo existem dois principais tipos de fibras, a multimodo e modo único. Na fibra multimodo existem raios de luz distintos, cada um ricocheteando em ângulos diferentes e o diâmetro do núcleo compreende 50 micra. Nesses casos, cada raio de luz pode ter sido gerado por um usuário diferente, auxiliando no compartilhamento do meio de transmissão entre os usuários de uma rede. Na fibra de modo único, também conhecida como mono modo, a luz é propagada em linha reta, sem ricochetear e o diâmetro do núcleo possui entre 8 e 10 micra. Nesta situação, a fibra fica alocada exclusivamente para representar os sinais de um único emissor, o que acarreta em um custo financeiro maior quando comparado com a fibra multimodo. Comparando o diâmetro destes dois tipos de fibras, a fibra de modo único é significativamente menor do que a multimodo.

ATENÇÃO: a fibra de modo único é normalmente utilizada para conectar pontos da rede distantes em até 100 km de distância.

FIGURA 46 – Exemplo de Propagação da Luz na Fibra Óptica



FONTE: Adaptado de Teltec. Disponível em: https://telteq.wordpress.com/2014/12/23/principio-de-funcionamento-e-tipos-de-fibra-optica/

Uma vez entendidos os componentes do cabo de fibra óptica, nos concentraremos na sua disposição física de instalação. Geralmente, os cabos de fibra óptica são enterrados aproximadamente a um metro da superfície. Nessas condições, ocasionalmente as fibras ópticas são rompidas por tratores ou retroescavadeiras. Em regiões litorâneas, os cabos de fibra óptica transoceânicos são enterrados em trincheiras. Quando passam pelo alto mar, normalmente quando as fibras ópticas são usadas para interconectar diferentes países, os cabos são dispostos no fundo do oceano para evitar de serem capturados por redes de pesca.

Outro aspecto importante das fibras ópticas consiste em como elas são conectadas. Existem três principais modos de conexões. No primeiro caso, as fibras podem possuir conectores nas extremidades do cabo e são plugadas em soquetes de fibra. A segunda forma de conexão compreende a união mecânica da fibra. Nesse caso, as extremidades são conectadas por meio de uma luva especial e um alinhamento cuidadoso pode ser realizado para maximizar a passagem do sinal. O terceiro modo de conexão compreende a fusão das extremidades. Usando a fusão proporciona um resultado muito semelhante a uma fibra sem emendas, todavia, existe uma pequena atenuação no sinal transmitido, mas mesmo assim este tipo de conexão se destaca em relação aos demais.

ATENÇÃO: o uso de conectores ocasiona uma perda de dez a vinte por cento da luz, no entanto essa perda é compensada pelo ganho na facilidade de instalação.

Usando a união mecânica, existe uma perda de dez por cento da luz propagada.

Mesmo considerando que fusão de fibras consiste em uma boa estratégia de conexão, ela apresenta um ponto negativo relacionado com o seu alto custo e dificuldade de instalação. Em virtude disto, existem muitos modelos de conectores disponíveis no mercado. Os principais conectores são, o ST, o SC, o FC, o FDDI, o LC e o MTRJ. A Figura 47 ilustra esses conectores.

FIGURA 47 – Tipos de Conectores de Fibra Ópticas

FONTE: Ricardo Silva e Marcos Paiva. Disponível em: https://rsilva1inf.wordpress.com/cabos-de-fibra-optica-2/

Na Figura 47 são apresentados os conectores ST, SC, FC, FDDI, LC e MTRJ. Os conectores ST (*Straight Tip*) podem ser utilizados em fibras de modo único ou multimodo. O exterior deste conector compreende um elemento metálico com um sistema de fixação do tipo baioneta. Os conectores SC (*Standard Connector*) também podem ser empregados em fibras de modo único ou multimodo. O exterior do conector SC é fabricado em plástico com um sistema de fixação do tipo PUSH/PULL. Os conectores FC (*Fiber Connector*) são normalmente utilizados em ambientes de alta vibração onde se necessita de uma conexão segura. Esses conectores também operam em fibras de modo único e multimodo. O conector FDDI (*Fiber Distributed Data Interface Connector*) provê uma taxa de transmissão de dados de 100 Mpbs em uma LAN token ring com uma faixa de 200 Km. O conector LC (*Lucent Connector*), popularmente referenciado como (*Little Connector*, ou conector pequeno), possui como principal característica o pequeno tamanho do seu arco de metal interno, o qual compreende apenas 1,25 milímetros. Existem três diferentes tipos de LC, sendo que dois deles são projetados para fibras de modo único e um para multimodo. O MTRJ (*Mechanical Transfer Registered Jack*) consiste em um conector muito popular para conectar duas fibras usando *plugs*.

Agora que conhecemos os tipos de conectores de um cabo de fibra óptica, nos concentraremos nas interfaces que suportam esses conectores. Diferentemente do que ocorre com os cabos de par trançado, normalmente os cabos de fibra óptica não são conectados diretamente nos computadores. Para realizar esta tarefa, geralmente os sinais da fibra são convertidos para o padrão do RJ45, de forma que um cabo de par trançado possa ser levado até o cliente. Neste caso, entram em cena os conectores SC e um conversor para portas RJ45. A Figura 48 ilustra um conversor de sinal de fibra óptica para oito portas RJ45 por meio de conectores SC. Outra necessidade ocasionada com a utilização de cabos de fibra óptica consistiu em formas de transferir dados por meio de portas USB. Esse tipo de necessidade vem de encontro com sistemas específicos de armazenamentos de dados. A Figura 49 ilustra um destes dispositivos usando um conector LC. A transmissão de

streaming de áudio sob cabos de fibra óptica também se mostrou necessário e foram desenvolvidos dispositivos para atender essa necessidade. A Figura 50 mostra um conversor de áudio RCA para fibra óptica usando conectores ST. No caso dos conectores FC e MTRJ são normalmente utilizados para interconectar um cabo de fibra óptica usando apenas *plugs* machos e fêmeas, dispensando um conversor com uma interface específica.

ATENÇÃO: foram desenvolvidos dispositivos customizados para converter dados de uma interface USB diretamente para a fibra óptica para suprir a necessidade de armazenamento.

FIGURA 48 – Conversor Fibra Óptica para 8 Portas RJ45 com Conector SC

FONTE: Aliexpress. Disponível em: goo.gl/tqcbCJ

FIGURA 49 – Transmissor de Sinais USB para Fibra Óptica via Conector LC

FONTE: AD net Technology. Disponível em: http://www.ad-net.com.tw/16-types-fiber-optic-connectors-choose/

FIGURA 50 – Conversor de Áudio RCA para Fibra Óptica com Conector ST

FONTE: AD-net Technology. Disponível em: http://www.ad-net.com.tw/16-types-fiber-optic-connectors-choose/

Um sistema de fibra óptica compreende três principais elementos-chave, a fonte de luz, o meio de transmissão e o detector. Até esse momento já analisamos muitos aspectos referentes ao meio de transmissão, mas pouca atenção foi dada a fonte de luz e ao detector. Portanto, focaremos agora nestes dois elementos. A aplicação da fonte de luz consiste na essência da transmissão por fibra óptica. É através dela que os bits são representados. Por meio deste sistema, o emissor gera um sinal elétrico, o qual é convertido e transmitido por pulsos de luz. Ao chegar na origem, o sistema realiza o processo inverso, ou seja, os pulsos de luz são convertidos em um sinal elétrico para ser encaminhado ao receptor.

ATENÇÃO: a função do detector consiste em gerar um pulso elétrico quando a luz incide sobre ele. Ao conectar um detector em uma extremidade da fibra óptica e na outra extremidade uma fonte de luz, temos um sistema de transmissão de dados unidirecional.

Existem dois tipos de fontes de luz que são normalmente usadas no processo de sinalização, os diodos emissores de luz (*light emitting diodes* – LEDs) e os lasers semicondutores. Essas fontes de luz possuem diferentes propriedades. A Tabela 2 descreve uma comparação entre ambas as fontes de luz. Entre a fonte e a fibra, o comprimento da onda pode ser ajustada ao empregar interferômetros, tais como o de Fabry-Perot ou de Mach-Zehnder. Os interferômetros de Fabry-Perot compreendem em cavidades ressonantes que atuam como dois espelhos paralelos. Ao usar este dispositivo, a luz incide perpendicularmente aos espelhos. Os interferômetros de Mach-Zehnder operam separando a luz em dois feixes, de modo que cada um percorra distâncias diferentes e sejam recombinados no destino.

TABELA 2 – Comparação das Fontes de Luz LED e Semicondutor

CARACTERÍSTICA	LED	LASER SEMICONDUTOR
Taxa de dados	Baixa	Alta
Tipo de fibra	Multimodo	Multimodo ou modo único
Distância	Curta	Longa
Vida útil	Longa	Curta
Sensibilidade à temperatura	Insignificante	Substancial
Custo	Baixo	Dispendioso

FONTE: Tanenbaum (2011).

Na extremidade de recepção da fibra óptica existe um fotodiodo responsável por emitir um pulso elétrico sempre que atingido pela luz. Este componente converte o sinal óptico para um sinal elétrico em taxas de dados de cerca de 100 Gbps. Considerando a transmissão por meio de cabos de fibra óptica, pode ocorrer ruídos térmicos e também precisam ser tratados para garantir que a energia de um pulso seja forte o suficiente para ser detectado na extremidade de destino.

A transmissão através de cabos de fibra óptica apresenta vantagens e desvan-

tagens. Dentre as principais vantagens pode-se citar as altas taxas de transmissão, número reduzido de repetidores e a baixa susceptibilidade à ruídos. Atualmente esse meio suporta uma taxa de 100 Gbps de dados e as tecnologias atuais ainda não alcançaram os limites teóricos deste meio de transmissão. Em relação ao número reduzido de repetidores, as fibras ópticas requerem repetidores somente a cada 50 Km, muito melhor do que cabo de cobre que requerem a cada 5 Km. Quanto aos ruídos, as fibras ópticas não são afetadas por picos de tensão, interferência eletromagnética ou faltas de energia elétrica.

No entanto, também existem desvantagens e as principais consistem no alto preço, na dificuldade de instalação e na fragilidade dos cabos. Atualmente, o preço dos cabos e conectores de fibra óptica são altos. Outro agravante consiste na necessidade de pessoas altamente qualificadas para realizar os procedimentos de instalação e manutenção da rede, uma vez que esta consiste em uma tecnologia emergente. Além disso, os cabos de fibra óptica são frágeis e podem ser facilmente rompidos. Apesar destas desvantagens, a utilização deste meio de transmissão está em alta nos dias atuais e existem indícios que permanecerá em destaque nos próximos anos. A principal utilização dos cabos de fibra óptica consiste nos enlaces de redes intercontinentais e em redes de empresas especializadas na prestação de serviços de Internet, visto que nestas situações existe uma alta demanda por conexões de alta velocidade.

Comparação entre os Meios de Transmissão Guiados

Como já discutimos sobre cada meio de transmissão guiado, tentaremos agora resumir as principais diferenças entre eles. A Tabela 3 apresenta uma comparação detalhada dos meios de transmissão guiados que já estudamos. Cada um dos meios é comparado considerando as características de custo, comprimento máximo, taxas de transmissão, flexibilidade, facilidade de instalação, susceptibilidade a interferências e utilização.

TABELA 3 – Comparação entre Meios de Transmissão Guiados

CARACTERÍSTICA	CABO COAXIAL FINO	CABO COAXIAL GROSSO	CABO PAR TRANÇADO	CABO FIBRA ÓPTICA
Custo	Maior que o UTP	Maior que o coaxial fino	UTP: barato STP: maior que o coaxial fino	Maior que o coaxial fino, mas menor que o coaxial grosso
Comprimento máximo	185 metros	500 metros	100 metros	2 quilômetros em 100 Mbps
Taxas de transmissão	4-100 Mbps	4-100 Mpbs	UTP: 4-100 Mbps STP: 16-500 Mbps	10-100 Mbps 1-10 Gbps
Flexibilidade	Relativamente flexível	Menos que o coaxial fino	UTP: Mais flexível STP: Menos que o UTP	Menos flexível que o *thincknet*
Facilidade de instalação	Fácil	Fácil a moderada	UTP: Muito fácil STP: Facilidade moderada	Difícil
Susceptibilidade a interferências	Boa resistência	Boa resistência	UTP: muito susceptível STP: Boa resistência	Nenhuma
Utilização	Sítios médios e grandes com necessidades de segurança	Conectando redes *thinnet*	UTP: sítios com orçamento restrito STP: Redes *token ring* de qualquer tamanho	Sítios de qualquer tamanho que necessitam de altas velocidades, segurança e integridade dos dados

FONTE: Battisti. Disponível em: https://www.juliobattisti.com.br/tutoriais/paulocfarias/redesbasico006.asp

Cada uma destas características possui um significado diferente. O custo compreende na quantidade de recursos financeiros necessários para comprar os meios de transmissão, conectores e interfaces. O comprimento máximo diz respeito à capacidade do meio de transmissão em transportar os sinais elétricos (ou ópticos no caso da fibra óptica) que representam a informação trocada por meio da rede de computadores sem a necessidade do emprego de repetidores. A taxa de transmissão descreve a quantidade de bits por segundo que um meio de transmissão suporta transportar. A flexibilidade detalha quão maleável é um meio de transmissão guiado, sendo muito útil na escolha do cabo utilizado em um determinado ambiente. A susceptibilidade a interferência apresenta um indicador de resistência do meio de transmissão. Esta característica geralmente deve ser cuidadosamente avaliada quando um meio de transmissão é empregado em um ambiente propenso a interferências físicas, tais como o calor. A utilização demonstra cenários onde cada meio de transmissão é aplicado.

Interpretando a Tabela 3, pode-se concluir que não existe um meio de transmissão guiado ideal para todas as situações, mas cada um apresenta benefícios em casos específicos. Os cabos coaxiais finos são recomendados para domínios de tamanho médio e com alta demanda por segurança, tal como no sistema de TV a cabo. O cabo coaxial grosso normalmente era empregado na conexão de redes *thinnet*, ou seja, nas redes de computadores que eram construídas com cabos coaxiais. Os cabos de par trançado UTP consistem em soluções ideais em projetos de rede com um orçamento restrito. Em contrapartida, os cabos de par trançado STP

são empregados em situações que existe uma necessidade maior de resistência à ruídos e em redes *token ring* de qualquer tamanho. Finalmente, os cabos de fibra óptica são mais indicados em domínios de tamanho variável que necessitam de alta velocidade, baixa susceptibilidade a interferências e alta segurança.

INTERATIVIDADE: mais informações sobre um comparativo entre os meios de transmissão guiados podem ser encontradas em: https://www.juliobattisti.com.br/tutoriais/paulocfarias/redesbasico006.asp

2.2.2 Meios de Transmissão não Guiados

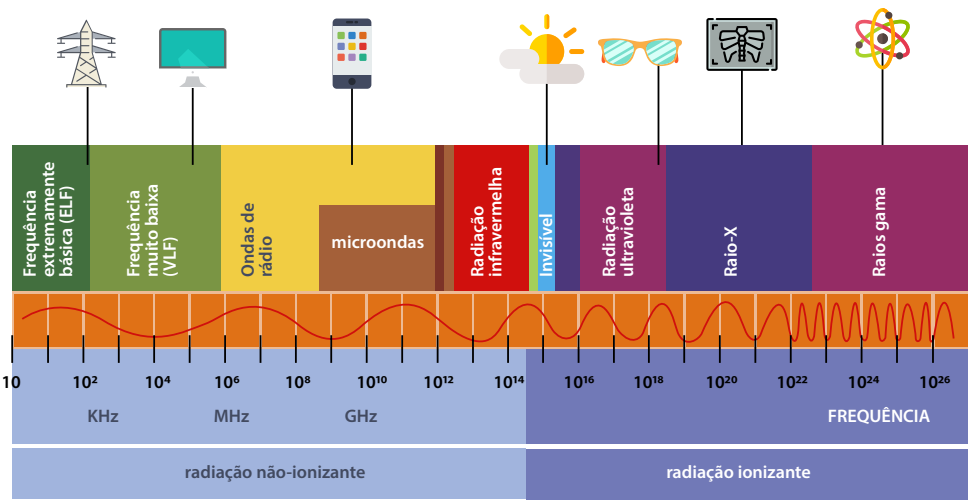
Neste momento abordaremos os seguintes meios de transmissão não guiados, a transmissão via rádio e a transmissão via satélite. Na sequência abordaremos cada um deles.

Espectro Eletromagnético

Todas as comunicações sem fio se baseiam no princípio da transmissão de ondas eletromagnéticas emitidas e recebidas através do ar por meio de antenas. No entanto, ao invés de utilizar o termo "ar", a literatura especializada da área geralmente usa o termo espectro eletromagnético para se referir ao ambiente como um todo onde as ondas podem se propagar. A Figura 51 ilustra como o espectro eletromagnético é empregado na comunicação.

TERMO DO GLOSSÁRIO: o espectro eletromagnético compreende todas as frequências de radiação eletromagnética, tais como as ondas de rádio, as ondas micro-ondas, os raios X, o infravermelho, os raios violeta e a luz captada pelos olhos humanos.

FIGURA 51– A maneira como o Espectro Eletromagnético é Usado na Comunicação



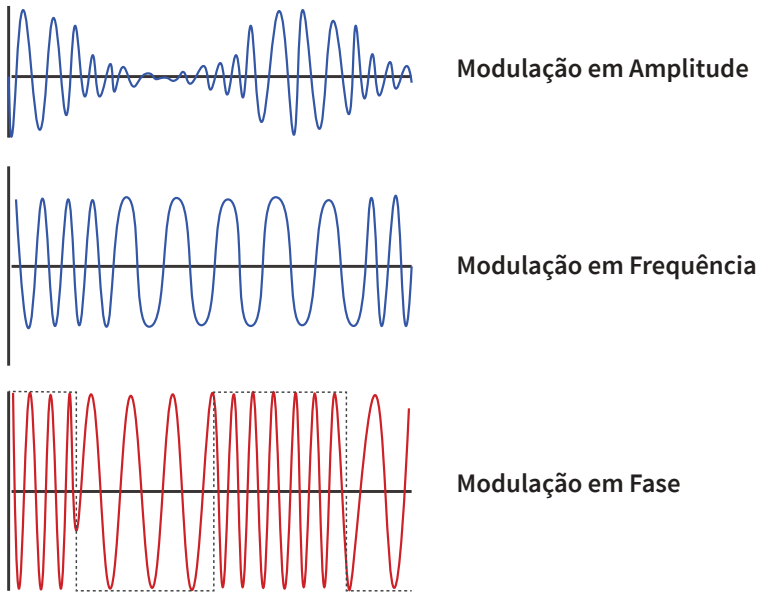
FONTE: Adaptado de Resumo Escolar. Disponível em: https://www.resumoescolar.com.br/fisica/espectro-eletromagnetico/

Na Figura 51, podemos observar diferentes frequências classificadas como ondas eletromagnéticas não-ionizante e ionizantes. Para entender esses conceitos, primeiramente precisamos entender que todas as ondas eletromagnéticas transportam energia e viajam na velocidade da luz. As ondas eletromagnéticas ionizantes são aquelas que possuem energia suficiente para remover elétrons do átomo ou quebrar ligações químicas. Em contrapartida as ondas eletromagnéticas não-ionizantes não possuem energia suficiente para remover elétrons ou quebrar ligações químicas. Dentre as ondas eletromagnéticas não-ionizantes, encontramos desde as frequências extremamente baixas (ELF), geralmente utilizadas em torres de comunicação cabeada, até as ondas de infravermelho. Separando as ondas não-ionizantes das ondas ionizantes, encontra-se a luz visível, ou seja, a luz percebida pelos seres humanos. Na sequência, seguem as ondas eletromagnéticas ionizantes, compreendendo desde a radiação ultravioleta até os raios gama.

As faixas de rádio, micro-ondas, infravermelho e luz visível do espectro eletromagnético podem ser usadas na transmissão de informações através da modulação da amplitude, da frequência, ou da fase das ondas. A modulação consiste em uma técnica criada para modificar as características da onda portadora do sinal. Na modulação por amplitude, a onda portadora do sinal é modificada em termos de amplitude para portar o sinal. A amplitude consiste na medida de oscilação da onda que pode ser positiva ou negativa. A modulação por frequência aplica técnicas para variar a frequência da onda portadora do sinal. A frequência indica o número de ocorrência de oscilações do sinal da onda em um determinado intervalo de tempo, sendo medida em Hz. A modulação de fase emprega técnicas para variar a fase da onda portadora do sinal. A fase de uma onda expressa o ângulo de uma onda. A Figura 52 ilustra exemplos de modulação em amplitude, frequência e fase de ondas.

SAIBA MAIS: a unidade de medida Hz surgiu em homenagem a Heinrich Hertz

FIGURA 52 – Exemplo de Modulação de Amplitude, Frequência e Fase



FONTE: Teleco. Disponível em: http://www.teleco.com.br/tutoriais/tutorialwimaxiee802/pagina_2.asp

A transmissão de informações por meio de ondas eletromagnéticas ionizantes, tais como a luz ultravioleta, os raios X e os raios gama, consistiria em uma opção ainda melhor do que empregar as ondas não-ionizantes. A principal razão desta possível melhoria acontece em função das ondas eletromagnéticas ionizantes suportarem frequências mais altas. Todavia, essas ondas são mais difíceis de produzir, modular e de se propagarem de modo eficiente através de obstáculos, tais como prédios. Além disso, as ondas ionizantes podem ser nocivas para os seres humanos.

Um conceito importante que deve ser abordado para um entendimento completo da comunicação por meio do espectro eletromagnético consiste na definição de bandas. Para entender de forma mais simples esse conceito, podemos pensar nas bandas como formas de determinar faixas específicas de comprimento das ondas que devem ser propagadas em um determinado sistema de comunicação. A definição das bandas de frequências é regulamentada por uma entidade governamental de cada país. Por exemplo, os EUA possuem a entidade FCC (*Federal Communications Commission*) para esse fim, bem como a ANACOM (Autoridade Nacional de Comunicações) atua em Portugal com o mesmo propósito e a ANATEL (Agência Nacional de Telecomunicações) opera de forma semelhante no Brasil.

TERMO DO GLOSSÁRIO: uma banda consiste em uma subseção do espectro eletromagnético usado para as frequências de radiocomunicação.

Dentre as principais bandas de frequência, encontram-se a LF, MF, HF, VHF, UHF e SHF. A banda LF (*Low Frequency*) agrega ondas de baixa frequência compreendendo o intervalo de 30 Hz até 300 KHz. A MF (*Medium Frequency*), ou frequência média, refere-se às frequências na escala de 300 KHz a 3000 KHz. A HF (*High Frequency*), ou frequência alta, compreende frequências de 3000 KHz até 30 MHz e opera por

meio da propagação ionosférica, a qual estudaremos com detalhes na Seção 2.2.4. A VHF (*Very High Frequency*), ou frequência muito alta, designa a faixa de radiofrequências de 30 a 300 MHz, a qual é comumente empregada na transmissão de rádio FM. A UHF (*Ultra High Frequency*), ou frequência ultra alta, regulamenta a faixa de radiofrequência compreendida entre 300 MHz e 3 GHz, sendo empregada principalmente na transmissão de sinal de TV analógica. A SHF (*Super High Frequency*), ou frequência super alta, compreende frequências de 3 GHz até 30 GHz. Uma característica interessante das SHF consiste no pequeno tamanho das ondas geradas, que variam de um a dez centímetros. Algumas aplicações das SHF consistem nas redes LAN sem fio, na comunicação via satélite e transmissões de radares.

Existem quatro principais estratégias que um transmissor pode empregar o espectro para enviar informações para um receptor, sendo eles a forma tradicional, por salto de frequência, dispersão de sequência direta e a comunicação UWB. Na abordagem tradicional, o transmissor envia sinais para o receptor dentro de uma banda específica. Na estratégia baseada em saltos de frequência, o transmissor salta de uma frequência para outra centenas de vezes por segundo e o receptor deve estar atento a receber estes sinais. A estratégia baseada na dispersão de sequência direta emprega um código para dispersar o sinal de dados por uma banda de frequência mais ampla. Nesta abordagem, o emissor e receptor possuem um código secreto para interpretar os sinais enviados e o principal benefício deste método consiste na possibilidade de compartilhar uma banda de frequência para vários sinais simultaneamente. A quarta e última estratégia consiste no UWB (*Ultra-Wide-Band*), a qual é projetada para bandas mais largas. Nesta abordagem uma série de pulsos rápidos são enviados variando suas posições na troca de informações. No decorrer desta unidade estudaremos em mais detalhes outras partes do espectro eletromagnético começando pelo rádio.

SAIBA MAIS: este tipo de abordagem possui uma aplicação prática na área militar, por exemplo, por dificultar a detecção das transmissões e pela dificuldade de obstruir o envio de sinais por meio desta estratégia.

ATENÇÃO: as principais vantagens da abordagem UWB consistem na capacidade de tolerar uma grande quantidade de interferências geradas por outros sinais de bandas, o método demanda pouca energia na transmissão de curta distância e não causar interferência em outros sinais de rádio.

Transmissão Via Rádio

Atualmente existem muitos dispositivos desenvolvidos para transmitir sinais por meio de ondas de rádio. O sucesso da grande popularidade desta tecnologia se dá devido a dois fatores, a facilidade técnica envolvida para efetuar transmissões eficazes e pelas ondas geradas possuírem a característica omnidirecionais. A com-

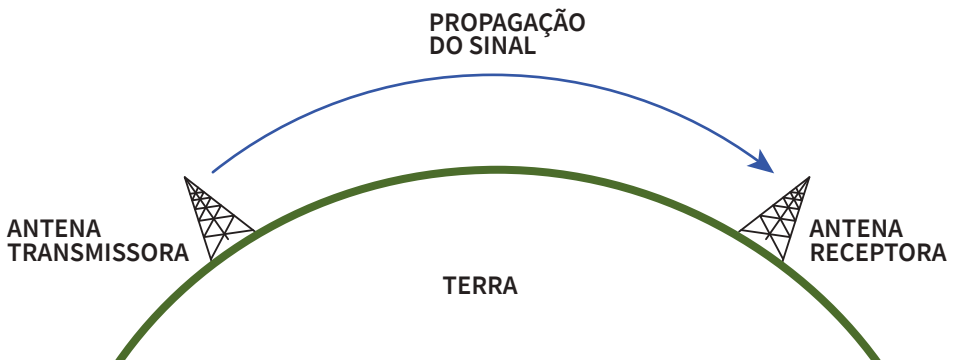
plexidade envolvida na geração de ondas de rádio é baixa e essas ondas podem geralmente ser propagadas através de obstáculos, tais como prédios. Devido a esta característica, as ondas de rádio podem ser empregadas em ambientes abertos e fechados. Além disso, as ondas de rádio são omnidirecionais, ou seja, eles podem se propagar em todas as direções a partir da origem. Como consequência, a transmissão via ondas de rádio não demanda um alinhamento físico cuidadoso entre o emissor e receptor.

Algumas propriedades das ondas de rádio determinam a sua eficácia em se propagar através de obstáculos. Ondas eletromagnéticas com frequências baixas atravessam bem os obstáculos. Todavia, a potência do sinal transmitido cai consideravelmente ao passo que a distância entre a origem e destino aumenta, pois a energia do sinal se espalha. As ondas de rádio com frequências altas tendem a viajar em linha reta e a ricochetear em obstáculos. Nesse caso também pode ocorrer a redução da potência devido a perda do caminho. No entanto, além disso as ondas com alta frequência podem sofrer reflexões e podem ser absorvidas pela chuva ou outros obstáculos de maneira mais intensa do que as ondas com baixa frequência. Independentemente do tipo de frequência empregada, as ondas de rádio estão propensas a interferências de equipamentos elétricos e motores.

SAIBA MAIS: este fenômeno também é referenciado como perda no caminho.

A propagação de ondas de frequências baixas e altas ocorrem de modo diferente. Nas bandas VLF, LF e MF, as ondas são propagadas perto do solo, tal como ilustra a Figura 53. Observando a figura, podemos notar que o sinal é propagado diretamente entre as antenas. As ondas propagadas em frequências baixas podem ser detectadas em um raio de cerca de mil quilômetros. Apenas para contextualizar a aplicação esta tecnologia, as rádios AM normalmente usam a banda MF. Usando bandas de frequências baixas, tal como a VLF, LF e MF, as ondas de rádio podem facilmente atravessar prédios e por este motivo podemos usar rádios portáteis em ambientes fechados sem problema. Todavia, esta tecnologia também apresenta limitações. A principal delas diz respeito à baixa largura de banda disponível.

FIGURA 53 – Exemplo de Transmissão Via Rádio de Frequências Baixas

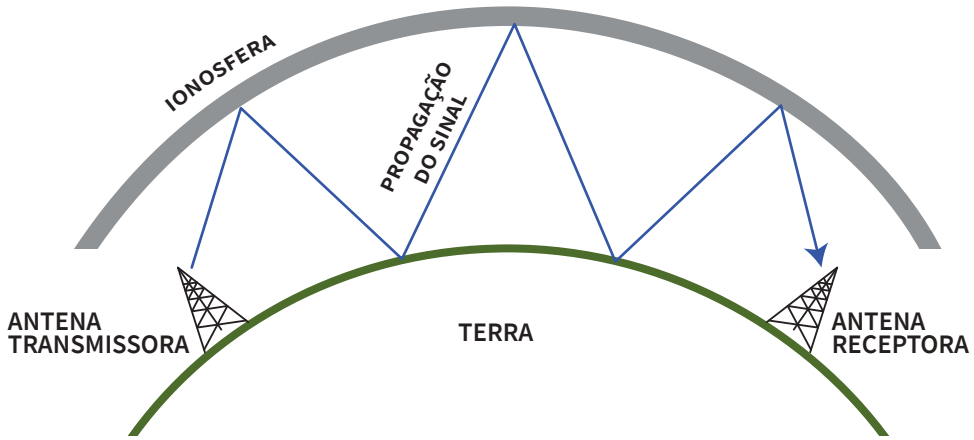


FONTE: Adaptado de Ebah. Disponível em: http://www.ebah.com.br/content/ABAAAfeXMAJ/meios-transmissao?part=2

Em contrapartida, diferentemente as ondas de frequência baixas, as ondas de frequência mais altas necessitam ser refratadas na ionosfera antes de chegar na antena receptora. Sempre que um sinal gerado com as frequências mais altas atinge a ionosfera, o mesmo é enviado de volta para a Terra. A Figura 54 ilustra uma situação deste tipo, na qual podemos observar um sinal refratado várias vezes após ser gerado por uma antena transmissora até atingir seu destino. Essas bandas são muitas vezes utilizadas por radioamadores em comunicação de alta distância. Além disto, os militares também costumam se comunicar nas bandas HF e VHF.

TERMO DO GLOSSÁRIO: a ionosfera consiste em uma camada de partículas carregadas dispostas em torno do nosso planeta a uma altura de cerca de 100 a 500 Km.

FIGURA 54 – Propagação Ionosférica para Transmissão de Ondas de Rádio de Alta frequência



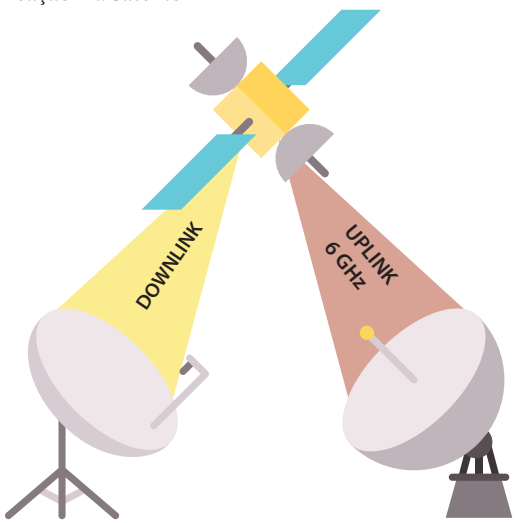
FONTE: Adaptado de Ebah. Disponível em: http://www.ebah.com.br/content/ABAAAfeXMAJ/meios-transmissao?part=2

Agora que estudamos a transmissão por meio das ondas de rádio, podemos estabelecer uma comparação com os meios de transmissão guiados em termos de atenuação do sinal. Empregando cabos de fibra óptica, par trançado ou coaxial, o sinal decresce por uma mesma fração por distância unitária. Por exemplo, considerando o cabo par trançado, um sinal de 20 decibéis (DB) pode percorrer 100 metros sem atenuações. No caso das ondas de rádio, o sinal cai pela mesma fração enquanto a distância dobra, por exemplo, perde 6 DB por duplicação em uma área livre. Analisando esses fatores, podemos perceber que as ondas de rádio podem percorrer distâncias longas com mais facilidade. Entretanto, uma limitação do emprego das ondas de rádio consiste na possibilidade de mais de um usuário transmitir simultaneamente na mesma banda, ocasionando interferências ou perda do sinal. Visando contornar essa limitação, o governo de um país controla de forma rígida o licenciamento da utilização de transmissores de rádio.

Transmissão Via Satélite

O princípio de funcionamento da transmissão via satélite é parecido com a transmissão de rádio por meio de frequências altas. Todavia, diferentemente de como acontece na transmissão de rádio, a refração não ocorre na ionosfera. Para realizar esta função essa tecnologia utiliza um satélite em órbita atuando como um grande repetidor de micro-ondas no céu. A Figura 55 ilustra a comunicação via satélite.

FIGURA 55 – Comunicação Via Satélite



FONTE: Adaptado de Melhor Escolha. Disponível em: https://blog.melhorescolha.com/tv-a-cabo-ou-via-satelite-qual-assinar/

Conforme ilustrado na Figura 55, a comunicação via satélite ocorre por meio de duas antenas, um canal de comunicação e o satélite propriamente dito. As antenas transmitem micro-ondas de forma que elas podem desempenhar o papel de transmissora ou receptoras. As antenas transmissoras enviam micro-ondas para os satélites, este processo é denominado *Uplink*, enquanto que as receptoras recebem as micro-ondas por meio do processo denominado *Downlink*. Essas transmissões podem ocorrer em diferentes bandas e com diferentes larguras de banda. A Tabela 4 apresenta as principais bandas utilizadas e suas respectivas larguras de banda.

TABELA 4 – Principais bandas de Satélite

BANDA	*DOWNLINK*	*UPLINK*	LARGURA DE BANDA
L	1,5 GHz	1,6 GHz	15 MHz
S	1,9 GHz	2,2 GHz	70 MHz
C	4 GHz	6 GHz	500 MHz
Ku	11 GHz	14 GHz	500 MHz
Ka	20 GHz	30 GHz	3.500 MHz

FONTE: Tanenbaum (2011).

Um satélite é composto por *transponders*. Além disso, pode ser adicionado um processamento adicional para manipular ou redirecionar os feixes de dados sepa-

radamente. Ao gerar os sinais deste modo, o desempenho é aprimorado, pois torna-se possível evitar a amplificação de um sinal que representa uma interferência.

ATENÇÃO: a função dos *transponders* consiste em receber um sinal enviando por uma antena, amplificar os sinais e entrada e transmiti-los novamente para a Terra em uma frequência diferente para evitar a ocorrência de interferências.

Existem três tipos principais de satélites, os geoestacionários, de órbita média e de órbita baixa. Os satélites geoestacionários, ou GEO (Geoestationary Earth Orbit) são aqueles que completam uma volta ao redor do planeta em 24 horas. Os satélites em órbita média ou MEO (*Medium-Earth Orbit*) se deslocam lentamente em longitude, tomando cerca de 6 horas para circular o nosso planeta, demandando um acompanhamento dos mesmos para efetuar a refração e implicando em uma área de cobertura menor do que os satélites GEO. Atualmente estes satélites não são usados para comunicação. Os satélites em órbita baixa, ou LEO (*Low-Earth Orbit*) estão fisicamente localizados bem mais próximos da Terra do que os satélites GEO e não precisam de sinais muito potentes para transmissão. As principais diferenças entre esses três tipos de satélites consistem na altitude em que eles estão posicionados, no tempo por órbita, velocidade, tempo de atraso e a cobertura global. A Tabela 5 apresenta uma comparação entre estes três tipos de satélites.

ATENÇÃO: os satélites GEO se encontram aparentemente parados em relação a um ponto fixo da Terra.

TABELA 5 – Comparação dos Tipos de Satélites

CARACTERÍSTICAS	GEO	MEO	LEO
Altura (quilômetros)	36.000	6.000-12.000	200-3000
Tempo por órbita (horas)	24	5-12	1,5
Velocidade (Km/hora)	11.000	19.000	27.000
Tempo de atraso (ms)	250	80	10
Cobertura global	3	10-12	50-70

FONTE: Autores

Uma vez estudadas as principais características sobre a comunicação via satélite, podemos agora comparar os benefícios desta tecnologia com a transmissão via cabos de fibra óptica. Desde a década de 1980, as companhias telefônicas começaram a substituir as suas redes de longa distância por fibra óptica, pois essa escolha parecia ser a melhor opção a longo prazo. Todavia, alguns nichos de mercados podem ser melhor explorados por meio da comunicação via satélite. Um fator que favorece a escolha da implantação da comunicação via satélite consiste na facilidade de instalação. Diferentemente dos cabos de fibra óptica que são frágeis e demandam a contratação de pessoas especializadas para realizar conexões e manutenções da fibra, a única demanda do satélite está relacionada com a existência das antenas e do satélite propriamente dito. Outro nicho de mercado consiste em

situações que se torna necessária a existência de uma rede, mas a infraestrutura terrestre é pouco desenvolvida. Nesse caso, a comunicação via satélite também se destaca ao dispensar o emprego de uma infraestrutura física complexa. Um terceiro nicho importante consiste em cenários onde a difusão do sinal é um requisito fundamental. Esse cenário diz respeito a necessidade de que uma mesma mensagem seja recebida por milhões de estações simultaneamente. Nesta situação a comunicação via satélite também supera a tecnologia de fibra óptica. Todavia, apesar destes cenários, existe ainda uma fragilidade existente na comunicação por satélite, o custo financeiro. Para amenizar esta fragilidade, existem muitas pesquisas que visam aprimorar a comunicação por meio de satélites LEO, mas isso parece que acontecerá em um futuro distante.

ATIVIDADES DE REFLEXÃO OU FIXAÇÃO

1. Explique o conceito da topologia ponto a ponto e forneça um exemplo de aplicação da mesma.

2. Quais as limitações do emprego da topologia física em anel?

3. Defina o conceito da topologia em estrela, apresentando suas vantagens e desvantagens.

4. O que é uma topologia em malha e qual sua principal aplicação?

5. Explique a topologia em árvore, bem como seus pontos positivos e negativos.

6. Quais os dois tipos de cabo coaxiais existentes e quais suas respectivas capacidades de transmissão sem o emprego de repetidores?

7. Diferencie um cabo de par trançado UTP (*Unshielded Twistead-Pair*) do STP (*Shielded Twistead-Pair*).

8. Quais os três principais modos de conexões de cabos de fibra óptica e seus respectivos percentuais de perda da luz?

9. Defina o conceito de espectro eletromagnético e como ele pode ser usado na comunicação.

10. Compare a transmissão via rádio com a transmissão via satélite.

3

ARQUITETURA, PROTOCOLOS E TRANSMISSÃO DE DADOS

INTRODUÇÃO

Neste momento, você já conhece os principais meios de transmissão empregados na criação de uma rede de computadores, bem como as diferentes topologias lógicas e físicas empregadas para organizá-las. Pensando na complexidade envolvida nestes conceitos somada aos diversos desafios existentes em nível de sistema operacional para possibilitar a comunicação de dados, provavelmente você tenha concluído que o projeto de uma rede de computadores consiste em uma tarefa difícil.

Se você ficou interessado em saber como a complexidade envolvida no projeto das redes de computadores, fique tranquilo, pois esta unidade abordará este assunto. Nela estudaremos como o conceito de camadas possibilita dividir a alta complexidade do projeto das redes de computadores em vários níveis e interconectá-los de maneira solucionar o problema como um todo. Além disso, veremos os principais modelos de camadas no projeto de redes de computadores, sendo eles o modelo de referência OSI (*Open System Interconnection*), elaborado pela ISO (*International Standards Organization*) e TCP/IP (*Transmission Control Protocol/Internet Protocol*) que consiste no padrão empregado de fato. Após estudar esta unidade você não apenas conhecerá estes modelos, como também estará apto para compará-los e conseguirá identificar pontos a serem aprimorados em ambos.

A unidade está organizada como segue. A Seção 3.1 apresenta o modelo de camadas, discutindo os principais conceitos deste trabalho. A Seção 3.2 descreve o modelo OSI. A Seção 3.3 detalha o modelo TCP/IP. A Seção 3.4 compara os modelos OSI e TCP/IP. As Seções 3.4 e 3.5 apresentam críticas aos modelos OSI e TCP/IP, respectivamente.

3.1
MODELO DE ORGANIZAÇÃO EM CAMADAS

O desenvolvimento de uma arquitetura de redes de computadores consiste em uma tarefa complexa, pois envolve inúmeros aspectos de hardware e software, como interface com o meio de transmissão, especificação, verificação e implementação de protocolos, integração com o sistema operacional, controle de erros, segurança e desempenho. O modelo de camadas surgiu para reduzir a complexidade do projeto de arquitetura de redes.

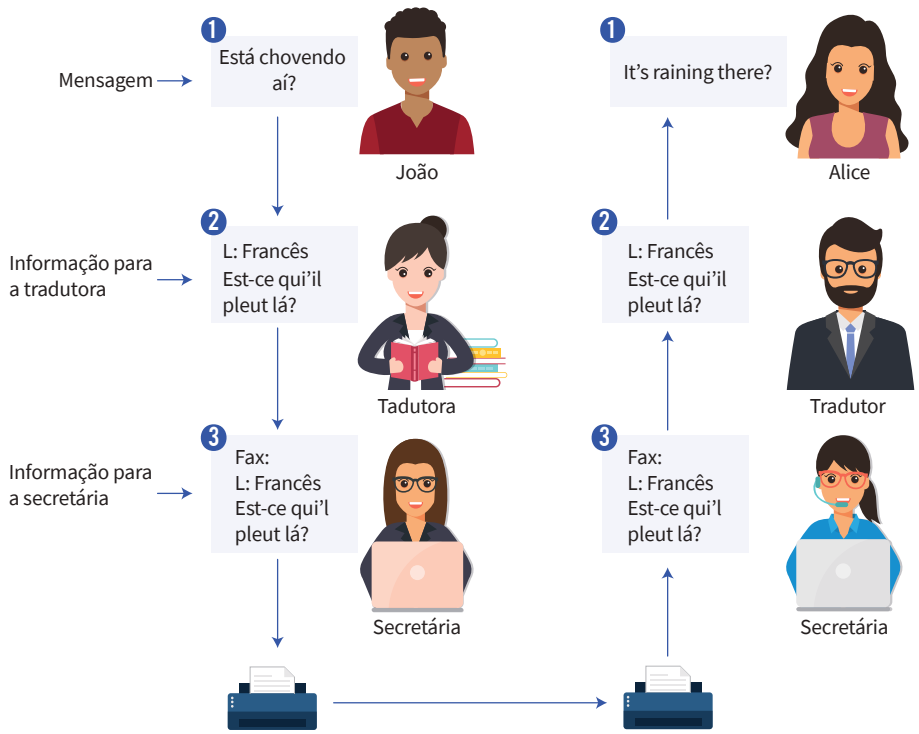
A ideia do modelo de camadas consiste em dividir o projeto de redes em funções independentes e agrupá-las em camadas. Dessa forma, cada nível é responsável por determinados serviços e apenas aquela camada pode oferecê-los. Além disso, o modelo implementa regras para a comunicação entre as camadas, isolando suas funções e garantido a independência entre elas.

ATENÇÃO: no modelo de camadas, os níveis são organizados hierarquicamente, formando uma espécie de pilha. Cada camada possui um nome e um número associado.

Para exemplificar o conceito de camadas, consideremos uma situação onde duas pessoas desejam se comunicar, mas não falam o mesmo idioma e para isso contam com um tradutor que trabalha com uma secretária. A Figura 56 ilustra essa situação. No nosso exemplo, João e Alice desejam conversar, sendo que João quer perguntar para Alice se está chovendo na cidade dela. Todavia, João fala português e Alice fala inglês. Essa situação pode ser resolvida empregando o conceito de camadas, sendo elas a mensagem, a tradução e a transmissão.

A mensagem criada por João e que será tratada para ser entregue à Alice consiste na primeira camada. Nessa camada, a responsabilidade do significado dessa mensagem depende apenas de João, o que representa uma espécie de isolamento em relação às demais camadas. Isto quer dizer que se o significado da mensagem não fizer sentido em algum momento, apenas esta camada precisa ser tratada e não as demais. No caso do nosso exemplo, a mensagem de João consiste na pergunta “Está chovendo aí?”. Uma vez gerada a mensagem, a mesma é encaminhada para a camada situada abaixo, a tradução.

FIGURA 56 – Exemplo do Emprego de Camadas



FONTE: Autores

A camada de tradução recebe como entrada uma mensagem em português e possui como saída uma mensagem em francês para a secretária da tradutora. No nosso exemplo, tanto João como Alice possuem acesso a um tradutor, sendo que a característica comum entre eles consiste no domínio da língua francesa. A diferença entre eles é que a tradutora de João além de dominar a língua francesa, também é fluente em português, enquanto que o tradutor de Alice domina a língua inglesa em adição da língua francesa. Seguindo o fluxo do envio da mensagem de João para Alice, a tradutora escreve a mensagem de João para o francês e repassa para a próxima camada, a transmissão.

Na camada de transmissão, possuímos uma secretária responsável por receber uma mensagem em francês e passar um fax para a secretária do tradutor de Alice. Nesse caso, a secretária possui todo o conhecimento necessário para realizar apenas essa tarefa, sem precisar conhecer nada sobre o processo de tradução. Dentre as habilidades exclusivas das secretárias podemos destacar o domínio do aparelho de fax e o conhecimento do contato da secretária do tradutor de Alice. Seguindo essa lógica, caso a folha com a mensagem traduzida fique mal posicionada durante o fax prejudicando sua legibilidade, temos como identificar que o problema ocorreu na camada de transmissão e poderemos tratar os problemas apenas entre as secretárias, dispensando intervir em nível de tradução e da criação da mensagem.

Após a transmissão da mensagem, realiza-se o processo inverso de operação das camadas. A secretária do tradutor de Alice recebe a mensagem e repassa para o tradutor. Em seguida, o tradutor transcreve a mensagem da língua francesa para a língua inglesa e repassa para Alice. Na sequência, Alice recebe a mensagem e

pode interpretá-la, realizando assim a comunicação entre João e Alice. Durante a recepção da mensagem, caso algum erro seja identificado, apenas a camada em questão entra em operação. Por exemplo, caso o tradutor de Alice não compreenda o texto em francês, ele deverá se comunicar somente com a tradutora de João, respeitando o fluxo das camadas. O mesmo ocorre em relação as demais camadas. Observando esse comportamento, podemos afirmar que uma camada se comporta como uma caixa-preta, pois as camadas que interagem com ela devem conhecer apenas suas entradas e saídas, sem a necessidade de conhecer como o processo interno se desenvolve.

Esse isolamento entre as camadas ocorre devido ao conceito de encapsulamento. O conceito de PDU (*Protocol Data Unit*), ou unidades de dados de protocolo, desempenha uma função importante neste conceito. O PDU descreve a unidade de dados tratados em uma camada, abrangendo os cabeçalhos necessários para dar continuidade ao seu processamento. Por exemplo, a camada de aplicação recebe um dado puro e transforma em um PDU-A, onde A descreve o cabeçalho da camada de aplicação. A camada de transporte processa o PDU-A e o transforma em PDU-T e encaminha para a camada de rede. A camada de rede processa o PDU-T e o transforma em PDU-R e assim por diante. Logo, o conceito de PDU descreve um termo genérico para descrever as informações tratadas em uma camada.

TERMO DO GLOSSÁRIO: o encapsulamento permite esconder de um determinado nível as informações de controle referentes às camadas superiores, criando o efetivo isolamento e a independência entre as camadas.

O modelo de camadas proporciona benefícios de projeto e benefícios comerciais. Primeiramente analisaremos os benefícios de projeto. Através do modelo de camadas, o projeto de rede pode ser dividido mais facilmente e como as camadas são isoladas, não importa como as funções de um nível são implementadas, desde que as regras de comunicação sejam respeitadas. Por meio desta abordagem, uma camada muito complexa poderia ser dividida em subcamadas, sem que essa decisão afete das demais camadas. Além disto, o modelo de camadas traz benefícios para a manutenção do projeto de rede, pois se houver um problema, basta identificar a camada responsável e corrigi-lo. Também se torna possível introduzir novas funcionalidades em uma camada sem afetar as demais, reduzindo o esforço para a evolução do projeto de rede.

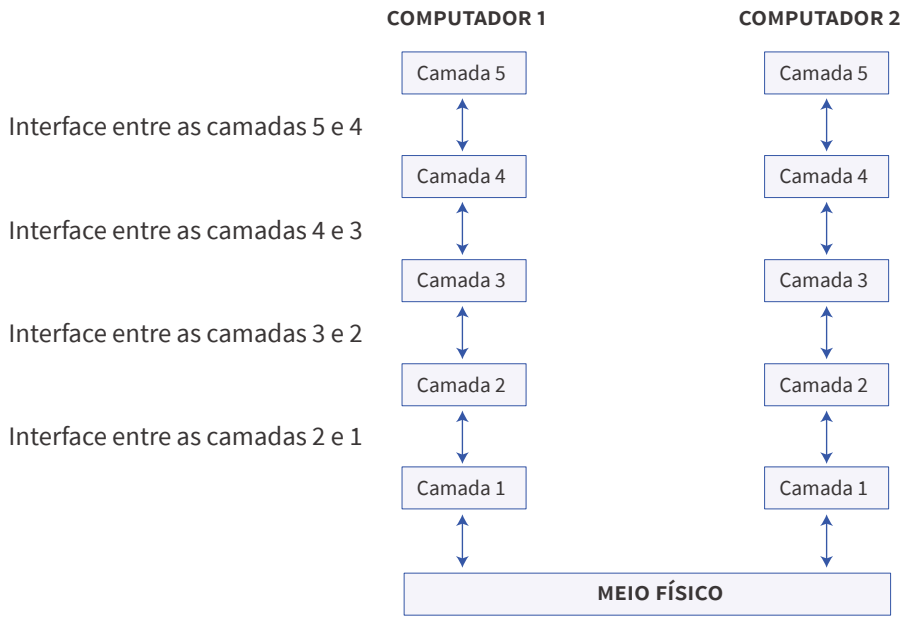
O modelo de camadas também oferece benefícios comerciais. Por meio deste modelo, diferentes empresas podem oferecer soluções para uma ou mais camadas, permitindo aos usuários adquirir produtos de diferentes fabricantes sem o risco de incompatibilidades entres os diferentes dispositivos. Dessa forma, o mercado se torna mais competitivo, tendendo a reduzir o custo dos produtos para os usuários.

Seguindo o modelo de camadas, pode haver duas perspectivas de comunicação, vertical e horizontal. Na perspectiva de comunicação vertical, cada camada se comunica apenas com as camadas adjacentes, proporcionando um entendimento da comunicação entre as camadas dentro de um mesmo dispositivo. A Figura 57 ilustra a perspectiva vertical. Por meio desta perspectiva, cada camada oferece um

conjunto de serviços para a camada imediatamente superior e utiliza serviços da camada inferior. Os serviços são oferecidos através de interfaces que permitem a comunicação entre as camadas adjacentes. Por exemplo, a camada de transporte oferece serviços para a camada de aplicação e utiliza serviços da camada de rede.

ATENÇÃO: essas perspectivas podem ser usadas para explicar o funcionamento de serviços de rede ou protocolos.

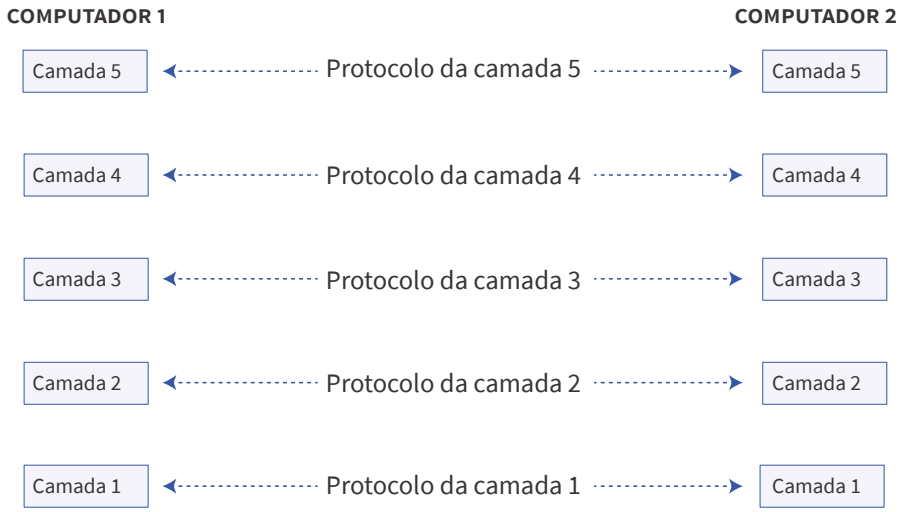
FIGURA 57 – Análise Vertical de uma Arquitetura em Camadas



FONTE: Autores.

A perspectiva de comunicação horizontal permite criar a abstração de que as camadas se comunicam diretamente. A Figura 58 ilustra a perspectiva horizontal de comunicação entre as camadas. Esta perspectiva fornece o entendimento da operação inversa de uma camada. Por exemplo, considerando a camada física. Analisando a perspectiva do emissor, a camada física codifica os bits dos dados em sinais e envia pelo meio físico. Considerando esta mesma camada, mas do ponto de vista do receptor, a função da camada física consiste em receber os sinais pelo meio físico e decodificá-los.

FIGURA 58 – Análise Horizontal do Modelo em Camadas



FONTE: Autores

Uma camada pode ter um ou mais protocolos associados. Um determinado protocolo é formado pelas informações de controle contidas no cabeçalho e pelo processamento dessas informações nas respectivas camadas de origem e destino. É importante não confundir os conceitos de serviço e protocolo. Um serviço define o que deve ser feito pela camada, ou seja, as interfaces e parâmetros que permitem a comunicação vertical entre as camadas adjacentes. O protocolo define como o serviço é implementado, ou seja, as informações de controle e processamento realizado pelas camadas no mesmo nível horizontal. O conjunto de protocolos implementados por todas as camadas do modelo é conhecido como pilha de protocolos.

TERMO DO GLOSSÁRIO: um protocolo de rede consiste em um conjunto de regras que determinam como determinados dispositivos devem se comunicar.

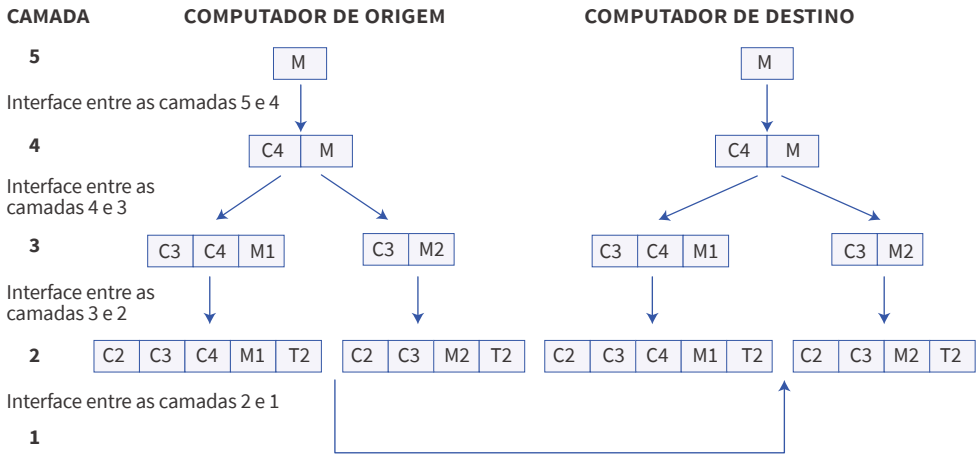
Podemos ainda analisar o modelo de camadas baseado na forma como as mensagens são enviadas. A partir deste ponto de vista, podemos novamente utilizar a perspectiva vertical e horizontal de camadas. Considere a perspectiva vertical do computador emissor da mensagem. A Figura 59 ilustra essa situação. Esse computador possui uma mensagem que deseja enviar para um computador de destino. Na camada mais acima da pilha de camada, por exemplo, na camada 5, encontra-se a mensagem *M* que deve ser encaminhada para o computador destino.

Na perspectiva vertical, logo abaixo da camada 5 existe uma interface com a camada 4, a qual estabelece o conjunto de informações de entrada para que seu serviço seja prestado. No nosso exemplo, o serviço da camada 4 consiste em agregar um cabeçalho em *M*. Um cabeçalho consiste em um conjunto de informações adicionais que possibilitam a execução de operações de controle, como por exemplo, o controle de fluxo ou de integridade da mensagem. Após processar os dados de entrada, a camada 4 repassa a saída do processamento ao aglutinar *M* com o cabeçalho 4 (C4) para a camada 3 por meio de uma interface entre essas duas

camadas. A camada 3, recebe esses dados e os fragmenta em pedaços menores. Nesse caso, a saída consiste em dois pacotes de dados, sendo o primeiro possui um pedaço de *M*, representado na figura como M1, e o cabeçalho C4. O segundo pacote possui a segunda metade da mensagem (M2). Ambos os pacotes possuem ainda um cabeçalho da camada 3 (C3) para agregar informações de controle referente aos serviços prestados por esta camada.

As camadas 2 e 1 também se comunicam por meio de interfaces bem definidas. Depois da fragmentação das mensagens, a camada 3 encaminha o resultado do seu processamento para a camada 2. Na camada 2, cada pacote recebe um cabeçalho de controle (C2) e uma informação auxiliares da transmissão dos dados em sinais digitais (T2). Usando a interface a camada 2 encaminha estes dados para a camada 1, a qual possui a função de transmitir os dados para o receptor.

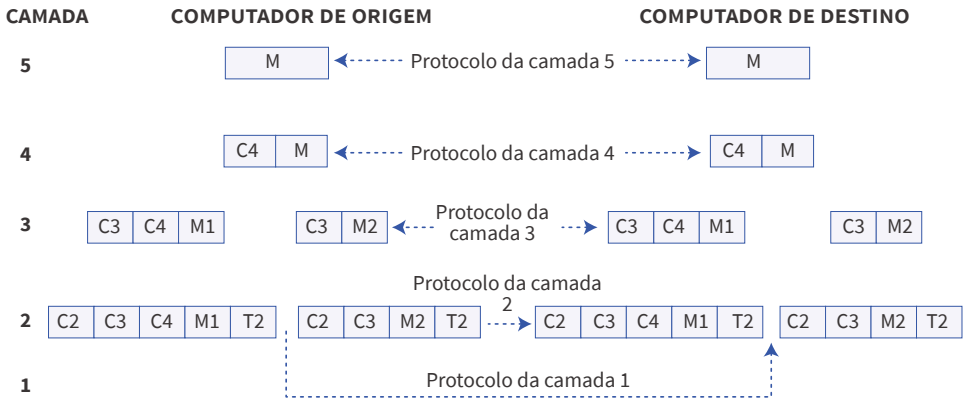
FIGURA 59 – Analisando o Envio de Mensagem sob a Perspectiva Vertical de Camadas



FONTE: Autores

O envio das mensagens também pode ser observado por meio da perspectiva horizontal. Ao considerar essa perspectiva, podemos pensar que as camadas se comunicam diretamente, mudando apenas sua função, sendo que uma atua como emissora e outra como receptora. Por meio desta perspectiva, podemos melhor entender os serviços oferecidos por uma camada nas situações de envio e recebimento de mensagens. Consideremos a mesma situação analisada na comunicação vertical, onde existe um computador que envia uma mensagem para outro computador. A Figura 60 mostra essa situação. Nesse caso, podemos perceber que a comunicação se dá por meio dos protocolos seguidos pelas camadas. Veja que essa perspectiva não objetiva demonstrar como de fato a informação foi transmitida, mas a forma como cada camada percebe a comunicação.

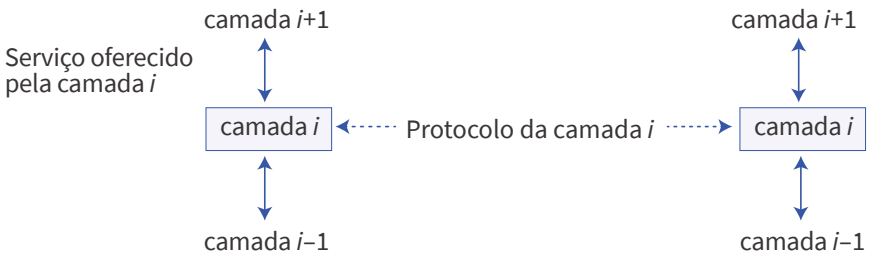
FIGURA 60 – Analisando o Envio de Mensagem sob a Perspectiva Horizontal de Camadas



FONTE: Autores

Ao observar a Figura 60, podemos ver que os protocolos desempenham um papel fundamental, pois ele descreve as entradas e saídas para camada. Vamos analisar a figura considerando as camadas mais inferiores até as superiores. Observado a comunicação entre a camada 1, podemos perceber que o protocolo dessa camada encaminha apenas os sinais elétricos, que ambas as camadas compreendem. No entanto, na camada 2, o emissor transforma a saída da camada 2 em sinais elétricos, enquanto que no receptor os sinais elétricos são transformados em pacotes compreensíveis pela camada 2. O mesmo ocorre com a camada 3, onde a máquina emissora recebe os dados da camada 2 complementa com os cabeçalhos da camada 3. Considerando a mesma camada no lado receptor ocorre o processo inverso. De forma geral, esse padrão se repete pelas demais camadas até que a mensagem original seja reconstituída no computador receptor da mensagem.

FIGURA 61– Relação entre os Conceitos de Protocolo e Interface



FONTE: Autores

Ao comparar a perspectiva horizontal e vertical, podemos identificar uma diferença na base pela qual a comunicação ocorre. Na perspectiva horizontal, os protocolos de comunicação de cada camada desempenham uma função mais importante. Na perspectiva vertical, as interfaces dispostas entre as camadas atuam de maneira mais significativa permitindo a troca de informações. A Figura 61 ilustra a relação entre protocolos e interfaces. Todavia, independentemente da perspectiva utilizada, podemos perceber que uma camada de uma arquitetura de redes deve oferecer um serviço bem definido.

Um serviço compreende uma funcionalidade de uma dada camada de rede. Um serviço de uma camada é oferecido de modo transparente na arquitetura de rede e pode ser acessado por intermédio das interfaces entre as camadas. Dentre os serviços que podem ser oferecidos por meio de uma camada, podemos citar o serviço de fluxo de mensagens confiáveis, o fluxo de bytes confiável, a conexão não confiável, o datagrama não confiável, o datagrama confirmado e o serviço de solicitação e resposta. A Tabela 6 mostra como esses serviços podem ser aplicados em alguns serviços do dia a dia das pessoas.

TABELA 6 – Exemplos de Serviço por Tipo

TIPO	SERVIÇO	EXEMPLO DE UTILIZAÇÃO
Orientado a conexão	Fluxo de mensagens confiáveis	Transação bancária
	Fluxo de bytes confiável	Streaming de vídeo
	Conexão não confiável	VoIP
Sem conexão	Datagrama não confiável	Lixo eletrônico
	Datagrama confirmado	Mensagem de texto

FONTE: Autores

Observando os exemplos de serviço da Tabela 6, talvez eles estejam um pouco abstratos para esse momento, todavia no decorrer da unidade vamos detalhar cada um deles. O mais importante no momento consiste em notar que todos esses serviços estão categorizados em dois grupos, os serviços orientados a conexão e sem conexão. No decorrer da unidade abordaremos de maneira mais profunda estes conceitos.

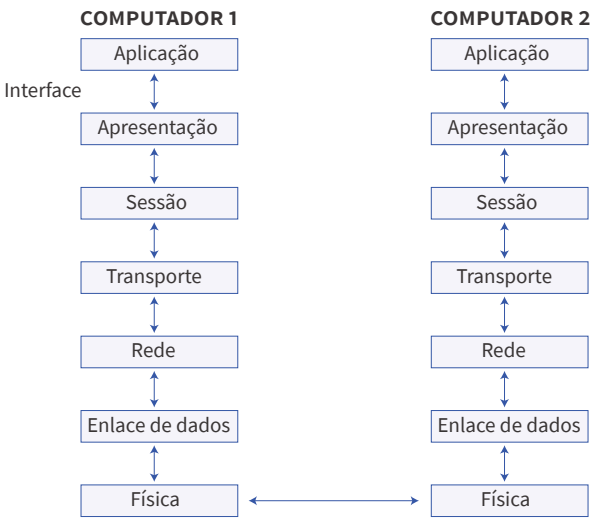
TERMO DO GLOSSÁRIO: um serviço orientado a conexão pode ser brevemente descrito por sua característica de estabelecer expressamente uma conexão antes de enviar os dados de modo a prover uma confiabilidade maior na comunicação. Em contrapartida, um serviço sem conexão dispensa essa característica ao enviar dados sem empregar medidas de controles de forma rígida visando proporcionar um desempenho mais eficiente na comunicação.

3.2
MODELO DE REFERÊNCIA OSI

O modelo de referência OSI (*Open Systems Interconnection*) trata da interconexão de sistemas abertos e baseia-se em uma proposta desenvolvida pela ISO (*International Standards Organization*) como um primeiro passo em direção à padronização internacional dos protocolos organizados em camadas. Uma informação importante é que o modelo OSI de fato não consiste em uma arquitetura de rede, pois ele não especifica os serviços e protocolos exatos que devem ser usados em cada camada. Ele informa apenas o que cada camada deve fazer.

ATENÇÃO: as camadas do modelo OSI são: a camada física, a camada de enlace de dados, a camada de rede, a camada de transporte, a camada de sessão, a camada de apresentação e a camada de aplicação.

FIGURA 62 – Camadas do Modelo OSI



FONTE: Autores

O modelo OSI tem sete camadas. A decisão para a escolha deste número de camadas foi baseado em cinco princípios, sendo eles: uma camada deve ser criada onde houver necessidade de outro grau de abstração; cada camada deve executar uma função bem definida; a função de cada camada deve ser escolhida tendo em vista a definição de protocolos padronizados internacionalmente; os limites de camadas devem ser escolhidos para minimizar o fluxo de informações pelas interfaces; o número de camadas deve ser grande o suficiente para que funções distintas não sejam colocadas na mesma camada e pequeno o suficiente para que a arquitetura não se torne difícil de controlar. A seguir cada uma das camadas do modelo OSI são detalhadas.

3.2.1 Camada Física

A camada física trata da transmissão de bits por um canal de comunicação. As questões mais comuns tratadas por esta camada são a quantidade de tempo que um bit deve durar, se a transmissão deve ser realizada simultaneamente nos dois sentidos, a forma como a conexão inicial será estabelecida e de que maneira ela será encerrada e quantos pinos o conector de rede terá e qual a finalidade de cada pino. As questões de projeto desta camada também consideram interfaces mecânicas, elétricas e de sincronização e com o meio físico de transmissão. Uma importante funcionalidade desta camada consiste em empregar esquemas de codificação do sinal digital em bits. A representação em formato binário permite representar a informação enviada de um emissor para um receptor no meio de transmissão. Visando detalhar deste processo, abordaremos primeiramente os fundamentos da representação de dados e sinais, seguindo pelos esquemas de codificação digital NRZ, Manchester, AMI-bipolar e o 4B/5B.

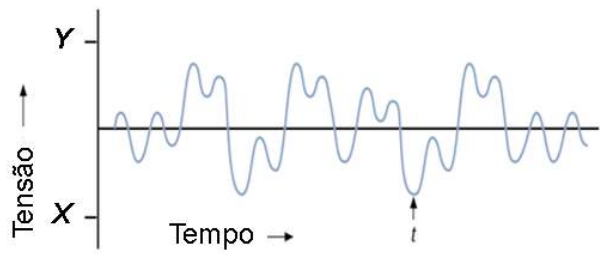
3.2.1.1 Dados e sinais

As informações transmitidas por meio de uma rede de computadores podem ser divididas em duas categorias, dados e sinais. Os dados consistem em entidades que portam significado dentro de um computador ou em um sistema computacional, por exemplo, um arquivo em formato TXT. Os sinais são impulsos elétricos ou eletromagnéticos utilizados para codificar e transmitir dados, por exemplo, um sinal de rádio. Os conceitos de sinais e dados se relacionam para efetuar uma transmissão, pois os dados precisam ser convertidos em sinais antes de serem transmitidos de um ponto ao outro.

Uma característica em comum entre dados e sinais é que ambos podem existir na forma analógica ou digital. A Figura 63 ilustra um exemplo de forma de onda analógica considerando um máximo A, um mínimo B e um tempo t. O exemplo mais comum de dados analógicos consiste na voz humana.

ATENÇÃO: os dados e sinais analógicos são representados por ondas contínuas capazes de assumir um número infinito de valores dentro de um determinado mínimo e máximo.

FIGURA 63 – Exemplo de Sinal Analógico

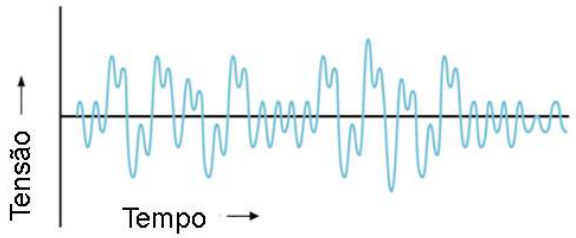


FONTE: Adaptação de White (2012).

Um dos principais pontos fracos dos dados e sinais analógicos compreende a dificuldade de separar o ruído da forma de onda original. Os efeitos do ruído podem ser desde pequenos chiados na linha de comunicação à perda completa de dados. Devido aos efeitos negativos dos ruídos, surge a necessidade de eliminá-lo ou minimizar ao máximo os seus efeitos. No entanto, quando um sistema representa dados e sinais de forma analógica torna-se difícil eliminar ou minimizar os efeitos dos ruídos, pois o ruído ocorre como uma forma de onda analógica, incrementando a dificuldade em separar o ruído da onda que representa os dados.

TERMO DO GLOSSÁRIO: o ruído consiste em uma energia elétrica ou eletromagnética indesejada que degrada a qualidade de sinais e dados.

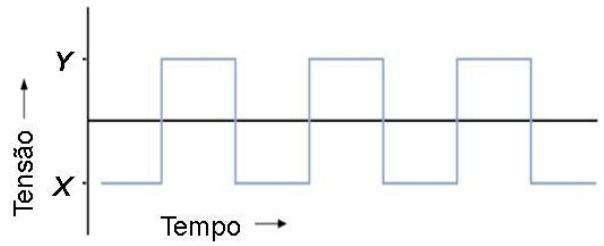
FIGURA 63 – Exemplo de Sinal Analógico



FONTE: Adaptação de White (2012).

Os dados e sinais digitais são formas de ondas discretas não contínuas. A forma de onda digital assume apenas um número finito de valores entre um valor mínimo X e um máximo Y. A Figura 65 ilustra um exemplo de forma de onda digital, mostrando que a forma da onda assume somente dois valores diferentes.

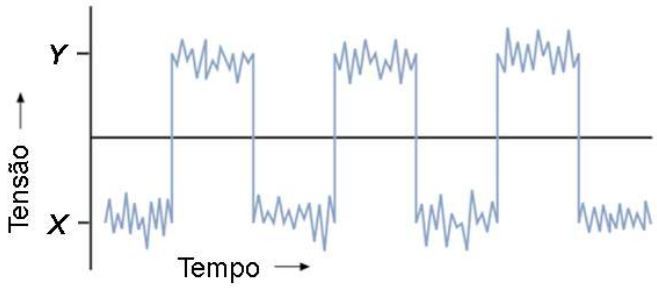
FIGURA 65 – Exemplo de Sinal Digital



FONTE: White (2012).

Um dos principais benefícios da representação dos dados e sinais em formato digitais consiste na facilidade de eliminar os efeitos dos ruídos. A forma da onda digital ocupa um número finito de valores e o ruído possui a propriedade de uma forma de onda analógica capaz de ocupar uma faixa infinita de valores. Quando o ruído e a forma de onda analógica são combinados, torna-se muito fácil identificar e separar a interferência provocada pelo ruído da informação sem prejudicar a qualidade da informação transmitida. A Figura 66 ilustra um exemplo da combinação do sinal digital com o ruído.

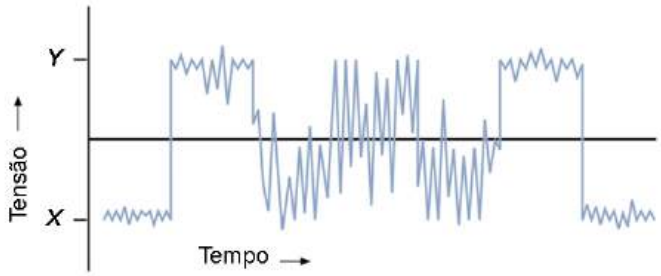
FIGURA 66 – Exemplo de Sinal Digital sob Interferência



FONTE: Adaptação de White (2012).

Observando o exemplo da Figura 66, podemos concluir que o ruído pode ser filtrado enquanto a quantidade do ruído for baixa o suficiente para que a forma de onda digital original possa ser interpretada. Todavia, se o ruído se tornar tão grande a ponto de impossibilitar essa distinção entre alto e baixo, ele será predominado, não sendo possível decifrar a interferência da forma de onda digital. A Figura 4 ilustra uma situação onde o ruído impossibilita o reconhecimento da forma digital.

FIGURA 67 – Situação onde o Ruído Afeta a Representação Digital



FONTE: Adaptação de White (2012).

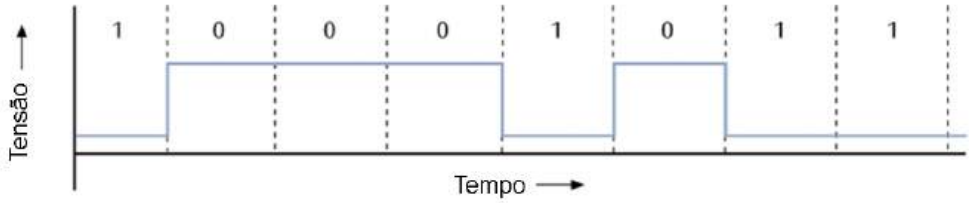
3.2.1.2 Esquemas NRZ

Este esquema de codificação se divide em dois grupos, o NRZ-L e o NRZI. Esse esquema é simples de gerar e a sua implementação em hardware não é cara. A Figura 68 mostra um exemplo do esquema NRZ-L.

TERMO DO GLOSSÁRIO: o esquema de codificação digital NRZ-L (*nonreturn to zero-level*) transmite "1s" como tensões elétricas nulas pelo meio e "0s" como tensões elétricas positivas.

O esquema NRZI (*nonreturn to zero inverted*) altera a tensão no início de um 1 e não altera a tensão no início de um zero.

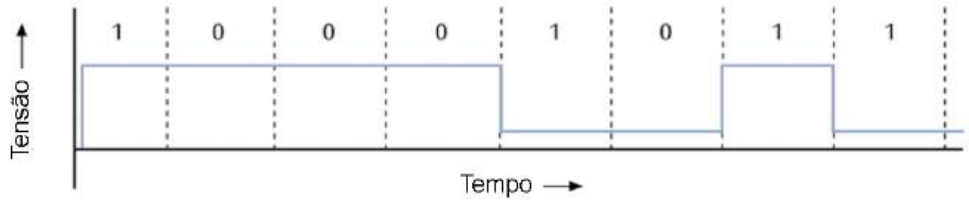
FIGURA 68 – Exemplo do Esquema NRZ-L



FONTE: Adaptação de White (2012).

A principal diferença entre estes esquemas é que com o NRZ-L o receptor precisa verificar o nível de tensão de cada bit para determinar se ele é 0 ou 1. Essa diferença pode ser percebida na Figura 69.

FIGURA 69 – Exemplo do Esquema NRZ-I



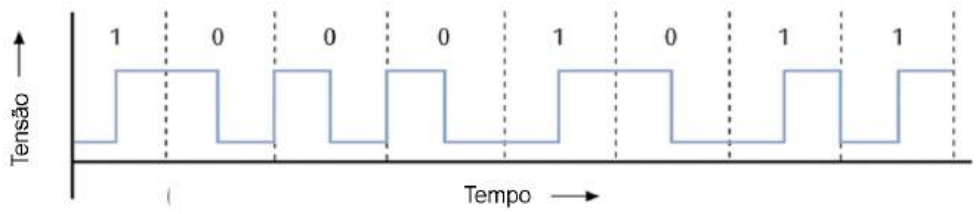
FONTE: Adaptação de White (2012).

Um problema inerente aos esquemas de codificação digital NRZ-L e NRZI é que longas sequências de "0s" nos dados produzem um sinal que nunca se altera. Quando uma sequência longa de "0s" e o sinal não se altera, o receptor não consegue diferenciar quando um bit acaba e o bit seguinte começa. Uma alternativa para este problema consiste em instalar um relógio interno no receptor, possibilitando assim a busca quando procurar cada bit. Todavia, se o relógio do receptor não estiver sincronizado com o relógio do transmissor, comprometendo esta estratégia. Uma abordagem para selecionar este problema consiste em gerar um sinal que se altere para cada bit, aumentando a precisão do sistema.

3.2.1.3 Esquemas Manchester

A classe de esquemas de codificação digital Manchester garante que cada bit apresente algum tipo de alteração de sinal, resolvendo assim o problema da sincronização. Este esquema possui as seguintes propriedades, o sinal altera-se de baixo para cima no meio do intervalo para transmitir o bit 1 e o sinal altera-se de cima para baixo no meio do intervalo para transmitir o bit 0. Quando o sinal estiver baixo e o bit seguinte a ser transmitido for 0, o sinal deve se mover de baixo para cima no início do intervalo, para em seguida poder fazer a transição de cima para baixo no meio. A Figura 70 ilustra o funcionamento do esquema de codificação digital Manchester. A codificação Manchester é utilizada na maioria das redes locais para a transmissão de dados digitais por um cabo de rede.

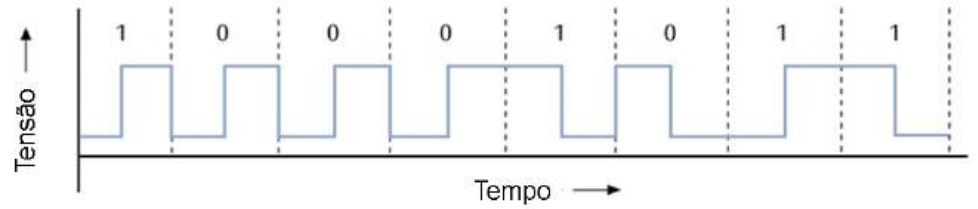
FIGURA 70 – Exemplo do Esquema Manchester



FONTE: Adaptação de White (2012).

O esquema de codificação digital Manchester diferencial é similar ao esquema Manchester, pois sempre há uma transição no meio do intervalo. Entretanto, a direção dessa transmissão no meio não diferencia um 0 de um 1. Pelo contrário, se há uma transição no início do intervalo, um 0 está sendo transmitido. Se não há uma transição no início do intervalo, um 1 está sendo transmitido. A Figura 71 apresenta um exemplo de codificação Manchester diferencial. Como o receptor precisa procurar o início do intervalo para determinar o valor do bit, o Manchester diferencial é similar ao esquema NRZI neste aspecto.

FIGURA 71– Exemplo do Esquema Manchester Diferencial



FONTE: Adaptação de White (2012).

Os esquemas Manchester apresentam uma vantagem em relação aos NRZ, pois neles sempre existe uma transição no meio de um bit. Assim, o receptor pode esperar uma alteração em intervalos regulares e sincronizar-se com o fluxo de bits de entrada.

ATENÇÃO: os esquemas de codificação Manchester são chamados autossincronizados, pois a ocorrência de transições regulares é similar aos segundos de um relógio. É muito importante que o receptor fique sincronizado com o fluxo de entrada e o código Manchester permite essa sincronização.

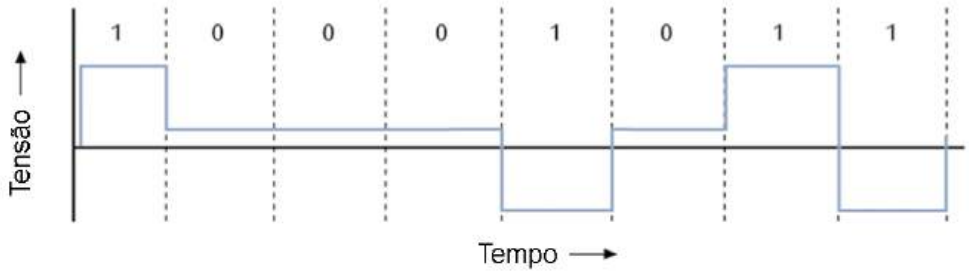
A grande desvantagem dos esquemas Manchester é que em cerca de metade dos casos haverá duas transições para cada bit. Por exemplo, considere o esquema de codificação Manchester diferencial transmitindo uma série de "0s". Neste caso, o sinal precisa ser alterado tanto no início como no meio de cada bit. Assim, para cada valor de dado 0, o sinal se altera duas vezes. A Figura 10 ilustra uma sequência de cinco "0s" sendo transmitidos por meio do esquema de codificação Manchester Diferencial. Nesta ilustração é possível visualizar que o sinal se altera duas vezes para cada bit. Após um segundo, o sinal foi alterado 10 vezes, ou seja, 10 *bauds*. A taxa de transmissão de símbolos (*bauds*) consiste no número de vezes que um

sinal se altera por segundo. Enquanto isto, a taxa de dados, medida em bits por segundo (bps) é 5, equivalendo a metade da taxa de transmissão de símbolos. Além do custo de transmissão, o hardware e o software que lidam com esquemas de codificação Manchester são mais elaborados e caros do que os que lidam com NRZ. Outra desvantagem dos esquemas Manchester é que os sinais que se alteram a uma taxa mais alta são mais suscetíveis a ruído e erros.

3.2.1.4 Esquema AMI-bipolar

Utiliza um princípio diferente dos outros esquemas estudados até o momento, pois emprega três níveis de tensão. Quando um dispositivo transmite um 0 binário, ocorre a transmissão de tensão nula. Quando transmite um 1 binário, pode ocorrer uma transmissão de uma tensão positiva ou negativa. Esta escolha depende de como o último valor binário 1 foi transmitido da última vez. Caso o último binário 1 tenha sido transmitido por meio de uma tensão positiva, o próximo binário de valor 1 será transmitido através de uma tensão negativa. Todavia, se o último binário 1 tenha sido transmitido por uma tensão negativa, o binário 1 seguinte usará uma tensão positiva. A Figura 72 ilustra o funcionamento deste esquema.

FIGURA 72 – Exemplo do Esquema AMI-Bipolar



FONTE: Adaptação de White (2012).

O esquema bipolar apresenta vantagens e desvantagens. A principal vantagem deste esquema é que a soma de todas as tensões de uma transmissão sempre deve ser nula, facilitando medidas de controle. Existem duas principais desvantagens. A primeira desvantagem consiste na mesma apresentada nos esquemas NRZ, no que diz respeito ao problema da sincronização de uma longa sequência de "0s". A segunda desvantagem compreende na dificuldade em implementar em hardware a capacidade de gerar e reconhecer voltagens positivas e negativas.

3.2.1.5 Esquema 4B/5B

O esquema 4B/5B tenta resolver o problema da sincronização do esquema de codificação bipolar e evitar o problema da "transmissão com o dobro de bps" do esquema de codificação Manchester. A utilização de 5 bits (ou cinco "0s" e "1s") possibilita um total de 32 combinações possíveis, pois (2^5 = 32). Destas combina-

ções, o esquema 4B/5B usa apenas as combinações que não possuem três ou mais "0s" consecutivos. Logo, das 32 combinações, são usadas apenas 16. Ao limitar a combinações possíveis e transmiti-las por meio do esquema de codificação digital NRZI, nunca haverá mais de dois "0s" em sequência, a menos que um caractere de 5 bits termine com 00 e o caractere seguinte comece com 0. A Figura 73 ilustra o funcionamento do esquema de codificação digital 4B/5B.

ATENÇÃO: para isto, este esquema recebe quatro bits de dados, converte os quatro bits em uma sequência única de cinco bits e codifica os cinco bits usando o NRZI.

FIGURA 73 – Exemplo do Esquema 4B/5B

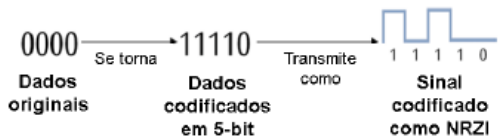
a)

4 bits originais	Novo código de 5 bits
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

b)

Códigos inválidos
00001
00010
00011
01000
10000

c)



FONTE: Adaptado de White (2012).

Para exemplificar o funcionamento do esquema 4B/5B, vamos considerar uma situação onde os próximos 4 bits de um fluxo de dados a ser transmitido são 0001. Observando a primeira coluna da Figura 73, percebemos que o esquema 4B/5B substitui 0001 por 01001. Usando o esquema de codificação digital NRZI, a sequência de cinco bits é representada pelos impulsos de tensão: baixa, alta, baixa, baixa e alta.

O emprego do NRZI melhora a taxa de transmissão em relação ao esquema Manchester, mas, mesmo assim, existe um excedente de dados. Ao empregar o esquema de codificação digital NRZI para transmitir os cinco bits, a taxa de transmissão se iguala ao bps, sendo assim mais eficiente. Infelizmente, a conversão do código de 4 para 5 bits cria um excedente de 20% (um bit extra). Comparando com o esquema Manchester ainda existe uma vantagem significativa, pois este esquema gera um excedente de 100%. Evidentemente, um excedente de 20% permanece melhor do que um de 100%.

3.2.2 Camada de Enlace

A principal tarefa da camada de enlace de dados é transformar um canal de transmissão normal em uma linha que pareça livre de erros de transmissão. Para fazer isso, a camada de enlace mascara os erros reais, de modo que a camada de rede não os veja. Essa tarefa é realizada fazendo que o transmissor divida os dados de entrada em um conjunto de quadro de dados e os transmita sequencialmente. Em geral, este conjunto de quadros têm algumas centenas ou alguns milhares de bytes. Se o serviço for confiável, o receptor confirmará a recepção correta de cada quadro, enviando um quadro de confirmação.

Outra questão que a camada de enlace aborda é como evitar que um transmissor rápido envie uma grande quantidade de dados para um receptor lento. Normalmente, é necessário que exista um mecanismo capaz de regular o tráfego para informar ao transmissor quando o receptor pode aceitar mais dados.

As redes de broadcast têm uma questão adicional a ser resolvida na camada de enlace, como controlar o acesso ao canal compartilhado. Uma subcamada especial da camada de enlace de dados, a subcamada de controle de acesso ao meio trata desse problema.

3.2.3 A camada de Rede

A camada de rede determina como os pacotes são roteados da origem até o destino considerando a passagem por redes intermediárias. As rotas podem se basear em tabelas estáticas ou podem ser atualizadas automaticamente, geradas no início de cada sessão ou altamente dinâmicas. As rotas baseadas em tabelas estáticas são alteradas raramente e quando escolhidas são suscetíveis a compreenderem rotas com dispositivos defeituosos, ocasionando custo de retransmissão. As tabelas atualizadas automaticamente evitam esse problema ao verificar o estado dos dispositivos que compõem uma rota. As rotas geradas no início de cada sessão consistem um tipo de geração automática de rota, podendo ser executada, por exemplo, após um *login* em uma máquina remota. As rotas altamente dinâmicas normalmente são geradas a cada pacote.

A camada de rede também controla o congestionamento de pacotes. Estas situações podem acontecer quando existe uma grande quantidade de pacotes que passam pelo mesmo caminho formando gargalos. A camada de rede, junto às camadas mais altas, adapta a carga sob a rede. Além disso, esta camada trata da qualidade do serviço fornecido, o atraso, tempo em trânsito e instabilidade dos pacotes.

Quando um pacote precisa trafegar de uma rede para outra, podem surgir problemas. O endereçamento utilizado pela segunda rede pode ser diferente do que é usado pela primeira rede. Pode ainda existir diferentes especificações do tamanho dos pacotes. Além disso, cada rede pode usar um tipo de protocolo diferente. A camada de rede deve resolver todos esses problemas para permitir que redes heterogêneas sejam interconectadas.

3.2.4 Camada de Transporte

A função básica da camada de transporte é aceitar dados da camada acima dela, dividi-los em unidades menores quando preciso e repassá-los à camada de rede, garantindo que todos os fragmentos chegarão corretamente à outra extremidade. A camada de transporte também determina que tipo de serviço deve ser fornecido à camada de sessão. O tipo mais popular de conexão de transporte consiste no canal ponto a ponto livre de erros. Este serviço entrega mensagens ou bytes na mesma ordem em que eles foram enviados. No entanto, esta camada também provê um serviço de transporte sem nenhuma garantia quanto à ordem da entrega e à propagação de mensagens para múltiplos destinos. A camada de transporte é uma verdadeira camada de ponta a ponta, que liga a origem ao destino.

3.2.5 A Camada de Sessão

A camada de Sessão permite que os usuários em diferentes máquinas estabeleçam sessões de comunicação entre eles. Uma sessão oferece diversos serviços, inclusive o controle de diálogo, o gerenciamento de *tokens* e a sincronização. O controle de diálogo descreve o controle de quem deve transmitir a cada momento. O gerenciamento de *tokens* impede que duas partes tentem executar a mesma operação crítica ao mesmo tempo. A sincronização realiza a verificação periódica de longas transmissões para permitir que elas continuem a partir do ponto em que estavam ao ocorrer uma falha e a subsequente recuperação.

3.2.6 A Camada de Apresentação

A camada de apresentação está relacionada com a sintaxe e com a semântica das informações transmitidas. Para possibilitar a comunicação entre computadores com diferentes representações internas de dados, as estruturas de dados a serem trocadas podem ser definidas de maneira abstrata, com uma codificação padrão adotada durante a comunicação. A camada de apresentação gerencia essas estruturas de dados abstratos e permite a definição e a troca de estruturas de dados de nível mais alto, por exemplo, registros bancários.

3.2.7 A Camada de Aplicação

Esta camada contém os protocolos para os usuários e aplicações. Um dos protocolos mais famosos desta camada consiste no HTTP (*HyperText Transfer Protocol*) que constitui a base para WWW (*World Wide Web*).

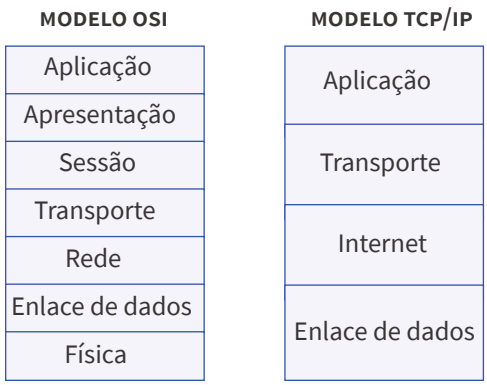
3.3
MODELO DE REFERÊNCIA TCP/IP

O Modelo de referência TCP/IP surgiu como uma alternativa para interconectar diferentes tipos de rede. A primeira rede de computadores baseada no conceito de comutação de pacotes consistiu na ARPANET. A ARPANET era uma rede de pesquisa do Departamento de Defesa do Estados Unidos. A sucessora da ARPANET foi a Internet. Durante o período de consolidação da Internet, várias redes isoladas surgiram, demandando uma arquitetura capaz de interligar essas redes para formar uma rede de escala global. O modelo de referência TCP/IP emergiu como uma solução para contornar este desafio.

ATENÇÃO: o modelo de referência TCP/IP possui quatro camadas, a camada de enlace, a camada de Internet, a camada de transporte e a camada de aplicação.

Uma característica importante modelo TCP/IP consistiu na capacidade de permanecer operacional mesmo se parte da rede estiver comprometida. A ARPANET consistia em um projeto militar e naquele momento, o Departamento de Defesa dos EUA temia um ataque da União Soviética capaz de comprometer a operacionalidade dos seus comutadores e roteadores, impossibilitando a comunicação por meio da ARPANET. Portanto, um requisito da arquitetura de interconexão proposta fosse capaz de sobreviver à perda do hardware de sub-redes. Devido a este objetivo, o projeto da arquitetura TCP/IP considerou este requisito, contribuindo para seu sucesso. A Figura 74 compara as camadas do modelo TCP/IP em relação ao modelo OSI.

FIGURA 74 – Comparação entre o Modelo OSI e o Modelo TCP/IP



FONTE: Autores

Observando a Figura 74, percebe-se que o modelo TCP/IP possui apenas quatro camadas, enquanto que o modelo OSI possui sete. Ao longo desta unidade vamos explicar com detalhes os motivos que impulsionaram as decisões de projeto que

resultaram neste modelo. Por enquanto, podemos adiantar que uma das principais razões que contribuíram para isto foi a empregabilidade prática do modelo e o surgimento de implementações mais eficientes. Todavia, você talvez também tenha notado que os nomes das camadas do modelo TCP/IP também aparecem no modelo OSI. Apesar dos nomes serem iguais, algumas das funções dessas camadas se diferem em relação a cada modelo. Na sequência, cada camada do modelo TCP/IP será abordada em detalhes.

3.3.1 Camada de Enlace

A camada de enlace descreve o que os enlaces como linhas seriais e a Ethernet clássica precisam fazer para cumprir os requisitos dessa camada de interconexão com o serviço não orientado a conexão. Ela não é uma camada propriamente dita, mas uma interface entre os hosts e os enlaces de transmissão. O material inicial sobre o modelo TCP/IP tem pouco a dizer sobre ela.

3.3.1.1 Quadros

Os quadros são formados por três estruturas básicas: cabeçalho, dados e o Código de Detecção de Erros (CDE). O cabeçalho possui informações de controle para que haja a comunicação horizontal entre as camadas de enlace da origem e do destino. O campo de dados encapsula a unidade de dados do protocolo PDU, que basicamente consiste na unidade da combinação dos dados e cabeçalho, e o passa para a camada de rede. O código de detecção de erros controla erros na camada física.

Um quadro pode ser formado por sequências de caracteres ou bits. Existem dois grandes grupos: os protocolos orientados a caracteres e os protocolos orientados a bit. O protocolo HDLC (*High-level Data Link Control*) consiste em um exemplo de protocolo orientado a bit e o protocolo BSC (*Binary Synchronous Control*) é um exemplo de protocolo orientado a caractere. Existem ainda protocolos híbridos entre essas duas categorias. Como por exemplo, o protocolo PPP (*Point-to-Point*) pode operar tanto com bits quanto com caracteres e consiste em um padrão internacional.

ATENÇÃO: essa propriedade ajuda na classificação dos protocolos que tratam os quadros da camada de enlace.

3.3.1.2 Enquadramento

O enquadramento consiste na capacidade do receptor de identificar o início e o final de cada bloco transmitido. A maioria dos protocolos usam uma *flag* para identificar os limites de cada quadro. Esta *flag* pode ser uma sequência de bits nos protocolos orientados a bit. Alguns protocolos podem usar a *flag* no início e no final do quadro para especificar claramente seus limites. Um problema ao utilizar a técnica de *flags* consiste na ocorrência da própria *flag* dentro do quadro.

SAIBA MAIS: este procedimento também pode ser referenciado como *framing*.

A técnica de byte *stuffing* e bit *stuffing* pode ser utilizada para contornar as limitações do uso de *flags*. A abordagem byte *stuffing* abrange os protocolos orientados a caracteres e emprega um caractere especial para identificar a ocorrência do delimitador dentro do quadro. Este tipo de abordagem ocorre, por exemplo, na escrita de documentos com o editor Latex, onde os comandos reservados da linguagem devem ser substituídos por um código reservado. A técnica bit *stuffing* é baseada no mesmo princípio, mas aborda os protocolos orientados a bits. Por exemplo, considerando seis 1s como uma *flag*. Utilizando a bit *stuffing*, sempre que aparecer uma sequência de cinco bits dentro de um quadro, um bit o é adicionado pelo transmissor para evitar o problema.

Um esquema alternativo para os protocolos orientados a caractere pode ser implementado considerando o tamanho do quadro. Nesse caso, o quadro possui no cabeçalho um campo que indica o número de bytes que compõem o restante do quadro. Usando este esquema, não existe a necessidade de um delimitador de término do quadro, apenas o delimitador de início.

3.3.1.3 Endereçamento

O endereçamento na camada de enlace está associado com a identificação da interface de comunicação que conecta o dispositivo à rede. Em nível de enlace, cada interface deve possuir um endereço único de identificação. O cumprimento desta necessidade é atendido diretamente pelo fabricante que descreve esta informação no hardware do dispositivo.

Estes endereços são empregados nos quadros utilizados nas redes locais Ethernet. Um quadro destas redes possui quatro campos principais, o endereço de destino, endereço de origem, tamanho, dados e CDE. O primeiro endereço identifica o receptor do quadro. O segundo endereço identifica o transmissor. O endereço da camada de enlace também é referenciado como endereço físico ou MAC (*Medium Access Control*).

SAIBA MAIS: cada endereço é formado por seis bytes, cada um representado em hexadecimais.

Existem três formas de endereçamento na camada de enlace: *unicast, multicast* e broadcast. No endereço *unicast*, a origem envia uma mensagem para apenas um destinatário. No endereçamento broadcast, a origem envia uma mensagem para todos os dispositivos da rede. No endereçamento *multicast*, a origem envia uma mensagem para um grupo de dispositivos. O endereçamento broadcast é utilizado quando o emissor não conhece o endereço do receptor. Em redes Ethernet, o endereçamento FF-FF-FF-FF-FF-FF

3.3.1.4 Detecção e Correção de Erros

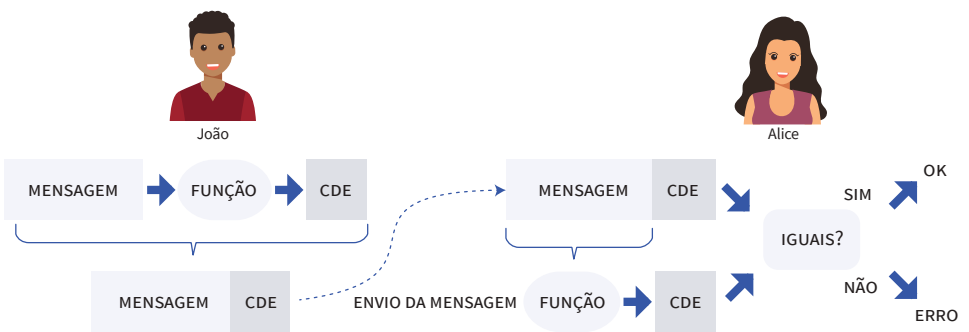
Qualquer transmissão está sujeita a problemas como ruídos e atenuações. Neste caso, a camada de enlace precisa tratar os possíveis erros. O controle de erros envolve duas etapas: a detecção e a correção. O mecanismo de detecção de erro é semelhante ao esquema de dígito verificador usado para garantir que nossa conta bancária esteja correta. O dígito verificador é gerado a partir dos números que compõem a conta corrente, utilizando uma função pré-definida.

ATENÇÃO: se o dígito verificador calculado for igual ao dígito da conta, a informação está correta, caso contrário existe um erro.

A detecção de erro é feita pelas informações de controle que são enviadas com os dados transmitidos. Antes de enviar uma mensagem, o transmissor usa uma função para gerar um CDE. O código é anexado ao final da mensagem. Em seguida o quadro é enviado. O destinatário ao receber a mensagem, recalcula o código de detecção de erro e o compara com o código recebido. Se ambos os códigos forem iguais, não houve erro. Caso contrário aconteceu um erro.

A Figura 75 ilustra uma situação de verificação do código de detecção de erro envolvendo a troca de mensagens entre João e Alice. Neste cenário, João assume o papel de emissor da mensagem e Alice atua como receptora da mensagem. Primeiramente, João possui uma mensagem que deseja repassar para Alice e para isso utiliza uma função geradora de CDE. Ao aplicar esta função, João obtém o CDE e o aglutina no final da mensagem, gerando o conjunto de dados que é enviado para Alice. Ao receber estes dados, Alice desempenha o caminho inverso, aplicando a mesma função geradora de CDE sob o campo correspondente a mensagem de João. Ao obter a resposta, Alice compara o CDE gerado por ela com o CDE recebido de João. Caso sejam iguais, a mensagem foi recebida sem erros. Caso contrário, existiu um erro de transmissão e Alice necessitará solicitar novamente a mensagem. Um ponto importante neste processo consiste no acordo prévio entre o emissor e receptor, neste caso João e Alice, sobre qual função geradora de CDE aplicar, pois uma função diferente comprometeria o funcionamento da abordagem.

FIGURA 75 – Verificação do Código de Detecção de Erro



FONTE: Autores

Existem duas técnicas principais para detecção de erros, o bit de paridade e a verificação de redundância cíclica. Existem duas formas de implementar a técnica de bit de paridade, a paridade simples e paridade múltipla. A técnica de paridade simples consiste em adicionar um bit ao final de cada caractere transmitido, de modo que, com esse bit, o total de bits 1 seja par (paridade par) ou ímpar (paridade ímpar). Esse tipo de mecanismo deve ser utilizado apenas em transmissões de baixa velocidade e que apresentem poucos erros.

ATENÇÃO: o problema desta técnica consiste na casualidade da alteração de dois bits ao mesmo tempo. Neste caso, o erro não será detectado.

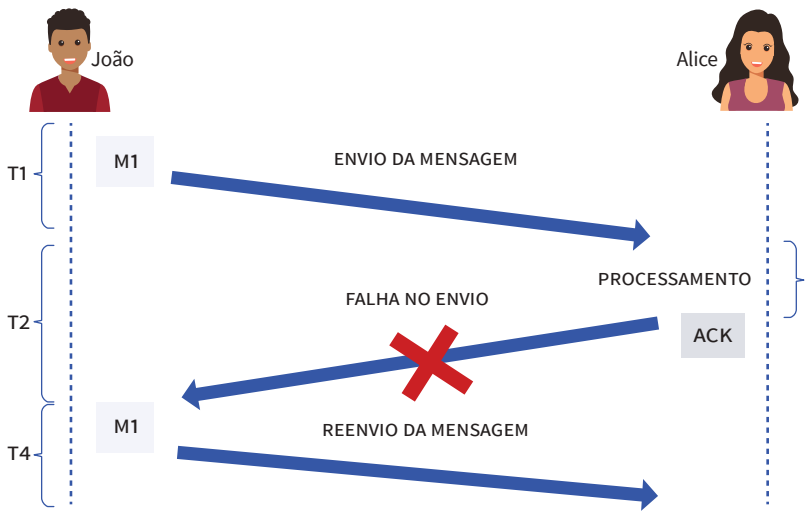
A técnica de paridade múltipla é uma melhoria da paridade simples. Na paridade múltipla, além do bit de paridade adicionado ao final de cada caractere, é adicionado outro bit para um bloco de caracteres transmitidos.

A técnica de verificação de redundância cíclica é baseada no princípio da operação de divisão. Os bits que representam os dados são divididos por um número predefinido. O resto da divisão é incorporado ao dado e transmitido. No destino, o dado recebido é dividido pelo mesmo número predefinido. Se o resto da divisão for zero, os dados enviados estão corretos; caso contrário, o dado sofreu alguma alteração.

A correção de erros pode ser implantada na camada de enlace, mas cabe salientar que nem sempre esta camada possui essa funcionalidade. Quando um quadro é transmitido corretamente, o receptor confirma o recebimento do pacote por meio de um ACK (*ACKnowledgement*). Por esse motivo, este esquema é conhecido como reconhecimento positivo. A Figura 76 ilustra o funcionamento do esquema ACK.

TERMO DO GLOSSÁRIO: o ACK consiste em tipo de quadro usado para que o transmissor reconheça que o destinatário recebeu corretamente um determinado quadro enviado.

FIGURA 76 – Exemplo de Funcionamento do Esquema ACK



FONTE: Autores

A Figura 76 ilustra o funcionamento do esquema ACK considerando uma situação onde João envia uma mensagem para Alice. Nesse caso, durante o instante de tempo T1, João envia o fragmento da mensagem M1 para Alice. Imediatamente depois, João inicia a contagem de um temporizador, cuja função consiste em esperar uma confirmação de recebimento de M1 por parte de Alice. No nosso exemplo, o fim da contagem deste temporizador é representado no intervalo de tempo T2. Em seguida, Alice recebe M1 e processa seu recebimento no instante de tempo T3. Como resultado, Alice envia um ACK para João confirmando o recebimento de M1. Todavia, surge uma situação inesperada durante a transmissão, ocasionando uma falha no envio do ACK responsável por confirmar o recebimento de M1. Na sequência, o temporizador utilizado por João expira, sinalizando o fim da espera de confirmação do recebimento do fragmento M1 por parte de Alice. Em virtude disto, João envia novamente M1 no instante de tempo T4. Supondo que não ocorram mais problemas durante a comunicação, Alice receberá novamente M1 de maneira duplicada. Nesse caso, a versão mais antiga do fragmento é descartada e Alice envia um novo ACK para João. Somente após o recebimento do ACK de M1 que João envia o próximo fragmento da mensagem.

Um ACK pode ser implementado de duas formas diferentes: como um quadro especial ou fazendo parte do cabeçalho de enlace. No primeiro caso, cada reconhecimento possui um cabeçalho, o ACK propriamente dito e o código de detecção de erro. No segundo caso, o reconhecimento é implementado por um ou mais bits de controle no próprio cabeçalho dos quadros de enlace. Seguindo a abordagem de reconhecimento positivo, podem acontecer dois problemas, o quadro não chegar ao destino, ou o quadro pode chegar ao destino com erro.

ATENÇÃO: se um quadro não chega ao destino, o receptor não tem nada a fazer a não ser aguardar que o transmissor resolva o problema. Nesse caso, o transmissor mantém um temporizador para cada quadro enviado, e se não chegar um ACK em certo intervalo de tempo, ocorre um timeout e o quadro é retransmitido.

A técnica de *piggybacking* possibilita a implementação do controle de ACK no cabeçalho de quadros. Nessa técnica, o reconhecimento é enviado junto com os dados, possibilitando a melhor utilização do canal de comunicação. Usando esta técnica, pode existir a situação onde o receptor não tenha dados para transmitir de volta ao transmissor. Nesse caso, o transmissor entenderia que o receptor não recebeu o quadro e retransmitiria o quadro, eliminando os benefícios da técnica de *piggybacking*. Para contornar esta situação, o receptor também deve implementar um temporizador para forçar um envio de um ACK, mesmo na ausência de dados.

Outra possibilidade de erro consiste na possibilidade de o quadro chegar ao destino, mas com erros. Existem duas estratégias possíveis para tratar essas situações, o reconhecimento negativo e a correção no destino. A técnica de reconhecimento negativo avisa o transmissor do problema enviando um NAK. Quando a origem receber o NAK, ela desativa o temporizador para evitar uma eventual retransmissão. Um possível problema do reconhecimento negativo pode ocorrer

quando os temporizadores não estão ajustados corretamente. Neste caso, o temporizador da origem expira antes do recebimento do NAK, impedindo os benefícios da técnica do reconhecimento negativo.

A técnica de correção no destino compreende o recebimento e análise de erros dos quadros. Se existir erros nos quadros, o próprio receptor corrige os erros. Para implementar a técnica de correção de erros no destino, o transmissor necessita enviar um número maior de informações de controle para possibilitar a correção dos quadros na origem. Esta técnica normalmente é aplicada em transmissões sem fio, onde existe uma alta taxa de erros e um custo alto de retransmissões.

ATENÇÃO: a vantagem desta técnica consiste em dispensar a retransmissão do quadro em caso de erros.

3.3.1.5 Protocolos de Repetição Automática de Requisição

Os protocolos de repetição automática de requisição utilizam o reconhecimento e a retransmissão de quadros como mecanismos para a correção de erros. Existem três implementações desses protocolos, o bit alternado, a retransmissão integral e a retransmissão seletiva.

No protocolo de bit alternado, o retransmissor aguarda o reconhecimento de cada quadro enviado antes de enviar o próximo. Existem dois problemas com esta abordagem, a duplicação de quadros e a subutilização do canal de comunicação. A duplicação de quadros ocorre com a falha do envio de um ACK. Neste caso, acontece a retransmissão do quadro correspondente ao ACK com problema e o receptor acaba obtendo duas cópias do mesmo quadro, tendo que descartar uma delas. Uma alternativa para corrigir esta limitação consiste em determinar que o receptor deve numerar os quadros recebidos, alternando entre o bit 0 e 1. Com base na numeração, o pacote recebido primeiro é mantido e o pacote mais novo é descartado.

A subutilização do canal de comunicação ocorre devido à necessidade de aguardar a confirmação de cada quadro. Esta limitação surge em enlaces com alta latência na entrega de pacotes. Nestes cenários, um quadro demora muito tempo para chegar ao receptor e neste período o enlace não pode ser utilizado para transmitir outros pacotes. Estas situações podem ocorrer em cenários onde o receptor e transmissor estão muito distantes.

O protocolo de retransmissão integral contorna o problema de subutilização do canal presente no protocolo de bit alternado. Por meio da retransmissão integral, vários quadros podem ser transmitidos sem a necessidade do reconhecimento individual dos quadros. Os protocolos que seguem esta abordagem implementam a técnica conhecida como janela deslizante. Na origem é utilizada uma janela de transmissão que permite controlar os quadros que podem ser transmitidos de forma a maximizar o uso do canal de comunicação. O protocolo de retransmissão integral utiliza uma janela de transmissão de tamanho variável, porém implementa uma janela de recepção de tamanho fixo e com apenas uma posição. Nesse caso,

cada quadro recebido é reconhecido individualmente, permitindo o reconhecimento do próximo quadro. Caso aconteça um erro com um quadro presente na janela de transmissão, todos os quadros não reconhecidos devem ser retransmitidos, gerando um custo adicional no enlace.

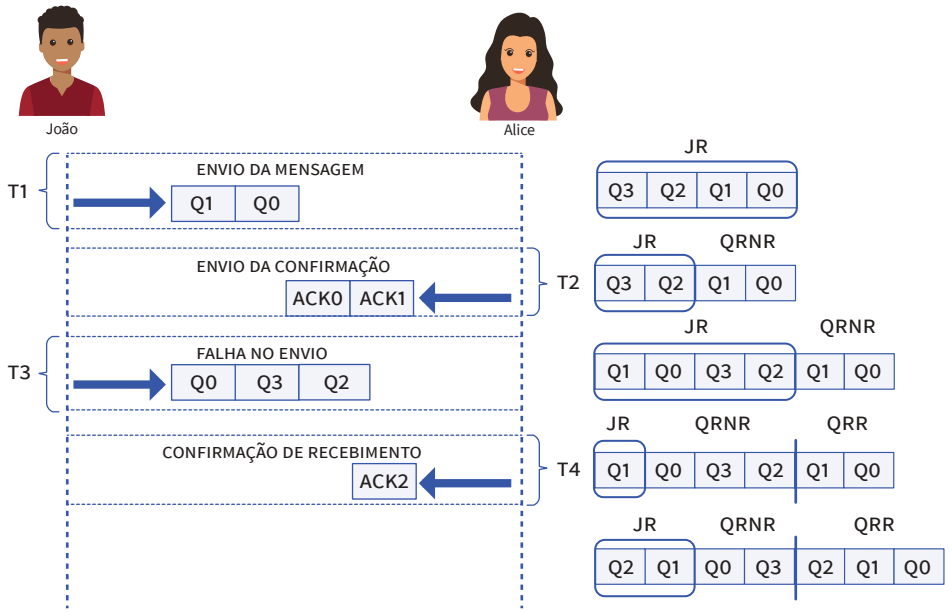
ATENÇÃO: esta técnica permite que as camadas de enlaces da origem e destino tenham mais flexibilidade para enviar e receber quadros.

O protocolo de retransmissão seletiva contorna o problema do protocolo de retransmissão integral. Através do protocolo de retransmissão seletiva, os quadros podem ser recebidos fora de ordem. Este protocolo utiliza uma Janela de Recepção (JR). A Figura 77 ilustra o funcionamento de uma janela de recepção envolvendo a troca de mensagens entre João e Alice.

TERMO DO GLOSSÁRIO: uma JR permite controlar os quadros que ainda podem ser recebidos, ou seja, esta janela define a capacidade máxima de quadros que a camada de enlace do destino pode gerenciar.

Na Figura 77, Alice atua como receptora da mensagem e João atua como emissor, onde percebemos que o tamanho da JR varia de acordo como os quadros são reconhecidos. Nessa situação, Alice possui uma JR que suporta no máximo quatro quadros enumerados de zero até três. Os quadros recebidos por ela podem estar em dois estados, Quadro Recebido e Reconhecido (QRR) ou Quadros Recebidos e Não Reconhecidos (QRNR). Inicialmente, no instante de tempo T1, a JR está vazia e pode receber até quatro quadros. Quando os quadros Q0 e Q1 são enviados por João e recebidos por Alice, a JR ocupa duas posições para representar seu recebimento, disponibilizando apenas duas posições vazias. Para sinalizar o recebimento dos quadros Q0 e Q1, Alice envia no instante de tempo T2 os ACK0 e ACK1 como forma de confirmação. Como consequência, no instante de tempo T3, mais duas posições na janela de recepção são abertas, proporcionando assim o recebimento de quatro quadros novamente. Nesse mesmo instante, os quadros Q0 e Q1 mudam seu estado de QRNR para QRR, indicando seu reconhecimento. Ainda no instante T3, João envia os quadros Q2, Q3 e Q0, ocasionando uma redução do tamanho de JR para apenas uma posição. No instante de tempo T4, Alice envia o ACK2, sinalizando o recebimento de Q2. Como resultado o status de Q2 se torna como QRR. Uma técnica utilizada para melhorar o funcionamento do protocolo de retransmissão seletiva consiste no reconhecimento cumulativo. Por meio desta técnica, apenas o reconhecimento do último quadro recebido corretamente é enviado.

FIGURA 77– Exemplo de Janela de Recepção



FONTE: Autores

Apesar da eficiência do protocolo de retransmissão seletiva, pode ocorrer um problema de sobreposição na janela de recepção, ocasionando duplicações de quadros. Por exemplo, considere que o receptor possui uma janela de recepção de quatro posições livres. O transmissor envia os quadros Q0, Q1 e Q2 que são recebidos e reconhecidos por um ACK, fazendo com que a janela de recepção deslize para aguardar os próximos quatro quadros. Por algum problema, o ACK enviado não chega ao destino e o quadro Q0 é retransmitido por timeout. Quando o quadro Q0 chega ao destino, o receptor não sabe que Q0 já foi recebido e reconhecido anteriormente. O receptor então considera que houve um problema com o quadro Q3 e armazena novamente Q0. Nesse caso, houve uma duplicação de quadros e o receptor não consegue identificar o problema. Para contornar esta dificuldade, a janela de recepção não pode ser maior que a metade do número de sequência utilizado para a numeração de quadros.

3.3.1.6 Controle de Fluxo

O controle de fluxo permite que o dispositivo transmissor regule o volume de dados enviados de forma a não gerar um overflow (transbordamento) no receptor. Caso uma situação como esta aconteça, o destino acaba tendo que descartar os dados transmitidos, obrigando a geração de novas retransmissões. Existem três estratégias clássicas de controle de fluxo, a pare e espere, envio de mensagens de aptidão e envio do tamanho da janela de recepção.

A forma mais simples de controle de fluxo é chamada de pare e espere (*stop-and-wait*). Nesta estratégia, o transmissor aguarda pela confirmação do recebimento do quadro para enviar o próximo. Dessa forma, o transmissor e receptor estão de certa forma sincronizados, eliminando o problema de overflow. No en-

tanto, assim como o protocolo de bit alternado, essa estratégia também apresenta o problema da subutilização do canal.

Na estratégia de envio de mensagens de aptidão, o receptor envia mensagens para o transmissor informando se está apto ou não para receber novos quadros. Usando essa abordagem, o transmissor pode regular o volume de dados enviados de forma a não sobrecarregar o destinatário. Os protocolos que utilizam a técnica de janela deslizante podem facilmente implementar a função de controle de fluxo apenas ajustando o tamanho da janela de transmissão.

A estratégia de envio do tamanho da janela de recepção faz com que o receptor informe o tamanho da sua janela de recepção a cada reconhecimento. Se em algum momento a janela de recepção ficar vazia, ou seja, não existirem mais espaço para novos quadros, o receptor informa ao transmissor uma janela de recepção de tamanho zero. Nesse caso, o transmissor não poderá transmitir novos quadros, voltando a fazê-lo apenas quando receber uma janela de recepção maior que zero. Esse mecanismo é implementado no protocolo TCP do modelo Internet.

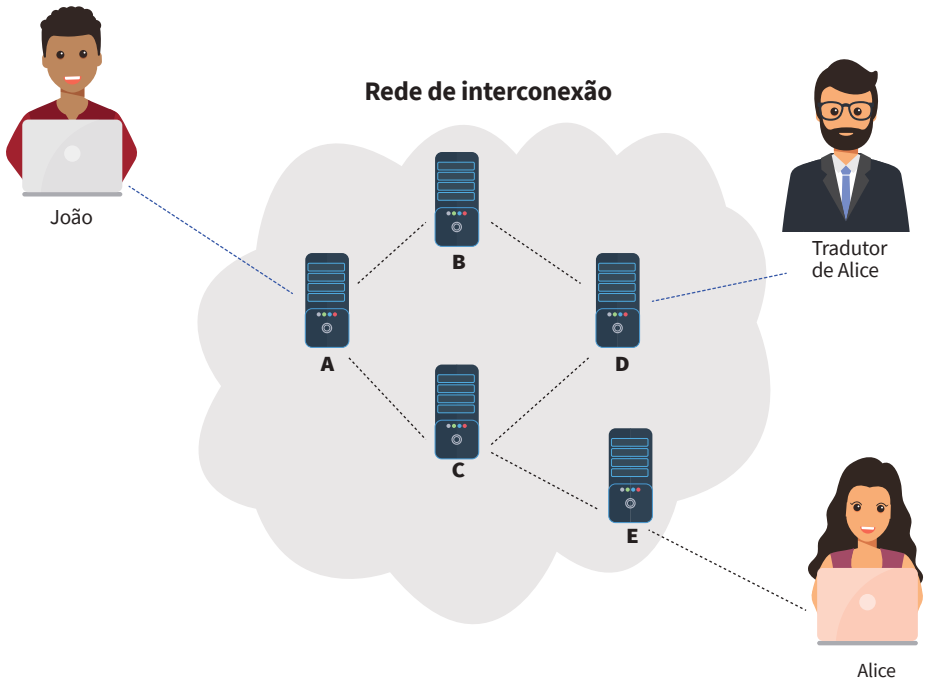
3.3.2 A Camada Internet (camada de rede)

A camada Internet integra toda a arquitetura, mantendo-a unida. Esa tarefa consiste em permitir que os hosts injetem pacotes em qualquer rede e garantir que eles trafegarão independentemente até o destino, assim como no modelo OSI. Todavia, o modelo TCP/IP expressamente determina que a ordem dos pacotes recebidos pode ser diferente daquela em que foram enviados, podendo percorrer inclusive redes diferentes.

Para entender a aplicabilidade da camada de rede, primeiramente precisamos compreender o conceito de rede de interconexão. A Figura 78 ilustra uma rede de interconexão envolvendo João, Alice e o tradutor de Alice.

TERMO DO GLOSSÁRIO: uma rede de interconexão compreende o conjunto de dispositivos para conectar dois nós da rede de computadores que podem trocar mensagens somente por meio do encaminhamento de mensagens através de nós intermediários.

FIGURA 78 – Rede de Interconexão



Fonte: Autores

No exemplo da Figura 78, existem diferentes caminhos na rede de interconexão que uma mensagem enviada de João para Alice pode percorrer. Por exemplo, a mensagem poderia partir do laptop de João, passar pelo servidor A, em seguida pelo servidor C, logo após pelo servidor E, e finalmente chegar até o laptop de Alice. Outro caminho possível envolve os seguintes nós da rede, laptop de João, servidor A, servidor B, servidor D, servidor C, servidor E, laptop de Alice. O processo de encaminhamento das mensagens na rede intermediária consiste no roteamento de mensagens. Esse conceito se assemelha ao roteamento logístico da entrega de produtos para consumidores de um conjunto de cidades e envolve o problema de determinar a melhor rota entre dois pontos. Desempenhar a função de roteamento de pacotes em uma rede de interconexão compreende uma das principais funções da camada de rede no modelo TCP/IP.

Outro diferencial desta camada em relação ao modelo OSI consiste no emprego do protocolo IP (*Internet Protocol*). Outro pacote desta camada consiste no ICMP (*Internet Control Message Protocol*). Por meio do ICMP, um roteador ou host destino pode reportar à estação origem uma condição de erro no processamento de um datagrama. O ICMP apenas informa erros ao nível IP de origem, não abordando a correção dos mesmos.

ATENÇÃO: o protocolo IP é responsável por endereçar e encaminhar os pacotes.

3.3.3 A Camada de Transporte

A camada de transporte permite que as entidades pares dos hosts de origem e destino mantenham uma conversação, exatamente como ocorre no modelo OSI. Dois protocolos de comunicação ponta a ponta são definidos, o TCP e o UDP (*User Datagram Protocol*). O TCP também implementa o controle de fluxo, impedindo que um transmissor rápido sobrecarregue um receptor lento com um volume de mensagens maior do que ele pode manipular. O protocolo UDP consiste em um protocolo sem conexões, não confiável, sendo utilizado em aplicações que não desejam o controle de fluxo do TCP. O UDP é muito usado para consultas isoladas, com solicitação e resposta, tipo cliente-servidor e em aplicações que a entrega imediata é mais importante do que a entrega precisa, tal como na transmissão de voz ou vídeo.

TERMO DO GLOSSÁRIO: o protocolo TCP consiste em um protocolo orientado a conexões confiável que permite a entrega sem erros de um fluxo de bytes originário de uma determinada máquina em qualquer computador da Internet.

ATENÇÃO: este protocolo é escolhido quando a aplicação implementa o controle de fluxo.

3.3.4 A Camada de Aplicação

O modelo TCP/IP não possui as camadas de sessão ou de apresentação, pois os criadores não identificaram qualquer necessidade para elas. Ao invés disso, as aplicações simplesmente incluem quaisquer funções de sessão e apresentação que forem necessárias. A camada de aplicação no modelo TCP/IP contém todos os protocolos de nível mais alto. Alguns exemplos de protocolos dessa camada são o FTP (*File Transfer Protocol*), o DNS (*Domain Name System*), o SMTP (*Simple Mail Transfer Protocol*) e o HTTP. Os protocolos pertencentes a esta camada serão estudados em detalhes na próxima unidade.

SAIBA MAIS: o protocolo FTP é utilizado para transferência de arquivos. O protocolo DNS mapeia nomes de fácil entendimento humano para um endereço IP. O protocolo SMTP é usado para correio eletrônico. O protocolo HTTP consiste no protocolo empregado na Web.

3.4
COMPARANDO OS MODELOS OSI E TCP/IP

Os modelos de referência OSI e TCP/IP possuem pontos em comum. Ambos se baseiam no conceito de uma pilha de protocolos independentes. Além disso, as camadas possuem praticamente as mesmas funcionalidades. Por exemplo, em ambos os modelos a camada de transporte oferece um serviço de transporte fim a fim. Apesar dessas semelhanças, os dois modelos também possuem diferenças. Essa seção foca principalmente nas diferenças entre os modelos. A diferença é óbvia consiste no número de camadas. O modelo OSI possui sete camadas e o modelo TCP/IP possui quatro.

Uma das principais diferenças entre os modelos consiste nos conceitos empregados. O modelo OSI se baseia em três conceitos fundamentais, serviços, interfaces e protocolos. A definição de serviço informa o que a camada faz e não a forma como as entidades acima dela a acessam ou como a camada funciona. A interface de uma camada informa como os processos acima dela podem acessá-la e especifica os parâmetros/resultados esperados sem revelar o funcionamento interno da camada. Os protocolos de uma camada são de responsabilidade somente desta camada. A distinção entre estes conceitos consiste em uma das maiores contribuições do modelo OSI.

O modelo TCP/IP original não distingue com clareza a diferença entre serviços, interface e protocolo. Por exemplo, os únicos serviços reais oferecidos pela camada de rede Internet são o de envio de pacote IP (*send ip packet*) e o recebimento de pacotes IP (*receive ip packet*). Em contrapartida, os protocolos no modelo OSI são mais encapsulados do que os do modelo TCP/IP e podem ser alterados com relativa facilidade.

O modelo de referência OSI foi concebido antes de os protocolos correspondentes terem sido criados. Isso significa que o modelo não sofreu influência de um determinado conjunto de protocolos, tornando-o bastante genérico. A desvantagem desta questão foi que os projetistas não tinham muita experiência no assunto e nem muita noção sobre a funcionalidade que deveria ser incluída em cada camada.

Com o TCP/IP ocorreu o contrário, como os protocolos vieram primeiro, o modelo foi realmente criado com uma descrição dos protocolos existentes. Não houve problemas para os protocolos serem adaptados ao modelo. Eles se encaixaram perfeitamente. O único problema foi o fato do modelo não se adaptar a outras pilhas de protocolos. Consequentemente, o TCP/IP não tinha muita utilidade para descrever outras redes que não faziam uso do protocolo TCP/IP.

ATENÇÃO: essa comparação se baseia no modelo de referência e não na pilha de protocolos correspondentes.

Outra diferença está na área da comunicação não orientada a conexões versus comunicação orientada a conexões. A camada de rede do modelo OSI suporta a comunicação não orientada a conexão e a comunicação orientada a conexão. Além disso, a camada de transporte do modelo OSI aceita apenas a comunicação orientada a conexões. Em contrapartida, a camada de rede do modelo TCP/IP suporta apenas a comunicação não orientada a conexões e aceita ambos os modos na camada de transporte.

3.5 CRÍTICAS AO MODELO OSI

Os modelos de referência OSI e TCP/IP não são perfeitos. Quando o modelo OSI estava sendo planejado, muitos especialistas tinham a impressão que este seria o padrão absoluto de mercado. As principais razões que impediram esta consolidação são: momento ruim, tecnologia ruim, implementações ruins e política ruim.

O momento de desenvolvimento de um modelo de referência consiste em uma decisão decisiva para seu sucesso. Se ele for desenvolvido muito cedo, antes da pesquisa ser concluída, o assunto poderá não estar devidamente compreendido, resultando em um padrão ruim. Se ele for desenvolvido muito tarde, muitas empresas já podem ter investido muitos recursos para descobrir maneiras diferentes de tirar proveito da nova tecnologia e ignorarão o padrão proposto. Se o intervalo para desenvolvimento for muito curto, a equipe de desenvolvimento de padrões não ter condições de terminar a tempo. Hoje se sabe que os protocolos do padrão OSI foram esmagados, pois os protocolos do TPC/IP já estavam sendo utilizados nas universidades de pesquisa na época em que apareceram os protocolos OSI. Nesse momento, as empresas ficaram esperando para ver qual delas daria o primeiro passo para adotar o novo padrão. Como nenhuma delas se manifestou, o OSI nunca foi adotado.

ATENÇÃO: quando surgiram os protocolos OSI, muitas empresas já haviam investido no modelo TCP/IP.

O segundo motivo consistiu na tecnologia ruim. A escolha das sete camadas do modelo foi mais política do que técnica. Do ponto de vista técnico, as camadas de sessão e de apresentação estão praticamente vazias, enquanto que as camadas de enlace de dados e de rede se encontram sobrecarregadas. Além disso, as funções de endereçamento e controle de fluxos/erros se repetem nas camadas.

As implementações iniciais do modelo OSI eram lentas, pesadas e gigantes devida alta complexidade do modelo. Com o passar do tempo acabaram sendo rotuladas como sendo de baixa qualidade. Em contrapartida, uma das primeiras implementações do TCP/IP era muito boa. Além disso, esta implementação fazia parte do UNIX de Berkeley. Estes fatos impulsionaram a comunidade a adotar as implementações do modelo TCP/IP.

A última razão consiste na política ruim. Devido à incorporação da implementação do TCP/IP no UNIX, muitas pessoas, em particular o universo acadêmico, pensaram que o TCP/IP era parte deste sistema operacional. Um agravante neste caso foi que as universidades possuíam verdadeira adoração pelo UNIX. Por outro lado, o OSI era considerado uma criação dos ministérios de telecomunicações europeus.

ATENÇÃO: de forma simplificada, a visão da época era que alguns burocratas estavam tentando impor um padrão tecnologicamente inferior aos pesquisadores e programadores que de fato trabalhavam no desenvolvimento de redes de computadores.

3.6
CRÍTICA AO MODELO TCP/IP

Os protocolos e o modelo TCP/IP também tiveram os seus problemas. Primeiramente, o modelo não diferencia com clareza necessária os conceitos de serviço, interface e protocolo. Consequentemente, o modelo TCP/IP não é o melhor guia para criação de novas redes para novas tecnologias. Em segundo lugar, o modelo não é nada abrangente e não consegue descrever outras pilhas de protocolos senão a pilha TCP/IP. Terceiro, a camada host/rede não é realmente uma camada no sentido em que o termo é usado no contexto dos protocolos hierárquicos, tratando-se na verdade de uma interface entre as camadas de rede e de enlace de dados.

Em quarto lugar, o modelo TCP/IP não faz distinção entre as camadas física e de enlace de dados. A camada física está relacionada com as características de transmissão pelo meio físico. A camada de enlace de dados delimita o início e fim dos quadros e os envia de um lado ao outro garantindo a confiabilidade. Um modelo mais adequado deve incluir as duas camadas como elementos distintos.

Além disso, apesar dos protocolos IP e TCP terem sido cuidadosamente projetados e bem implementados, o mesmo não aconteceu com muitos outros protocolos. Alguns protocolos foram produzidos por alunos sem experiência necessária e eram distribuídos gratuitamente. Como consequência, esses protocolos eram largamente difundidos de forma que era difícil substituí-los. Por exemplo, o protocolo virtual TELNET foi projetado para um terminal mecânico, capaz de processar dez caracteres por segundo, sendo incapaz de reconhecer o mouse e interfaces gráficas. No entanto, esse protocolo ainda é usado em larga escala atualmente, mais de trinta anos depois do seu surgimento.

ATIVIDADES DE REFLEXÃO OU FIXAÇÃO

1. Explique como o emprego de camada de rede pode contribuir para o projeto de uma arquitetura de redes de computadores.

2. Compare a perspectiva horizontal e vertical na análise do modelo em camadas.

3. Explique como o conceito de interface atua no modelo de comunicação de camadas.

4. Quais as camadas que compõem o modelo de referência OSI (*Open Systems Interconnection*)?

5. Qual a diferença entre os sinais analógicos e digitais? Qual deles é empregado na representação de informações na camada física?

6. Compare os esquemas de codificação digital NRZ-L e NRZI.

7. Quais as camadas do modelo de referência TCP/IP?

8. Explique em que consiste uma rede de interconexão.

9. Realize uma breve comparação entre o modelo OSI e TCP/IP.

10. Descreva brevemente duas críticas aos modelos OSI e TCP/IP, respectivamente.

4

INTERNET E WEB

INTRODUÇÃO

Esta seção irá abordar em sua essência os conceitos de Internet e Web, que apesar de estarem em um mesmo propósito, constituem funções diferentes. A internet hoje é provavelmente o maior sistema de engenharia já criado pela humanidade, com inúmeros computadores conectados, links de comunicação, milhares de usuários que se conectam através de diferentes dispositivos. Entender este contexto é vital para entender as redes de computadores e suas diferentes formas de concepção.

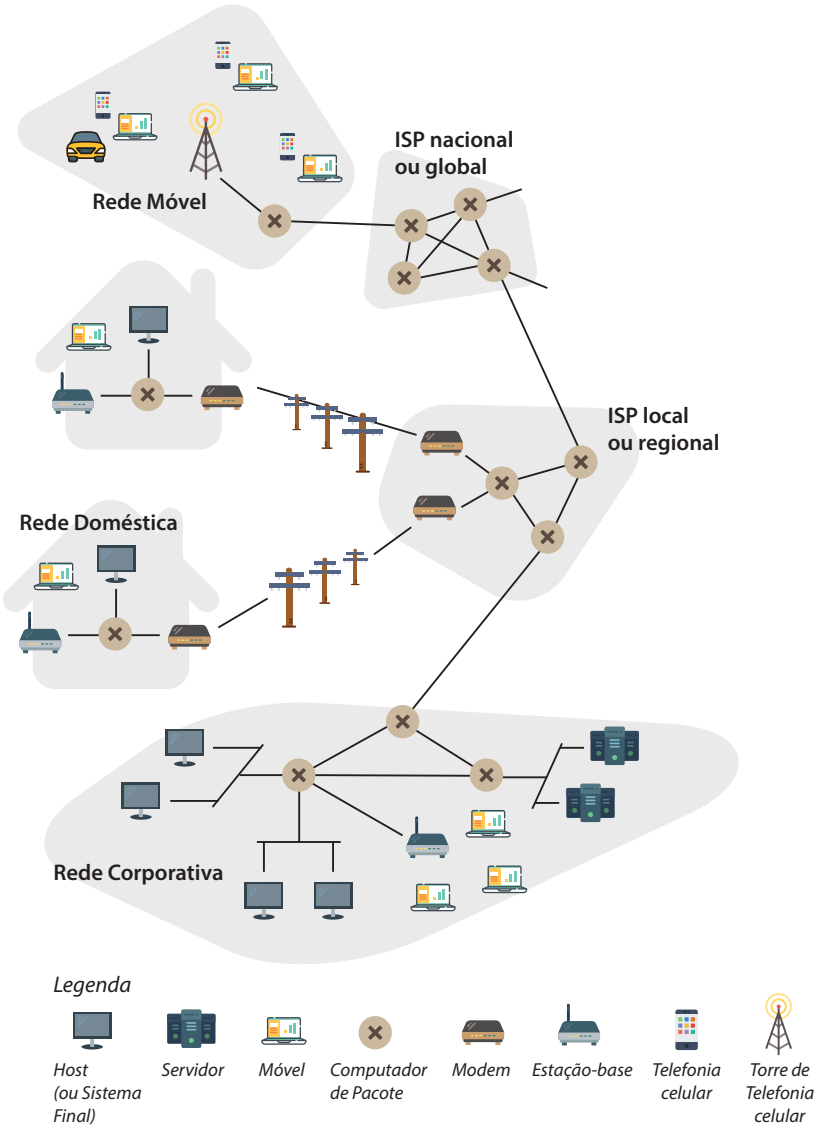
Desta forma, a primeira seção descreve sobre as características que compõe a grande rede chamada "Internet" e como a "Web" e outros serviços essenciais para nosso dia a dia digital estão inseridos neste meio. Ainda, nesta seção inicial são descritos em detalhes como se dá a comunicação cliente/servidor, desde a origem de um acesso a um site por parte do usuário e a resposta pelo servidor que hospeda a respectiva página requerida.

Na seção 4.2, os principais serviços de internet são apresentados, explicados e exemplificados, com ênfase para os protocolos: HTTP (utilizado quando acessamos uma página na internet, através de um navegador), SMTP (protocolo utilizado para envio de e-mails), POP3 (protocolo utilizado para receber e-mails), FTP (protocolo utilizado para transferência de arquivos, bastante semelhante ao protocolo HTTP, mas com suas devidas funções), DNS (resolução de nomes de domínio em endereços IP), DHCP (protocolo responsável por entregar endereços IP automaticamente aos computadores conectados à uma rede), SNMP (protocolo para gerenciamento de rede) e SSH (protocolo para acesso remoto a computadores).

4.1
O CONCEITO DE INTERNET E WEB

Apesar de muitos usuários entenderem Internet e Web como sendo a mesma coisa, existem diferenças entre o funcionamento e objetivo de cada um, então vamos à explicação. Para isso, temos que conceituar e entender o que vem a ser a Internet. Existem diferentes formas de responder a este questionamento. Primeiramente, é possível descrever de forma detalhada os aspectos principais da Internet, ou seja, os componentes de hardware e software que a compõem. Segundo, é possível descrever a Internet na forma da infraestrutura de rede que fornece serviços para aplicações distribuídas. Na figura 79, é possível visualizar alguns componentes da Internet.

FIGURA 79 – Principais componentes da Internet em uma visão geral



FONTE: Adaptado de Kurose (2010).

Uma descrição dos componentes da rede

A Internet pode ser caracterizada como uma rede de computadores que conecta milhares de dispositivos computacionais ao redor do mundo. Há pouco tempo, esses dispositivos eram basicamente computadores desktop, estações Linux, e os servidores responsáveis por armazenar e transmitir informações, como páginas web e mensagens de e-mail. Entretanto, cada vez mais dispositivos finais estão sendo conectados à rede, tais como: Smart TVs, laptops, smartphones, consoles para jogos, webcams, automóveis, dispositivos de sensoramento, sistemas elétricos e de segurança, entre outros. Ao analisar o contexto acima citado, o termo "redes de computadores" soa como desatualizado, ao considerar os diversos equipamentos não tradicionais que estão sendo ligados à Internet. A estes equipamentos dá-se o nome de hospedeiros ou sistemas finais.

Sistemas finais, por sua vez, são conectados entre si por enlaces de comunicação (links) e comutadores de pacotes. Existem diferentes tipos de enlaces de comunicação, que são formados de diferentes tipos de meios físicos, entre os quais destacam-se: as fibras óticas, os fios de cobre, os cabos coaxiais (em tipos específicos de conexão) e as ondas de rádio (comunicação *wireless*). É importante salientar aqui que enlaces diferentes (quanto ao meio físico) podem transmitir dados em taxas diferentes, sendo a taxa de transmissão de um enlace medida em bits por segundo.

A partir do momento em que um sistema final possui dados para envio a outro sistema final, o emissor segmenta estes dados e faz a adição de bytes de cabeçalho a cada segmento. Os pacotes de informações gerados, também denominados de pacotes no contexto das redes de computadores, são então enviados através da rede ao sistema final de destino, onde são reagrupados aos dados originais.

Cabe a um comutador de pacotes a tarefa de encaminhar os pacotes que estão chegando em um dos seus enlaces de comunicação de entrada para um enlace de comunicação de saída. Existem comutadores de pacotes de diferentes tipos e formas, mas os dois mais utilizados na Internet hoje são os roteadores e os *switches*. Tanto um quanto o outro encaminham pacotes aos seus destinos finais. Os *switches* são utilizados com frequência em redes de acesso, enquanto que os roteadores são mais frequentemente utilizados principalmente no núcleo da rede. Desta forma, a sequência de enlaces de comunicação e comutadores que um pacote percorre desde o sistema final de origem até o sistema final de destino é denominada de rota ou caminho através da rede.

Redes que transportam pacotes são em sua maioria semelhantes às redes de transporte de rodovias, ruas, estradas e cruzamentos que transportam veículos. Tomamos como exemplo uma indústria que necessita transportar uma grande quantidade de carga a algum depósito localizado a quilômetros de distância. Na origem (indústria), a carga é segmentada (dividida) e carregada em uma frota de caminhões. Cada caminhão trafega por seu caminho, passando por diferentes rodovias, estradas e cruzamentos, até chegar ao depósito de destino. Chegando ao depósito, cada carga é descarregada e agrupada com o restante das cargas pertencentes à mesma remessa. Seguindo a mesma analogia apresentada, os pacotes de rede se assemelham aos caminhões, os enlaces de comunicação são semelhantes

às rodovias e estradas, os comutadores de pacote são os cruzamentos e cada sistema final se assemelha aos prédios. Desta forma, assim como um pacote utiliza uma rede de computadores para chegar ao sistema final, um caminhão precisa de uma rede de transporte para fazer seu percurso e vice-versa.

Os sistemas finais conectam-se à Internet através de ISPs (*Internet Service Providers* – Provedores de Serviços de Internet), entre eles estão os ISPs residenciais (empresas de telefonia e TV a cabo); ISPs corporativos, de universidades, de locais públicos, entre outros tipos. Cada ISP corresponde a uma rede de comutadores de pacotes e de enlaces de comunicação. Os ISPs podem prover aos sistemas finais diferentes formas de acesso à rede, que pode ser através do acesso residencial de banda larga (modem e DSL), acesso via LAN de alta velocidade e acesso sem fio. ISPs podem fornecer também acesso a provedores de conteúdo, conectando sites web à Internet.

Assim, para que esta grande rede funcione de forma adequada, tanto aos sistemas finais, os comutadores de pacotes e outros dispositivos que compõe a Internet executam protocolos que controlam o envio e recebimento de informações. Aí entra em ação os protocolos TCP e IP estudados em capítulos anteriores, que correspondem aos dois protocolos mais importantes da Internet. Os protocolos, por sua vez, são definidos através de padrões da Internet, também denominados de RFCs. As RFCs (documentos técnicos padronizados) tiveram sua origem com o intuito de resolver problemas de arquitetura quanto ao funcionamento da Internet. Os RFCs geralmente constituem documentos bastante técnicos e detalhados e definem protocolos como o TCP, IP, HTTP, SMTP, entre diversos outros, que serão abordados na seção relativa aos principais serviços da internet.

Uma descrição de serviço de rede

Conforme descrito no início desta seção, é possível visualizar a internet através dos componentes que a compõe ou da infraestrutura que provê serviços a aplicações. Partindo da segunda premissa, tais aplicações podem ser e-mail, navegação a Web, mensagens instantâneas, VoIP, vídeo em tempo real, jogos em rede, compartilhamento de arquivos P2P, acesso remoto, entre outros tantos que aqui poderíamos citar. Essas aplicações são denominadas de aplicações distribuídas, uma vez que envolvem diferentes sistemas finais, que trocam informações entre si. As aplicações da Internet são executadas (em sua grande maioria) em sistemas finais e não em comutadores de pacote, pertencentes ao núcleo da rede.

Para que seja possível que um sistema final se comunique com outro sistema final e estes troquem informações na Internet (consideramos, neste exemplo, uma aplicação se comunicando com outra utilizando a Internet como infraestrutura) faz-se necessária a utilização de uma API (Interface de Programação de Aplicação) que é responsável por especificar como o componente de software que é executado no sistema final solicita à infraestrutura da Internet que envie dados a um componente de software de destino específico, executado em outro sistema final. Neste caso, a API da Internet corresponde a um conjunto de regras que a aplicação emissora deve cumprir para que a Internet seja capaz de enviar dados ao sistema final de destino.

Cada vez mais, dado o avanço na tecnologia dos componentes que compõe a Internet, estes são orientados pelas necessidades de novas aplicações. Desta forma, entendemos que a Internet é uma infraestrutura que permite que novas aplicações possam ser inventadas e disponibilizadas na grande rede, para que sistemas finais possam dela se utilizar em sua totalidade.

Criando uma descrição de Internet e Web

Analisando o contexto acima apresentado e respaldado pelos conhecimentos das seções anteriores, podemos conceituar de uma forma objetiva a **Internet** como **uma rede global que interconecta computadores**, ou de forma mais específica, **uma rede que conecta outras redes de computadores, utilizando uma série de regras de comunicação para trocarem informações entre si**. A infraestrutura presente na internet é composta por bilhões de dispositivos como: servidores, roteadores, computadores, *smartphones*, *tablets*, entre outros, interligados por diferentes estruturas de comunicação como satélites, cabos ópticos, etc.

Dentro desta infraestrutura temos vários serviços que funcionam como telefonia (VoIP), correio eletrônico (e-mail), transferência de arquivos (FTP), resolução de nomes de domínio (DNS), entre outros tantos que aqui poderiam ser citados, além claro da *World Wide Web* (www).

ATENÇÃO: você conheceu os principais serviços que operam na internet, na seção 1.3.

A *World Wide Web*, por sua vez, pode ser caracterizada como uma aplicação onde documentos e/ou páginas web são interligados através de links e que se utiliza da infraestrutura da internet para funcionar. Utilizamos o navegador web, também denominado de *browser*, e através das URLs acessamos estas páginas web e, ao clicar em um link, este processo todo é repetido para uma nova página que será aberta.

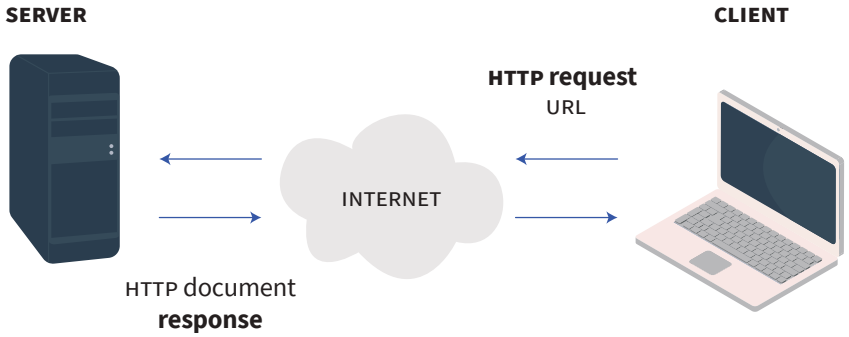
É através dos navegadores que podemos acessar sites e aplicações web, tais como: *Google, Youtube, Twitter, Gmail, Facebook, Netflix, Wikipedia, Spotify, Dropbox,* entre outros tantos exemplos de aplicações que temos atualmente e outras que surgem a cada dia.

Sendo assim, resumidamente podemos dizer que a Internet corresponde a uma rede global de computadores que permite a interconexão entre os dispositivos conectados a ela, bem como a transferência de dados entre eles. Já a *World Wide Web* pode ser definida como uma aplicação onde páginas são interligadas através de links e que se utiliza da Internet para poder funcionar. Vamos agora entender como se dá essa comunicação entre a Web e a Internet.

4.1.1 Clientes e Servidores

Computadores de um modo geral, que estão conectados à Web, recebem o nome de **clientes** ou **servidores**. Estes, por sua vez, se comunicam através de requisições e respostas, conforme pode ser visualizado na figura 80.

FIGURA 80 – Modelo de comunicação cliente x servidor

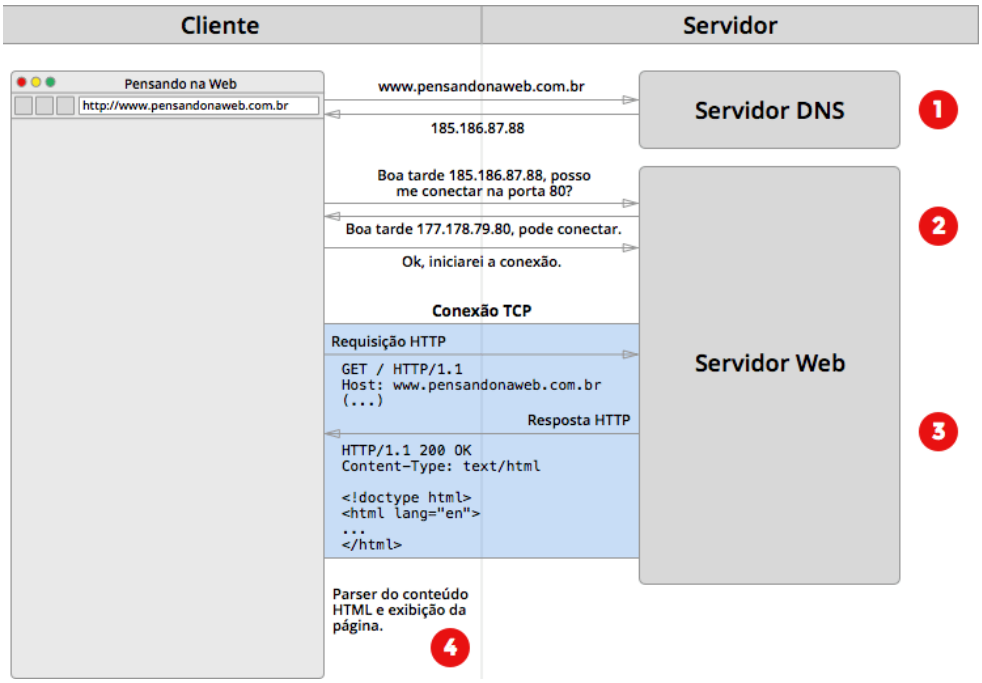


FONTE: NTE/UFSM

Os clientes são os usuários da web, conectados à internet (como, por exemplo, seu computador conectado à sua rede Wi-Fi em casa ou no trabalho, ou então seu *smartphone* conectado à rede de dados móveis) e softwares de acesso à Web instalados nesses aparelhos, exemplo dos navegadores Google Chrome, Safari, Mozilla, etc. Já os servidores são computadores que armazenam páginas ou aplicativos. Desta forma, quando o computador de um cliente quer acessar uma URL (página na internet), uma cópia desta é baixada do servidor à máquina do cliente para ser mostrada no *browser*.

O HTTP tem um papel fundamental nesta comunicação, pois ele é o protocolo utilizado pelos navegadores e servidores web se comunicarem. Assim, quando o navegador solicita uma página web, este procedimento é chamado de requisição e quando o servidor web envia a página solicitada de volta é chamado de resposta. Esta abordagem é conhecida como arquitetura cliente-servidor. A figura 81 mostra um exemplo de requisição e resposta, bem como a troca de mensagens entre cliente e servidor, até que a página seja exibida no navegador do usuário.

FIGURA 81 – Comunicação cliente/servidor em uma requisição HTTP



FONTE: Pensando na Web. Disponível em: https://pensandonaweb.com.br/content/images/2014/Jul/client-server-approach.png

Na figura 81, podemos observar o seguinte cenário:

1 e 2 – Inicia-se a requisição a uma página web através da inserção do domínio (URL a ser acessada) por parte do usuário (na figura denominado de "cliente"). O servidor responsável por este domínio, envia uma resposta por meio do protocolo HTTP, informando o endereço IP correspondente. A segunda parte nesta troca de informações refere-se ao cliente solicitar acesso à porta 80 junto ao servidor. O servidor em seguida responde "OK" à solicitação do cliente, que aí então inicia a conexão.

3 – Uma vez estabelecida a conexão entre cliente e servidor (usuário que acessa uma página e computador/servidor que responde a esta solicitação) as mensagens de origem e destino (produzidas pelo navegador e servidor) são quebradas em pacotes menores e transmitidas através da rede utilizando o protocolo TCP nesta comunicação (e, respectivamente, suas regras e confirmações de ambos os lados).

4 – Por fim, o conteúdo da página web é gerado e exibido ao usuário final.

O entendimento do funcionamento da internet e da web é fundamental para os assuntos das seções subsequentes. A ideia de protocolos de comunicação, dispositivos de rede, bem como demais componentes que servem de suporte às redes de computadores, é fundamental para o entendimento das redes de computadores, sua comunicação, transmissão e funcionamento em geral. Conheceremos na seção a seguir os principais protocolos da internet, que servem de base para uma série de aplicativos e funcionalidades que utilizamos em nosso dia-a-dia.

4.2
PRINCIPAIS SERVIÇOS DE INTERNET

Os protocolos da camada de aplicação determinam para qual tipo de serviço a rede será utilizada, seja e-mail, navegação, troca de arquivos, entre outros. Em outras palavras os protocolos da camada de aplicação fazem a conexão entre as redes e os aplicativos instalados em um computador. Conheceremos agora os principais serviços da camada de aplicação e consequentemente os respectivos protocolos que dão suporte a estes serviços.

4.2.1 HTTP

O HTTP (*HiperText Transfer Protocol*) ou Protocolo de Transferência de Hipertexto, corresponde a um protocolo da camada de aplicação (considerando o conceito de camadas do modelo OSI) e é definido em detalhes pelas RFCs 1945 e 2616. O protocolo HTTP é implementado através de dois programas: cliente e servidor. Estes, executados em sistemas finais diferentes, conversam entre si por meio da troca de mensagens HTTP. O HTTP define a forma destas mensagens e o modo de troca entre cliente e servidor.

Uma página ou documento Web, é formada por objetos. Um objeto corresponde a um arquivo, assim como um arquivo HTML, JPEG, um *applet* em Java, enfim, que se possa acessar através de uma URL única. A maior parte das páginas Web são formadas por um arquivo base HTML e diversos objetos referenciados. Os navegadores Web implementam também o lado cliente do HTTP. Já os servidores Web implementam o lado servidor deste protocolo, hospedando as páginas Web, endereçadas respectivamente por uma URL. São exemplos de servidores Web populares o Linux Apache, o Microsoft IIS e o multiplataforma Nginx.

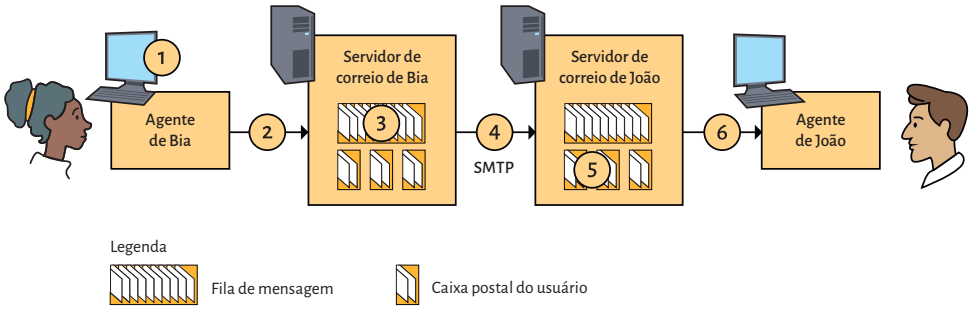
Basicamente, o HTTP define como clientes Web requisitam páginas Web aos servidores e como elas as transferem a clientes. Quando um usuário solicita uma página Web (acessa uma URL), o navegador envia ao servidor mensagens de requisição HTTP para os objetos da página. O servidor, por sua vez, recebe estas requisições e responde com mensagens de resposta HTTP que contém os objetos, conforme detalhado na seção anterior. O protocolo HTTP utiliza por padrão a porta 80 para comunicação.

4.2.2 SMTP

Definido através da RFC 5321, o SMTP (*Simple Mail Transfer Protocol*) é o protocolo responsável por transferir mensagens de servidores de correio remetente para servidores de correio destinatários. Por padrão o SMTP utiliza a porta 25 para comunicação, entretanto a porta pode ser modificada junto à configuração do respectivo servidor. Como forma de elucidar o funcionamento básico do protocolo STMP no

envio de um e-mail, utilizaremos a demonstração a seguir, conforme figura 82.

FIGURA 82 – Etapas no envio de e-mail de Alice para Bob



FONTE: Adaptado de Kurose (2010).

Supomos em um cenário comum que Alice deseja enviar um e-mail a Bob.

Passo 1 – Alice executa seu agente de usuário para e-mail (*webmail, outlook, thunderbird*, etc.), e digita o endereço de e-mail de Bob. Ela escreve a mensagem e informa o agente de usuário a enviar a mensagem que acabou de digitar.

Passo 2 – O agente de usuário de Alice envia a mensagem para seu servidor de correio, onde este e-mail é colocado em uma fila de mensagens.

Passo 3 – O lado cliente do SMTP, que funciona no servidor de correio de Alice, visualiza o e-mail na fila e inicia uma conexão TCP, para um servidor SMTP, que executa no servidor de correio de Bob.

Passo 4 – Realizado alguns procedimentos de apresentação, o cliente SMTP envia a mensagem de Alice para dentro da conexão TCP.

Passo 5 – No servidor de correio eletrônico de Bob, o lado servidor do SMTP recebe a mensagem e a coloca na caixa postal dele.

Passo 6 – Bob executa seu agente de usuário para ler o e-mail que acabara de chegar.

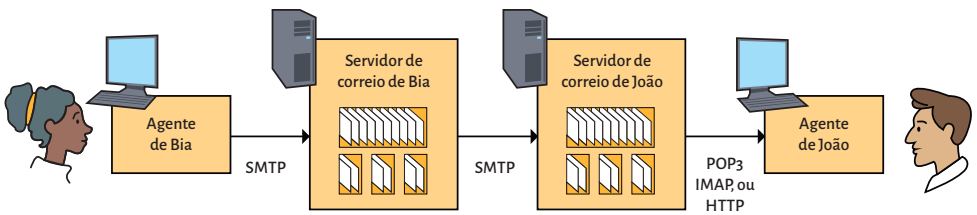
Vale salientar que o SMTP geralmente não usa servidores de e-mail intermediário para enviar mensagens, mesmo quando estes servidores possam estar em duas extremidades geográficas distantes do mundo. Se por acaso a mensagem de Alice não conseguir se comunicar com o servidor STMP de Bob, a mensagem permanecerá no servidor de correio de Alice, esperando por uma nova tentativa; desta forma, a mensagem não é colocada em nenhum servidor de e-mail intermediário.

4.2.3 POP3

O protocolo POP3 (*Post Office Protocol*) é responsável pelo recebimento de e-mails. Definido pela RFC 1939, é ele que controla a conexão entre um servidor e um cliente de e-mail. Em outras palavras, ele é usado para transferir e-mails do servidor de e-mails destinatário para o agente de usuário destinatário.

Lembra na história da seção anterior onde Alice desejava enviar um e-mail para Bob? Pois bem, ainda faltava uma peça naquele quebra-cabeça. Então vamos à explicação! Como é possível para Bob, que está executando um agente de usuário de e-mail em seu computador pessoal, obter seus e-mails que estão em um servidor de e-mails dentro de seu ISP? Temos que pensar que o usuário Bob não pode utilizar um servidor SMTP para receber mensagens por que o protocolo SMTP é destinado a enviar e-mails e não receber. Pois bem, o quebra-cabeça é solucionado com a introdução de um protocolo especial de acesso a caixa de e-mails que transfere as mensagens do servidor de e-mails para o computador pessoal de Bob. Atualmente, existem diversos protocolos que executam a função de recebimento de e-mails, entre eles estão o POP3 (um dos mais usuais), o IMAP e o HTTP. A figura 83, apresenta o caminho completo realizado desde o envio do e-mail até o recebimento pelo usuário destinatário.

FIGURA 83 – Caminho de comunicação de e-mail através dos protocolos SMTP e POP3



FONTE: Adaptado de Kurose (2010).

O POP3 inicia quando o agente de usuário (cliente) abre uma conexão do tipo TCP com o servidor de e-mail junto a porta 110. Com a conexão estabelecida, o protocolo passa por três fases: autorização, transação e atualização. Na primeira fase (autorização), um nome de usuário e uma senha são fornecidos. Na segunda fase (transação), ele recupera mensagens (nesta etapa é possível também marcar e apagar mensagens, assim como obter estatísticas de e-mail). A terceira fase, chamada de atualização, ocorre após o cliente encerrar a conexão POP3.

4.2.4 E-mail pela Web

Atualmente, é crescente o número de usuários que acessam, enviam e recebem e-mails através de seus navegadores Web. Um dos precursores deste tipo de serviço de e-mail Web foi o Hotmail, em meados de 1990; hoje, esse tipo de serviço é disponibilizado com frequência por quase todos os sites ISP, assim como universidades e empresas importantes.

Neste tipo de serviço, o agente de usuário é um navegador Web comum na qual o usuário se comunica com sua caixa postal remota via protocolo HTTP. Quando um destinatário, quer acessar um e-mail em sua caixa de entrada, a mesma é enviada do servidor de e-mails, para o navegador usando o protocolo HTTP, e não protocolos POP3 ou IMAP, contextualizados anteriormente. Da mesma forma, quando este usuário quiser enviar um e-mail, esta será feita via navegador para seu servidor de e-mails por HTTP, e não via protocolo SMTP.

São exemplos de e-mails pela web os seguintes serviços:

- Gmail: https://gmail.com/mail/
- Microsoft Outlook: https://outlook.live.com
- Yahoo: https://login.yahoo.com/m?.intl=br&.lang=pt-BR

4.2.5 FTP

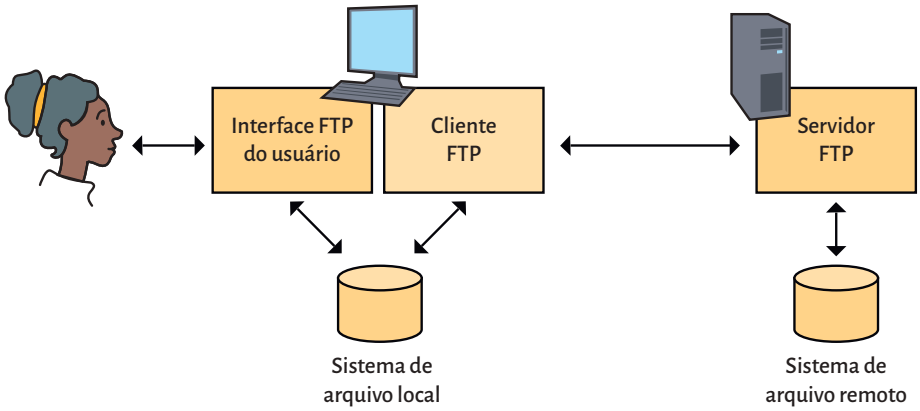
O protocolo FTP (*File Transfer Protocol*) é utilizado na transferência de arquivos (tanto *upload* como *download*) e possui muitas características similares com o protocolo HTTP, como por exemplo a utilização do protocolo TCP no transporte de dados. O FTP utiliza duas conexões TCP paralelas para transferir um arquivo: uma conexão de controle e uma conexão de dados. Estas duas conexões, por sua vez, operam em portas distintas. A porta 21 é utilizado para controle das informações, enquanto que a porta 20 é usada para transmissão de dados.

A conexão de controle é utilizada para enviar informações de controle entre os dois hospedeiros, como por exemplo identificação do usuário, senha, comandos para acesso a diretórios, entre outros. Já a conexão de dados é utilizada para efetivamente enviar arquivos. Os serviços de FTP podem ser classificados basicamente em dois tipos: os servidores de FTP e os clientes de FTP. Os servidores FTP provêm uma estrutura de hospedagem de arquivos e conexão a estes, geralmente disponibilizados através de uma URL ou endereço IP público. Já os clientes de FTP são programas (softwares aplicativos) que são utilizados para acessar os servidores de FTP. Este acesso por sua vez, pode ser público (sem autenticação) ou privado (requerendo a autenticação do usuário, mediante nome de usuário e senha). Como exemplos de softwares aplicativos para FTP estão:

- Filezilla: https://filezilla-project.org/
- CuteFTP: https://www.techtudo.com.br/tudo-sobre/cute-ftp.html
- WS FTP: https://www.techtudo.com.br/tudo-sobre/ws-ftp.html

A figura 84, demonstra o funcionamento básico de um serviço de FTP.

FIGURA 84 – Funcionamento básico de um serviço de FTP



FONTE: Adaptado de Kurose (2010).

Quando um usuário inicia uma sessão FTP com um hospedeiro remoto, o lado cliente do FTP (usuário) inicia prioritariamente uma conexão TCP de controle com o servidor na porta 21 do servidor e envia por essa conexão de controle a identificação e a senha do usuário, além de comandos de FTP para mudar o diretório remoto, por exemplo. Quando o lado servidor recebe, pela conexão de controle, um comando para uma transferência de arquivos, abre-se uma conexão TCP de dados para o lado cliente. O FTP envia um arquivo pela conexão de dados e em seguida fecha o mesmo. Desta forma, com FTP, a conexão de controle permanece aberta durante toda a sessão do usuário, mas uma nova conexão de dados é criada para cada arquivo transferido dentro de uma sessão.

4.2.6 DNS

O protocolo DNS tem a função de traduzir nomes de domínios na Internet em endereços IP. Esta é a principal tarefa do DNS (*Domain Name Server* – Servidor de Nomes de Domínio) da Internet. O DNS corresponde a um banco de dados distribuído de gerenciamento de nomes e um protocolo de camada de aplicação que permite que hospedeiros consultem o banco de dados distribuído. Na Internet a função do DNS é manter, organizar e traduzir nomes e endereços de dispositivos de rede.

Os servidores de nomes são em sua grande maioria máquinas Linux que executam o software BIND. O protocolo DNS utiliza o protocolo UDP no transporte das informações e a porta padrão 53. Vamos utilizar um exemplo do dia a dia para demonstrar a funcionalidade do DNS. Imagine que um usuário queira acessar o endereço "http://www.ufsm.br". Ao executar este endereço em seu navegador Web, o computador do usuário faz uma requisição HTTP ao servidor Web que hospeda o site www.ufsm.br para primeiramente obter o endereço IP do site em questão. Isso é realizado da seguinte forma:

Passo 1 – O computador do usuário executa o lado cliente da aplicação DNS.

Passo 2 – O navegador extrai o nome da URL e passa este nome para o lado cliente da aplicação DNS.

Passo 3 – O cliente DNS envia uma consulta contendo o nome de hospedeiro para um servidor DNS.

Passo 4 – O cliente DNS recebe uma resposta, que inclui o endereço IP correspondente ao nome de hospedeiro.

Passo 5 – Uma vez recebido o endereço DNS, o navegador pode abrir uma conexão do tipo TCP com o processo servidor HTTP localizado naquele endereço IP.

É importante entender que nenhum servidor DNS presente na Internet possui todos os mapeamentos para todos os demais hospedeiros. Ao invés disso, os mapeamentos são distribuídos pelos servidores DNS.

Hierarquia de nomes

Uma hierarquia de nomes é utilizada para caracterizar o uso de cada extensão do domínio. Na tabela 7, são caracterizados alguns dos principais domínios utilizados e seu respectivo significado.

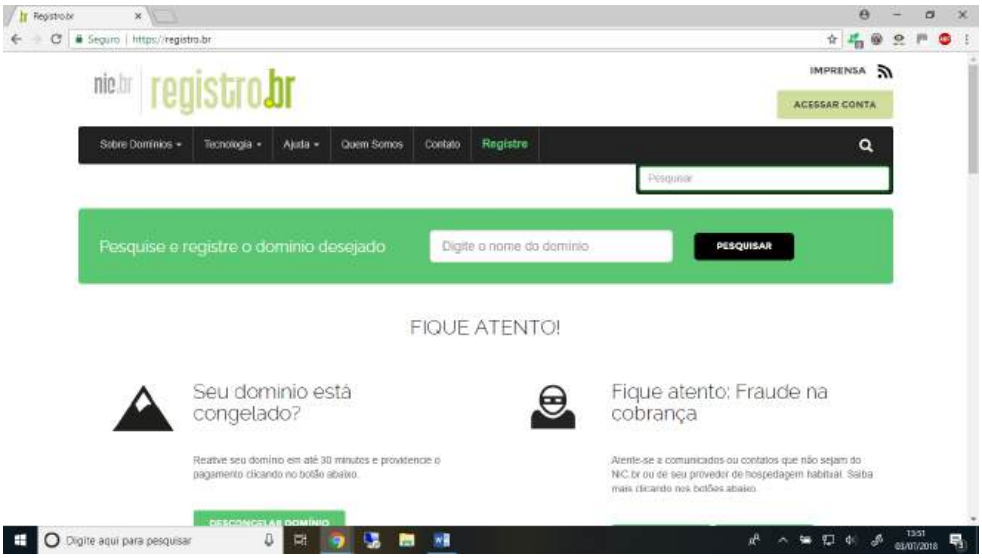
TABELA 7 – Tipos de Domínios

TIPOS DE DOMÍNIOS	
NOME DO DOMÍNIO	**SIGNIFICADO**
.com	Organizações comerciais
.edu	Instituições educacionais
.gov	Instituições governamentais
.mil	Agências militares
.net	Organizações da rede
.org	Organizações não comerciais
.int	Organizações internacionais
Código de países	Identificador de 2 letras para domínios de países específicos

FONTE: (TANEMBAUM, 2010).

Ainda, no Brasil a entidade responsável pelo registro de nomes de domínio de uma determinada pessoa ou organização denomina-se “Registro.br”. Através deste site podemos criar domínios com diferentes terminações e utilizá-los na grande rede. A figura 85, apresenta o site oficial do “Registro.br”.

FIGURA 85 – Site oficial do "Registro.br"



FONTE: Registro.br. Disponível em: https://registro.br/

SAIBA MAIS: O Registro.br (www.registro.br) é a entidade nacional que trata do registro de domínios para a internet no Brasil, ou seja, que estão sob a faixa ".br". Desta forma, ao registrar um novo domínio na internet com a extensão final ".br" é necessário consultar se o domínio em questão não está registrado e se o mesmo é possível de ser registrado. Para registrar um novo domínio, além de cadastrar-se no portal é necessário informar onde este domínio ficará hospedado (servidor de hospedagem), bem como pagar uma taxa anual para exercer a utilização deste domínio.

4.2.7 SNMP

O protocolo SNMP (*Simple Network Management Protocol*) ou Protocolo Simples de Gerência de Rede é responsável por transmitir as informações referentes ao status dos diferentes dispositivos que compõe uma rede de computadores (podendo obter desta forma informações como desempenho, características, status na rede, entre outros). Esta tarefa de coleta das informações é realizada por um agente SNMP, que obtêm estas informações dos dispositivos e envia para um servidor de gerenciamento onde as informações são armazenadas e podem ser posteriormente analisadas. A utilização do protocolo SNMP propicia o monitoramento dos dispositivos de rede em tempo real.

4.2.8 DHCP

O protocolo DHCP (*Dynamic Host Configuration Protocol*) tem a função de gerar e administrar endereços IP em uma rede de computadores. Este protocolo, atuando junto a um servidor DHCP devidamente configurado, permite distribuir endereços IP, máscaras de sub-redes, *gateway* padrões, entre outras configurações, para os diferentes dispositivos que podem compor uma rede de computadores. Para que o DHCP possa desempenhar sua função em uma rede faz-se necessário:

- Computador do usuário (denominado cliente, que irá requisitar um endereço IP) deve possuir o pacote DHCP cliente devidamente instalado.
- Dado o passo acima, o computador cliente faz uma requisição na rede pedindo um número IP.
- Um servidor DHCP devidamente configurado na rede, responde a solicitação do usuário, com um pacote contendo o endereço IP e demais configurações necessárias (sub-rede, *gateway*, etc).

4.2.9 SSH

O SSH (*Secure Shell*) corresponde a um protocolo de rede criptográfico, destinado a conexão remota segura, permitindo basicamente a administração total de computadores a distância (ou em uma mesma rede, se assim for necessário). O SSH utiliza a porta padrão 22, além de permitir tunelamento, redirecionamento de portas TCP e conexões X11. Atualmente existem uma grande variedade de softwares aplicativos que permitem administrar computadores e servidores a distância, através de outro computador ou de um smartphone (através de aplicativos específicos para tal).

Abaixo são apresentados alguns exemplos de softwares para conexão SSH:

- **OpenSSH**: https://www.openssh.com/.
- **Putty**: https://www.putty.org/.

ATIVIDADES DE REFLEXÃO OU FIXAÇÃO

1. Diferencie Internet e Web.

2. Quais passos são realizados para que um cliente receba a informação de uma página web, desde a sua solicitação? Explique sua resposta.

3. Qual a diferença entre o modelo OSI e o Modelo TCP/IP?

4. Descreva para que servem os principais serviços de internet abaixo:

a. HTTP
b. SMTP
c. POP3
d. FTP
e. DNS
f. DHCP
g. SNMP
h. SSH

5

SEGURANÇA E GERENCIAMENTO DE REDES

INTRODUÇÃO

O capítulo a seguir trata da segurança e gerenciamento das redes de computadores. A segurança está associada a diversas ameaças digitais presentes nas redes locais, no compartilhamento de informações, no acesso à web, entre outras tantas variantes. Já o gerenciamento de redes propicia conhecer a rede, monitorá-la e responder a possíveis problemas detectados.

Desta forma, na seção 5.1 a segurança de redes é o tema principal. Dentro dela os mecanismos de segurança da informação são detalhados, como, por exemplo, as políticas de segurança (definição, criação de regras, categorias de políticas de segurança, entre outros), as contas e senhas de usuários (como elaborar uma senha forte), os métodos de criptografia existentes (*hash*, criptografia de chave pública e chave privada, algoritmos de criptografia mais usuais, entre outros), cópias de segurança (a importância dos backups), ferramentas *antimalware* (exemplos das mais utilizadas), *firewall* pessoal (exemplos de *firewall* pessoal), cuidados gerais sobre segurança em redes de computadores e, por fim, um conteúdo extra sobre segurança em redes Wi-Fi.

Na seção 5.2, o tema a ser estudado é sobre o gerenciamento de redes. Esta seção por sua vez é dividida em duas seções menores: monitoramento e controle de rede, que compreende entender como se dá o monitoramento e posteriormente o controle sobre uma rede de computadores e em seguida os softwares para que efetivamente seja possível gerenciar uma rede. Entre os softwares principais para esta função destacam-se o CACTI, Nagios e Zabbix.

5.1
SEGURANÇA EM REDES

O STMP no As redes de computadores constituem atualmente um item básico para o trabalho nas organizações de todos os tamanhos (de pequeno a grande porte). Apesar de todos os benefícios proporcionados pelas redes de computadores, ao interligar máquinas em rede, estas ficam mais vulneráveis a ataques, necessitando de cuidados específicos no que diz respeito a "proteção da informação" que ali trafega, no intuito de evitar que estes dados possam ser alterados, destruídos ou roubados.

Ao abordar o tema "segurança em redes de computadores", fazemos automaticamente referência a rede local onde nos conectamos (via wi-fi, cabo, em casa, escritório, empresa, etc.), mas principalmente nos reportamos a grande rede chamada "Internet", pois é nessa rede mundial onde nossos computadores podem sofrer ataques com alguma frequência. Diante deste cenário, onde precisamos estar "online" em uma grande rede que conecta milhares de computadores ao redor do mundo, o que é e como podemos definir "segurança"?

Pois bem, segurança vem acompanhada de seu antônimo "vulnerabilidade". Segundo a ISO (*International Standardization Organization* – Organização Internacional para Padronização), no contexto da computação, vulnerabilidade refere-se a qualquer fraqueza, ou falha, que possa ser explorada para violar um sistema ou as informações que nele contém. Dessa forma, independentemente do tipo de tecnologia utilizada, ao conectar o seu computador à rede, o mesmo estará sujeito a várias possíveis violações de segurança (várias ameaças), dentre as quais destacam-se:

> TERMO DO GLOSSÁRIO: ISO é a sigla de *International Organization for Standardization*, ou Organização Internacional para Padronização, em português. A ISO é uma entidade de padronização e normatização, e foi criada em Genebra, na Suiça, em 1947. A ISO tem como objetivo principal aprovar normas internacionais em todos os campos técnicos, como normas técnicas, classificações de países, normas de procedimentos e processos, etc. No Brasil, a ISO é representada pela ABNT (Associação Brasileira de Normas Técnicas).

- **Furto de dados e Interceptação de tráfego**: corresponde à obtenção de forma não autorizada a informações pessoais (entre outros dados sigilosos), através da interceptação de tráfego da rede não criptografado ou, ainda, através da exploração de vulnerabilidades conhecidas existentes em computador pessoal (seja em um serviço, software aplicativo ou sistema operacional).

- **Uso indevido de recursos**: um atacante (quem efetua um ataque) obtém acesso a um computador e de posse deste dispositivo pode utilizá-lo de forma maliciosa, obtendo arquivos, enviando spans, gerando ataque a outros computadores e ocultando sua identidade original.

- **Varredura**: corresponde ao processo de vasculhar uma rede de computadores com o propósito de identificar outros dispositivos que compõe esta rede, suas configurações, serviços, sistema operacional que utilizam, entre outros. A varredura compõe uma parte inicial de um ataque quanto ao mapeamento de uma determinada rede, para que de posse desta informação, possa direcionar alvos de ataques.

- **Exploração de vulnerabilidades**: consiste em explorar possíveis falhas existentes em softwares aplicativos, plug-ins, serviços ou no próprio sistema operacional instalado. Ao explorar uma vulnerabilidade e obter acesso ao computador, um atacante pode disparar ataques, coletar dados indevidamente, além de poder propagar códigos maliciosos em geral. Dispositivos de rede como roteadores, também podem ser invadidos, reconfigurados e direcionar usuários a sites fraudulentos.

- **Ataque de negação de serviço e de força bruta**: na primeira modalidade de ataque o atacante utiliza uma rede de computadores para poder enviar uma grande quantidade de dados para um computador destino, a fim de que o mesmo possa parar ou ser incapaz de continuar respondendo. Já no ataque de força bruta a ideia é automatizar o processo de descobrimento de senhas fracas (softwares podem realizar tal trabalho através de uma *wordlist*) que podem ter sido utilizadas pelo administrador do sistema (na autenticação), com o propósito de identificá-las e obter acesso.

Além das ameaças de rede, citadas acima, existem ainda as ameaças virtuais, que crescem diariamente e representam riscos a qualquer computador conectado à internet. Entre as principais, citamos algumas relacionadas abaixo:

- **Vírus de Computador**: comum no meio virtual, um vírus de computador é um programa, feito com código malicioso, que tem o objetivo de causar algum dano ao computador, como, por exemplo: obter informações, alterar o funcionamento e configuração de serviços/arquivos, apagar dados, entre outros. O termo "vírus" possui tal denominação pois tem característica a capacidade de se multiplicar (rapidamente em uma rede local de comutadores, por exemplo), assim como ocorre com os vírus reais que atacam os seres vivos. Existem vários meios de propagação dos vírus de computadores. Eles podem ser transmitidos por meio de arquivos infectados, mensagens de e-mail, programas de compartilhamento, entre outros. Entre os meios mais comuns atualmente de propagação de vírus, estão os anexos de mensagens de e-mails, além dos links que direcionam a serviços falsos na internet. Uma vez o computador infectado por um vírus, este pode se comportar de forma passiva ou ativa. Na forma passiva, um vírus contamina um arquivo e esse é enviado via e-mail por um usuário, por exemplo. Na forma ativa, o próprio vírus consegue infectar outros computadores da rede. Um vírus de computador pode realizar desde ações simples, como a execução de um programa, até a danificação irreversível de um sistema operacional. Os vírus em sua grande

maioria são desenvolvidos para atingir o sistema operacional Windows (pois é um dos sistemas operacionais mais utilizado no mundo), mas também existem vírus para sistemas Linux e MacOS apesar desta representatividade ser bem menor.

- **Trojan**: semelhante à ideia que está por trás de um vírus de computador, um trojan tem o objetivo de se infiltrar em computador e a partir de então permitir que pessoas mal-intencionadas possam acessar a máquina remotamente por meio das portas TCP desprotegidas. Os trojans podem também capturar informações do usuário e executar instruções capazes de: apagar arquivos, destruir aplicativos, entre outros. A propagação do trojan se assemelha com a dos vírus em geral. Utilizada por hackers o trojan visa explorar as vulnerabilidades do sistema operacional, como por exemplo, localizar portas abertas e desprotegidas. Através do acesso remoto é possível capturar informações que foram digitadas pelo usuário e transmiti-las para outro computador permitindo que pessoas mal-intencionadas utilizem informações sigilosas como senhas, números de contas, cartões de créditos, etc.

- **Spywares**: são softwares que realizam ações como publicidade, coleta de informações pessoais, alteração da configuração do computador, tudo isso sem o consentimento do usuário. Geralmente um *spyware* se instala no computador do usuário, junto com a instalação de um outro software (por isso a importância de sempre ler todos os avisos e concordâncias na instalação de qualquer programa de computador – contrato de licença e declaração de privacidade, por exemplo). Dois tipos comuns de *spywares* são os *adwares* e os *keyloggers*. Um *adware*, depois de instalado secretamente no computador, verifica os hábitos de navegação do usuário armazenados nos *cookies* do navegador de internet (essas informações uma vez catalogadas, podem ser vendidas a outras empresas, por exemplo). Já um *keylogger*, tem o poder devastador de gravar tudo que é digitado pelo usuário via teclado. Com estas informações gravadas um e-mail secreto pode ser disparado para um atacante que remotamente recebe em sua caixa de mensagens estes dados.

SAIBA MAIS: conheça mais sobre *spywares*, o que são, como se proteger, entre outros, acessando o link abaixo: https://br.ccm.net/contents/753-spyware

- **Engenharia Social**: trata-se de uma técnica que explora a vulnerabilidade de seres humanos em fornecer informações. Na engenharia social não há utilização de nenhum software ou programa de computador específico, mas sim a habilidade de um atacante em extrair informações confidenciais de um funcionário de uma empresa, sobre a mesma, através de perguntas, se passando por um prestador de serviços, colaborador externo, etc. Os principais ataques de engenharia social que acontecem na internet são por meio de e-mails falsos, na qual induzem funcionários despreparados ou instruídos de forma ineficaz a fornecer dados sigilosos em geral.

5.1.1 Mecanismos de Segurança da Informação

Uma vez conhecendo os principais riscos, ameaças e vulnerabilidades, tanto em redes locais, quanto na grande rede mundial de computadores (internet), faz-se necessário o entendimento dos principais mecanismos de segurança que nos auxiliam na tarefa de proteger nosso computador, dispositivo conectado à rede ou a internet de um modo geral. Vamos conhecer agora os principais mecanismos voltados a segurança da informação.

5.1.1.1 Política de Segurança

Uma política de segurança corresponde a um conjunto de regras, que especificam o que pode e o que não pode ser feito, geralmente aplicada a uma rede local de computadores (principalmente em uma rede corporativa – ambiente de trabalho), bem como as penalidades as quais estão sujeitos os usuários que dela não cumprem. Uma política de segurança, pode ser única (aplicada a somente um foco), assim como pode abranger uma série de políticas de segurança integradas, tais como:

- **Política de senhas**: define as regras do uso de senhas em uma rede, bem como recursos computacionais que dela fazem parte. Entre as informações contidas nesta política estão a periodicidade da troca de senha, tamanho mínimo e máximo, composição da mesma, etc.
- **Política de *backup***: define regras específicas da realização da cópia de segurança, como o tipo mídia a ser utilizado no backup, frequência de execução (diária, semanal, mensal) e período de retenção.
- **Política de privacidade**: define como serão tratadas as informações pessoais, sejam elas de usuários, clientes, funcionários, entre outros (bastante utilizada também em serviços da internet).

A construção de uma (ou mais) políticas de segurança de forma clara e objetiva, seguida da explanação e envolvimento dos usuários que utilizam esta rede, permite minimizar problemas conhecidos de segurança, bem como adicionam um nível extra de proteção a mesma.

5.1.1.2 Contas e Senhas

As contas e senhas de usuários são geralmente a forma de autenticação mais utilizada em todo mundo, uma vez que sistemas operacionais, aplicativos comerciais, sites, portais, entre outros serviços, utilizam-se deste tipo de autenticação para identificar e autorizar, ou não, usuários e respectivos conteúdos/serviços a que se tenha acesso. A autenticação pode ser classificada em três grupos básicos:

- Informações pessoais do usuário (biometria em geral – impressão digital, palma da mão, olho, etc.).

- Informações que o usuário possui (token, cartão de senhas, etc.).
- Informações que o usuário sabe (perguntas e respostas, senhas, etc.).

Elaboração de Senhas

Uma boa senha é aquela que é fácil de ser lembrada e difícil de ser descoberta. Seguindo esta lógica, não é recomendável criar uma senha complexa mas que não seja possível memorizá-la, nem tampouco criar uma senha fácil demais a ponto de um atacante descobrir rapidamente a mesma. Abaixo são listados alguns itens que NÃO devem ser utilizados na elaboração de uma senha:

- **Qualquer tipo de dado pessoal**: evitar nomes, sobrenomes, contas de usuário, número de documentos, placas de carro, telefones ou data de aniversário por exemplo (este tipo de informação pode ser obtido através de observação, busca na internet, redes sociais, entre outros, sendo de fácil associação a uma possível senha do usuário).
- **Sequências de teclado**: evite senhas que sejam uma sequência do teclado, pois as mesmas podem ser descobertas por observação, enquanto digita.
- **Palavras que façam parte de listas**: evitar nomes públicos, nomes de times de futebol, músicas, filmes ou que possam ser encontrados em dicionários. Existem softwares que tentam descobrir essas senhas fazendo associação com uma lista pré-definida de palavras deste contexto apresentado.

Quanto as boas práticas para elaboração de senhas, temos:

- **Números aleatórios**: quanto mais ao acaso forem os números aleatórios, melhor.
- **Grande quantidade de caracteres**: quanto mais longa for constituída a senha, maior a dificuldade em descobri-la.
- **Diferentes tipos de caracteres**: quanto mais misturada uma senha, mais forte a mesma será. Procure combinar números, letras maiúsculas, minúsculas e sinais de pontuação, de modo que você tenha uma associação a esta senha (por exemplo, uma frase com as iniciais de cada palavra).

5.1.1.3 Criptografia

A criptografia de modo geral está relacionada a um conjunto que contempla o uso de conceitos e técnicas utilizados em sistemas computacionais, com o propósito de cifrar determinado conteúdo, de forma que somente emissor e receptor conseguem decifrá-la e, posteriormente, entendê-la. Tal técnica se faz necessária devido à necessidade de proteção de informações confidenciais.

Quanto à forma de funcionamento de um mecanismo de criptografia, a mesma se baseia na utilização de um algoritmo e de uma chave. O algoritmo tem a função de cifrar e decifrar os dados utilizando para isso a chave correta. Analisando por

esta perspectiva, mesmo que um atacante consiga interceptar os dados durante uma comunicação criptografada, sem a chave correta, o mesmo não conseguirá decifrar e entender o conteúdo ali transmitido. Desta forma, quanto maior a chave utilizada (medida em bits), mais segura será a criptografia empregada. Através do emprego da criptografia torna-se possível:

- Proteger dados confidenciais armazenados no computador (arquivos de senhas, arquivos com conteúdo específico), proteger backups contra acesso não-autorizado, proteger comunicações via internet (autenticação, inserção de informações sigilosas, compras em sites de e-commerce) entre outros.

Criptografia de chave simétrica e chaves assimétricas

Existem dois métodos criptográficos que, de acordo com a chave usada, podem ser divididos em duas grandes categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

- *Criptografia de chave simétrica*: este método utiliza uma mesma chave no processo de codificação e no de decodificação dos dados. Também denominada de criptografia de chave única ou secreta, seu objetivo é a confidencialidade dos dados. Como exemplos de criptografia que utilizam este método estão: 3DES, AES, IDEA e Blowfish.
- *Criptografia de chaves assimétricas*: este método criptográfico, também denominado de criptografia de chave pública, faz a utilização de duas chaves distintas: uma chave pública e uma chave privada. A chave pública pode ser divulgada livremente, já a chave privada deve ser mantida em sigilo por seu dono. Quando um dado precisa ser enviado em uma comunicação, o emissor cifra estes dados, utilizando a chave pública do receptor, que então utilizará a sua chave privada para descriptografar e ter acesso aos dados. Esta chave privada pode ser armazenada no computador de diferentes formas, como, por exemplo: arquivo, token, etc. Como exemplos de métodos criptográficos que utilizam chaves assimétricas, podemos citar: ECC, DAS, RSA, etc.

Assinatura digital

A assinatura digital corresponde a um código utilizado para garantir ao destinatário da informação que o remetente é realmente quem diz ser. No mundo da computação, a assinatura digital é o recurso utilizado para assinar documentos digitais para que esses não possam ser adulterados. Para isso, é necessário que:

- O destinatário consiga verificar a identidade alegada pelo remetente.
- O remetente não possa renegar o conteúdo da informação.
- O destinatário não consiga alterar a informação.

Com estes três itens presentes em uma assinatura digital, o destinatário da mensagem tem certeza de quem a enviou, o remetente não tem como negar o envio da mensagem e o destinatário não pode forjar a mensagem recebida.

5.1.1.4 Cópias de Segurança (backups)

As cópias de segurança, também conhecidas como *backups*, permitem a um usuário se resguardar quanto aos dados que estão gravados em seu computador. Diversos são os fatores que podem ocasionar a perda de dados, como, por exemplo, uma descarga elétrica, queima de um dispositivo, entre outros fatores. Por isso o backup é um procedimento tão importante quando o assunto é segurança da informação, pois permite:

- **Proteção dos dados**: o *backup* propicia que dados sejam recuperados em situações como falha de disco, atualização malsucedida do sistema operacional, exclusão acidental de arquivos, ação de vírus, furto/perda de dispositivos, entre outros.
- **Recuperação de versões**: a possibilidade de retomar uma determinada versão do sistema, de um banco de dados, de uma imagem de um disco rígido, enfim, tudo isso só é possível através de um backup realizado previamente.

5.1.1.5 Ferramentas Anti-malware

As ferramentas anti-malware são aqueles softwares capazes de detectar, anular (colocar em quarentena) ou remover códigos maliciosos de um computador. Na categoria de ferramentas anti-malware estão os antivírus, antispyware, antirootkit e antitrojan. Existem diferentes tipos de programas anti-malware, atuando da seguinte forma:

- **Método de detecção**: assinatura, na qual uma lista de assinaturas é utilizada à procura de padrões. Heurística – baseia-se nas estruturas, instruções e características que o código malicioso possui em si. Por fim, comportamento – que se refere ao comportamento apresentado pelo código malicioso quando executado.
- **Forma de obtenção**: podem ser gratuitos (obtidos livremente na internet e usados por prazo indeterminado), experimentais (obtidos através de versões *trial*, com utilização até determinado prazo), ou pagos (paga-se uma licença para usar o software de proteção de sua versão completa).
- **Execução**: geralmente são instalados no computador, de onde são executados. É possível também utilizar (quando disponível pelo fabricante do mesmo) versões portáveis, ou seja, que não exigem instalação, somente execução do mesmo (opção interessante para pendrives, discos externos, etc.). Existem ainda as ferramentas online de verificação de vírus, disponíveis através de sites da web.

Exemplos de ferramentas anti-malware:

- **MalwareBytes – Anti-malware**: atualmente um dos melhores anti-malware gratuito, disponível no mercado. Através deste software é possível fazer regularmente uma verificação no computador (ou unidades móveis) para garantir que os mesmos estão livres de vírus e outras pragas virtuais. A exceção da versão gratuita é que a mesma não possui proteção em tempo real. Na figura 86, é apresentada a tela inicial do software Malwarebytes Anti-Malware, versão *free*.

FIGURA 86 – Tela inicial do Software Malwarebytes Anti-Malware versão free

FONTE: Malwarebytes. Disponível em: http://www.malwarebytes.org/mwb-download/

- **IOBit Malware Fighter**: software anti-malware gratuito criado pela empresa IOBit. Apesar de ser considerado menos eficiente que o Anti Malware Bytes, possui o recurso de proteção de tempo real, possibilitando, desta forma, detectar arquivos maliciosos assim que os mesmos entrem em ação junto ao sistema operacional. Disponível em: http://www.iobit.com/malware-fighter.html.

- **Dr. Web CureIt!**: prático e intuitivo, este software anti-malware é uma excelente opção para remoção de pragas virtuais e arquivos maliciosos, apesar de não contar com proteção em tempo real, ou seja, é necessário executar o programa e acioná-lo toda a vez que se deseja escanear determinada partição ou o sistema como um todo. Disponível em: ftp://ftp.drweb.com/pub/drweb/cureit/launch.exe

- **Super AntiSpyware**: mais uma opção entre os softwares de combate a spywares. Não possui proteção em tempo real, porém é de fácil utilização e conta com recursos intuitivos para proteção do computador. Disponível em: http://cdn.superantispyware.com/SUPERAntiSpyware.exe

- **Emsisoft Emergency Kit**: software portátil (não necessita instalação) utilizado para verificar a limpar computadores, contra pragas virtuais e arquivos maliciosos. Com interface fácil e intuitiva permite quatro níveis diferentes de verificação: buscar por spywares de forma fácil, busca inteligente por spywares em arquivos do Windows, busca profunda (mais demorada, porém mais minuciosa na busca por spywares) e a busca personalizada, onde é possível definir o que será verificado em busca de spywares. Disponível em: http://www.emsisoft.com/en/software/eek/.

5.1.1.6 Firewall Pessoal

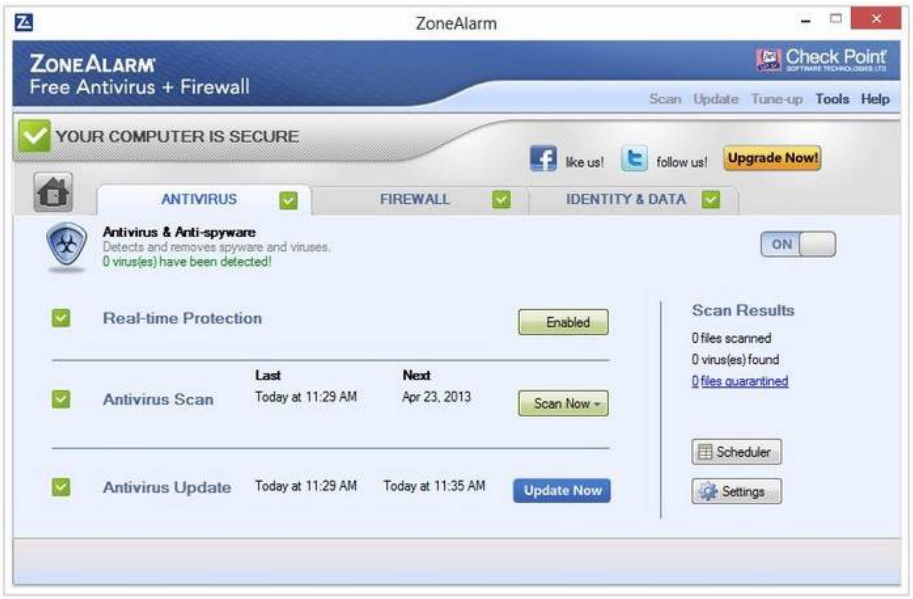
Um firewall (ou parede de fogo – tradução livre) é um mecanismo de segurança (um software), que muitas vezes já vem no próprio sistema operacional, mas que também pode ser instalado no computador e configurado para que possa proteger o mesmo contra acessos não autorizados vindos da internet e ajudam a impedir que *malwares*, *worms* e hackers, tenham acesso ao computador. A ideia por trás de um firewall é criar uma barreira entre a internet e o computador. Um firewall devidamente configurado torna-se uma ferramenta importante e eficaz para:

- Alertar e armazenar as tentativas de acesso não autorizados ao computador em questão.
- Realizar o bloqueio de tentativas de invasão, identificando a origem destas tentativas.
- Analisar de forma contínua o conteúdo das conexões que trafegam na rede, através da filtragem de pacotes, bloqueando a comunicação entre um possível invasor e um código malicioso, previamente instalado (*backdoor*).

Exemplos de firewall (para sistemas operacionais Microsoft):

- **ZoneAlarm Free Firewall 2018:** oferece proteção em tempo real e ferramentas extras para segurança Wi-Fi. Como características deste firewall que é um dos mais utilizados atualmente, temos: modo invisível completo, atualizações de segurança e backup online integrado. Na figura 87, é mostrado a interface inicial do software ZoneAlarm.

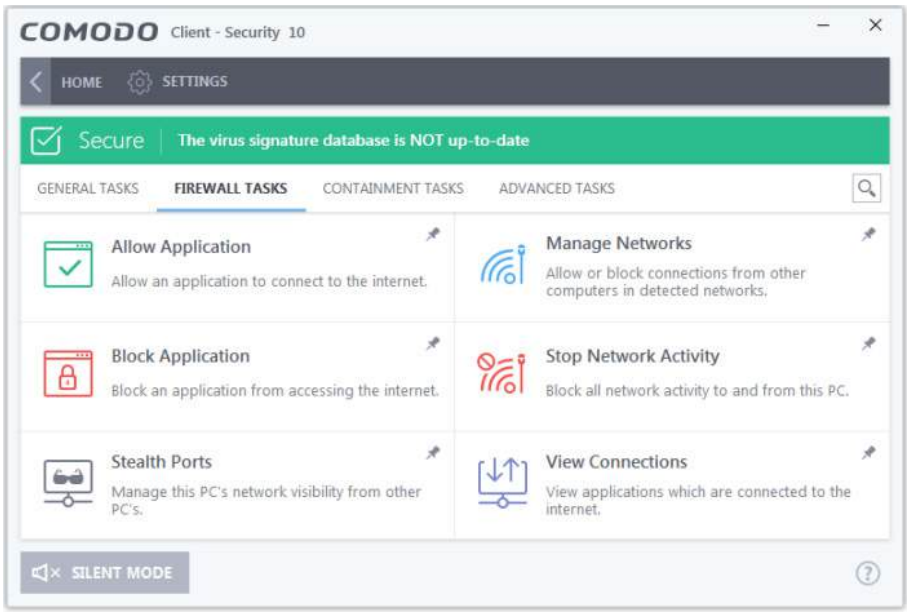
FIGURA 87 – Firewall software ZoneAlarm



FONTE: ZoneAlarm. Disponível em: https://www.zonealarm.com/software/free-firewall

- **Comodo Free Firewall:** solução eficaz em firewall pessoal, conta com inúmeros recursos, como: sandbox para programas menos seguros, monitoramento de atividades suspeitas, interface intuitiva de uso. Além disso, dispõe de um navegador extra, para uma navegação mais segura. A figura 88 apresenta a interface do software Comodo.

FIGURA 88 – Software Comodo Free Firewall



FONTE: Comodo. Disponível em: https://personalfirewall.comodo.com/

- **GlassWire:** uma solução completa de firewall pessoal, bem planejado, que entre suas características, possui: exibição do uso de tráfego de rede, opção

de bloquear programas individuais, análise de aplicativos por comportamento suspeito, entre outros. Disponível em: http://www.glasswire.com.

- **TinyWall:** pequeno aplicativo que permite controle extra do próprio firewall do Windows. Possui uma interface simples e limpa, além de não exibir nenhum tipo de propagandas. Disponível em: https://tinywall.pados.hu/.

5.1.2 Cuidados Gerais sobre Segurança em Redes de Computadores

Alguns cuidados gerais devem ser adotados, quanto ao uso de computadores junto a uma rede de computadores, como forma de minimizar alguns riscos, tais como:

- manter o computador sempre atualizado (é possível configurar o próprio sistema operacional, para que realize esta rotina de forma automática);
- utilizar e manter sempre atualizados, softwares de proteção do computador, como *anti-malware* e *firewall* pessoal;
- utilizar senhas fortes, em mecanismos que necessitem de tal autenticação por parte do usuário;
- utilizar conexão segura (https) sempre que a comunicação envolver dados confidenciais;
- ao utilizar compartilhamento de recursos em rede, definir sempre acesso condicionado a senha de autenticação, definindo a mesma de maneira segura (ou difícil de ser descoberta por dedução).

5.1.3 Segurança em Redes Wi-Fi (Extra)

As redes Wi-Fi (*Wireless Fidelity*), também conhecidas como redes sem fio, utilizam sinais de rádio para comunicação. Este tipo de rede caracteriza-se por dois modos básicos de operação: o modo **Infraestrutura** (que faz uso de um concentrador de acesso ou roteador wireless) e o modo **ponto a ponto** (também conhecido como *ad-hoc*, que permite criar redes pequenas, com as máquinas se comunicando entre si, sem o uso de um concentrador de acesso).

SAIBA MAIS: sobre os cuidados a serem tomados ao utilizar redes Wi-Fi em: https://cartilha.cert.br/redes/:

Hoje em dia as redes Wi-Fi tornaram-se bastante usuais pela mobilidade que proporcionam, facilidade de instalação e de uso em diferentes tipos de ambientes. Embora bastante convenientes, estas redes apresentam alguns riscos que devem ser considerados, tais como:

- por utilizarem ondas de rádio em sua comunicação, as redes wireless, podem ser interceptadas sem que um atacante esteja fisicamente conectado a esta rede, como acontece em uma rede cabeada, por exemplo. Desta forma, um atacante mal-intencionado, utilizando um *tablet* ou *notebook*, pode interceptar os dados que trafegam neste tipo de rede.
- consideradas redes de fácil instalação, é comum a instalação e configuração das mesmas por usuários menos experientes (substituindo o papel do administrador de redes) o que aumenta o risco de invasão ou acesso não autorizado;
- em redes Wi-Fi públicas, que não utilizam mecanismos de criptografia, os dados podem ser indevidamente coletados por atacantes. Além disso, redes Wi-Fi abertas podem ser propositalmente, configuradas de tal modo, para direcionar os usuários ali conectados a sites falsos, propiciando o roubo de suas informações.

5.2
GERENCIAMENTO DE REDES

O gerenciamento de redes trata de uma área fundamental relacionada as redes de computadores, pois objetiva o controle das atividades e o monitoramento do uso de recursos no ambiente de redes. As redes de computadores atuais são compostas por uma variedade de dispositivos que precisam se comunicar e realizar o compartilhamento de dados. Para que isso ocorra de forma eficiente, faz-se necessário um bom desempenho dos sistemas de rede. E para que este desempenho possa ser obtido de forma correta, um conjunto eficiente de ferramentas de gerenciamento de ser implementada.

O gerenciamento ou administração de redes de computadores, pode ser conceituado como a coordenação (de atividades, monitoramento, uso) de dispositivos de rede como computadores, servidores, roteadores ou recursos lógicos, como os protocolos TCP, UDP e IP, fisicamente distribuídos em uma rede, com o objetivo de prover confiabilidade, tempo de resposta aceitável e segurança nas informações que ali trafegam. No que diz respeito às tarefas básicas que contemplam o gerenciamento de redes, é possível classificá-las da seguinte forma:

- **Coleta de dados**: consiste em obter informações gerais dos dispositivos conectados à rede, geralmente de forma automatizada, através de agentes de software.
- **Diagnóstico**: prevê o tratamento e posterior análise dos dados catalogados.
- **Ação ou Controle**: identificado um problema na rede de computadores, encaminha-se uma ação ou controle sobre o problema em questão.

A ISO (*International Standardization Organizational*) propõe três estruturas, indicadas para resolução dos problemas relacionados a gerência de redes de computadores, os quais são:

- **Modelo Organizacional** (prevê uma hierarquia entre os sistemas de gerência, dividindo em diferentes subdomínios), **Modelo Informacional** (operações) e **Modelo Funcional** (funcionalidades da gerencia de redes, como por exemplo, gerência de falhas, configuração, desempenho, contabilidade e segurança).

5.2.1 Monitoramento e Controle de Rede

As funções principais de gerenciamento de redes podem ser agrupadas em duas categorias: monitoramento e controle de rede. O monitoramento, como o próprio nome já diz, tem como função a observação e análise do estado da rede, configurações, componentes, sendo basicamente uma função de "leitura do que acontece na rede". Já o controle da rede corresponde a função de "escrita", ou seja, está relacionada com a tarefa de alteração e execução de determinadas ações.

5.2.1.1 Monitoramento

O monitoramento de rede consiste basicamente na observação de informações relevantes ao gerenciamento de uma rede de computadores, que pode ser classificada em três categorias:

- **Estática**: monitora os elementos em sua configuração atual, tal como portas de roteadores, endereços IP, etc.
- **Dinâmica**: dados que trafegam na rede, são um exemplo de informação dinâmica que pode ser monitorada.
- **Estatística**: correspondem aos dados estatísticos que podem ser quantidades de pacotes enviados e recebidos por determinada interface da rede, total de conexões estabelecidas por um computador, etc. de forma a formar subsídios para a análise dos dados.

A informação de gerenciamento em uma rede é efetuada por agentes (softwares que executam em computadores e dispositivos da rede, coletando os dados) e repassada para um ou mais gerentes (softwares que agrupam estes dados, classificam e geram dados estatísticos ou em forma gráficos, geralmente).

5.2.1.2 Controle de Rede

O gerenciamento de uma rede para que seja efetivo necessita de um correto e eficaz sistema de controle de rede. Esta parte provê a modificação de parâmetros e a execução de ações em um sistema remoto. Se nos basearmos no modelo FCAPS (falhas, desempenho, contabilização, configuração e segurança), todas as etapas presentes envolvem em algum momento monitoramento e controle. Entretanto, nas duas últimas (configuração e segurança), o controle de rede tem sido mais utilizado.

Abaixo as principais funções do controle de configuração de rede:

– Definição da informação a configuração que será controlada.
– Inicialização e terminação de operações de serviços de rede.
– Relatórios de *status* de configuração.

No que diz respeito ao controle de segurança, aplicado sobre os dispositivos que compõem uma rede de computadores, as principais ameaças à segurança referem-se à interrupção de serviços, interceptação de dados, modificação das informações e mascaramento da mesma. As funções de gerenciamento de segurança podem por sua vez, serem classificadas em três categorias: manutenção da informação de segurança, controle de acesso aos recursos e controle do processo de criptografia.

Com o aumento de uma rede de computadores, em uma organização por exemplo, não exercer o gerenciamento adequado da mesma pode trazer riscos e prejuízos imensuráveis à empresa. A unificação de ambientes computacionais

torna cada vez mais necessária a integração dos sistemas de informação e unidades de trabalho dentro das empresas. À medida que uma rede de computadores cresce, crescem também a complexidade, capacidade e o surgimento de gargalos, juntamente com a necessidade de integração de serviços diversos, trazendo situações distintas para um administrador de redes (profissional que gerência uma rede de computadores), tais como:

- garantir o nível de qualidade de serviços em uma rede, alocando recursos e garantindo a interoperabilidade de missões críticas;
- avaliar o impacto de um novo sistema junto à organização e o impacto que a mesma trará;
- analisar o desempenho da rede quanto à implantação de um sistema de telefonia via VoIP, por exemplo;
- planejar *upgrades* quanto a velocidade do link de acesso à internet na organização, bem como, equipamentos para suportar a expansão e crescimento de tráfego na rede;
- identificar e controlar dispositivos que mais apresentam problemas ao longo do tempo;
- conhecer a configuração e localização física de determinado dispositivo da rede.

Desta forma, a gerência de redes de computadores pode melhorar significativamente a atuação de administradores de redes, pois possui o objetivo principal de observar e controlar os eventos que ocorrem em um ambiente de informação, permitindo a adoção de soluções que garantam a prestação de serviços pela rede corporativa, dentro dos requisitos estipulados.

5.2.2 Softwares para o Gerenciamento de Redes

Para que o monitoramento e controle de redes possa efetivamente "sair do papel", são necessários meios automatizados (softwares de gerência de redes) que possam ser instalados, configurados e devidamente analisados, pelos gerentes de redes de computadores. Estas ferramentas devem ser capazes de interagir com diferentes hardwares existentes em uma rede, bem como diferentes sistemas operacionais encontrados nos dispositivos da rede.

Em sua grande maioria, as ferramentas disponíveis para monitoramento de rede são baseadas do *Multi Router Traffic Grapher* (MRTG). O MRTG em si consiste de um script escrito via linguagem de programação PERL, que usa o protocolo SNMP para ler os contadores de tráfego de seus roteadores e um rápido programa em C, que autentica os dados do tráfego e cria gráficos representando o tráfego da conexão de rede monitorada. Estes gráficos, por sua vez, são incluídos em páginas web, que podem ser visualizadas através e qualquer navegador.

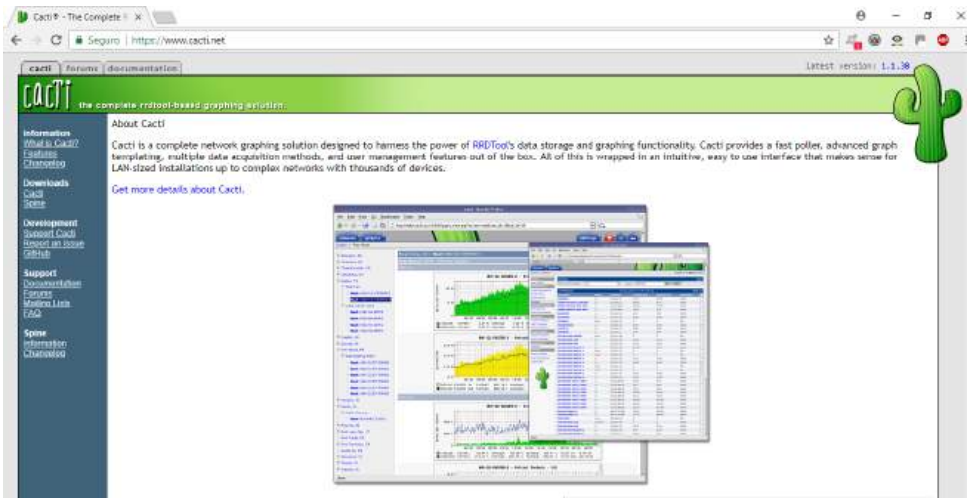
Veremos agora algumas das principais ferramentas para o gerenciamento de redes de computadores, que são baseadas nos conceitos acima sobre MRTG, mas que evoluíram em muitos aspectos, acompanhando as novas tendências voltadas para a web.

5.2.2.1 CACTI

CACTI é uma ferramenta *freeware* que recolhe e exibe informações sobre o estado de uma rede de computadores através de gráficos, sendo um *frontend* para a ferramenta RRDTool, que armazena todos os dados necessários para criar gráficos e inseri-los em um banco de dados Mysql.

Através do CACTI torna-se possível gerar gráficos referentes a uso de memória física, memória virtual, quantidade de processos, processamento, tráfego de rede, quantidade de espaço e disco, etc. Através do SNMP é possível gerar gráficos de sistemas operacionais Linux, Windows e de dispositivos de rede como roteadores e switches. A Figura 89 demonstra o site oficial da ferramenta CACTI.

FIGURA 89 – Site oficial da ferramenta de monitoramento CACTI



FONTE: CACTI. Disponível em: https://www.cacti.net/

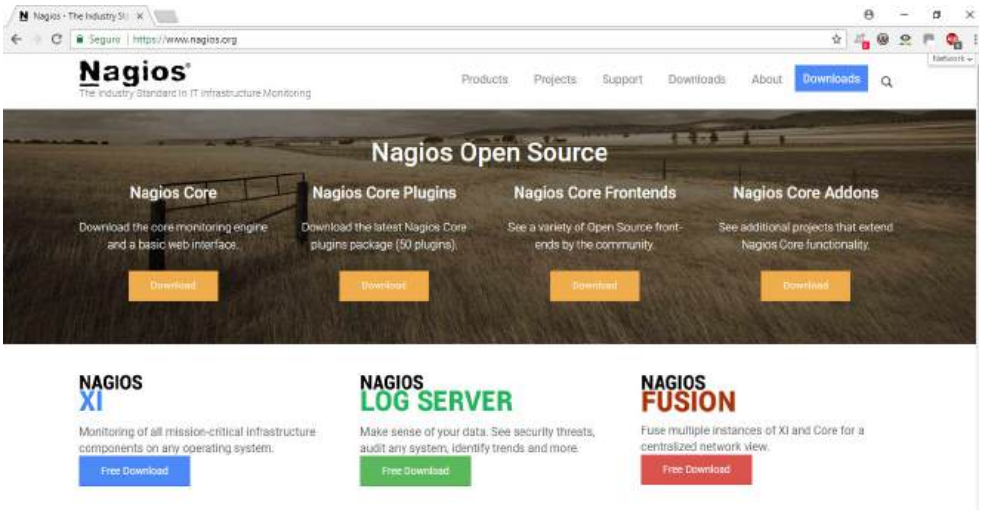
5.2.2.2 Nagios

O Nagios é um completo sistema de gerenciamento de dispositivos de rede, possuindo uma ampla quantidade de plug-ins que podem ser adicionados, como forma de aumentar suas funcionalidades. O Nagios é um sistema desenvolvido para executar em computadores com o sistema operacional Linux, distribuído de forma gratuita (licença GPL) e pode ser amplamente redistribuído/alterado. Algumas das várias ferramentas do Nagios, incluem:

- Monitoramento de rede e serviços diversos (POP3, SMPT, HTTP, PING, etc.).
- Monitoramento dos recursos computacionais (processador, uso de disco, memória, etc.).
- Notificação quando problemas de rede e dispositivos ocorrerem e forem resolvidos.
- Suporte para implementação de clientes de monitoramento redundantes.

- Interface web para visualização do status da rede, histórico de notificação e problemas, arquivos de log, etc. A Figura 90, apresenta o site oficial da ferramenta Nagios.

FIGURA 90 – Site oficial da ferramenta Nagios



FONTE: Nagios. Disponível em: https://www.nagios.org/

5.2.2.3 Zabbix

Zabbix é uma ferramenta de monitoramento de rede de computadores, capaz de monitorar uma infraestrutura completa. Possui licença GPL de uso gratuito e dispõe de uma grande variedade de opções. Através dele é possível monitorar em tempo real através de uma interface web centralizada todos os dispositivos da rede e seus status. Os monitores de performance, segurança, utilização de processador, disco rígido, entre outros, são de fácil acesso e respondem rapidamente aos comandos. Como principais características do Zabbix, podemos citar:

- Suporte a uma grande variedade de sistemas operacionais: Linux, Windows, Solaris, OpenBSD, Mac OS X, entre outros.
- Realiza a monitoria de serviços simples, como HTTP, POP3, IMAP, SSH, entre outros.
- Possui suporte nativo ao protocolo SNMP.
- Possui interface de gerenciamento web de fácil utilização.
- Integração com banco de dados (MySQL, Oracle, PostgreSQL ou SQLite).
- Geração de gráficos em tempo real.
- Fácil instalação e customização.
- Agentes para as plataformas de 32 e 64 bits.
- Integração com contadores de performance no Windows.
- Envio de alertas por e-mail e SMS, entre outros recursos.

A figura 91, mostra o site oficial da ferramenta Zabbix.

FIGURA 91 – Site oficial da ferramenta de monitoramento Zabbix

FONTE: Zabbix. Disponível em: https://www.zabbix.com/

ATIVIDADES DE REFLEXÃO OU FIXAÇÃO

1. Cite 5 ameaças de segurança e de que forma elas podem afetar uma rede de computadores.

2. O que é uma política de segurança? Cite um exemplo e explique para que serve.

3. Como posso elaborar uma boa senha? Quais as recomendações mais indicadas?

4. Qual a ideia por trás de uma assinatura digital? Qual sua utilidade?

5. Escolha um dos *antimalwares* citados nas seções anteriores, bem como um software de firewall, instale o mesmo e relate qual foi sua experiência na utilização de ambas as ferramentas de defesa.

6. No que diz respeito ao gerenciamento de redes, o que é o modelo FCAPS? Cite e explique as categorias do mesmo.

6

INFRAESTRUTURA PARA EDUCAÇÃO A DISTÂNCIA

INTRODUÇÃO

Este capítulo tem por objetivo descrever as principais tecnologias para infraestrutura de redes de computadores aliadas às principais ferramentas para educação a distância. Para que isso seja possível, será descrita uma subseção sobre servidores, onde será explicada sua função, os tipos de servidores e serviços de rede, além dos sistemas operacionais específicos para este fim. A ideia desta seção é preparar o aluno ao entendimento de servidores, serviços, sistemas operacionais e o que é possível fazer com eles.

Faremos na sequência um estudo de caso (seção 6.1.3), onde instalaremos e configuraremos um servidor web local, através da ferramenta XAMPP, para Windows. Esta contempla um servidor web Apache, um sistema gerenciador de banco de dados MySQL, além da linguagem de programação PHP e diversos outros módulos que podem ser adicionados a partir da instalação de plug-ins extras.

Na continuação as ferramentas para educação a distância são abordadas, com o intuito de conceituá-las, conhecê-las e explorá-las. Para isso o entendimento de plataforma EaD é conceituado e caracterizado, bem como, a ideia por trás dos AVAs (Ambientes Virtuais de Aprendizagem). Além disso, foi preparado também um estudo de caso com o ambiente Moodle. O objetivo deste estudo de caso é unir os conceitos de servidores, visto na primeira seção e no estudo de caso (seção 6.1.3), com um AVA em específico (no caso, será instalado o módulo Moodle junto a ferramenta XAMPP, para que o aluno possa trabalhar livremente com a ferramenta em seu computador). A escolha do ambiente Moodle para este estudo de caso se dá por ser um dos AVAs mais utilizados no mundo, por possuir suporte a diversos idiomas e uma vasta comunidade que contribui para evolução do mesmo, além de se tratar de uma ferramenta 100% gratuita.

6.1 TECNOLOGIAS PARA INFRAESTRUTURA

Existem diferentes tipos de tecnologias relacionadas às redes de computadores, que propiciam o suporte a um ambiente virtual de aprendizagem (AVA), por exemplo. Neste contexto estão os servidores (computadores dedicados a servir um ou mais computadores em uma rede local ou na grande rede), os sistemas operacionais e os softwares que dão suporte às aplicações ali hospedadas, como, por exemplo, um servidor LAMP (Linux, Apache, Mysql e PHP). Conheceremos agora as principais tecnologias voltadas para a infraestrutura de TI.

Servidores

Um computador servidor, ou simplesmente "Servidor", corresponde a uma máquina na rede de computadores, com a função de servir os demais computadores, denominados de clientes. Podemos dizer que servidores são computadores dedicados (podendo ser um computador desktop para este fim ou um servidor com infraestrutura física diferenciada) a desempenhar uma determinada tarefa, ou diversas delas ao mesmo tempo, com o objetivo de atender os demais computadores conectados à rede (provendo a estes os serviços que necessitam). Aos servidores cabe a tarefa de processar e organizar dados, gerenciar o acesso a arquivos e recursos, entre outros. Entre os serviços mais comuns que um servidor pode realizar estão: servidor de arquivos, impressão, e-mail, backup, acesso remoto, etc.

Quanto às vantagens em se utilizar um servidor em uma rede de computadores, estão:

- **Serviços**: a centralização de serviços de rede em um único local propicia um melhor gerenciamento dos recursos por parte do administrador da rede, bem como, facilidade de implantação, manutenção e suporte.
- **Backup**: um servidor de backup (cópias de segurança) ou de redundância por ser implementado garantindo a interoperabilidade do sistema e da infraestrutura em funcionamento.
- **Acesso Remoto**: implantando esta solução, um servidor pode ser acessado localmente ou totalmente a distância, podendo gerenciar os sistemas de qualquer local geográfico com acesso à internet.

Tipos de Servidores e Serviços de Rede

Em uma rede de computadores, os servidores podem agregar diversos serviços, ou seja, hospedar diferentes tipos de serviços que irá disponibilizar aos clientes da rede, como podem, também, atender a uma única tarefa – isso dependerá exclu-

sivamente da necessidade de cada rede de computadores. Existe atualmente uma ampla variedade de servidores, com os mais variados fins. A tabela 8 apresenta alguns dos principais servidores, suas características e descrições.

TABELA 8 – Tipos de serviços para Servidores de Rede

SERVIDOR	FUNÇÃO	CARACTERÍSTICAS
Servidor de Arquivos	Armazenar dados compartilhados entre diferentes usuários de uma rede de computadores.	O servidor de arquivos mais comum em ambientes Microsoft é denominado Active Directory, que além de gerenciar o compartilhamento de arquivos, pastas e subpastas, controla também usuários, grupos e listas de acesso. No sistema operacional Linux, quem realiza esta tarefa é o servidor SAMBA.
Servidor de Impressão	Processar os pedidos de impressão demandados pelos usuários da rede de computadores e ordenar a impressão (fila).	Cotas de impressão podem ser configuradas aos usuários, como forma de limitar e controlar a quantidade de impressões.
Servidor de E-mail	Armazenar, gerenciar e processar o envio e recebimento de e-mails.	Pode ser instalado um serviço de gerenciamento de e-mails como o Postfix (Linux), assim como pode ser utilizado um servidor na nuvem para tal serviço (como o e-mail do Google corporativo).
Servidor Web	Armazenar as páginas dos usuários (sites) que ficarão públicas na internet (URL específica).	Geralmente estes servidores funcionam juntamente com outros servidores que se comunicam entre si, como é o caso de um SGBD e uma linguagem de interpretação (ASP, PHP, etc.).
Servidor de DNS	Traduzir endereços digitados nas URLs dos navegadores em endereços IPs.	O servidor mais tradicional nesta categoria é o servidor BIND (Linux), onde é possível configurar uma série de características relacionadas e resolução de nomes.
Servidor de FTP	Permitir a transferência de arquivos entre uma máquina cliente e o servidor.	É possível adicionar uma camada de segurança neste serviço utilizando o protocolo SFTP, garantindo uma maior confiabilidade na troca de dados.
Servidor de Acesso Remoto	Permitir o acesso remoto (de fora da rede) a um servidor da rede local.	Com a implementação do protocolo SSH, presente na camada de aplicação, é possível prover acesso seguro, mediante mecanismos de autenticação externamente a rede local que se deseja administrar.

FONTE: Autores.

Tipos de sistemas operacionais de servidores

Os sistemas operacionais de computadores servidores caracterizam-se como um tipo específico de software projetado para tal função, ou seja, prover serviços de rede que podem ser configurados para que os demais clientes da rede tenham acesso e usem de tais recursos e serviços em uma rede de computadores. Os sis-

temas operacionais de servidores podem ser pagos (versões Microsoft Windows, como o Windows server 2012, 2016, etc., onde ao adquirir o mesmo geralmente paga-se pelo sistema operacional e pela quantidade de clientes que poderão se conectar ao mesmo) ou livres (*free*) como as versões baseadas em Linux (Ubuntu Server, Debian, OpenSuse, RedHat, entre outros, podendo estas serem alteradas, modificadas e distribuídas livremente). Nesta categoria de sistema operacionais para computadores servidores, destacam-se (são mais populares) as versões Windows, Linux e Mac OS, conforme pode ser visualizado na tabela 9.

TABELA 9 – Sistemas Operacionais para Servidores

WINDOWS	LINUX	MAC OS X
Windows 2000 Server	Suse	Mac OS X v10.0 Cheetah
Windows 2003 Server	Debian	Mac OS X v10.1 Puma
Windows 2008 Server	Ubuntu	Mac OS X v10.2 Jaguar
Windows 2012 Server	Red Hat	Mac OS X v10.3 Panther
Windows 2016 Server	Fedora	Mac OS X v10.4 Tiger
	Slackware	Mac OS X v10.5 Leopard
	CentOS	Mac OS X v10.6 Snow Leopard
	OpenSuse	Mac OS X v10.7 Lion
	Gentoo	Mac OS X v10.8 Mountain Lion
	CoreOS	Mac OS X v10.9 Mavericks
		Mac OS X v10.10 Yosemite
		Mac OS X v10.11 El Capitan
		Mac OS X v10.12 Sierra
		Mac OS X v10.13 High Sierra

FONTE: Autores.

6.1.2 Instalando e Configurando um servidor local no sistema operacional Windows – Estudo de Caso

Como forma de facilitar nosso entendimento sobre servidores e sua utilização, faremos agora um estudo de caso utilizando um software que faz a instalação local de um servidor Web para Windows denominado XAMPP. O XAMPP é um software freeware de fácil instalação, que conta com um servidor Web Apache, um sistema gerenciador de banco de dados (MySQL), suporte às linguagens de programação PHP e Perl, além de diversas outras ferramentas que podem ser instaladas conjuntamente, como Drupal, Wordpress, Moodle, entre outros. Então, vamos ao trabalho!

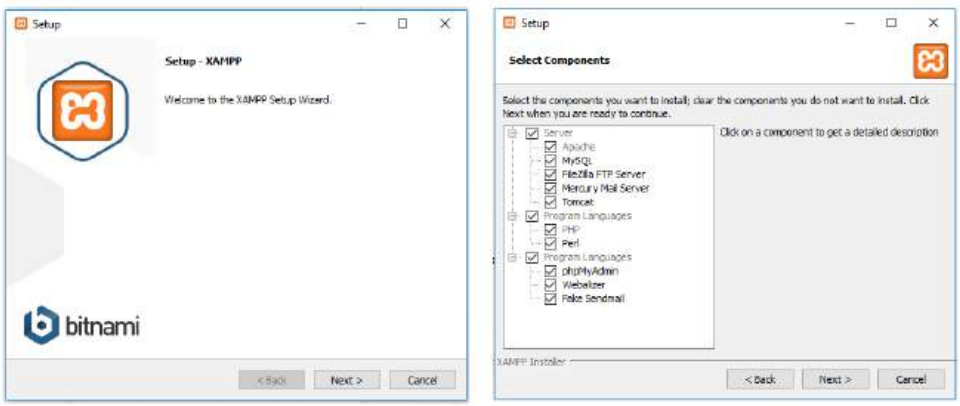
O primeiro passo para podermos utilizar a ferramenta é acessar o site oficial da mesma (https://www.apachefriends.org/pt_br/index.html) e realizar o download (para isso basta clicar em XAMPP para Windows – balão vermelho em destaque), conforme figura 92 (o tamanho do arquivo é de aproximadamente 125MB e o tempo de download dependerá da velocidade de sua conexão à internet).

FIGURA 92 – Site oficial da ferramenta XAMPP

FONTE: XAMPP. Disponível em: https://www.apachefriends.org/pt_br/index.html

O segundo passo, de posse do arquivo baixado (localizar em que pasta você fez o download do arquivo), é executar o mesmo (para isso basta dar dois cliques sobre o arquivo e ter permissões junto ao sistema operacional para instalação de softwares). Realizado o passo acima, uma tela semelhante à figura 93, irá aparecer para iniciarmos a instalação e personalização do XAMPP. Clicamos no botão "Next" e novamente "Next", deixando todas as caixas de seleção habilitadas, conforme ilustração.

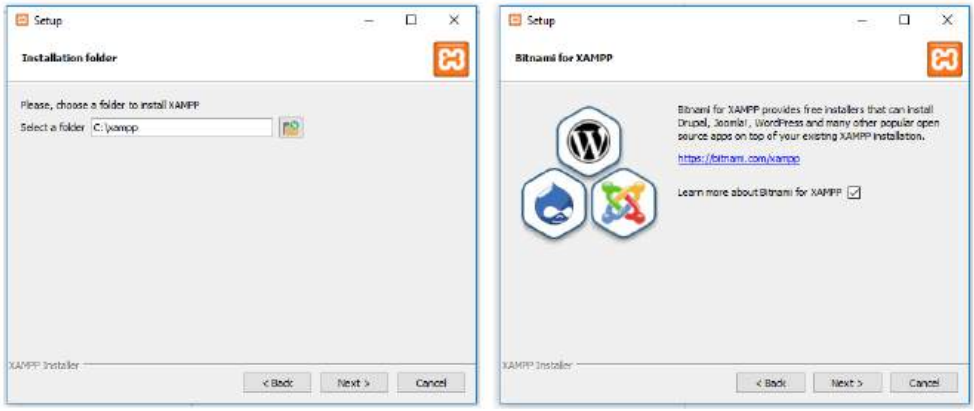
FIGURA 93 – Instalação inicial do XAMPP



FONTE: Autores

O terceiro passo é escolher o local onde o XAMPP será instalado. Em seguida, deixaremos selecionada a opção "Learn more about Bitnami for XAMPP" para conhecer mais sobre as ferramentas externas que estão sendo instaladas juntamente com o XAMPP. A figura 94, ilustra estas duas etapas.

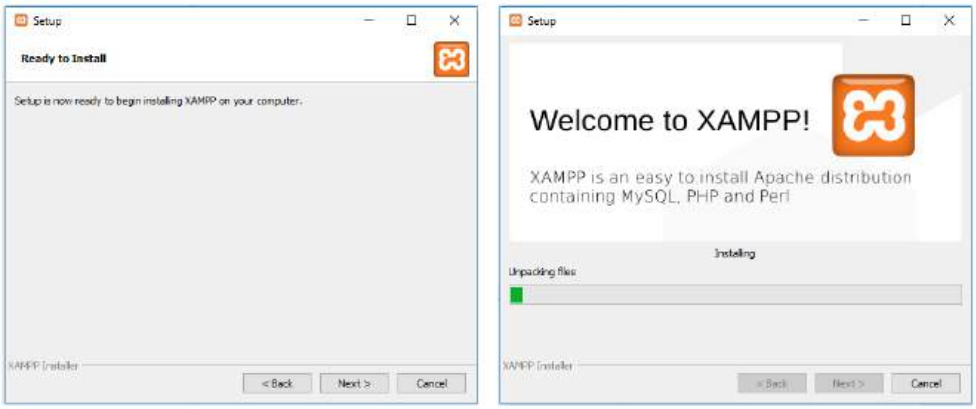
FIGURA 94 – Local de instalação e softwares adicionais a serem instalados com o XAMPP



FONTE: Autores

O quarto passo é clicar em "Next" novamente para finalmente iniciar a instalação. A figura 95 demonstra o processo de instalação do XAMPP juntamente com a barra de progresso da mesma.

FIGURA 95 – Local de instalação e softwares adicionais a serem instalados com o XAMPP



FONTE: Autores

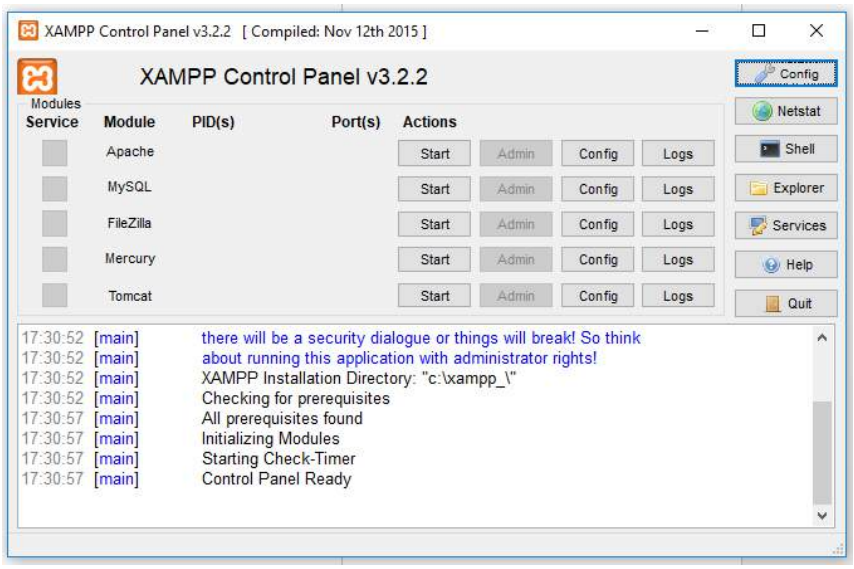
Completado o processo de instalação uma tela semelhante à figura 96 será mostrada, perguntando se você deseja iniciar neste momento o painel de controle do XAMPP ("*Do you want to start the Control Panel now?*"). Devemos clicar na opção "*Finish*".

FIGURA 96 – Inicialização do Painel de Controle do XAMPP

FONTE: Autores

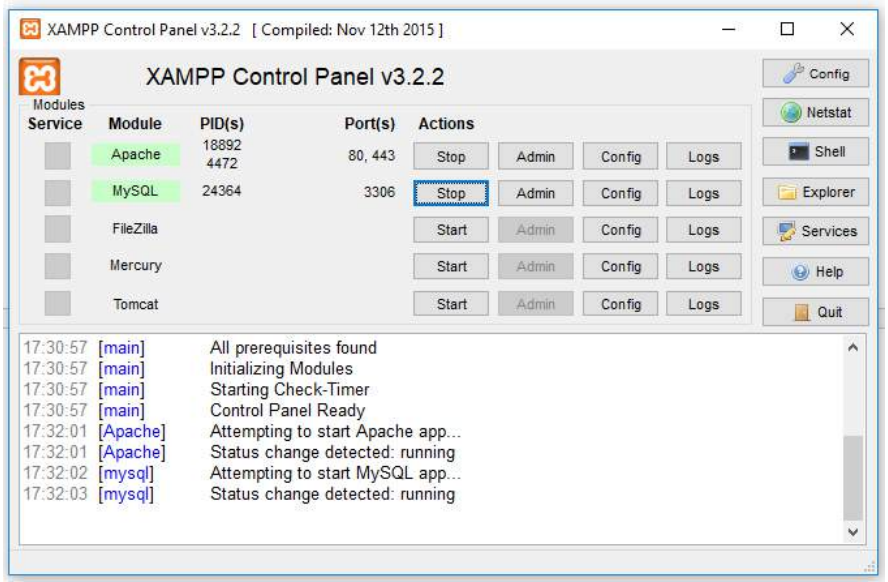
O quinto passo, considerando aberto o Painel de Controle do XAMPP, conforme figura 97, é iniciarmos os serviços do Apache e MySQL. Para isso, devemos clicar sobre o primeiro e segundo botão "Start", conforme balão vermelho em destaque na figura 98.

FIGURA 97 – Painel de Controle do XAMPP



FONTE: Autores

FIGURA 98 – Painel de Controle do XAMPP com Apache e MySQL



FONTE: Autores

O sexto passo, finalizado o processo de instalação e inicialização dos serviços básicos, é finalmente acessar nosso servidor web local, para poder utilizar de seus recursos. Para isso, basta abrir um navegador de sua preferência e digitar o seguinte comando na URL: http://localhost. Se uma tela semelhante à figura 99 for exibida em seu navegador, parabéns, você conclui a instalação e configuração do servidor XAMPP com sucesso!

FIGURA 99 – Acesso a página inicial do servidor XAMPP

FONTE: Autores

6.2
FERRAMENTAS PARA EDUCAÇÃO A DISTÂNCIA

Este subcapítulo destina-se a apresentar as principais ferramentas para implantação de soluções para EaD, que possam de fato ser utilizadas para este fim. Entretanto, faz-se necessário entender alguns conceitos básicos que fazem parte deste contexto. E é exatamente isto que veremos a partir de agora.

O que é plataforma EaD?

Uma plataforma EaD corresponde a um sistema de gestão de aprendizagem, com o objetivo de promover o ensino online de forma eficiente e bem estruturada, utilizando uma metodologia pedagógica específica para o ambiente a distância. É através de uma plataforma EaD que cursos a distância são ofertados, ministrados e gerenciados, pelos respectivos professores, tutores, orientadores, entre outros profissionais.

Como funcionalidades de uma plataforma EaD, temos:

- Personalização (definir menus, estilos, cores, padrões, etc.).
- Página de e-commerce (que pode ou não ser implementada, dependendo do tipo de plataforma a ser implementada/gerenciada).
- Integrações (com recursos, plug-ins ou componentes externos).
- Gestão completa de alunos, professores e tutores.
- Criação de provas e diferentes tipos de avaliações.
- Comunicação com o aluno (através de mensagens, chat, fórum, etc.).

Em resumo, uma plataforma EaD corresponde a toda uma infraestrutura preparada para dar suporte ao ensino a distância e demais fluxos que o mesmo necessitar. Já um AVA (Ambiente Virtual de Aprendizagem), corresponde a um recurso (muito importante) presente dentro de uma plataforma EAD.

AVA (Ambiente Virtual de Aprendizagem)

Quando nos referimos a um Ambiente Virtual de Aprendizagem ou simplesmente AVA, podemos conceituá-lo como um espaço online de gerenciamento de alunos, turmas, conteúdos e cursos, que permite entre outras funções a troca de informações e interação entre seus participantes com o objetivo de propiciar um ambiente online de ensino e aprendizagem. Além do AVA, o termo LMS (*Learning Management System*) ou Sistema de Gerenciamento de Aprendizado também é utilizado com frequência para a mesma designação. Ao se referir a um AVA ou LMS, estamos fazendo referência a um ambiente de ensino a distância

(EaD), ou seja, o ambiente online utilizado para a execução e gerenciamento de conteúdos, turmas, alunos, etc.

Ainda, em um AVA temos fundamentalmente duas categorias principais: a parte tecnológica envolvida e a parte pedagógica. Quanto a parte tecnológica, a mesma se constitui do gerenciamento de cursos, alunos, senhas, turmas, acompanhamento e relatório de acessos, publicação de conteúdo em diferentes formatos, correção de atividades e ferramentas de comunicação como fóruns, chats, entre outros. Já a parte pedagógica refere-se à abordagem educacional que norteia o desenvolvimento computacional, por exemplo, o tipo de aula a ser ministrada, as múltiplas formas de disponibilização do conteúdo (múltiplos estímulos), as diferentes formas de avaliação a serem aplicadas, etc.

Vantagens em se utilizar um AVA

- suporte para a educação a distância totalmente online;
- apoio às atividades presenciais e semipresenciais, também chamados de *blended learning*;
- registro e acompanhamento de etapas de uma atividades, avaliações, acessos, entre outros;
- acesso a materiais didáticos, downloads, links, vídeos, etc;
- interação constante e ferramentas de apoio a produção de materiais.

SAIBA MAIS: https://www.edools.com/blended-learning/

Lembrando que a escolha de um ambiente virtual de aprendizagem deve levar em conta, o projeto institucional previsto, a abordagem pedagógica adotada e o público participante.

Ferramentas e recursos existentes nos ambientes virtuais de aprendizagem

Quanto aos recursos existentes em um Ambiente Virtual de Aprendizagem, podemos dizer que os mesmos podem ser classificados em cinco categorias principais, os quais são: suporte para conteúdos, comunicação e interação entre os participantes, ferramentas de auxílio ao aluno, atividades e avaliação e por fim, gestão de alunos e do curso. Veremos agora uma breve descrição de cada categoria.

1 – Suporte para conteúdos: permite a utilização e suporte a diferentes formatos de arquivos, como os tradicionais PDF, PPT e ZIP; scorm; glossário (termos mais utilizados em determinado conteúdo) e perguntas frequentes (repositório que pode ser criado como forma de armazenar e catalogar as perguntas mais frequentes dos alunos, sem que haja repetição deste conteúdo em outras seções do curso).

2 – Comunicação e interação entre os participantes: fórum (com o objetivo de estimular a troca de ideias/experiências), chat, wiki (produção colaborativa de textos), grupos (de atividades, discussão), comunicação instantânea via mensagens e e-mail (que pode ser configurado e utilizado de dentro da própria ferramenta).

3 – Ferramentas de auxílio ao aluno: perfil do mesmo (podendo ser personalizado com uma grande variedade de informações), calendário, acompanhamento de notas e atividades (de turmas, semestres, avaliações individuais); relatórios, entre outros.

4 – Atividades e avaliação: questionários com avaliação automática (verdadeiro ou falso, lacunas, múltipla escolha, etc.); questões dissertativas; envio de arquivos como atividades; revisão entre pares.

5 – Gestão de alunos e do curso: inscrições em geral, usuários e senhas de acesso; controle de matrículas em cursos, estatísticas e relatórios de acessos (contendo data, hora, endereço IP, entre outros); administração de alunos, tutores e professores; backup e restauração de cursos; configuração e customização de cursos; pesquisa de opinião e emissão de certificados.

Exemplos de AVAS

Como exemplos de ambientes virtuais de aprendizagem, temos ferramentas gratuitas e pagas. As ferramentas gratuitas permitem que seu sistema possa ser modificado, redistribuído, adaptado e conta com uma comunidade colaborativa no desenvolvimento de plug-ins e demais extensões no intuito de aprimorar estes ambientes. Já as versões pagas, oferecem diferentes funcionalidades, mas cobram geralmente mensalidades, para utilização e gerenciamento de cursos, e respectivas turmas e alunos.

São exemplos de AVAS gratuitos:

- Moodle (https://moodle.org/?lang=pt_br).
- e-Proinfo (http://e-proinfo.mec.gov.br/).
- Teleduc (http://www.teleduc.org.br/?q=downloads).
- Dokeos (https://www.dokeos.com/).
- Sakai (https://sakaiproject.org/).
- Canvas (https://www.canvaslms.com/), etc.

Já entre os AVAS comerciais, estão:

- Blackboard (http://www.blackboard.com/index.html).
- Webaula (http://webaula.com.br/index.php/pt/).
- Saba (https://www.saba.com/products/learning/learning-management-system), entre outros.

6.2.1 Estudo de Caso – Moodle

Esta seção tem o objetivo de ensinar um passo-a-passo da instalação do Moodle deixando o mesmo pronto para utilização. A ideia é apresentar um caminho para usuários que queiram implementar a ferramenta em um servidor web local ou na grande rede. Para complementar este estudo de caso, alguns links são compartilhados ao final da seção como forma a prover mais informações sobre o ambiente de aprendizagem em questão.

O nome MOODLE é o acrônimo de *"Modular Object-Oriented Dynamic Learning Environment"*, ou em tradução livre "Ambiente de Aprendizagem Dinâmico Modular Orientado a Objetos". Trata-se de um software livre, de apoio a aprendizagem, executado num ambiente virtual.

SAIBA MAIS: definição disponível em: https://pt.wikipedia.org/wiki/Moodle.

Características do ambiente virtual de aprendizagem Moodle

Utilizado no contexto do *e-learning*, o ambiente permite a criação de cursos "on-line", páginas de disciplinas, grupos de trabalho e comunidades de aprendizagem, estando disponível em 75 (setenta e cinco) idiomas diferentes. Conta com mais de 25.000 (vinte e cinco mil) websites registrados, em mais de 175 (cento e setenta e cinco) países.

- Software disponibilizado livremente na forma de software livre (licença GNU/GPL), podendo ser instalado tanto em sistemas Windows, quanto Linux.
- Requisitos técnicos para instalação e utilização:

Servidor: servidor WEB com suporte a PHP.

Cliente: navegador e software específico para visualização dos recursos (PDF, DOC, etc).

- Informações do projeto Moodle:

Desenvolvedor: Martin Dougiamas.

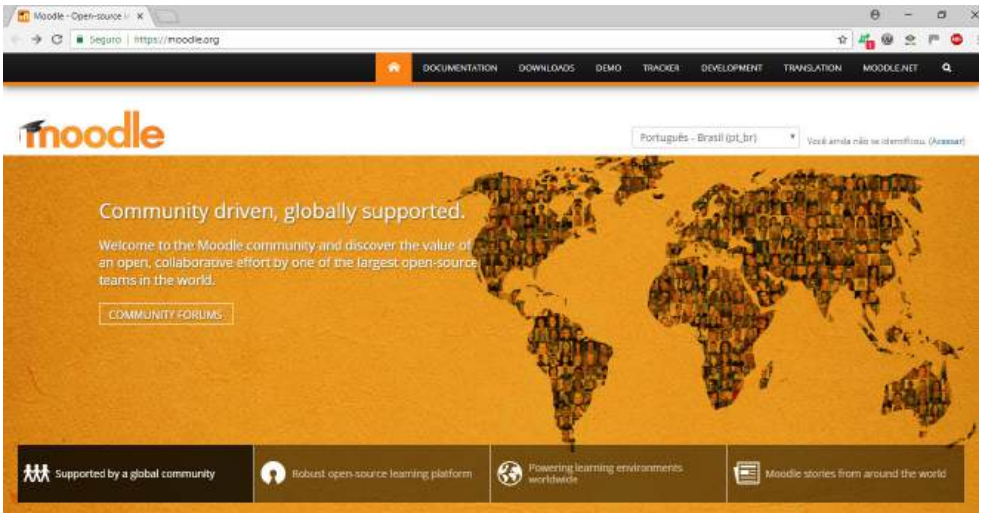
Lançamento: 2001.

Linguagem: PHP.

Sistema Operacional: Multiplataforma.

Na figura 100, é apresentado o site oficial do Moodle e diversas informações sobre suas características, funcionalidades, ferramentas, plug-ins, suporte, entre outros.

FIGURA 100 – Site oficial do Ambiente Virtual de Aprendizagem Moodle

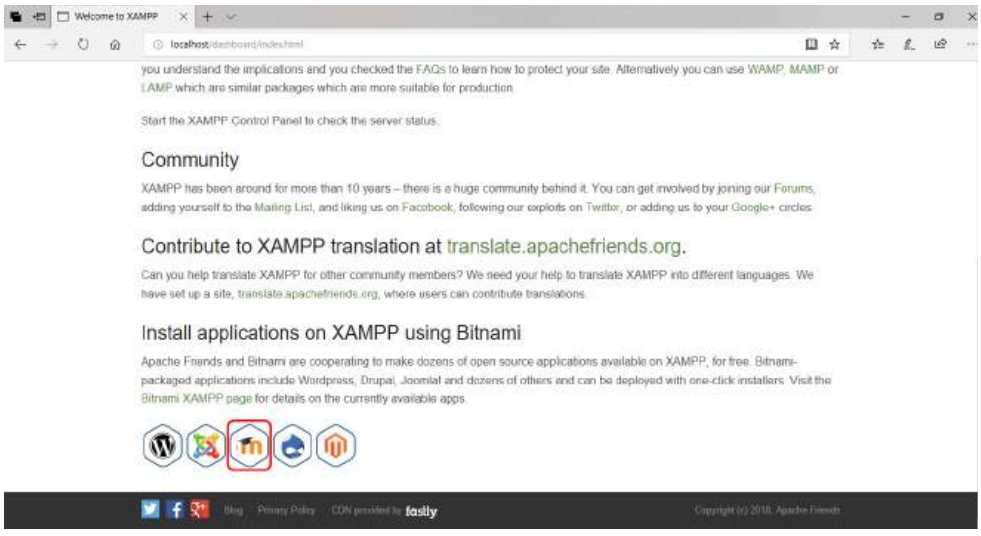


FONTE: Moodle. Disponível em: http://moodle.org

Instalando e configurando o Moodle no servidor local XAMPP

Como forma de configurarmos e utilizarmos o ambiente Moodle localmente para que seja possível conhecer as potencialidades da ferramenta, criar turmas, adicionar usuários, entre outras tantas funções que o ambiente Moodle possui, faremos agora a configuração do mesmo junto a ferramenta XAMPP, que instalamos e configuramos na seção 6.1.3. Nosso primeiro passo agora é abrir um navegador e digitar o seguinte endereço: http://localhost (não esqueça de verificar se o painel de controle do software XAMPP está ativo e que os serviços Apache e MySQL estão iniciados). Devemos descer com a barra de rolagem até o final da página e clicar no ícone do Moodle, conforme figura 101.

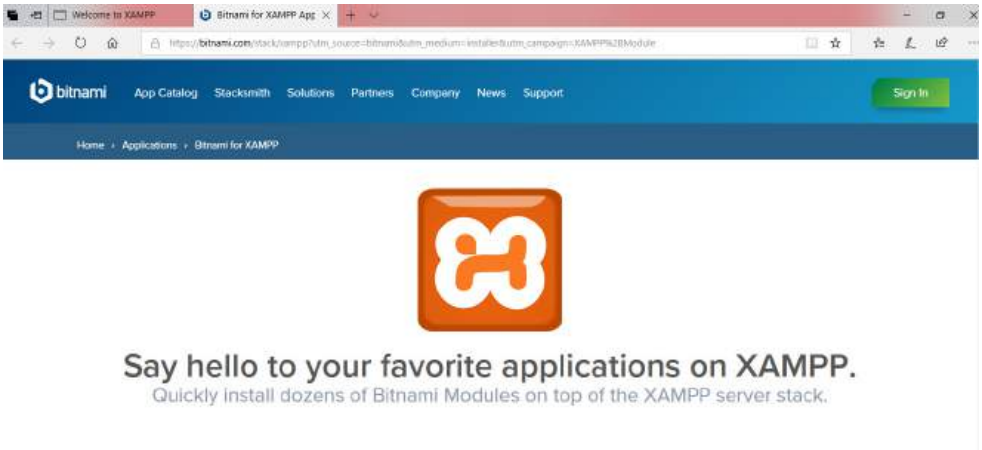
FIGURA 101 – Acessando localhost e iniciando instalação do Modulo do ambiente Moodle



FONTE: Autores

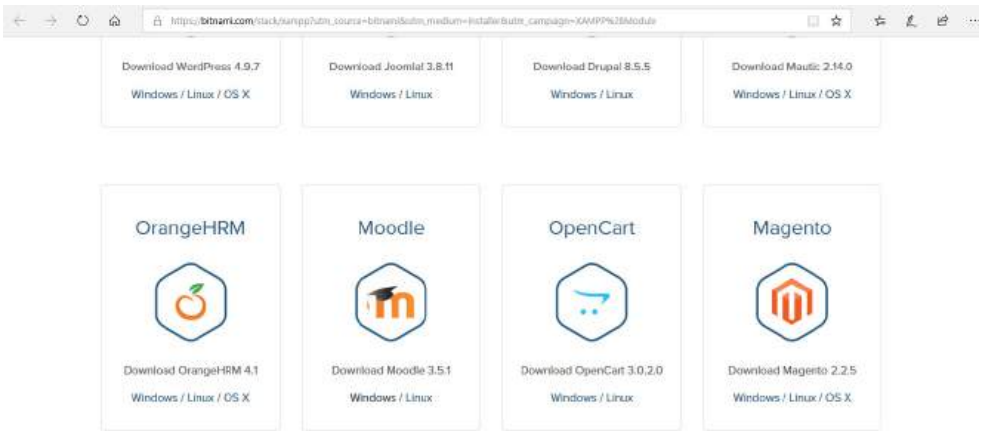
Você será redirecionado ao site: https://bitnami.com/stack/xampp?utm_source=bitnami&utm_medium=installer&utm_campaign=XAMPP%2BModule, conforme figura 102. Ao descer com a barra de rolagem, repare que uma grande quantidade de módulos de diferentes ferramentas está disponível para download e instalação junto ao XAMPP. Desta forma, devemos localizar e clicar sobre o Módulo "Moodle – Windows", conforme representado na figura 103.

FIGURA 102 – Site bitnami contendo os módulos que podem ser adicionados ao XAMPP



FONTE: Autores

FIGURA 103 – Localização do Módulo Moodle para download



FONTE: Autores

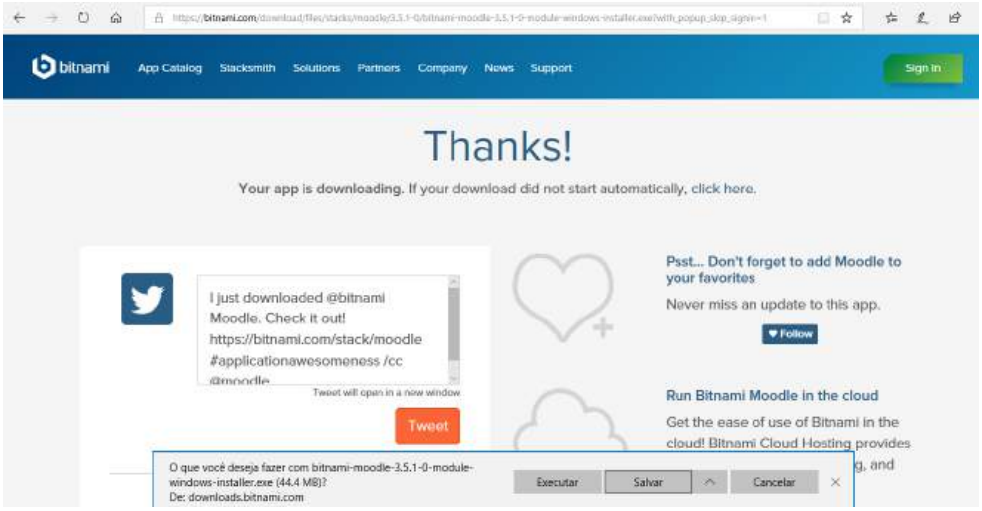
Ao aparecer a mensagem representada na figura 104, basta clicar na opção *"No thanks, just take me to the download"*, para que o download seja iniciado.

FIGURA 104 – Fazer download do modulo Moodle sem autenticação

FONTE: Autores

O próximo passo é salvar o arquivo "bitnami-moodle-3.5.1-0-module-windows--installer.exe" com tamanho aproximado de 45MB em uma pasta em seu computador (por padrão Windows geralmente esta pasta é "Downloads"), conforme apresenta a figura 105.

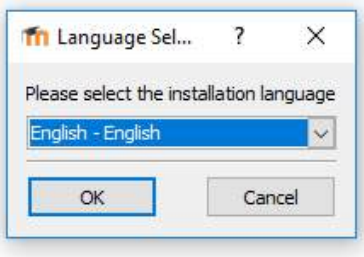
FIGURA 105 – Tela de início de download do modulo Moodle para XAMPP



FONTE: Autores

Concluído o download do arquivo, o próximo passo é realizar a instalação do módulo Moodle para o XAMPP. Para isso clique duas vezes no arquivo que acabou de fazer o download, uma tela semelhante a figura106, será exibida, onde devemos selecionar a linguagem. Por padrão manteremos a linguagem em Inglês selecionada e clicaremos no botão "OK".

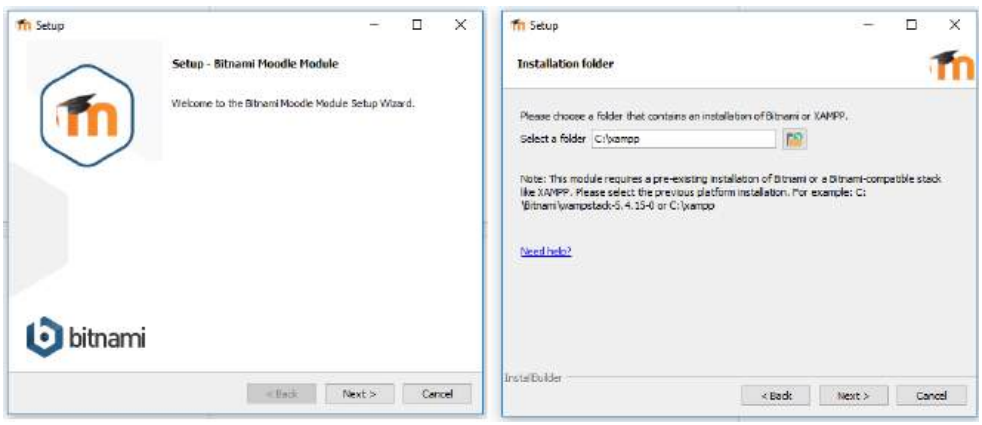
FIGURA 106 – Seleção de linguagem para instalação do modulo Moodle para o XAMPP



FONTE: Autores

Na sequência, conforme figura 107, clicamos no botão "Next" para iniciar o processo de instalação do módulo Moodle e em seguida selecionamos o local onde está instalado o nosso servidor local XAMPP, para que o plug-in seja instalado em uma subpasta deste diretório. Realizados estes dois procedimentos basta clicar no botão "Next" novamente.

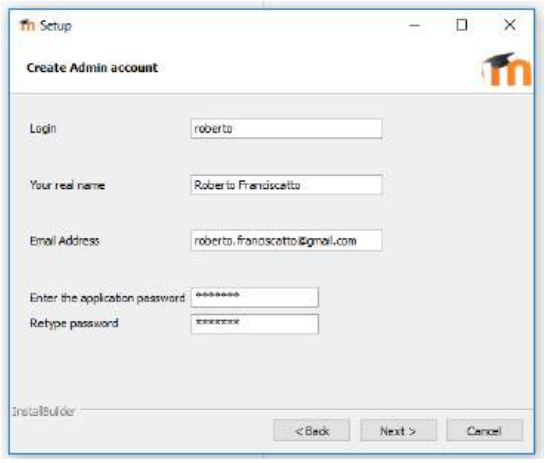
FIGURA 107 – Tela de início de instalação do módulo e localização da pasta com o XAMPP instalado



FONTE: Autores

A próxima tarefa é informar os dados relativos a criação de conta de administrador junto ao Moodle. Para isso, deveremos informar um nome de login (campo *"Login"*), seu nome completo (*"Your real name"*), seu e-mail (*"Email Address"*), definir uma senha (*"Enter the application password"*) e repetir a mesma (*"Retype Password"*), logo após informar estes dados, clicar no botão "Next", conforme figura 108.

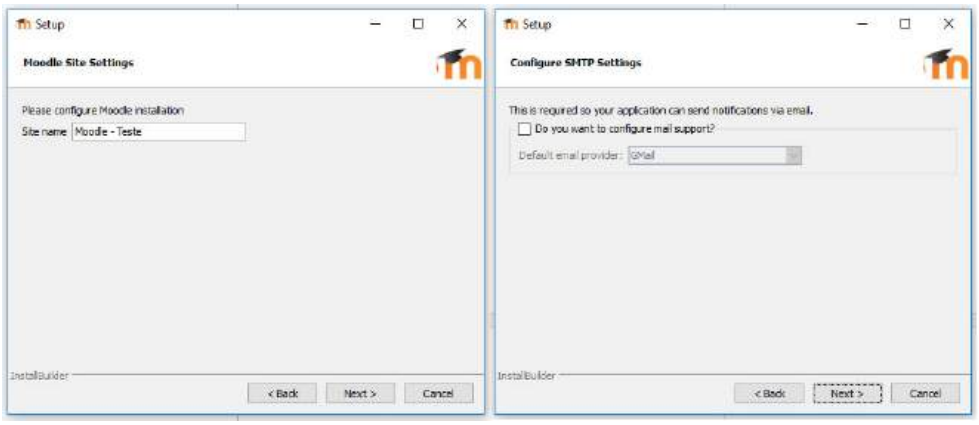
FIGURA 108 – Criação da conta de Administrador



FONTE: Autores

Em seguida, definimos um nome para o site e desmarcamos a opção "*Do yo want to configure mail support?*", conforme pode ser visualizado na figura 109.

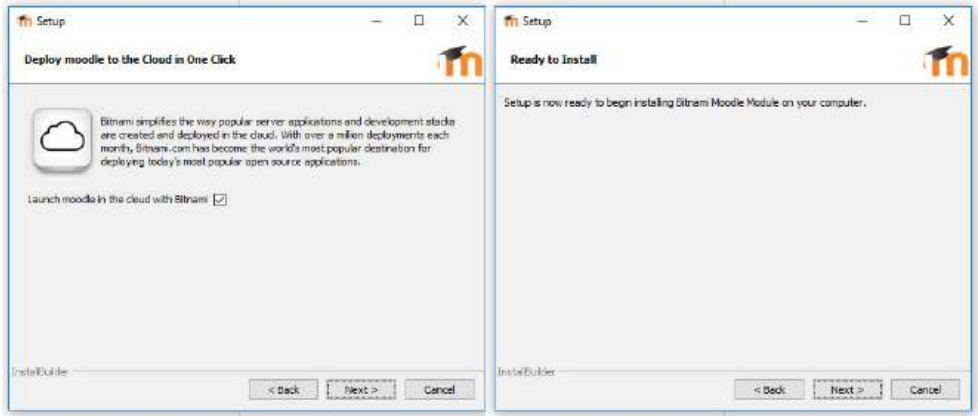
FIGURA 109 – Nome do site e configurações de SMTP



FONTE: Autores

Como sequência da instalação do módulo Moodle para o XAMPP, o próximo passo será desabilitar a opção *"Launch Moodle in the cloud with Bitnami"* e clicar no botão "Next" duas vezes, para que a instalação do módulo possa enfim ter início, conforme podemos observar na figura 110.

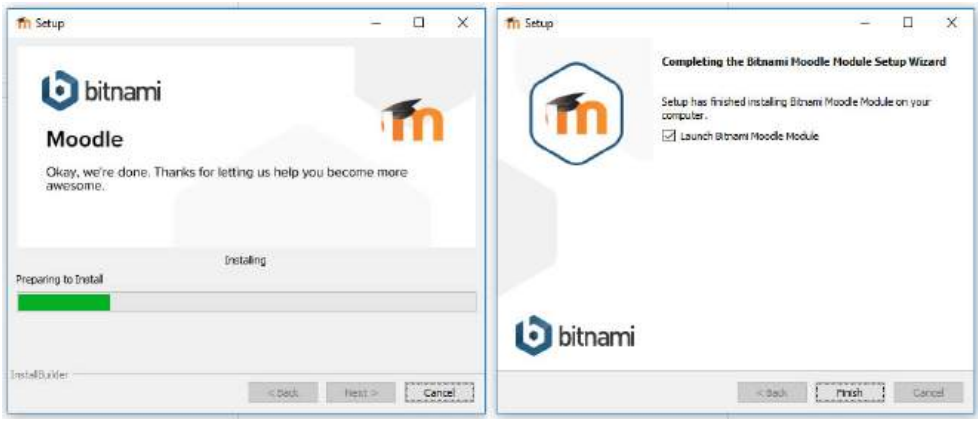
FIGURA 110 – Desabilitar cloud e iniciar instalação do módulo Moodle



FONTE: Autores

O processo de instalação com a respectiva barra de progresso será mostrado, sendo a sua velocidade proporcional as configurações de hardware do computador em questão. Ao final da instalação uma tela semelhante a apresentada na figura 111, será exibida.

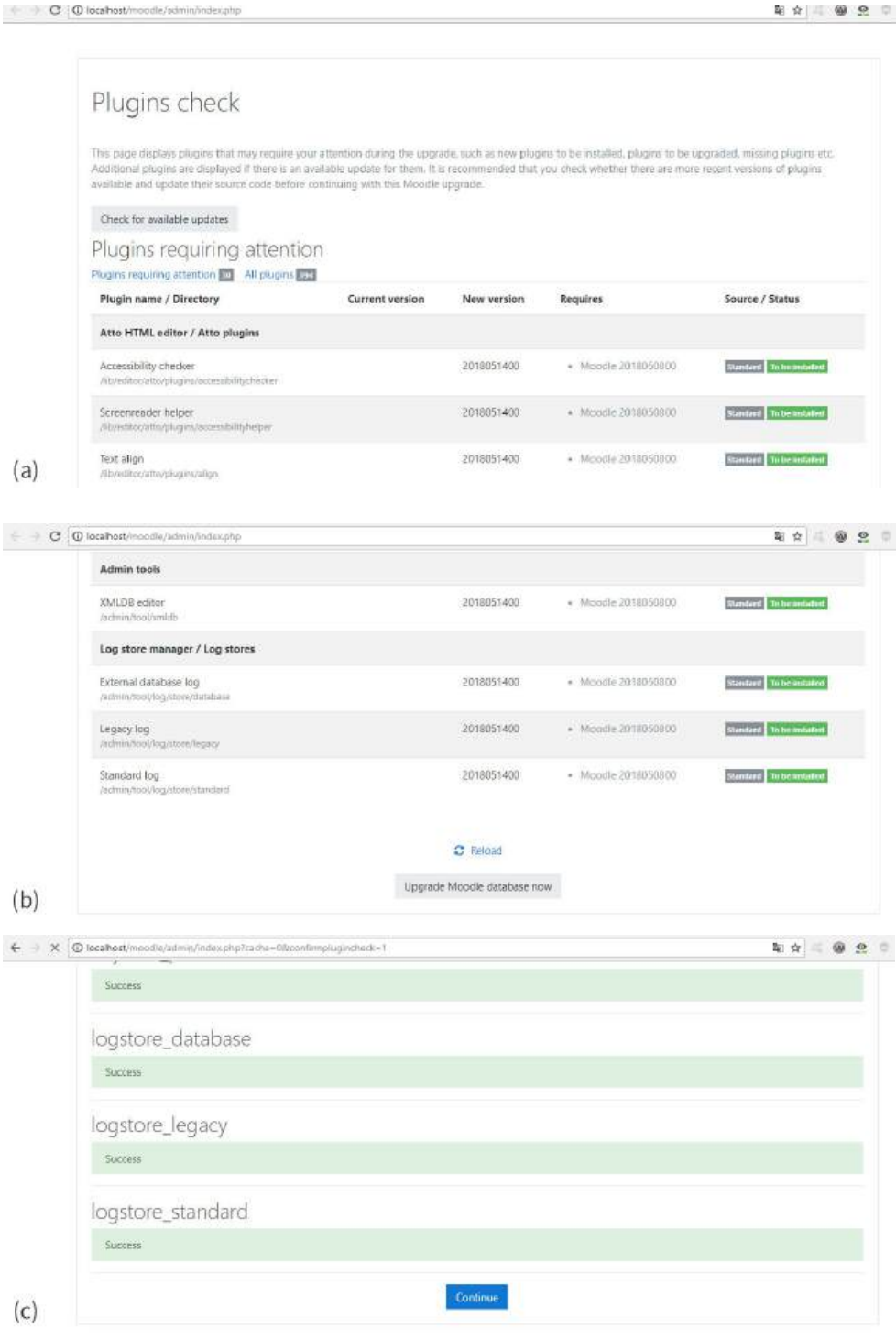
FIGURA 111 – Processo de instalação e execução do modulo Moodle



FONTE: Autores

Ao clicar no botão “Finish”, o usuário é direcionado para o navegador web, com as operações finais de configuração do módulo Moodle. A primeira etapa de verificação é relativa aos plug-ins instalados, conforme figura 112 (quadro “a”). Devemos ir com o cursor do mouse até o final da página (rodapé) e clicar na opção *“Upgrade Moodle Database Now”* (quadro “b”) e em seguida clicar no botão “Continue” (quadro “c”).

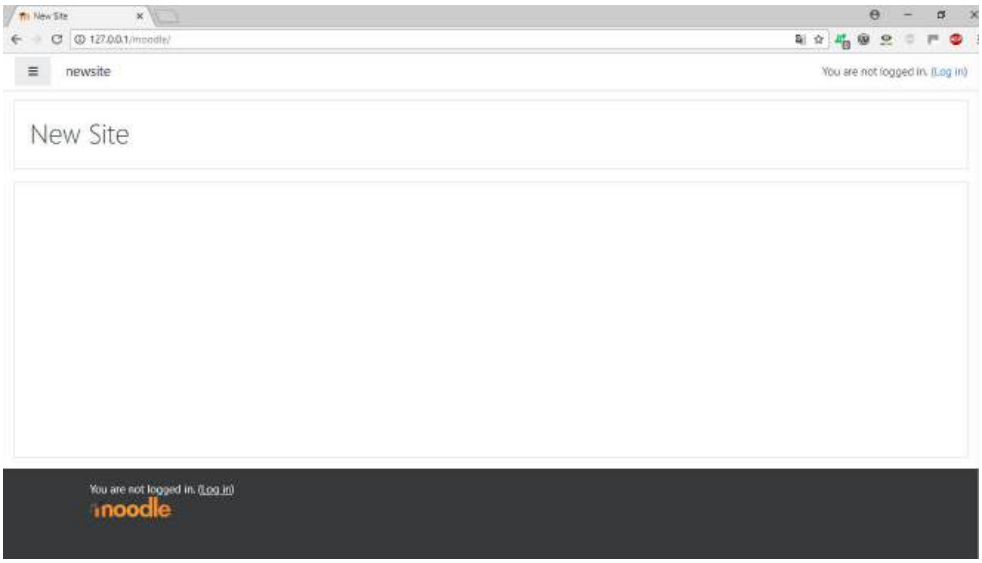
FIGURA 112 – Checagem de plug-ins



Fonte: Autores

Finalmente, chegamos ao final da instalação e conforme figura 113, esta é a tela inicial do Moodle plenamente funcional e pronto para ser usado localmente em um servidor utilizando a ferramenta XAMPP.

FIGURA 113 – Tela Inicial do sistema Moodle junto ao software XAMPP



FONTE: Autores

ATIVIDADES DE REFLEXÃO OU FIXAÇÃO

1.Qual a função de um Servidor de Rede? Explique em detalhes.

2. Cite 3 tipos de serviços de servidores de rede, explicando cada um deles.

3. Na tabela referente aos sistemas operacionais para servidores, selecione um sistema operacional Windows, um Linux e um MAC OS X e descreva as principais características de cada um (para isso faça uma pesquisa online sobre o SO escolhido).

4. Diferencie plataforma EaD de AVA, expondo as características de cada um.

5. Escolha dois AVAs gratuitos e dois comerciais, pesquise sobre as vantagens e desvantagens de cada um e construa uma tabela comparativa entre eles.

CONSIDERAÇÕES FINAIS

Este material apresentou os principais conceitos sobre a montagem e manutenção de computadores. Através deste material, você obteve uma visão geral de como funciona um computador e como os principais componentes de hardware e software se relacionam para colocar um computador em operação. O material também apresentou a evolução dos computadores, compreendendo desde os primeiros dispositivos criados para executar operações matemáticas até as principais contribuições tecnológicas dos circuitos integrados. Também estudamos os principais componentes de hardware do computador, onde abordamos o propósito de cada componente, fornecendo detalhes sobre seu modo de operação e descrevendo a função de cada componente em relação aos demais. Estudamos ainda como usar os simuladores para criar um ambiente virtual capaz de colocar em prática as técnicas de montagem e manutenção de computadores, dispensando a necessidade da aquisição dos componentes físicos reais do computador apenas para obter um contato inicial com estas técnicas. Aprendemos ainda sobre a instalação de diferentes tipos de sistemas operacionais e como adicionar e remover os programas aplicativos utilizados pelos usuários comuns. Para finalizar, estudamos como montar um computador, abordando os principais conceitos sobre as técnicas envolvidas neste processo.

REFERÊNCIAS

ALMEIDA, Alan. **Como Instalar e Configurar Moodle no Ubuntu 14.04.** Ubuntu Dicas e Tutoriais. Disponível em: <https://ubuntu.blog.br/como-instalar-e-configurar-moodle-no-ubuntu-14-04/>. Acesso em: 11 mar. 2018.

CERT.BR (São Paulo). Comitê Gestor da Internet No Brasil. **Cartilha de Segurança de redes.** Disponível em: <https://cartilha.cert.br/redes/>. Acesso em: 14 mai. 2018.

CÔNSOLO, Adriane. **O que é Ambiente Virtual de Aprendizagem?** CoachEAD. Disponível em: <http://www.coachead.com.br/ambiente-virtual-de-aprendizagem/>. Acesso em: 19 abr. 2018.

EDOOLS. **O que é plataforma EAD?** FAQ. Disponível em: <https://www.edools.com/faq/o-que-e-plataforma-ead/>. Acesso em: 01 mai. 2018.

KUROSE, Keith W. Ross; JAMES F. 2010. **Redes de Computadores e a Internet:** Uma Abordagem Top-down. S.l.: Addison-Wesley, 2010.

MAIA, Luiz Paulo. **Arquitetura de Redes de Computadores.** 2. ed. Rio de Janeiro: Editora LTC, 2015

MARSHALL, Carrie, et al. **The best free firewall 2018.** TechRadar. Disponível em: <https://www.techradar.com/news/the-best-free-firewall>. Acesso em: 01 mai. 2018.

MORIMOTO, Carlos Eduardo. **Redes, Guia Prático.** 2. ed. Guia do Hardware. 2008. Disponível em http://www.hardware.com.br/livros/redes. Acesso em: 12 fev. 2018.

MORIMOTO, Carlos Eduardo. **Servidores Linux, Guia Prático.** Guia do Hardware. 2008. Disponível em: <http://www.hardware.com.br/livros/servidores-linux/.> Acesso em: 20 fev. 2018.

MOTTA, Sérgio. **Top 5 anti-malwares gratuitos para Windows**. Top Freewares. Disponível em: <https://www.topfreewares.com.br/top-5-anti-malwares-gratuitos--windows/>. Acesso em: 17 jun. 2018.

PERCÍLIA, Eliene. **Segurança em Redes de Computadores.** Brasil Escola. Disponível em: <https://brasilescola.uol.com.br/informatica/seguranca-redes.htm>. Acesso em: 07 fev. 2018.

PINHEIRO, S. Maurício José. **Gerenciamento de Redes de Computadores:** Uma Breve Introdução. Projeto de Redes. Disponível em: <https://www.projetoderedes.com.br/artigos/artigo_gerenciamento_de_redes_de_computadores.php>. Acesso em: 27 abr. 2018.

SANTOS, Marcel. **Como funciona a Internet e a World Wide Web.** 2015. Disponível em: <https://tableless.com.br/como-funciona-internet-e-world-wide-web/>. Acesso em: 13 mar. 2018.

SILVA, Camila Ceccato da. **Redes de Computadores** – Conceito e Prática. Santa Cruz do Rio Pardo – SP: Viena, 2010.

SCRIMGER, Rob. **TCP/IP a Bíblia**. Rio de Janeiro: Campus, 2001.

TANENBAUM, Andrew S. **Redes de Computadores.** Tradução de Daniel Vieira. Revisão técnica de Isaías Lima. 5. ed. São Paulo: Pearson Prentice Hall, 2011.

TANENBAUM, Andrew S. **Organização estruturada de computadores.** 5. ed. São Paulo: Pearson Prentice Hall, 2007.

TANENBAUM, Andrew S. **Redes de Computadores**. São Paulo: Campus, 2003.

TELECO. **Gerenciamento e Monitoramento de Rede I:** Teoria de Gerência de Redes. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialgmredes1/pagina_3.asp>. Acesso em: 19 abr. 2018.

WHITE, Curt. **Redes de Computadores e Comunicação de Dados.** Tradução de All Tasks. Revisão técnica de Elvio J. Leonardo. 6. ed. São Paulo: Cengage Learning, 2012.

APRESENTAÇÃO DOS PROFESSORES RESPONSÁVEIS PELA ORGANIZAÇÃO DO MATERIAL DIDÁTICO

Este material foi elaborado por professores altamente qualificados na área da computação. **Ricardo Tombesi Macedo** é professor adjunto da Universidade Federal de Santa Maria (UFSM), obteve o título de Doutor em Ciência da Computação pela Universidade Federal do Paraná com período sanduíche na *Université de La Rochelle* na França, o título de Mestrado em Engenharia da Produção pela UFSM e de Bacharel em Ciência da Computação pela Universidade de Cruz Alta (Unicruz).

Roberto Franciscatto é professor adjunto da UFSM, doutor em Informática na Educação pela Universidade Federal do Rio Grande do Sul, mestre em Computação Aplicada pela Universidade do Vale do Rio dos Sinos (UNISINOS) e Bacharel em Informática pela Universidade Regional Integrada (URI).

Cristiano Bertolini é professor adjunto da UFSM, possui graduação em Ciência da Computação pela Universidade de Passo Fundo, mestrado em Ciência da Computação pela Pontifícia Universidade Católica do Rio Grande do Sul e doutorado em Ciência da Computação pela Universidade Federal de Pernambuco.

Guilherme Bernardino da Cunha é professor adjunto da UFSM, possui graduação em Ciência da Computação, mestrado em Ciências com ênfase em inteligência artificial e processamento digital de imagens e doutorado em Ciências com ênfase em Engenharia Biomédica pela Universidade Federal de Uberlândia.

A equipe de professores autores deste material acredita em você e deseja sucesso na sua formação profissional!