INTRODUÇÃO A REDES DE COMPUTADORES

CAPÍTULO 1 – O QUE SÃO REDES DE COMPUTADORES E MODELOS DE REFERÊNCIA?

Josiane Boeira Kirinus Fernandes

INICIAR

Introdução

Não se pode negar que as redes de computadores transformaram e estão transformando a maneira como os usuários e as organizações — dos mais variados segmentos e tamanhos — realizam seus negócios. O processo de tomada de decisão necessita ser cada vez mais rápido e preciso. Atualmente, organizações não precisam aguardar a chegada de algum documento importante pelos correios, como um relatório de uma unidade que fica localizada em outro Estado ou, até mesmo, outro país. Hoje, as informações são transmitidas quase que instantaneamente pelas redes de computadores.

Um fato importante é que as organizações dependem das redes de computadores e de suas ligações para trocarem e compartilharem informações e recursos. Mas você sabe a respeito do conceito de redes de computadores?

Como elas funcionam? Quais são as tecnologias e os recursos necessários para que elas operem com desempenho avançado e conforme o esperado pelas organizações?

Neste capítulo, apresentaremos e descreveremos o conceito de redes de computadores e da grande rede mundial de computadores, a internet, bem como seu histórico e os serviços e recursos disponíveis e necessários para seu funcionamento, incluindo os principais modelos de referências utilizados: OSI e TCP/IP. Além disso, você também verá a quanto a segurança de redes e informações, fator determinante para a manutenção de funcionamento das tarefas diárias de qualquer organização.

Vamos conhecer um pouco mais do mudo das redes de computadores?

Bons estudos!

1.1 Introdução a redes de computadores

Os computadores se tornaram ferramentas de extrema importância para a automatização de tarefas e agilidade na realização destas. Aos poucos, percebeu-se que existia facilidade na troca de informações entre computadores, daí surgiram as redes de computadores, que, antigamente, interligavam poucos computadores, mas, hoje, conseguem interligar computadores de todo o mundo pela internet.

Sendo assim, a partir de agora, você verá a respeito do conceito de redes de computadores e internet, bem como o seu funcionamento.

1.1.1 Definição de redes de computadores e internet

Uma rede de computadores é um conjunto de computadores e dispositivos interligados por meio de um sistema de comunicação, com o intuito de compartilharem informações e recursos. Para Soares, Lemos e Colcher (1995, p. 10),

> [...] uma rede de computadores é formada por um conjunto de

> módulos processadores capazes de trocar informações e compartilhar recursos, interligados por um sistema de comunicação. Já o sistema de comunicação vai se constituir deum arranjo topológico interligando os vários módulos processadores através de enlaces físicos (meios de transmissão) e de um conjunto de regras com o fim de organizar a comunicação (protocolos).

Já para Tanenbaum (2003), uma rede de computadores é um conjunto de computadores autônomos interconectados por uma única tecnologia. Dois ou mais computadores estão interconectados quando conseguem trocar informações. Esta interconexão não necessariamente é obtida por um fio de cobre, visto que podem ser usadas outras tecnologias de conexão, como as fibras ópticas, o micro-ondas, as ondas de infravermelho e os satélites de comunicações.

As redes de computadores podem ter tamanhos diversos, topologias e modelos.

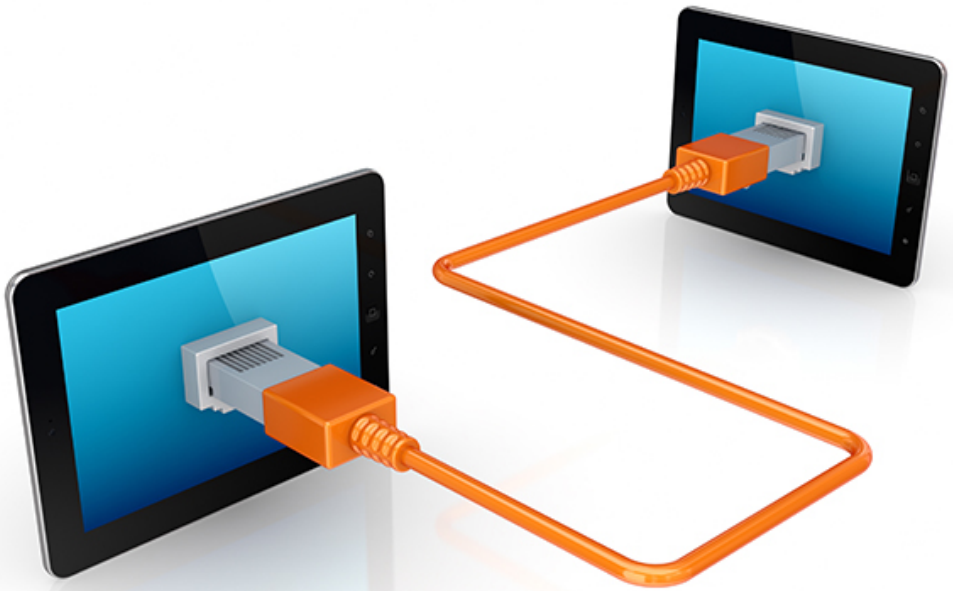


Figura 1 - Dispositivos interligados com o objetivo de compartilhar e trocar informações por meio da rede de comunicação. Fonte: 3Dstock, Shutterstock, 2018.

A internet não é uma rede de computadores, mas, sim, uma rede de redes de computadores. Inclusive, você sabe como a internet surgiu? Clique nos itens a seguir para conhecer os principais acontecimentos que culminaram no seu surgimento.

Na década de 1960, no momento em que acontecia a Guerra Fria nos Estados Unidos, informações estratégicas militares eram armazenadas em computadores que ficavam localizados em diferentes locais no país, com o objetivo de serem protegidas contra um possível ataque nuclear soviético.

> A partir de então, surgiu a ideia de interligar os centros de computação no intuito que os sistemas de informações do país fossem capazes de continuar funcionando, mesmo que um dos centros ou, até mesmo, a interligação entre dois deles fossem atingidos e destruídos.
>
> Mais tarde, o Departamento de Defesa, com a Advanced Research Projects Agency (ARPA), desenvolveu uma maneira mais segura e flexível para que acontecesse a interligação de computadores. Com base nisso, em 1970, foi desenvolvido o princípio do que seria a internet. Felizmente, a Guerra Fria havia acabado, mas o legado deixado por aqueles dias foi muito importante.

Assim, o que se tornaria a internet, começou como uma rede destinada a pesquisas científicas que funcionava por meio da Nacional Science Foundation. O governo dos Estados Unidos destinou investimentos na criação dos chamados *backbones*, que são conectados em redes de menor tamanho.

VOCÊ QUER VER?

O filme *Jogos de Guerra* (LASKER; PARKES, 1983), apresenta a história de um *hacker* habilidoso que consegue a façanha de ter acesso ao Sistema de Segurança dos Estados Unidos, desencadeando um novo conflito mundial. Este filme mostra como eram os computadores e as redes de computadores. Vale a pena assistir e se aprofundar no assunto!

Para facilitar o entendimento sobre o que é a internet, é possível pensar nela como uma rede de redes. A internet não possui donos, indivíduos ou empresas para administrá-la. Cada rede individual conectada a ela pode ser administrada por uma instituição governamental, uma instituição ligada à educação e até por empresas privadas. Assim, a internet não possui um poder centralizado, é uma auto-organização.

De acordo com Tanenbaum e Wetherall (2011), a internet não é uma rede, mas, sim, um conjunto imenso de diversas redes que fazem uso de certos protocolos comuns e disponibilizam o fornecimento de determinados serviços, também comuns. Ela não foi planejada e não é controlada por ninguém.

A ideia de que a internet não seja controlada de maneira centralizada, para muitas pessoas, pode ser motivo de espanto. Entretanto, não existe alguém que detenha este papel ou um local central da internet no Planeta. Desta forma, a administração e a organização do sistema são realizadas pelos administradores das redes — que fazem parte dela — e dos próprios usuários.

A internet, no aspecto físico, é uma grande rede de computadores, porém é percebida pelos usuários que a utilizam como um conjunto de recursos capaz de proporcionar compartilhamentos de informações entre os demais computadores e usuários conectados a ela.

Figura 2 - A internet é um conjunto de recursos e serviços disponíveis aos usuários que estão conectados a ela. Fonte: Haywiremedia, Shutterstock, 2018.

Tanenbaum (2003) menciona que a internet e suas predecessoras possuíam quatro aplicações principais: correio eletrônico (*e-mail*), *newsgroup*, *logon* remoto e transferência de arquivos. Clique nas abas a seguir para conhecer cada um deles.

Correio eletrônico

Newsgroups

***Logon* remoto**

Transferência de arquivos

O serviço de correio eletrônico é um dos serviços essenciais e mais importantes disponível na internet. Através dele, usuários conseguem trocar mensagens e informações com outros usuários que também fazem

parte da internet. Atualmente, as pessoas recebem dezenas de mensagens por dia e transformam o correio eletrônico em uma das principais maneiras de interação e comunicação com o mundo exterior, deixado de lado outras formas de comunicação, como o telefone e o correio tradicional.

Além disso, até o início dos anos de 1990 a internet era bastante utilizada por profissionais ligados a pesquisa e universidades, ao governo e, também, à indústria, por isso, surgiu um novo recurso que transformou a realidade e despertou e atraiu milhares de novos usuários, sem vínculo com a área acadêmica e de pesquisa: a *World Wide Web*, também conhecida como **WWW**.

De acordo com Tanenbaum (2003), a WWW foi criada pelo físico da CERN (Organização Europeia para a Investigação Nuclear), Tim Bernes-Lee, que facilitou sobremaneira seu uso sem aplicar alterações nos recursos oferecidos pela internet. Juntamente com o navegador “Mosaic”, desenvolvido por Marc Andreessen — no National Center for Supercomputer Applications (NCSA), em Urbana, Illinois —, a WWW conseguiu tornar realidade a configuração de variadas páginas de informações de um *site* contendo textos, imagens, vídeos e até *links* para outras páginas e *sites*. Se o usuário clica em um *link*, ele é transferido para a página que foi indicada nele.

VOCÊ QUER LER?

O livro “ Desconstruindo a *web*: as tecnologias por trás de uma requisição”, de Willian Molinari (2016), é uma opção para quem quer conhecer todo o processo envolvido na WWW, desde o momento em que o usuário aperta a tecla “*Enter*” até a exibição da página completamente carregada na tela do computador.

Disponibilizando esses e outros recursos, a internet é capaz de interligar diversos tipos de computadores, com *hardwares* e *softwares* variados, ou seja, computadores e programas de tipos e marcas diferentes. Para que a comunicação aconteça, é necessário que os computadores “falem” a mesma língua, o chamado TCP/IP (*Transmission Control Protocol*/*Internet Protocol*), protocolo oficial da internet.

VOCÊ SABIA?

O TCP/IP é um conjunto de regras contendo linguagem e comportamento, e tem o intuito de estabelecer como deve ocorrer a comunicação para quem deseja enviar e receber mensagens na internet. Todos os computadores que estão conectados à internet “conversam” pelo TCP/IP, pois ele transfere a informação em pedaços menores — denominados “pacotes” — e direciona ao computador ao qual o pacote se destina.

Atualmente, o número de redes, computadores e usuários conectados à internet é imenso, impossível mensurar com exatidão.

Na sequência, aprofundaremos nossos estudos quanto aos componentes de uma rede de computadores e da internet.

1.1.2 A periferia da internet

Segundo Kurose e Ross (2014), em uma rede de computadores, os

computadores e outros dispositivos conectados à internet são denominados **sistemas finais**, pois se encontram na periferia da internet, conforme vemos na figura a seguir.

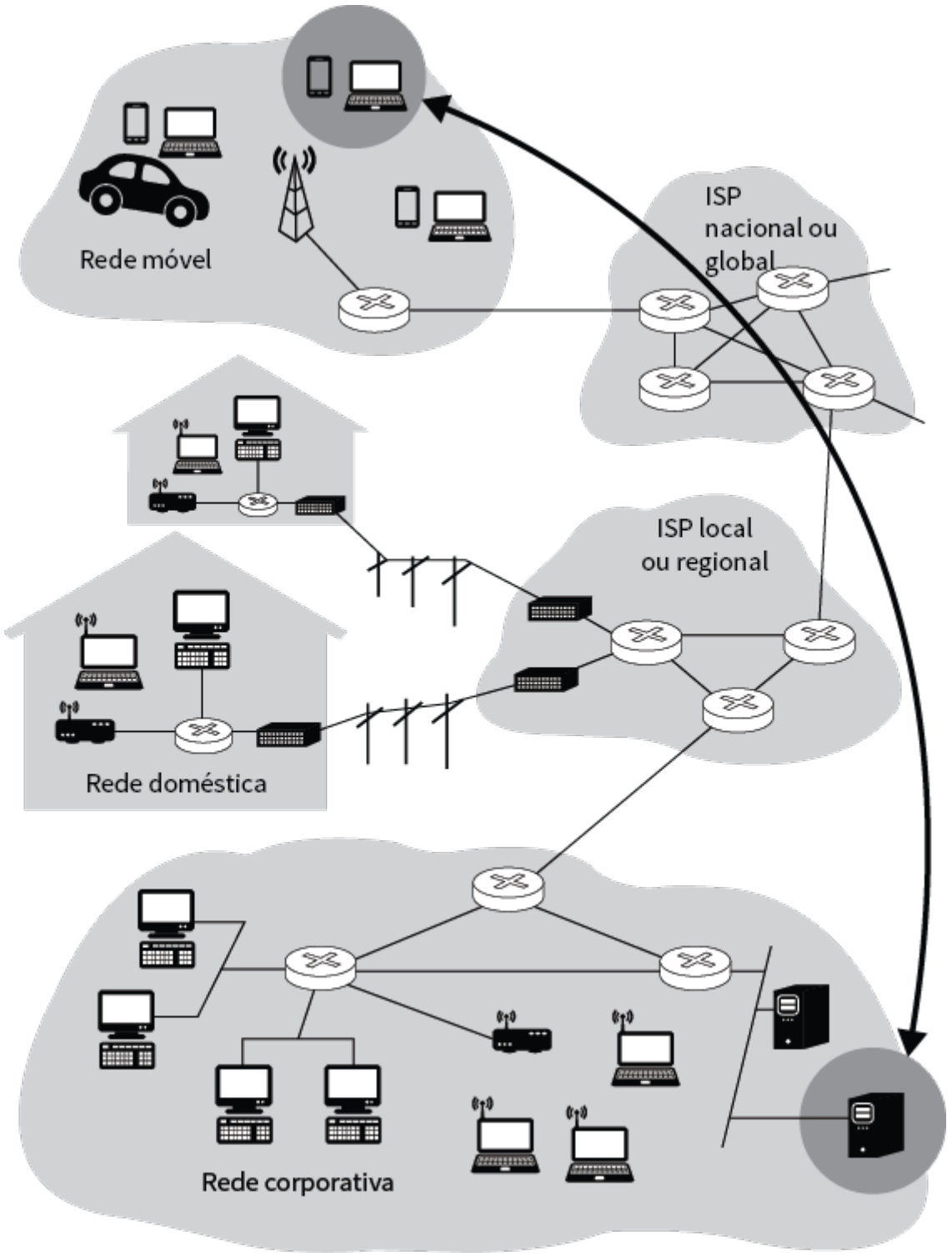


Figura 3 - Interação entre sistemas finais, por meio de computadores, servidores e computadores móveis que realizam a comunicação entre si. Fonte: KUROSE; ROSS, 2014, p. 8.

Fazem parte de um sistema final equipamentos, como os computadores;

servidores e dispositivos portáteis, como PDAs; e *smartphones* com conexão à internet. Também fazem parte de um sistema final o que denominados de **hospedeiros**, que executam programas de aplicação, como um navegador da *web* e um servidor de *e-mail*.

Pode-se dizer que o sistema final e o hospedeiro são a mesma coisa e podem ser divididos em clientes, que são os computadores de mesa ou computadores e dispositivos portáteis; e servidores, que são computadores mais robustos, com poder de processamento e armazenamento maiores que realizam tarefas, como a distribuição de páginas *web*, a transmissão e retransmissão de *e-mails*, entre outros.

1.1.3 O núcleo da internet

Uma rede comutada é composta por um conjunto de nós interligados denominados de **comutadores**. Mas o que são comutadores? Pode-se dizer que os comutadores são dispositivos com capacidade de estabelecer conexões por tempo determinado entre dois ou mais dispositivos conectados ao comutador.

O núcleo da internet está diretamente ligado à rede de comutadores de pacotes e enlaces, que realizam a interconexão dos sistemas finais da internet, conforme podemos observar na figura a seguir.

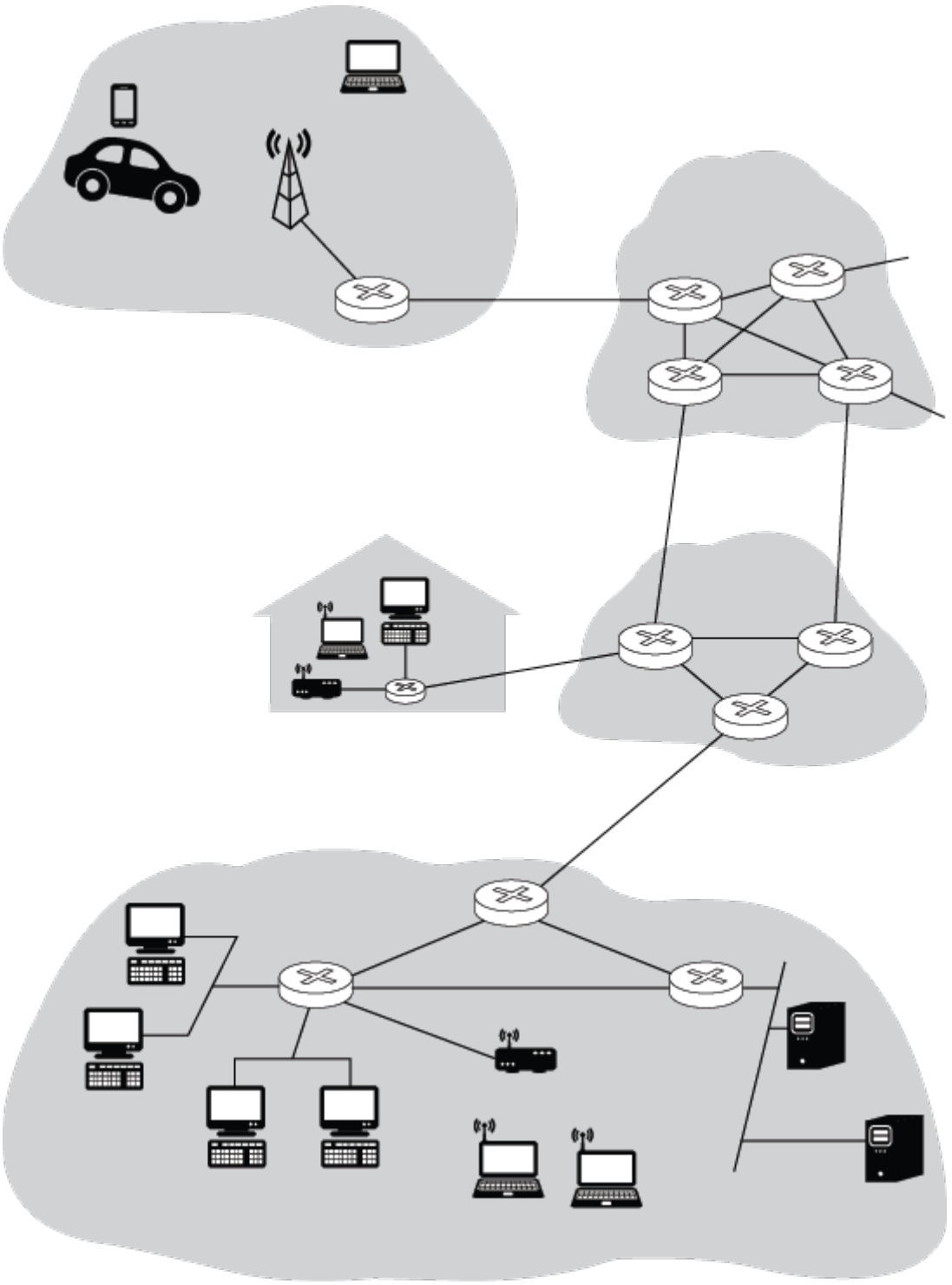


Figura 4 - O núcleo da rede é formado por redes móveis conectadas pelo ISP nacional ou global, redes domésticas e redes corporativas conectadas a ISP local ou regional. Fonte: KUROSE; ROSS, 2014, p. 19.

Em uma rede de comunicação, a comutação, também conhecida como **chaveamento**, está relacionada à alocação de recursos da rede, como meios de transmissão e repetidores, para a efetivação da transmissão pelos variados dispositivos que estão conectados.

Em uma rede comutada, parte dos nós são diretamente conectados aos sistemas finais, ou seja, computadores ou telefones e outros são usados somente para a realização de roteamento.

Segundo Forouzan (2008), existem três métodos de comutação: comutação de circuitos, comutação de pacotes e comutação de mensagens, sendo que os dois primeiros são bastante utilizados nos dias de hoje, enquanto que o terceiro foi deixado de lado e está sendo retirado pouco a pouco do mercado de comunicações.

Em redes onde a **comutação de circuitos** ocorre, alguns recursos são necessários ao longo de um trajeto (*buffer* e taxa de transmissão) para possibilitar a comunicação entre estações. Eles são reservados e alocados pelo tempo da sessão de comunicação entre elas.

De acordo com Soares, Lemos e Colcher (1995), a comunicação por meio de circuitos abrange a existência de um percurso dedicado de comunicação entre dois pontos, e envolve fases distintas. Clique na interação a seguir para ver quais são.

Primeira fase: estabelecimento do circuito

Se refere ao estabelecimento de um circuito fim a fim, para que estações consigam se comunicar. Para tanto, é necessário determinar e alocar uma rota entre as estações onde, em cada nó, um canal é alocado e deve permanecer dedicado para a realização da conexão até o momento em que ocorre a desconexão do circuito.

Segunda fase: transferência de informação

Relacionada ao momento do estabelecimento da conexão. Uma vez estabelecida, os dados podem ser enviados e recebidos pelas estações

Na **comutação de mensagens** não é necessário o estabelecimento de um trajeto dedicado entre as estações, ao contrário: se uma estação precisa enviar uma mensagem, ela inclui o endereço de destino para esta mensagem que será enviada pela rede de nó em nó. A mensagem inteira passa de nó em nó e o próximo trajeto de rota é estabelecido com base no endereço incluso na mensagem. É importante salientar que o trajeto pode estar sendo ocupado pela transmissão de outra mensagem ou, então, outras mensagens já podem estar na espera para serem transmitidas pelo mesmo trajeto. Quando isto acontece, a mensagem aguarda em uma fila até que sua vez de ser transmitida chegue e o trajeto esteja liberado. Assim, a transmissão é iniciada. Então, uma mensagem anda de nó em nó pela rede fazendo uso somente de um canal por vez, sendo armazenada e retransmitida em cada nó.

Segundo Soares, Lemos e Colcher (1995, p. 78, grifos dos autores),

> [...] existem algumas características na comutação de mensagens em relação à comutação de circuitos, como *aproveitamento das*

linhas de comunicação é maior, já que os canais podem ser compartilhados por várias mensagens ao longo do tempo, devido ao fato de não haver alocação dos canais, as mensagens são transmitidas por demanda e quando o tráfego se torna alto em uma rede de comutação de circuitos, pedidos de novas conexões podem ser recusados devida à falta de recursos ou caminhos livres. As mensagens são sempre aceitas em uma rede de comutação de mensagens, o tempo de transferência é que aumenta devido às filas que as mensagens encontrarão em cada nó de comutação de rede.

Por fim, o funcionamento de redes de **comutação de pacotes** é parecido com a comutação de mensagens, entretanto, existe uma diferença com relação ao tamanho da unidade de dados enviada na comutação de pacotes, que é limitado. As mensagens que possuem tamanho maior do que o limite, devem ser quebradas em pedaços menores, denominados **pacotes**. Os pacotes que fazem parte da mesma mensagem podem ser transmitidos de forma simultânea pela rede em variados nós, o que facilita a redução do atraso de transmissão total de uma mensagem. Além disso, as redes com comutação de pacotes necessitam de nós de comutação com menor capacidade de armazenamento, e os processos de recuperação de erros para pacotes são mais eficientes do que para mensagens.

Assim, pudemos entender um pouco mais da periferia e do núcleo da internet, a rede de comutação de pacotes e os enlaces que possibilitam a interconexão dos sistemas finais. Na sequência, abordaremos questões relacionadas a atrasos, perdas e vazão em redes de comutação de pacotes, que normalmente acontecem durante a transmissão.

1.2 Noções de avaliação de desempenho

Existem medidas que podem caracterizar o desempenho de um sistema, como o atraso de transferência, a perda e a vazão. Mas o que é desempenho?

Desempenho é considerado a capacidade efetiva de transmissão da rede. Conseguir utilizar um sistema de comunicação de forma efetiva está associada a ideia de utilização de apenas uma porcentagem da capacidade que ele poderia oferecer.

Vamos entender melhor sobre o assunto, a partir de agora.

1.2.1 Atraso, perda e vazão em redes de computadores

Pode-se afirmar que a internet é uma grande infraestrutura capaz de fornecer diversos serviços para as aplicações distribuídas, que são efetuadas nas estruturas finais. O ideal seria que todos os serviços realizassem de forma eficiente a transmissão de todos os dados desejados entre duas estruturas finais, de forma instantânea e sem perda alguma. Entretanto, não é assim que ocorre na prática.

Segundo Kurose e Ross (2014, p. 26), "[...] as redes de computadores necessariamente, restringem a vazão, ou seja, a quantidade de dados por segundo que podem ser transferidos entre sistemas finais, apresentam atrasos entre sistemas finais e podem perder pacotes".

A transmissão de um pacote de dados inicia em uma estrutura final de origem e percorre uma cadeia de roteadores, terminando sua trajetória em outra estrutura final de destino. Durante a transmissão de pacotes de um nó para outro, variados tipos de atrasos podem acontecer em cada nó. Para Soares, Lemos e Colcher (1995), o atraso de transferência está diretamente ligado à soma dos atrasos de acesso (intervalo de tempo decorrido desde que uma mensagem a transmitir é gerada pela estação, até o momento em que a estação consegue obter para ela, e somente ela, o direito de transmitir, sem a existência de colisão de mensagens no meio) e o atraso de transmissão (intervalo de tempo decorrido desde o início da transmissão).

Kurose e Ross (2014) nos explicam os tipos mais comuns de atrasos. Clique nas abas a seguir para ler sobre cada um deles.

Atraso de processamento

Está relacionado ao tempo necessário para que se consiga examinar

o cabeçalho do pacote e estabelecer a direção. Outro fator é o tempo necessário para a verificação de erros em bits existentes no pacote, que aconteceram no momento da transmissão dos bits a partir do nó antecessor ao roteador. Esta situação de atraso em roteadores de alta velocidade, habitualmente, é de microssegundos ou até menos. Após o processamento nodal, o roteado determina a direção do pacote até a fila que antecede o enlace com o roteador B.

Atraso de fila

Ocorre quando um pacote aguarda para ser transmitido no enlace. A extensão deste tipo de atraso para um pacote determinado depende do número de outros pacotes que chegaram anteriormente e que já estão na fila aguardando para serem transmitidos. Se, por acaso, a fila se encontrar vazia e nenhum pacote estiver em transmissão no momento, o tempo de fila do pacote não existirá, ou seja, será igual a zero. Contudo, se há tráfego intenso e muitos pacotes estiverem aguardando para serem transmitidos, o atraso será maior.

Atraso de transmissão

Parte da premissa de que todos os pacotes serão transmitidos de acordo com a ordem de chegada, ou seja, o primeiro que chegar é o primeiro a ser processado. O pacote será habilitado para ser transmitido depois que todos os que anteriormente chegaram tiverem sido enviados.

Atraso de propagação

Está diretamente relacionado ao tempo indispensável para que a

propagação do bit ocorra, desde o princípio do enlace até chegar ao roteador B. De acordo com Kurose e Ross (2014), a propagação do bit ocorre à velocidade de propagação do enlace, dependente do meio físico do enlace, que pode ser fibra ótica, par de fios de cobre trançado e está na faixa de 2.108 m/s a 3.108 m/s, sendo comparada à velocidade da luz ou até menor. Pode-se afirmar, ainda, que o atraso de propagação é a longitude entre dois roteadores, dividida pela velocidade de propagação.

Para exemplificar o processo no qual ocorre no **atraso de processamento**, veja a figura a seguir:

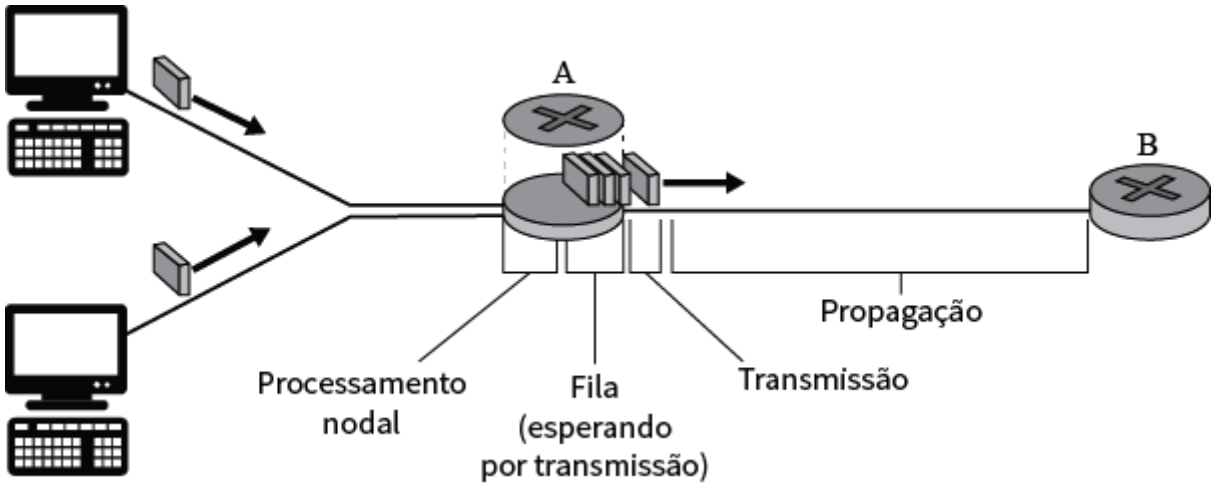


Figura 5 - O atraso nodal no roteador A (um pacote é transmitido do nó que antecede o roteador A) até o próximo, roteador B. Os atrasos ocorrem neste tempo.

Kurose e Ross (2014) ainda nos explicam que uma perda de pacotes pode ser considerada como um pacote que foi enviado para o núcleo da rede, porém sem nunca ter emergido dele no destino. A parcela de pacote perdido é maior com o aumento da intensidade de tráfego. A *performance* de um nó é, normalmente, mensurada não somente pelo atraso, mas, também, pelas perdas de pacotes. Para tanto, um pacote, quando perdido, poderá ser retransmitido para que ocorra a garantia de que todos os dados sejam finalmente transferidos do nó de origem para o nó de destino.

A questão do atraso de pacotes, bem como a perda destes, compromete o

desempenho da rede. Entretanto, é necessária atenção em outro quesito importante na medição de desempenho das redes de computadores: a vazão. Por **vazão**, entende-se a transferência de um arquivo de um hospedeiro A para outro hospedeiro (B) por meio de uma rede de computadores, conforme nos mostra a figura a seguir.

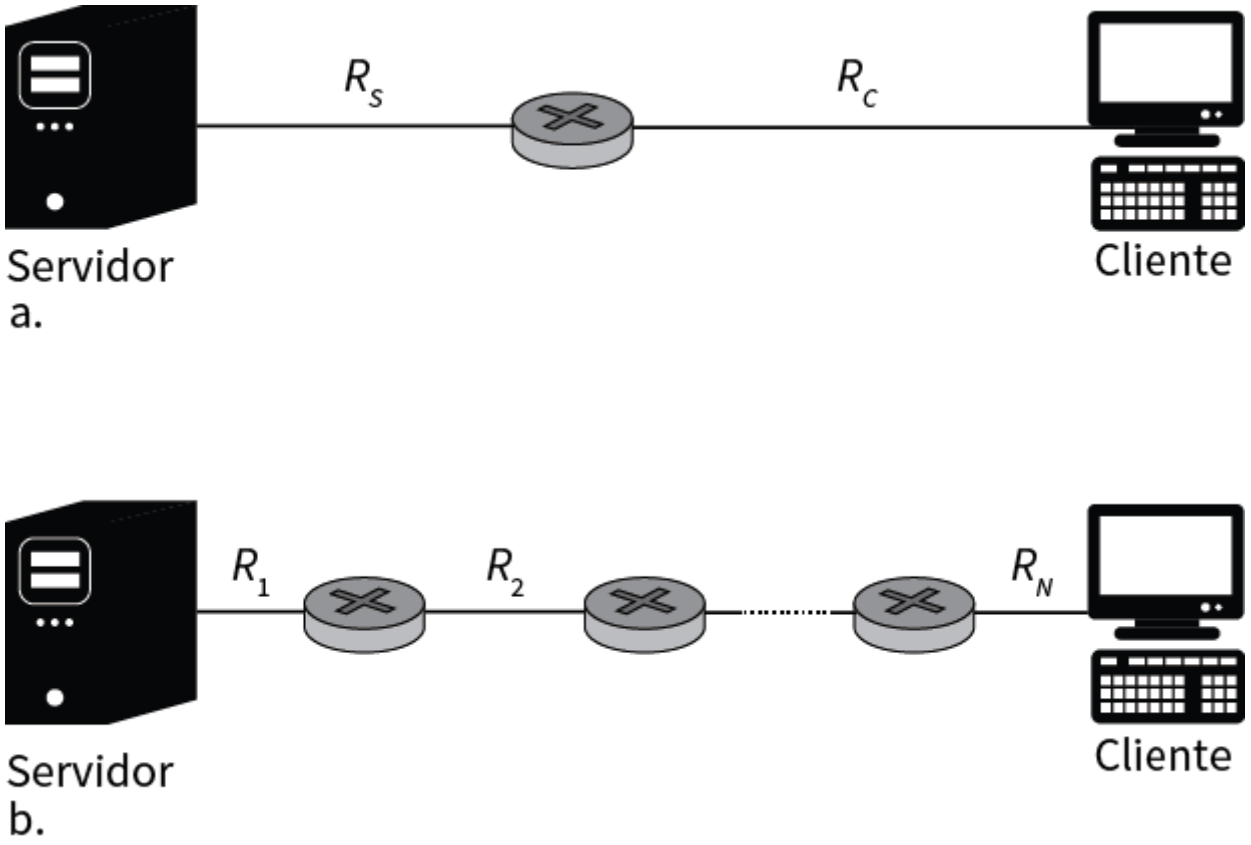


Figura 6 - Vazão para uma transferência de arquivo do servidor até o cliente. Fonte: KUROSE; ROSS, 2014, p. 33.

De acordo com Kurose e Ross (2014, p. 33, grifos nossos),

> [...] a vazão instantânea a qualquer momento é a taxa (em *bits*/s) em que o Servidor B está recebendo o arquivo. Se o arquivo consistir em F *bits* e a transferência levar T segundos para o Servidor B receber todos os F *bits*, então a vazão média de transferência do arquivo é F/T *bits*/s. Para algumas aplicações, como a telefonia via Internet, é desejável ter um atraso baixo e uma vazão instantânea acima de algum limiar (por exemplo, superior a 24 kbps para telefonia via Internet, e superior a 256

kbps para alguns aplicativos de vídeo em tempo real). Para outras aplicações, incluindo as de transferência de arquivo, o atraso não é importante, mas é recomendado ter a vazão mais alta possível.

Dessa forma, a internet é considerada uma infraestrutura que provê serviços a aplicações distribuídas e realizadas nos sistemas finais. O ideal seria que os serviços da internet fossem capazes de transmitir todos os dados desejáveis entre dois ou mais sistemas finais, de forma imediata e sem perdas, todavia, isto é algo difícil e impossível de se alcançar devido aos atrasos, as perdas e as vazões.

Agora, vamos compreender um pouco mais a respeito dos modelos de referência de arquitetura de redes: modelo OSI e modelo TCP/IP.

1.3 Modelos de referência

Existem duas importantes arquiteturas de redes: o modelo de referência OSI e o modelo de referência TCP/IP. Protocolos que fazem parte do modelo de referência OSI não são tão utilizados atualmente, entretanto, suas características são muito relevantes. Já o modelo de referência TCP/IP possui características contrárias, ou seja, o modelo em si não é muito usado, porém os protocolos são.

VOCÊ QUER LER?

O livro “Introdução às redes de computadores: modelos OSI e TCP/IP”, de Ademar Felipe Fey e Raul Ricardo Gauer (2015), aborda o histórico do surgimento das redes de computadores nos anos de 1970. A obra explica detalhadamente os modelos TCP/IP e OSI, apresentando seus principais fundamentos e conceitos.

Vamos entender melhor sobre o assunto? Acompanhe a seguir.

1.3.1 Modelo de referência OSI

De acordo com Torres (2004), para que houvesse facilidade de interconexão entre sistemas computacionais, a ISO criou o modelo de referência denominado **OSI** (*Open Systems Interconnection*), com o intuito de possibilitar que fabricantes e desenvolvedores conseguissem produzir protocolos baseado no modelo de referência. Com a figura a seguir, podemos compreender o modelo OSI.

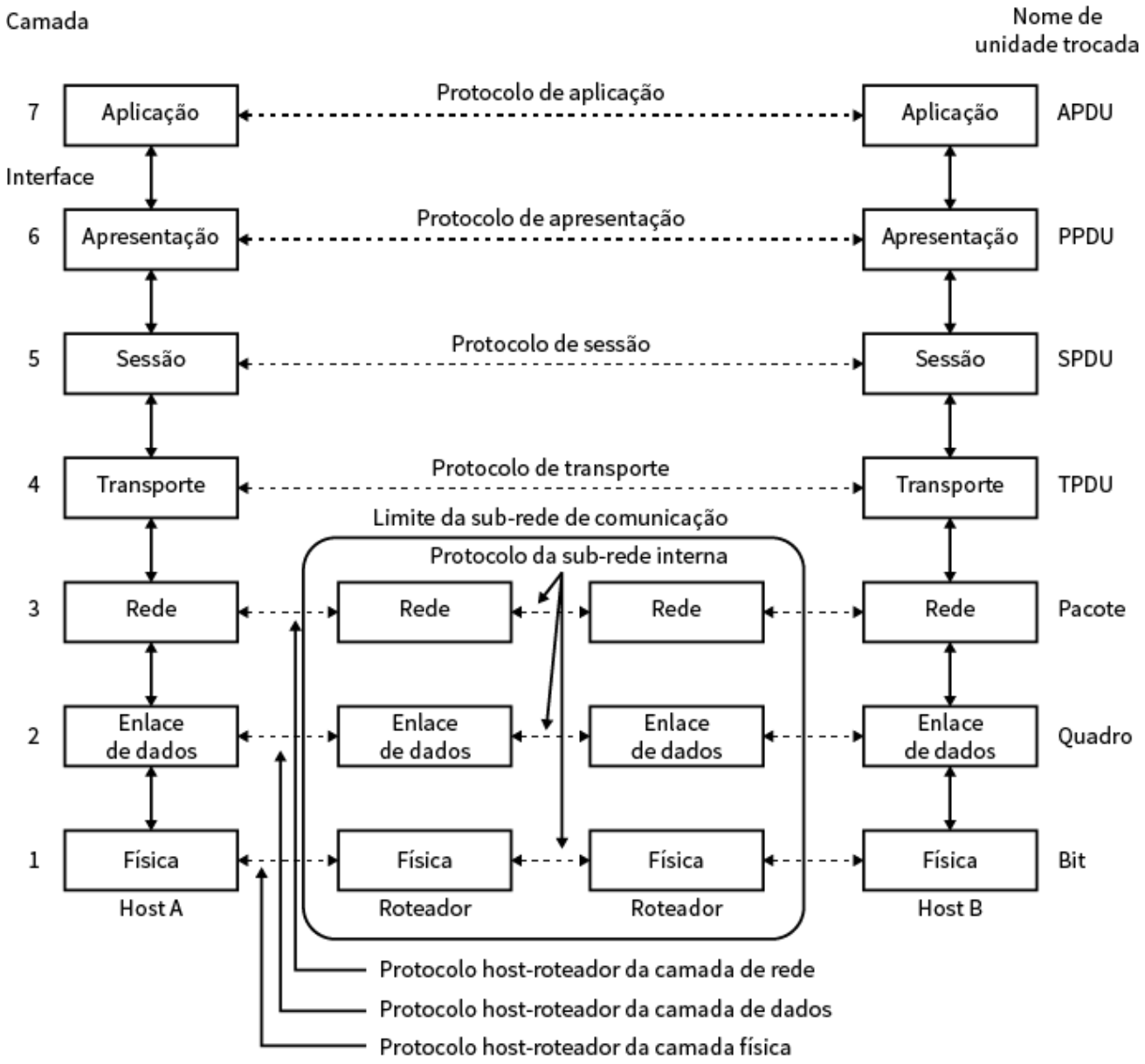


Figura 7 - O modelo OSI é composto por sete camadas: física, enlace, rede, transporte, apresentação e aplicação. Fonte: TANENBAUM, 2003, p. 41.

O modelo OSI é composto por sete camadas, clique na interação a seguir para ler sobre cada uma delas.

Camada física

É a responsável pela transmissão de *bits* brutos por meio de um canal de comunicação.

Camada enlace de dados

Tem como principal atribuição a transformação de um canal de transmissão bruto em um canal que seja livre de erros de transmissão não detectados para a camada de rede. Para tanto, a camada de enlace de dados é responsável por fazer com que o transmissor realize uma divisão dos dados de entradas em quadros de dados, executando a transmissão em sequência.

Camada de rede

Faz o controle da operação da sub-rede. Uma questão importante é a maneira como os pacotes serão roteados da origem até o destino. Para isto, são usadas rotas que podem ser baseadas em tabelas estáticas fixas à rede e que quase nunca sofrem alterações.

Camada de transporte

Possui como função básica a aceitação de dados da camada superior a ela e realiza a divisão em unidades menores quando houver necessidade. Também repassa as unidades menores à camada de rede e assevera que todos os pedaços conseguirão chegar de forma correta até o outro extremo.

Camada de sessão

Possibilita que usuários de variadas máquinas consigam estabelecer sessões entre elas. Uma sessão consegue oferecer variados serviços, como o controle de diálogo, que mantém o controle de quem está apto para realizar a transmissão em cada momento; o gerenciamento de *token* , que impossibilita que duas partes consigam executar a mesma transação crítica ao mesmo tempo; e a sincronização, a qual realiza a verificação regular de transmissões longas com o intuito de permitir que elas continuem a partir do ponto que estavam quando ocorreu alguma falha.

Camada de apresentação

Ao contrário das camadas inferiores, que tem a preocupação principal com a transmissão de *bits* , ela faz relação com a sintaxe e a semântica das informações que são transmitidas.

Camada de aplicação

> Possui protocolos frequentemente importantes e necessários para os usuários, como o protocolo HTTP (*HyperText Transfer Protocol*), que é a base de funcionamento da WWW.

De acordo com Tanenbaum (2003, p. 41),

> [...] o modelo OSI possui sete camadas e alguns princípios aplicados para que se consiga chegar às sete camadas: 1) Uma camada deve ser aplicada onde houver necessidade de um grau de abstração adicional; 2) cada camada deve executar uma função bem definida; 3) a função de cada camada deve ser escolhida tendo em vista a definição de protocolos padronizados internacionalmente; 4) os limites de camadas devem ser escolhidos para minimizar o fluxo de informações pelas interfaces e 5) o número de camadas deve ser grande o bastante para que funções distintas não precisem ser desnecessariamente colocadas na mesma camada e pequeno o suficiente para que a arquitetura não se torne difícil de controlar.

O principal objetivo do modelo OSI é facilitar a interconexão e a comunicação entre diferentes sistemas, sem precisar efetuar mudanças relacionadas a *hardware* e *software* pertencentes a eles.

1.3.2 Modelo de referência TCP/IP

O modelo de referência **TCP/IP** ficou conhecido em função de dois protocolos: TCP e IP. Este modelo foi desenvolvido em quatro camadas, conforme vemos com a ilustração a seguir.

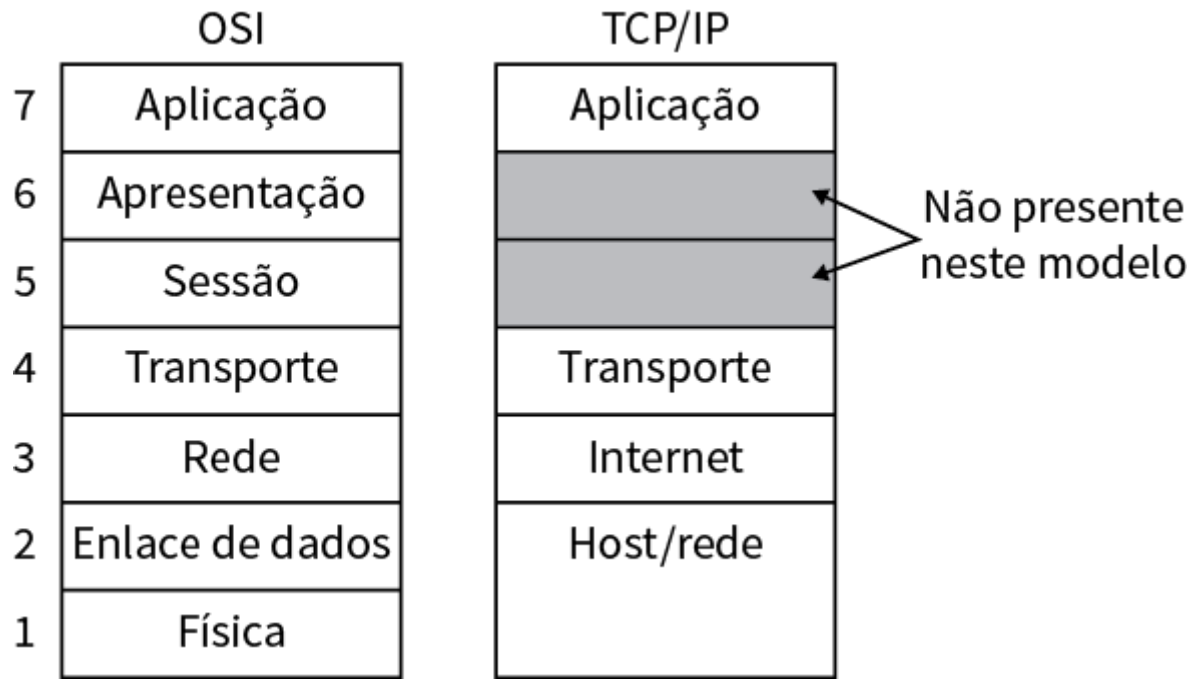


Figura 8 - Modelo de referência TCP/IP comparado ao modelo de referência OSI. Fonte: TANENBAUM, 2003, p. 46.

Clicando na tabela a seguir, você verá a função de cada um destas camadas.

Interface de redes	A camada de **interface de redes** é a de aceso à rede, considerada a primeira. Ela tem como função dar suporte à camada de rede por meio dos serviços de acessos físico e lógico ao meio físico.
Inter-redes	A camada de **inter-redes** tem a responsabilidade pelo envio de datagramas de um computador qualquer para outro computador, deforma independente de suas localizações na rede.
Transporte	Já a camada de **transporte** é a responsável por proporcionar suporte à camada de aplicação de maneira confiável, independentemente dos serviços oferecidos pelas camadas de interface de rede e inter-rede.

Aplicação	Com relação à camada de **aplicação**, Tanenbaum (2003), nos explica que, nela, é possível encontrar todos os protocolos de nível mais alto e que fornecem suporte para as aplicações dos usuários, como o protocolo de terminal Telnet, o protocolo de transferência de arquivos (FTP) e o protocolo de *e-mail* (SMTP).

No próximo tópico você irá aprender sobre a segurança em redes. Acompanhe!

1.4 Introdução à segurança em redes

Com a crescente utilização e disseminação de computadores ligados a redes, considerando-se que mais pessoas dentro de uma empresa ou organização possuem acesso a dados e informações; é crescente, também, a preocupação com a segurança.

A segurança das redes de computadores e da informação é uma questão de suma importância para empresas e organizações de todos os tipos.

Figura 9 - Empresas necessitam ter a preocupação constante com a proteção de suas informações.

Fonte: Lightspring, Shutterstock, 2018. ID: 104489465

Essa preocupação não deve ser somente da área de Tecnologia da Informação, mas, sim, da empresa como um todo. Por isso, técnicas e sistemas de segurança têm sido criados para que indivíduos mal-intencionados não consigam acessar e violar sistemas de computadores, os denominados *hackers* e *crackers*.

VOCÊ O CONHECE?

Ainda existe certa confusão envolvendo o *hacker* e o *cracker*, visto que ambos são indivíduos que possuem muito conhecimento e habilidades com computadores. O *hacker* é aquele indivíduo que é capaz de elaborar e modificar *softwares* ou *hardwares*, seja desenvolvendo funcionalidades novas ou realizando adaptações em funcionalidades já existentes. O *hacker* usa seu conhecimento para a melhoria de sistemas de segurança de forma legal, ou seja, sem causar danos. Por outro lado, o *cracker* é aquele indivíduo que realiza a quebra de sistemas de segurança, ou seja, usa seu conhecimento com o intuito de causar danos, de forma ilegal e criminosa, as informações.

Atualmente, onde quer que hajam dados e informações, deve existir, também, a atenção e preocupação relacionada à sua segurança. Esta envolve algumas formas e medidas.

A segurança física dos dados e informações possui relação com medidas físicas para que a proteção ocorra, como fechaduras, sistema de câmeras e monitoramento, guardas, entre outras. A segurança física deve ser levada em consideração não somente por indivíduos que violam a segurança de forma proposital, mas com a possibilidade de que desastres naturais possam acontecer, como incêndios e inundações, os quais podem causar danos aos dados e informações de forma muito mais eficiente do que um indivíduo criminoso.

VOCÊ SABIA?

Para ilustrar o acesso sem controle e indiscriminado à estrutura física, temos o caso de um reservatório de água da Sabesp, em São Paulo. Dois homens conseguiram entrar e subiram até o reservatório, abriram a tampa, pularam e se banharam na água que era servida à população. Entretanto, ocorreu a fatalidade de serem sugados pela tubulação e acabaram morrendo. Este fato fez com que cerca de 70 mil pessoas ficassem sem água por duas semanas. Imagine, agora, o risco envolvido se, em vez de nadarem dentro do reservatório, os indivíduos colocassem veneno na água (CARUSO; STEFFEN, 1999).

Além da preocupação com a estrutura física, é de extrema necessidade a preocupação com os *softwares*. O acesso aos *softwares* organizacionais pode ser dado pelo uso de senhas e por restrições e limitações ao acesso apenas de algumas funcionalidades específicas dos programas utilizados. Como medida para evitar que situações perigosas ocorram, as empresas utilizam sistemas de *backup* e armazenam suas informações em locais mais seguros.

VOCÊ SABIA?

O conceito de segurança significa o conjunto de outros três conceitos: privacidade, integridade e autenticidade do emissor. A privacidade está relacionada a salvaguarda de que a mensagem não será compreendida por um terceiro que, por ventura, consiga lê-la no canal; a integridade tem relação com a salvaguarda de que a mensagem não sofra modificações por um terceiro no momento da transmissão; enquanto que a autenticidade do emissor é a salvaguarda de que o emissor da mensagem em questão é o próprio.

Como destacado, as redes de computadores, normalmente, são compartilhadas e usadas por diferentes aplicações e para diversos fins e propósitos. Por isso, podem estar vulneráveis a ataques de diferentes tipos. A seguir, vamos conhecer aos ataques mais comuns e as técnicas de defesa as redes de computadores.

1.4.1 Ataques e técnicas de defesa a redes de computadores

Atualmente, grandes quantidades de dados e informações são armazenadas no formato eletrônico e estão expostas a mais riscos e ameaças do que se estivessem em formato manual. Os sistemas de informações disponíveis aos usuários, espalhados em diversos e diferentes locais, são interconectados pelas redes de computadores. Portanto, acessos não autorizados, usos indevidos e fraudes podem acontecer em qualquer ponto de acesso à essas

redes de computadores.

De acordo com Laudon e Laudon (2007), em um sistema de computação cliente/servidor multicamada é possível perceber que as vulnerabilidades estão em cada camada e na comunicação entre elas. Os dados, enquanto estão trafegando pela rede, podem ser acessados, roubados no momento de transmissão ou alterados sem a devida autorização. Além disso, indivíduos não autorizados podem ocasionar ataques de recusa de serviço ou instalarem *softwares* mal-intencionados. Se estes indivíduos conseguirem o acesso à rede de computadores, os sistemas de informações ficam sujeitos à destruição e alteração dos dados contidos nos bancos de dados corporativos e em arquivos.

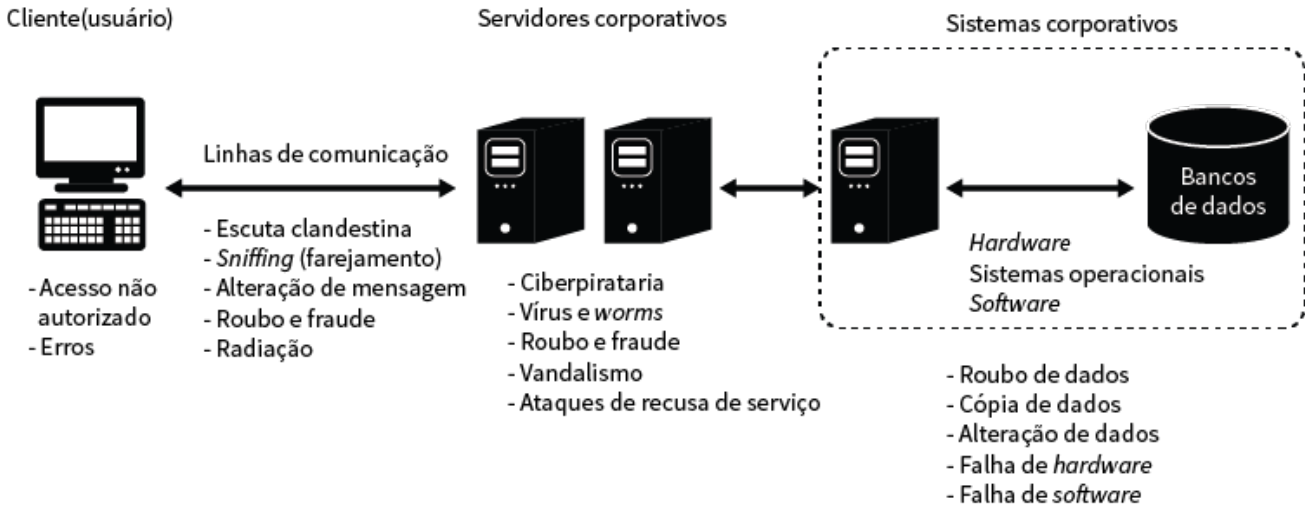


Figura 10 - As ameaças que afetam os sistemas de informações podem ter origem em fatores técnicos, organizacionais, ambientais e em decisões errôneas da administração. Fonte: LAUDON; LAUDON, 2007, p. 210.

Os *softwares* mal-intencionados também são conhecidos como ***malwares***, que podem incluir diferentes ameaças. As mais comuns são os vírus de computadores, como *worms* e cavalos de Tróia, mas existem algumas particularidades entre essas ameaças. Clique na interação a seguir para saber mais sobre este asssunto.

Sendo assim, existem muitas ameaças rondando as redes de computadores e os sistemas de informações. A grande maioria dos problemas relacionados à segurança é ocasionada por indivíduos mal-intencionados e maliciosos que

Os **vírus de computador** são programas, *softwares* que conseguem se anexar a outros programas ou arquivos, com o intuído de serem executados sem que o usuário tenha conhecimento e sem ter permitido. Eles são propagados de computador para computador no momento que usuários executam tarefas específicas, como enviar um *e-mail* anexando arquivos infectados.

Os vírus de computador podem ser desenvolvidos para ações sem muitos prejuízos aos dados e sistemas, como realizar a exibição de uma mensagem; mas, na maioria dos casos, são desenvolvidos para danificação e, até mesmo, destruição de programas, arquivos e informações, prejudicando o desempenho do computador, a memória e dificultando a realização de formatação de discos rígidos.

Um vírus de macro que ficou bastante conhecido foi o “Melissa”. Ele teve sua origem em 1999 e se disseminou muito rapidamente. Seu foco era atacar o modelo “Normal.dot” do editor de textos do Pacote Office, o Microsoft Word, infectando todos os novos documentos gerados. Além disso, o vírus ainda enviava os arquivos para os endereços contidos no catálogo de endereços do

Microsoft Outlook.

Temos, também, os ***worms***, que são programas com independência, ou seja, capazes de se copiarem e se propagarem de computador para computador, por meio de uma rede. Uma diferença importante é que, diferentemente dos vírus, eles funcionam sozinhos, sem a necessidade de um arquivo ou da ação do usuário para realizar a disseminação, o que possibilita que se espalhem com muito mais rapidez do que um vírus.

Como os vírus, os *worms* também causam a destruição de dados e informações, prejuízos e até a interrupção do funcionamento da rede. Na maior parte dos casos, eles são espalhados pela internet no momento que o usuário faz *downloads* de *softwares* e *downloads* de arquivos anexados em *e-mails*.

Um exemplo de *worm* é o "MyDooom", que teve seu surgimento em meados de 2004, espalhando-se pela rede como um anexo de *e-mail* com o intuito de afetar

computadores que usavam o sistema operacional Windows. Este *worm* realizava o envio de *e-mails* para endereços levantados nas máquinas que estavam infectadas, realizando a falsificação do remetente.

Por fim, os **cavalos de Tróia** são programas que, aparentemente, realizam uma execução diferente do que é esperado. O nome deriva de que, durante a Guerra de Tróia, gregos usaram um cavalo de madeira muito grande para enganar os troianos, que realizaram a abertura dos portões de sua cidade. O cavalo continha soldados gregos escondidos em seu interior.

Um cavalo de Tróia que ficou conhecido em 2004 foi o "StartPage". Ele era transmitido pelo compartilhamento de mídias de armazenamento, como disquetes e *downloads* de programas, e alterava a página do *browser* Internet Explorer para exibir mensagens falsas, com alerta de infecção por *spyware*, tentando levar o usuário a acessar um *site* no qual *malwares* poderiam ser instalados no computador.

Outro exemplo de cavalo de Tróia foi o “DSNX-05”, que apareceu em 2005. Ele distribuía uma mensagem de *e-mail*, aparentemente enviada pela Microsoft, incentivando os usuários a acessarem um *site* muito semelhante ao do Microsoft Windows. No entanto, o *link* baixava e instalava programas mal-intencionados no computador, permitindo que *hackers* tivessem acesso as informações de forma remota.

A segurança das informações também pode ser afetada por ***spywares***, também conhecidos como *softwares* espiões mal-intencionados, que são instalados nos computadores com o intuito de monitorar os passos do usuário e utilizar as informações coletadas para marketing. Isto é, são *softwares* que conhecem o perfil e o comportamento do usuário em relação ao que compram, passando a exibir anúncios personalizados.

Um *spyware* muito prejudicial é o “Key Logger”, programa que compila todas as teclas acionadas em um determinado computador com o objetivo de se apropriar de códigos seriais de *softwares*, ter aceso a contas de *e-mails*, descobrir senhas, entre outros.

possuem como objetivo alcançar benefícios, prejudicar pessoas ou empresas e, até mesmo, chamar a atenção. Tanenbaum (2003) relata que registros policiais de problemas de segurança nas organizações demostram que grande parte dos ataques não são efetuados por indivíduos estranhos que grampeiam uma linha telefônica, por exemplo, mas por pessoas magoadas e ressentidas com a empresa a qual faziam parte.

CASO

Uma empresa americana do ramo de biotecnologia possuía mais de 6.000 colaboradores se conectando à rede corporativa quando estavam viajando. Este acesso remoto já apresenta risco de segurança por si só, mas existia um agravante: o sistema de gerenciamento de senhas era considerado difícil para realizar as alterações, segundo os colaboradores, por isso, raramente o faziam. Outro problema era que funcionários que não faziam mais parte da empresa não tinham seus *logins* e senhas bloqueados imediatamente assim que fossem desligados da organização, ou seja, permaneciam com as contas ativas por alguns dias.

Para sanar esses e outros problemas de segurança, a empresa decidiu investir em um sistema de autenticação baseada em *token*. *Tokens* foram instalados nos computadores dos colaboradores gerando uma senha numérica. Quando os usuários tentassem acessar a rede da empresa, o colaborador precisaria lembrar seu número de identificação pessoal. Assim, os *tokens* geravam novas senhas numéricas cada vez que o usuário se conectava (LAUDON; LAUDON, 2007). Assim,

a empresa, ao implantar o sistema de *tokens*, tornou sua rede mais segura, minimizando a eficácia de programas *spyware* mal-intencionados que tentam capturar informações pessoais.

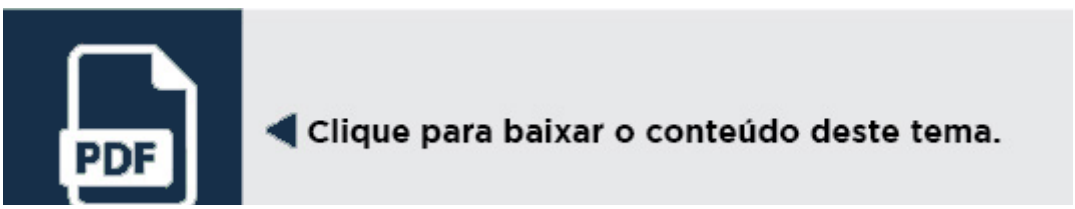
As redes de computadores e tecnologias da informação em geral, quando usadas de forma correta e adequada, proporcionam grandes benefícios aos usuários, organizações e empresas. Entretanto, as tecnologias podem ser mal utilizadas e causarem problemas e consequências muito sérias. Portanto, a questão de segurança das redes e das informações deve ser uma preocupação constante para usuários e organizações.

Síntese

Aqui, foram apresentados o conceito de redes de computadores, o histórico da internet, bem como os principais serviços disponíveis por ela. Também pudemos analisar como se dá o funcionamento da periferia e do núcleo da internet, além de entender a respeito dos modelos de referência OSI e TCP/IP. Outro ponto destacado foi a questão de segurança nas redes de computadores, fator de extrema relevância para organizações que usam suas redes para efetivação de diversas transações, como compartilhamento de informações entre clientes, fornecedores, parceiros, entre outros. A segurança é um assunto amplo e complexo, pois, atualmente, as ameaças e riscos são inúmeros.

Neste capítulo, você teve a oportunidade de:

- introduzir termos, terminologias e conceitos básicos sobre telecomunicações e redes de computadores;
- identificar e compreender todas as camadas e suas funções no modelo de referência OSI e na arquitetura TCP/IP;
- ter uma visão geral sobre a arquitetura OSI e TCP/IP.



Bibliografia

CARUSO, A. A. C.; STEFFEN, F. D. **Segurança em informática e de informações**. São Paulo: Senac, 1999.

FEY, A. F.; GAUER, R. R. **Introdução às redes de computadores**: modelos OSI e TCP/IP. 3. ed. S.l: ITIT, 2015.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw-Hill, 2008.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet**: uma abordagem *top-down*. 6. ed. São Paulo: Pearson, 2014. Disponível em: <https://bv4.digitalpages.com.br /?term=Redes%2520de%2520computadores%2520e%2520a%2520Internet %3A%2520uma%2520abordagem%2520Top-Down&searchpage=1& filtro=todos&from=busca#/edicao/3843 (https://bv4.digitalpages.com.br /?term=Redes%2520de%2520computadores%2520e%2520a%2520Internet %3A%2520uma%2520abordagem%2520Top-Down&searchpage=1& filtro=todos&from=busca#/edicao/3843)>. Acesso em: 14/11/2018.

LASKER, L.; PARKES, W. F. **Jogos de Guerra**. Direção: John Badham. Produção: Warner Bros. Cor. 114 min. Estados Unidos; Austrália, 1983.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informações gerenciais**. São Paulo: Pearson, 2007.

MOLINARI, W. **Desconstruindo a *web***: As tecnologias por trás de uma requisição. São Paulo: Casa do Código, 2016.

PETERSON, L. L.; DAVIE, B. S. **Redes de computadores**: uma abordagem de sistemas. 5. ed. Rio de Janeiro: Elsevier, 2013.

SOARES, L. F. G.; LEMOS, G.; COLCHER, S. **Redes de computadores**: das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Elsevier, 1995.

TANENBAUM, A. S. **Redes de computadores**. 4. ed. Rio de Janeiro: Elsevier,

2003.

_____.; WETHERALL, D. **Redes de computadores**. 5. ed. São Paulo: Pearson, 2011.

TORRES, G. **Redes de computadores**: curso completo. Rio de Janeiro: Axcel Books, 2004.