



FUNDAMENTOS DE REDES DE COMPUTADORES

Professor Esp. Rafael Alves Florindo
Professor Esp. Rafael Maltempe da Vanso

UNICESUMAR

Av. Guedner, 1610 - Jardim Aclimação
Cep 87050-900 - MARINGÁ - PARANÁ
unicesumar.edu.br
44 3027.6360

UNICESUMAR EDUCAÇÃO A DISTÂNCIA

NEAD - Núcleo de Educação a Distância
Bloco 4 - MARINGÁ - PARANÁ
unicesumar.edu.br
0800 600 6360

as imagens utilizadas neste
livro foram obtidas a partir
do site SHUTTERSTOCK.COM

FICHA CATALOGRÁFICA

C397 **CENTRO UNIVERSITÁRIO DE MARINGÁ.** Núcleo de Educação a Distância; **FLORINDO**, Rafael Alves; **VANSO**, Rafael Maltempe da.

Fundamentos de Redes de Computadores. Rafael Alves Florindo; Rafael Maltempe da Vanso.

Maringá-Pr.: UniCesumar, 2016. Reimpresso em 2022.

217 p.

"Graduação - EaD".

1. Fundamentos. 2. Redes. 3. Computadores. 4. EaD. I. Título.

ISBN 978-85-459-0344-4

CDD - 22 ed. 658.3
CIP - NBR 12899 - AACR/2

Ficha catalográfica elaborada pelo bibliotecário
João Vivaldo de Souza - CRB-8 - 6828

Impresso por:

Reitor

Wilson de Matos Silva

Vice-Reitor

Wilson de Matos Silva Filho

Pró-Reitor Executivo de EAD

William Victor Kendrick de Matos Silva

Pró-Reitor de Ensino de EAD

Janes Fidélis Tomelin

Presidente da Mantenedora

Cláudio Ferdinandi

NEAD - Núcleo de Educação a Distância**Diretoria Executiva**

Chrystiano Mincoff

James Prestes

Tiago Stachon

Diretoria de Graduação

Kátia Coelho

Diretoria de Pós-graduação

Bruno do Val Jorge

Diretoria de Permanência

Leonardo Spaine

Diretoria de Design Educacional

Débora Leite

Head de Curadoria e Inovação

Tania Cristiane Yoshie Fukushima

Gerência de Processos Acadêmicos

Taessa Penha Shiraishi Vieira

Gerência de Curadoria

Carolina Abdalla Normann de Freitas

Gerência de Contratos e Operações

Jislaine Cristina da Silva

Gerência de Produção de Conteúdo

Diogo Ribeiro Garcia

Gerência de Projetos Especiais

Daniel Fuvorki Hey

Supervisora de Projetos Especiais

Yasminn Talyta Tavares Zagonel

Coordenador de Conteúdo

Danillo Xavier Saes

Designer Educacional

Maria Fernanda Canova Vasconcelos

Ana Claudia Salvadego

Projeto Gráfico

Jaime de Marchi Junior

José Jhanny Coelho

Arte Capa

Arthur Cantareli Silva

Ilustração Capa

Bruno Pardinho

Editoração

Fernando Henrique Mendes

Qualidade Textual

Hellyery Agda

Pedro Afonso Barth

Ilustração

Bruno Cesar Pardinho Figueiredo



Professor
Wilson de Matos Silva
Reitor

Em um mundo global e dinâmico, nós trabalhamos com princípios éticos e profissionalismo, não só para oferecer uma educação de qualidade, mas, acima de tudo, para gerar uma conversão integral das pessoas ao conhecimento. Baseamo-nos em 4 pilares: intelectual, profissional, emocional e espiritual.

Iniciamos a Unicesumar em 1990, com dois cursos de graduação e 180 alunos. Hoje, temos mais de 100 mil estudantes espalhados em todo o Brasil: nos quatro campi presenciais (Maringá, Curitiba, Ponta Grossa e Londrina) e em mais de 300 polos EAD no país, com dezenas de cursos de graduação e pós-graduação. Produzimos e revisamos 500 livros e distribuímos mais de 500 mil exemplares por ano. Somos reconhecidos pelo MEC como uma instituição de excelência, com IGC 4 em 7 anos consecutivos. Estamos entre os 10 maiores grupos educacionais do Brasil.

A rapidez do mundo moderno exige dos educadores soluções inteligentes para as necessidades de todos. Para continuar relevante, a instituição de educação precisa ter pelo menos três virtudes: inovação, coragem e compromisso com a qualidade. Por isso, desenvolvemos, para os cursos de Engenharia, metodologias ativas, as quais visam reunir o melhor do ensino presencial e a distância.

Tudo isso para honrarmos a nossa missão que é promover a educação de qualidade nas diferentes áreas do conhecimento, formando profissionais cidadãos que contribuam para o desenvolvimento de uma sociedade justa e solidária.

Vamos juntos!



Janes Fidélis Tomelin

Pró-Reitor de Ensino de EaD

Kátia Solange Coelho

Diretoria de Graduação e Pós

Débora do Nascimento Leite

Diretoria de Design Educacional

Leonardo Spaine

Diretoria de Permanência

Seja bem-vindo(a), caro(a) acadêmico(a)! Você está iniciando um processo de transformação, pois quando investimos em nossa formação, seja ela pessoal ou profissional, nos transformamos e, consequentemente, transformamos também a sociedade na qual estamos inseridos. De que forma o fazemos? Criando oportunidades e/ou estabelecendo mudanças capazes de alcançar um nível de desenvolvimento compatível com os desafios que surgem no mundo contemporâneo.

O Centro Universitário Cesumar mediante o Núcleo de Educação a Distância, o(a) acompanhará durante todo este processo, pois conforme Freire (1996): “Os homens se educam juntos, na transformação do mundo”.

Os materiais produzidos oferecem linguagem dialógica e encontram-se integrados à proposta pedagógica, contribuindo no processo educacional, complementando sua formação profissional, desenvolvendo competências e habilidades, e aplicando conceitos teóricos em situação de realidade, de maneira a inseri-lo no mercado de trabalho. Ou seja, estes materiais têm como principal objetivo “provocar uma aproximação entre você e o conteúdo”, desta forma possibilita o desenvolvimento da autonomia em busca dos conhecimentos necessários para a sua formação pessoal e profissional.

Portanto, nossa distância nesse processo de crescimento e construção do conhecimento deve ser apenas geográfica. Utilize os diversos recursos pedagógicos que o Centro Universitário Cesumar lhe possibilita. Ou seja, acesse regularmente o Studeo, que é o seu Ambiente Virtual de Aprendizagem, interaja nos fóruns e enquetes, assista às aulas ao vivo e participe das discussões. Além disso, lembre-se que existe uma equipe de professores e tutores que se encontra disponível para sanar suas dúvidas e auxiliá-lo(a) em seu processo de aprendizagem, possibilitando-lhe trilhar com tranquilidade e segurança sua trajetória acadêmica.

Professor Esp. Rafael Alves Florindo

Bacharel em Ciências da Computação pela Faculdades Adamantinenses Integradas FAI (2003), possui Especialização em Desenvolvimento de Sistemas Web pela Universidade Estadual de Maringá UEM (2008) e Formação Pedagógica - PARFOR pela Universidade Estadual de Maringá UEM (2012). Professor de cursos técnicos profissionalizantes em Informática pela SEED-PR e professor mediador dos cursos de graduação ADS – Análise e Desenvolvimento de Sistemas e SI – Sistemas para Internet na modalidade de ensino EAD pela UniCesumar (2015). Mestrando em Gestão do Conhecimento nas Organizações na linha de pesquisa Educação e Conhecimento pela (UniCesumar).

<http://lattes.cnpq.br/7246554526271622>

Professor Esp. Rafael Maltempe da Vanso

Bacharel em Ciências da Computação pela Faculdade de Filosofia, Ciências e Letras de Mandaguari - FAFIMAN (2007), possui Especialização em Engenharia de Sistemas pela Escola Aberta do Brasil - ESAB (2010), formação complementar em Tecnologia em Telecomunicações e Gerência de Projetos, pela Escola Aberta do Brasil - ESAB (210). Atualmente é Professor Mediador dos cursos de graduação ADS – Analise e Desenvolvimento de Sistemas e SI – Sistemas para Internet na modalidade de ensino EAD pela UniCesumar (2015).

Lattes: <http://lattes.cnpq.br/5466282901446539>

FUNDAMENTOS DE REDES DE COMPUTADORES

SEJA BEM-VINDO(A)!

Caro(a) acadêmico(a).

Vivemos em uma nova sociedade e, de acordo com as nossas necessidades, os sistemas de informações e as redes de computadores tiveram que evoluir, para proporcionar suporte necessário ao conhecimento. Praticamente todas as organizações, sejam elas grandes corporações, pequenas e médias dos mais diversos setores, como comércio, serviços, indústrias e educação, utilizam-se de sistemas computacionais nos quais as redes de computadores representam a infraestrutura de transmissão e compartilhamento da informação.

Este material foi pensando em você, iniciante em redes de computadores, fornecendo diversos conceitos fundamentais da disciplina de Fundamentos de Redes de Computadores. Serão fornecidos subsídios para que o leitor tenha condições de compreender o pleno funcionamento de uma rede de informática.

Este livro está dividido em cinco unidades. Iremos abordar desde os conceitos básicos de redes de computadores aos mais atuais, como a internet das coisas. O objetivo deste livro é fomentar em você o desejo em continuar com os estudos deste conteúdo, que é de grande valia para as empresas.

Logo na primeira unidade, estudaremos os fundamentos que circundam as redes de computadores existentes no mercado de trabalho, assim como suas topologias, para que possamos classificá-las quanto ao meio de transmissão.

A segunda unidade é dedicada exclusivamente a conexões existentes: seja ela com fio, sem fio, remota, infravermelho ou por Bluetooth, bem como os tipos de protocolos mais utilizados em redes de computadores, como: UDP, TCP, DHCP, FTP, HTTP, SSL, SSH, DNS, SNMP e, para finalizarmos o tópico, uma breve introdução ao Modelo ISO/OSI e realizar uma breve classificação das 7 camadas.

A terceira unidade consistirá na apresentação ao modelo OSI – em suas 7 camadas (física, enlace de dados, rede, transporte, sessão, apresentação e aplicação), e você aprenderá para qual finalidade eles foram criados.

Da unidade II até a unidade IV, descreveremos o funcionamento das redes, no tocante a protocolos, tipos de transmissões e como classificá-las. Na quarta unidade, abordaremos sobre conceitos de segurança em redes de computadores, passando pela criptografia, assinaturas digitais, os tipos de ataques e como se defender. E, para finalizar, o que vem a ser um sistema operacional de redes.

E para finalizarmos o nosso livro, abordaremos sobre o conteúdo do momento, a computação em nuvem como serviço ou armazenamento, os tipos de virtualização e a famosa internet das coisas. Desta forma, iniciamos a quebra do modelo tradicional de informática, saindo do mundo “físico” de enormes data centers para o mundo “virtual”, reduzindo custos com equipamentos e pessoas.

Bom estudo.

SUMÁRIO

UNIDADE I

ENTENDENDO REDES DE COMPUTADORES

15 Introdução

16 Aplicações das Redes de Computadores

26 Tipos de Redes de Computadores

33 Hardware e Software de Rede

38 Switch

40 Roteador

41 Meios de Transmissão

51 Topologias de Redes

55 Considerações Finais

61 Referências

62 Gabarito



SUMÁRIO

■ UNIDADE II

CONEXÕES, PROTOCOLOS E MODELOS

65	Introdução
66	Tipos de Conexões
74	Redes Móveis
77	Protocolos e Padrões de Rede
88	Endereços de Ip, Subredes e Roteamento
93	Modelos de Referência
97	Considerações Finais

■ UNIDADE III

INTRODUÇÃO AO MODELO OSI - CAMADAS (FÍSICA, ENLACE DE DADOS, REDE, TRANSPORTE, SESSÃO, APRESENTAÇÃO E APLICAÇÃO)

111	Introdução
112	Camada Física
115	Camada de Enlace de Dados
125	Camada de Transporte
130	Camada de Sessão
131	Camada de Apresentação
132	Camada de Aplicação
135	Considerações Finais
143	Gabarito



SUMÁRIO

UNIDADE IV

INTERNET E SEGURANÇA DA INFORMAÇÃO

-
- 147 Introdução
 - 148 Criptografia E Segurança
 - 151 Assinaturas Digitais
 - 155 Segurança Da Comunicação
 - 165 Tipos de Ataques
 - 169 Sistemas Operacionais Para Rede
 - 175 Considerações Finais
 - 184 Gabarito
-

UNIDADE V

CLOUD COMPUTING E VIRTUALIZAÇÃO

-
- 187 Introdução
 - 188 Princípios da Computação na Nuvem e Acesso
 - 193 Software, Infraestrutura e Plataforma Como Serviço
 - 194 Sua Empresa e a Computação em Nuvem
 - 197 Virtualização
 - 202 Internet das Coisas
 - 204 Considerações Finais
 - 214 Referências
 - 216 Gabarito
 - 217 Conclusão
-



ENTENDENDO REDES DE COMPUTADORES

UNIDADE

I

Objetivos de Aprendizagem

- Entender o que é uma Rede de Computadores.
- Classificar as diversas Redes existentes.
- Estudar as Tecnologias utilizadas em Redes e Principais Dispositivos de Redes.
- Conhecer os diversos meios de Transmissão de Dados.
- Categorizar as Topologias de Redes, relacionando-os com os meios de Transmissão.

Plano de Estudo

A seguir, apresentam-se os tópicos que você estudará nesta unidade:

- Aplicações das Redes de Computadores
- Tipos de Redes de Computadores
- Hardware e Software de Rede
- Meios de Transmissão
- Topologias de Redes

INTRODUÇÃO

Desde os primórdios da humanidade, a comunicação é uma das maiores necessidades da sociedade. Nessa época, a comunicação era realizada por vários tipos de sinais, tais como: fumaça, geração de ruídos, gravuras em cavernas, entre outros. Essa necessidade de se comunicar com o próximo resume especificamente cada época; sendo para segurança, sobrevivência e continuação da espécie.

A evolução da comunicação se deu pelas passagens dos séculos XVIII, com os sistemas mecânicos, as máquinas a vapor do século XIX, e agora, os séculos XX e XXI com grandes conquistas tecnológicas, tanto para computadores *desktop*, pessoais e sistemas de comunicação, como satélites, smartphones, tablets, entre outros.

Com a união dos computadores e das comunicações, os sistemas computacionais sofreram uma profunda mudança na sua organização, com o intuito de se aproximar, facilitar e padronizar a forma de comunicação entre dois ou mais dispositivos ou pessoas. Nesse contexto, afirmamos que as redes de computadores surgiram da necessidade de se compartilhar recursos e informações entre computadores e seres humanos, facilitado nos dias atuais pela internet.

Nesta unidade, iremos abordar as aplicações das Redes de Computadores, qual a sua importância para as organizações, e como classificar os tipos de redes. Também abordaremos os itens de hardware de uma rede, os tipos de cabeamentos utilizados para a transmissão dos dados, os meios de transmissão e, por fim, os diferentes tipos de topologias de redes.

Após esses conceitos, você poderá entender e auxiliar na elaboração e implantação de uma rede de computadores. Pois em quase todas as empresas você encontrará uma rede de computadores, ou simplesmente no uso de uma rede doméstica, referente à tecnologia da Informação e comunicação! Vamos começar?



APLICAÇÕES DAS REDES DE COMPUTADORES

Neste tópico, iremos abordar alguns conceitos de redes, tais como seu surgimento, sua finalidade, suas aplicações, sua colaboração com as redes internet, intranet e extranet.

Entendemos rede de computadores como uma interligação de dispositivos, sendo estes por meio físico (cabeada) ou sem fio (*wireless*). Essa interligação pode ser composta de dispositivos de informática (computadores, impressoras, dispositivos de redes, entre outros) ou dispositivos de comunicação (celulares, *smartphones*, *tablets*, centrais de PABX, entre outros). O objetivo desta interligação unicamente é para a troca de informações e compartilhamento de recursos (MORIMOTO, 2011).

De acordo com Morimoto (2011), as primeiras redes de computadores surgiram na década de 60 com o objetivo de transferir informações de um computador a outro, substituindo assim uma das funções dos antigos cartões perfurados.

Podemos encontrar redes de computadores em qualquer ambiente (residencial, comercial e universitário), desde que tenha pelo menos dois dispositivos físicos ou portáteis. Por exemplo, imaginemos um *shopping* com a rede *wireless* aberta aos clientes e visitantes, as suas lojas poderiam utilizar este recurso. Quando os seus clientes fossem ao *shopping*, receberiam uma mensagem de boas vindas, uma oferta para o dia, desconto especial em algum produto, enfim, a loja poderia proporcionar um atendimento especial ao cliente.

Outro exemplo de compartilhamento de recursos, comentado em vários livros sobre o assunto, é o compartilhamento de impressoras. Imaginemos agora um departamento de uma empresa, independente do gênero e do porte, que dispõe de uma impressora para cada terminal. Podemos imaginar as despesas que teríamos com compra, acessórios, manutenções e gastos indevidos com as impressoras. Colocando algumas impressoras de alto poder de impressão em pontos estratégicos, a empresa irá economizar em acessórios, manutenção, e reduzirá as impressões desnecessárias.

SAIBA MAIS



Podemos trazer outros exemplos de compartilhamento, agora com compartilhamento de programas e arquivos. Tomamos como exemplo prático o que está ocorrendo para a escrita deste livro. Os autores, o designer educacional, o revisor e o diagramador estão utilizando o compartilhamento em nuvem tanto de serviço quanto de arquivo, ou seja, estamos utilizando um recurso de editor de textos na nuvem e estamos editando o mesmo arquivo ao mesmo tempo. Vamos assistir um vídeo para ilustrar o compartilhamento. Este vídeo está disponível em: <<https://www.youtube.com/watch?v=pEWWpgUoguo&spfreload=5>>. Acesso em: 14 abr. 2016.

Fonte: o autor

A partir deste compartilhamento ganhamos tempo e qualidade do serviço, pois todos os responsáveis já podem ir adequando a escrita e os padrões em fase de construção, acelerando e controlando a qualidade da escrita do livro. O recurso de nuvem será mais detalhado na unidade V (*Introdução ao Cloud Computing e virtualização*).

As redes de computadores também podem ser encontradas em residências, onde podemos conectar todos os computadores desktops, notebooks, tablets, smartphones a um dispositivo de rede cabeada ou sem fio, para troca de informações, lazer com jogos em redes e navegação pela internet. Normalmente este tipo de rede é chamado de *LAN*, e será descrita mais à frente em nossa unidade.

As empresas e universidades são as que mais utilizam das redes de computadores, conectando todos os departamentos, utilizando serviços de servidores para controle de usuários, compartilhamento de arquivos e serviços. É possível conectar várias redes em longa distância. Normalmente, esse tipo de rede é chamado de *intranet* e *extranet*, que também será abordado mais à frente.



Figura 1 - Redes de computadores



REFLITA

Cada vez mais as redes de computadores estão adentrando em nossas residências e nas organizações. Nesse sentido, será possível uma organização ou uma residência ficar sem acesso à rede de comunicação?

Fonte: o autor.



ANOTAÇÕES



Figura 2 - Internet

Reprodução proibida. Art. 184 do Código Penal e Lei 9.610 de 19 de fevereiro de 1998.

Internet

A internet é um conjunto de redes de computadores conectadas pelo mundo inteiro, com o objetivo de compartilhamento de informações, sejam elas textuais, por vídeos ou imagens.

De acordo com os autores Tanenbaum e Wetherall (2011) e Ross e Kurose (2005), a internet surgiu em 1969 pela necessidade de comunicação entre laboratórios do Departamento de Defesa do governo norte-americano. O surgimento da internet veio com a ideia de descentralização das bases de informações, uma vez que os EUA estava no auge da Guerra Fria. Durante uma guerra poderiam haver perdas, se estes laboratórios fossem atingidos. Para que esta rede não ficasse inoperante, cada nó da rede¹ tinha mais duas conexões independentes com outros nós, ou seja, cada nó tinha três conexões, para caso uma falhasse, a outra conexão funcionaria.

¹ Nós de rede ou terminal são equipamentos físicos que enviam e recebem dados em uma rede, dentre eles podemos citar: modem, hub, switch, impressora ou um computador (MORIMOTTO, 2011; TANENBAUM; WETHERALL, 2011).

Logo em seguida, conforme Morimoto (2011), em meados de 1970 foi criada a Arpanet com o objetivo de aproveitar os recursos de redes de computadores, conectar os laboratórios da defesa norte-americana e as quatro grandes universidades situadas respectivamente em *Stanford Research Institute*, na Universidade da Califórnia, na Universidade de Santa Barbara e na Universidade de Utah, sendo que cada centro tinha uma rede específica, sem padrões de comunicação. Ainda na mesma década, outros 30 centros universitários estavam conectados, dessa forma, deu-se o nome de Internet.

Desde 1970 até os dias atuais, os computadores, os softwares e toda a infraestrutura de redes, tais como os equipamentos, os cabos e os protocolos de comunicação evoluíram muito, proporcionando à Internet mais agilidade, segurança e uma ampla gama de serviços e informações disponibilizados (ROSS; KUROSE, 2005).

Para conectar-se à internet, basta ter um dispositivo de conexão, um dispositivo de acesso e navegação, os dados de acesso, como usuário e senha, e um navegador (*browser*).

A internet que conhecemos hoje é bem diferente de seu início. Não havia interatividade, usabilidade e navegabilidade, pois tudo era baseado em modo texto, de forma estática.

Conforme estudos de Bittencourt e Isotani (2015), a *Web* nasceu em 1991, seu criador foi Tim Berners Lee, que desenvolveu uma linguagem para interligar computadores do laboratório e outras instituições de pesquisa e exibir documentos científicos de forma simples e fácil de acessar. Foi também criador dos navegadores, o mais conhecido Nexus, desde então, várias empresas foram criando navegadores sofisticados, permitindo que mais recursos fossem contemplados.

A linguagem de programação nativa da internet podemos chamar de *HTML* (*Hypertext Markup Language* – Linguagem de Hipertexto de marcação), mesmo que seja uma linguagem interpretativa, pois é por meio dessa e de outras linguagens de programações (*PHP*, *JAVA*, *ASP* etc.), recursos de estilo de páginas (*CSS*), recursos de efeitos (*JS*, *JQUERY*) e de banco de dados (*MYSQL*, *POSTGRE*, *ORACLE* etc.), que podemos encontrar desde sites estáticos (parados sem interação com usuário) a sites dinâmicos, com a interação do usuário.

Dispomos hoje na internet serviços de correio eletrônico, blogs, portais de notícias, sites de comércio eletrônico, ensino a distância, portais de vídeos, redes sociais, livrarias digitais, compra de passagens terrestres e aéreas, sites de pesquisa, base de dados para pesquisa acadêmica, web conferência, voz sobre IP, internet *banking*, enfim, temos tantos serviços disponibilizados na internet, que ficaria difícil relacionar todos eles em um livro.

As páginas WEB são conectadas entre si por meio de *hyperlinks* (ou *links*), que podem ser texto ou imagem. Quando você clica em um *link*, será redirecionado para algum endereço *URL* (*Uniform Resource Locator*) indicado, por exemplo: quando você clicar sobre alguma propaganda da Unicesumar, provavelmente você será redirecionado para o link <<http://www.unicesumar.edu.br>>, em que o *http://* significa (*Hipertext Transfer Protocol*, ou Protocolo de Transferência de Hipertexto).



Figura 3: Servicos da Internet

Os sites ou dispositivos dispostos na *Web* necessitam de um endereço virtual, igual ao seu endereço residencial. Para endereços virtuais, damos o nome de *IP* (*Internet Protocol*), que é um número específico de controle do dispositivo dentro de uma rede, ou seja, idêntico ao residencial, não podendo ter em uma mesma cidade duas ruas com o mesmo nome. Este endereço *IP* é capaz de diferenciá-lo de todos os outros na rede mundial.

Além dos computadores, os serviços de sites e roteadores também possuem esses números para identificá-los. O endereço *IP* consiste em quatro sequências de três números, como por exemplo: 192.168.001.001. Toda vez que você se conectar com a internet, seu computador será registrado com um endereço diferente disponível na rede.



SAIBA MAIS

Com a popularização dos dispositivos móveis (celulares, notebooks, smartphones e tablets), e dos dispositivos “vestíveis” que podem ser utilizados por pessoas (tais como: relógios inteligentes, marca passo, entre outros) que se comunicam via rede, de acordo com o site CisoAdviso, 72% do total de dispositivos terão conexões móveis em 2020. Os dispositivos inteligentes serão responsáveis por 98% do tráfego de dados móveis em 2020.

Leia a matéria na íntegra em: <<https://www.cisoadvisor.com.br/70-do-mundo-usara-dispositivos-moveis-em-2020/>> Acesso: 24 set. 2020

Em complemento à matéria acima, leia a matéria sobre o já esgotado IPV4 e o IPV6 que está disponível no link: <<http://www.infowester.com/ipv6.php>> Acesso em: 14 abr. 2016.

Fonte: Brito (2016, on-line).

Alguns serviços na *Web* necessitam de endereços fixos para funcionar. Para que seja possível uma conexão remota, por exemplo, nesse caso, a empresa compra um endereço IP fixo dela, desta forma, toda vez que se conectar com a internet, esse endereço será atribuído a ela, pois o endereço IP está reservado exclusivamente para ela.



Figura 4 - Endereço IP

Agora imagine você ter que decorar todos estes endereços IP para acessar determinado serviço na Web, teríamos que andar com uma planilha contendo os endereços e os nomes dos sites, ou então memorizar. Para evitar isso, surgiu o *DNS* (*Domain Name Systems* – Sistemas de Nome de Domínio), ou seja, é um nome que serve para localizar e identificar sites ou grupos de computadores na Internet.

No Brasil, o site REGISTRO.BR é o responsável pelo registro de todos os sites e domínios. Para ter um domínio, é necessário ter identificação física e jurídica e um local de hospedagem, para que quando um usuário inserir o endereço do seu site em algum navegador ou sistema de busca, o seu provedor de acesso saiba onde localizar o site por meio desse serviço. Estes domínios podem ser assim classificados: .edu, .net, .gov, .com, .org, .mil etc.

A internet só chegou ao Brasil no final da década de 80 (1988). Os primeiros computadores conectados foram os centros acadêmicos de São Paulo (pela FAPESP – Fundação de Amparo à Pesquisa do Estado de São Paulo) e Rio de Janeiro (UFRJ – Universidade Federal do Rio de Janeiro e LNCC – Laboratório Nacional de Computação Científica), com intuito de compartilhar as pesquisas científicas (TANENBAUM; WETHERALL, 2011).

Figura 5 - Nomes de domínio



Em 1989, foi criado o primeiro *backbone* nacional, chamado de RNP (Rede Nacional de Pesquisa), interligando 11 estados brasileiros. Com a necessidade de interligar novas instituições, criado a partir desta espinha dorsal, foram criados outros *backbones*, chamados de *backbones* regionais, que interligavam o centro de ensino de várias regiões dos estados (TANENBAUM; WETHERALL, 2011).

Até a metade da década de 90, o acesso à internet era restrito ao meio acadêmico, e em pouco tempo depois (1995), foram iniciando as conexões comerciais a partir do *link* da Empresa Embratel, inicialmente por conexões discadas e futuramente com conexões ADSL, rádio etc. Veremos mais detalhes dessas conexões na unidade II deste livro.

Intranet

A intranet é uma rede de computadores interna de uma empresa, que não precisa estar conectada com a internet, e que tem por objetivo geral o compartilhamento de informações e de serviços. Estas redes só podem ser acessadas pelos seus usuários ou colaboradores de forma interna por questões de segurança. Por exemplo: uma empresa pode disponibilizar aos seus funcionários a comodidade de imprimir sua folha de pagamento, disponibilizar também serviços de protocolos para abertura de chamados técnicos, solicitação de compra de produtos de expediente, disponibilização de boletins internos, disponibilização de manuais de processos, pode também disponibilizar um canal de troca de mensagens que visa facilitar e proporcionar um ganho de tempo no treinamento de novos colaboradores.

A intranet está sendo considerada, atualmente, um dos principais veículos de comunicação em corporações. Por ela, o fluxo de dados (centralização de documentos, formulários, notícias da empresa etc.) é constante, pretendendo reduzir os custos e ganhar velocidade na divulgação e distribuição de informações, mantendo assim um repositório de conhecimento que pode ser acessado, reutilizado e disseminado.

Atualmente, os sistemas de intranet utilizam os navegadores de internet e recursos de servidores de hospedagem WEB de forma privada, utilizando para o seu funcionamento os protocolos de internet (*TCP/IP*). Estas intranets podem ser sistemas *ERP*², junção de sistemas *SIG*³, sistemas de *CRM*⁴, entre outros.

Extranet

Podemos partir do princípio de que a rede denominada extranet refere-se a uma rede de computadores que é conectada com alguma outra rede de computadores externa, e para que isso seja possível, utilizamos a internet como meio de comunicação. A utilização da Internet para essa rede facilita a troca de informações com segurança por meio de acesso controlado por login e senha. Vamos a um exemplo de extranet.

Tomemos uma empresa comercial (A) que realiza vendas de produtos. Seus vendedores têm acesso ao sistema de vendas que está na intranet para realizar orçamentos e vendas aos clientes. Quando o cliente solicita um produto que a loja não possui em estoque, automaticamente o sistema “entra” em contato com a empresa (B) que é sua fornecedora, que por sua vez, realizará o pedido para a loja com a finalidade de atender o cliente. Devemos lembrar que, todo este procedimento é automatizado por algum sistema, e neste exato momento as duas redes se comunicaram, ou seja, a rede da empresa A com a rede da empresa B. Para que esta comunicação aconteça, as duas intranets devem seguir os mesmos padrões de troca de informações, mantendo o relacionamento com seus parceiros, clientes e fornecedores.

As duas empresas devem possuir sua própria Intranet, ambas com sua gerência, e devem também estar interligadas para troca de informações, pedidos, pagamentos, emissão de relatórios etc. O resultado desta transação fornece às altas gerências subsídios para melhor atender seus clientes em determinadas épocas

² *ERP - Enterprise Resource Planning* (ou Planejamento de Recursos Empresariais, em português) é um sistema de gestão empresarial que contemplam vários módulos da empresa.

³ *SIG - Management Information Systems* (ou Sistemas de Informações Gerenciais, em português) é um sistema de informação que fornece indícios para tomadas de decisões gerenciais.

⁴ *CRM – Customer Relationship Management* (ou Gestão do Relacionamento com o Cliente, em português) é um sistema de relacionamento com o cliente.

do ano, pois toda transação realizada resulta em um registro de conhecimento e em uma base de dados, para o relacionamento comercial produtivo entre ambos.

Outro exemplo de acesso pela rede extranet são as conexões remotas realizadas normalmente pela alta gerência da organização, pois é comum que estes gerentes fiquem a maior parte do tempo fora da organização em reuniões, e precisam estar informados de todas as transações da empresa para que possam tomar decisões a qualquer momento. Geralmente, tais gerentes têm acesso ao sistema SAD (Sistema de Apoio a Decisão), que fornece subsídios para tomadas de decisões.

Sendo assim as redes intranet e extranet, são utilizadas constantemente pelas empresas de pequeno, médio e grande porte. Para que essas redes funcionem de forma correta, no próximo tópico iremos estudar os tipos de redes de computadores e você perceberá as diferenças entre cada rede disposta, podendo fazer uma correlação em qual a intranet e a extranet se enquadram.

TIPOS DE REDES DE COMPUTADORES

Neste tópico, iremos abordar alguns conceitos de tipos de redes. Estudaremos como são formadas e utilizadas as redes de computadores em uma *LAN*, *MAN*, *WAN*, *Wireless* e suas derivações.

A classificação de redes de computadores pode ser descrita conforme o quadro 1.

TIPO	DESCRÍÇÃO	SUGESTÕES
<i>LAN (Local Area Network)</i>	Redes locais	
<i>MAN (Metropolitan Area Network)</i>	Rede cidade	
<i>WAN (Wide Area Network)</i>	Rede de Longa Distância	
Redes Domésticas	Rede doméstica	
<i>WPAN (Wireless Personal Area Network)</i>	São consideradas redes pessoais ou de curta distância sem fio	
<i>WLAN (Wireless Local Area Network)</i>	Redes locais sem fio	
<i>WMAN (Wireless Metropolitan Area Network)</i>	Rede metropolitana sem fio	
<i>WWAN (Wireless Wide Area Network)</i>	Celular móvel	

Quadro 1 - Classificação de Redes de Computadores

Fonte: os autores

LAN

As redes locais (ou *Local Area Networks*) são consideradas redes de funcionamento interno de uma empresa ou de uma residência. São compostas por dispositivos

de redes (*switch*, *hub*, roteador etc.), utilizando mídias de transmissão conectadas via cabo (par trançado, coaxial ou fibra ótica), ou sem fio, que interconectam cada placa de rede utilizando uma topologia (TANENBAUM; WETHERALL, 2011).

Essa rede possui uma alta taxa de transferência, podendo chegar à casa de gigabytes. Utilizam o protocolo *TCP/IP* como forma de comunicação entre dispositivos e o método de transporte *ETHERNET*.

Uma rede local pode dispor de tantos dispositivos quanto forem necessários em uma pequena área geográfica, variando de alguns metros a até quilômetros.



Figura 6 - Rede Local

Os usuários de uma rede local podem executar suas tarefas a partir de suas estações de trabalhos ou de dispositivos móveis. Estas tarefas podem ser das mais variadas possíveis, desde um editor de texto até uma conexão remota local.

Para um correto funcionamento da *LAN*, são necessárias estações de trabalho ou dispositivos móveis, mídia de transmissão, dispositivos de rede e protocolos de comunicação e o uso de servidores.

A rede local pode ser distinguida de duas formas, sendo elas: rede ponto a ponto (*peer to peer*, ou ainda *P2P*), em que as estações de trabalho ou dispositivos móveis são ligados em dispositivos de rede, permanecendo a administração para cada dispositivo, ou seja, cada dispositivo pode ser um servidor, compartilhando algum recurso ou dispositivo. Nesse caso, a administração se torna mais difícil, pois se deve administrar cada dispositivo.

Ao contrário dessa rede, temos a rede local como “cliente/servidor”, neste caso, é necessário o uso de um dispositivo denominado de servidor, que proverá serviços de rede, tais como: autenticação, *backup*, impressão, *firewall*, *Proxy*, entre outros, desta forma, a administração e manutenção torna-se menos onerosa.



Figura 7 - Rede local

MAN

Uma “*Metropolitan Area Network*” é considerada uma rede *LAN*, com alcance metropolitano, com um raio dimensão que abrange no máximo a uma cidade. Elas podem ser utilizadas para interligar redes locais de empresas, universidades, outras organizações, dispersos numa cidade (TANENBAUM; WETHERALL, 2011).

Normalmente, são interligados por internet, TV a cabo, fibra ótica ou a rádio, possibilitando assim uma taxa de velocidade alta na casa dos Gbits.

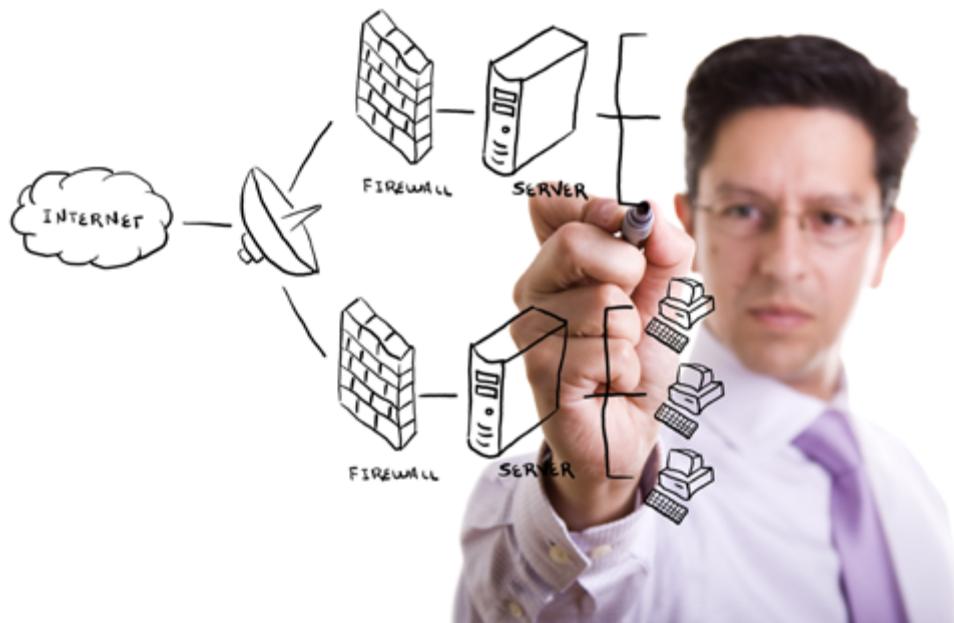
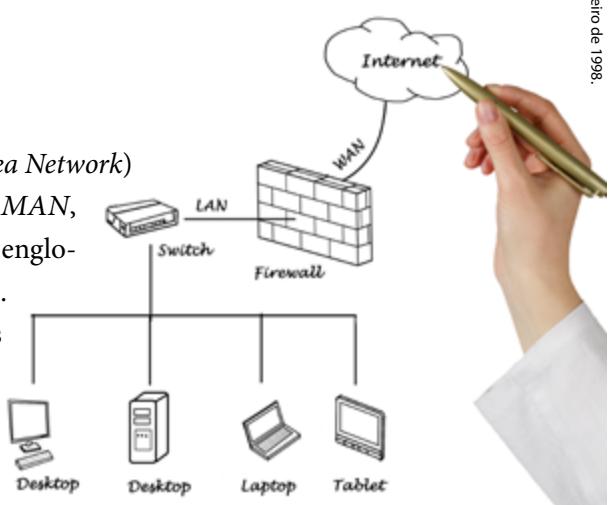


Figura 8 - Rede Man

WAN

A Rede de Longa Distância (*Wide Area Network*) é uma rede que vai além da rede *MAN*, ultrapassando as barreiras da cidade, englobando estados, países e até continentes.

Normalmente essa rede utiliza de linhas de transmissão de dados oferecidos por empresas de telecomunicações, provedores de internet e Empresas de cabeamento.



Essa rede está em constante atualização devido às novas tecnologias de telecomunicação, atendendo transmissões de áudio, vídeo, teleconferências, Voz-IP em tempo real (*Real Time*), entre outras. O limite de velocidade desta rede é dos computadores ou dispositivos conectados entre si, pois a mídia de transmissão atualmente é fibra ótica, que viaja na velocidade da luz.

Redes Domésticas

O uso de redes domésticas está em crescente expansão, imagine você poder ter uma rede dentro de sua casa, poder compartilhar impressoras, jogar em rede com amigos e familiares e várias outras coisas. Para isso, precisamos de uma rede *LAN* (ver tópico sobre rede *LAN*), que pode ser conectada com fio ou sem fio (*Wireless*). Bom, não é só computadores, *notebooks*, *smartphones* e *tablets* que se conectam em uma rede, hoje temos a internet das coisas conectando televisores, geladeiras etc. (veremos mais sobre este assunto na Unidade V).

Redes Wireless

A rede *Wireless* (sem fio) é o meio de transmissão que interliga dois ou mais dispositivos sem a presença de cabos. Podemos ver esta rede em *shoppings*, conveniências, supermercados, universidades, organizações e em residências.

Devido à facilidade e à praticidade dessa rede, ela corrobora perfeitamente para as redes domésticas, ou seja, encontrávamos em nossas residências *modem*, *HUB* e cabos espalhados nos cômodos onde se necessitava de computadores. Hoje, com esta facilidade, utilizamos um único aparelho, chamado de *modem roteador*, conectando apenas o cabo telefônico e o de energia; e automaticamente estamos interligados.

Esta forma de comunicação (sem fio) não é a única. Temos as formas de comunicação via satélite, a rádio, código Morse, infravermelho, todos com o mesmo objetivo, a troca de mensagens entre dispositivos.



Figura 10 - Rede Wireless

As redes sem fio também podem ser utilizadas fora de residências ou empresas, vejamos as suas classificações (*WPAN*, *WLAN*, *WMAN* e *WWAN*), assim como mais detalhes sobre as mesmas respectivamente.

WPAN – As redes *WPAN* (*Wireless Personal Area Network*) são consideradas redes pessoais ou de curta distância sem fio. Essa rede é bem restrita em questão de distância, é muito utilizada por infravermelho ou até mesmo *Bluetooth*.

WLAN – A rede *WLAN* (*Wireless Local Area Network*) foi projetada para redes domésticas ou redes particulares de organizações, *shoppings*, restaurantes etc. Esta rede permite uma diminuição no custo de implantação e manutenção, uma vez que não se utiliza de cabos para conexão com os dispositivos e pode fornecer um benefício maior aos usuários por compartilhar o sinal *Wi-fi* liberado para todos.

WMAN – A rede *WMAN* (*Wireless Metropolitan Area Network*) é a mesma rede metropolitana, só que agora sem fio, com alcance de alguns quilômetros. Aqui predomina a comunicação via rádio.

WWAN – A rede *WWAN* (*Wireless Wide Area Network*), mais conhecida como rede celular móvel pelo seu uso em pacotes de internet das operadoras de telefonia. Suas principais tecnologias são: *GSM* – *Global System for Mobile Communication*; *GPRS* – *General Packet Radio Service*; e, *UMTS* – *Universal Mobile Telecommunication System*. A tecnologia mais utilizada atualmente é a tecnologia *GSM*, que inicialmente foi amplamente utilizada com o sinal 2G, hoje, devido ao avanço das telecomunicações, chega-se ao sinal 4G.

HARDWARE E SOFTWARE DE REDE

Neste tópico, iremos abordar alguns conceitos físicos de redes, tais como, alguns concentradores (*hub*, *switch* e roteador), placa de rede e o padrão *Ethernet*.

Padrão Ethernet

O padrão *ethernet* foi criado pela Xerox em meados de 1980 e padronizado pelo IEEE como 802.3, com o intuito de definir um padrão de comunicação entre dispositivos dispostos em uma rede local, especificando padrões para a camada física e de enlace do Modelo OSI (TANENBAUM; WETHERALL, 2011).

De acordo com Tanenbaum e Wetherall (2011, p. 18) o padrão IEEE 802.3, é

mais conhecido como Ethernet, é uma rede de difusão de barramento com controle descentralizado, em geral operando em velocidades de 10 Mbps a 10 Gbps. Os computadores em uma rede Ethernet podem transmitir sempre que desejam; se dois ou mais pacotes colidirem, cada computador aguardará um tempo aleatório e fará uma nova tentativa mais tarde.

A tecnologia *ethernet* possui uma série de padrões que definem como serão feitas as instalações físicas, as conexões elétricas e as conexões lógicas entre os dispositivos de uma rede. O modo de transmissão deste padrão pode ser:

Tipo	Descrição	
<i>Half-duplex</i> :	Cada estação transmite ou recebe informações, não acontecendo transmissão simultânea, ou seja, enquanto a estação estiver enviando, a mesma não recebe, e vice-versa.	

Tipo	Descrição	
Full-duplex	Cada estação transmite e/ou recebe, podendo ocorrer transmissões simultâneas, desta forma, pode enviar e receber ao mesmo tempo.	 O diagrama mostra dois computadores conectados por um switch central. Cada computador tem uma interface de rede (NIC) com dois portos. Um porto de cada NIC está conectado ao switch, permitindo que ambos os computadores transmitam e recebam simultaneamente.

Quadro 2 - Modos de transmissão

Fonte: os autores

Hoje, existem vários padrões além da *Ethernet* e, dentre os principais, destacam-se *Fast Ethernet* e *Gigabit Ethernet*. Inicialmente o padrão *ethernet* tinha a velocidade de 10 Mbps, posteriormente passou a ser o *Fast Ethernet* com 100 Mbps, e depois chegando a 1000 Gbps, hoje já existem tecnologias que passam de 10 Gbps.

Os computadores e outros dispositivos, como impressoras, *smartphones*, *tablets* etc., interligados em uma rede *Ethernet* (física ou sem fio), podem transmitir mensagens (pacotes = informações) sempre que desejam; se dois ou mais pacotes colidirem, cada computador ou dispositivo terá de aguardar e realizar uma nova tentativa mais tarde (TANENBAUM; WETHERALL, 2011).

Placa de rede

Para que um computador se conecte com outro computador, ou com um dispositivo de rede, é necessário que cada dispositivo contenha uma placa de rede com os padrões *ethernet*, ou um *NIC* (*Network Interface Card*), para que possam conectar a mídia de transmissão (com ou sem fio) e o método de transmissão (*Ethernet*, *Fast Ethernet* etc). Alguns dispositivos, como a impressora, já trazem consigo a sua própria placa de rede, permitindo que possam conectar os dispositivos de rede. Temos também as placas de rede *on-board*, que já vêm embutidas na placa mãe (*Mother Board*), sendo consideradas, neste caso, de interface de rede.

Inicialmente, nas redes de computadores antigas, utilizavam-se as placas seguindo o padrão de slots ISA⁵, chegando à velocidade máxima de 10 Mbps, enquanto a PCI⁶ alcançava uma velocidade máxima de 100 Mbps, e o PCMCIA⁷, para dispositivos portáteis. A velocidade de transmissão destes equipamentos podem chegar até 1 GB. Contudo, esta velocidade ficará limitada sempre ao equipamento com menor taxa de transferência, ou seja, se você tiver em sua rede um dispositivo com velocidade de 10 Mbps, e o restante em 100 Mbps, a velocidade de sua rede se limitará a 10 Mbps.



Figura 11 - Placa de rede

5 ISA é abreviação de “Industry Standard Architeture”. “O ISA foi o primeiro barramento de expansão utilizado em micros PC. Existiram duas versões: os slots de 8 bits, que foram utilizados pelos primeiros PCs e os slots de 16 bits, introduzidos a partir dos micros 286”. Disponível em: <<http://www.hardware.com.br/termos/isa>>. Acesso em: 15 abr. 2016

6 PCI - Peripheral Component Interconnect. “Em 1992 foi introduzido o barramento PCI, que manteve a mesma frequência de operação, mas incorporou suporte nativo a plug-and-play e bus mastering, além de romper os laços de legado com o ISA, o que simplificou muito a pinagem do barramento.” Disponível em: <<http://www.hardware.com.br/livros/hardware/pci.html>>. Acesso em: 15 abr. 2016

7 PCMCIA - Personal Computer Memory Card International Association. “O padrão PCMCIA surgiu em 1990 como um padrão para a expansão de memória em notebooks. A ideia era permitir a instalação de memória RAM adicional sem precisar abrir o notebook e instalar novos módulos o que, na maioria dos modelos da época, era bem mais complicado do que hoje em dia.” Disponível em: <<http://www.hardware.com.br/livros/hardware/card-pcmcia.html>>. Acesso em: 15 abr. 2016.

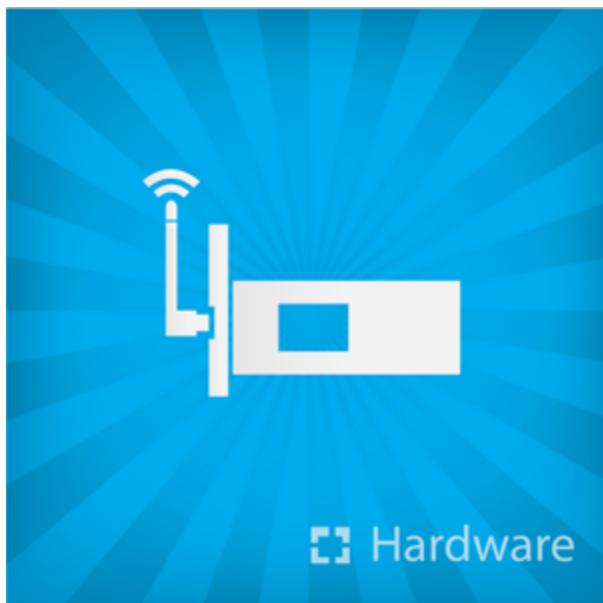


Figura 12 - Placa de rede *wireless*



SAIBA MAIS

Para saber mais sobre os outros tipos de barramentos que fizeram parte da história da computação, sugiro a você a leitura dos artigos Placas-mãe e barramentos: ISA, AGP, PCI, PCI Express, AMR disponíveis respectivamente nos seguintes links: <<http://www.hardware.com.br/guias/placas-mae-barramentos/isa-eisa-vlb-pci.html>> Acesso em: 15 abr. 2016; e <<http://www.infowester.com/barramentos.php>> Acesso em: 15 abr. 2016.

Fonte: os autores.

HUB

O *HUB* é um dispositivo de rede que tem uma única função: interligar fisicamente os dispositivos de uma rede, e seu funcionamento se assemelha a uma régua de energia.



Figura 13 - Hub

Reprodução proibida. Art. 184 do Código Penal e Lei 9.610 de 19 de fevereiro de 1998.

O *HUB* está caindo em desuso, pois o mesmo envia apenas um pacote por vez, e mesmo assim não tem controle de fluxo, não sabe qual rota tomar e nem sabe o local de início (remetente) e término (destinatário) da transferência dos pacotes, ou seja, quando enviamos um pacote direcionado para certo computador ou dispositivo da rede, ele enviará para todos, e quem for o destinatário do pacote “pega” o pacote para si, e em caso de erro, o pacote ficará perdido na rede.

Outro ponto que deixa este dispositivo obsoleto é devido ao mesmo nivelar a velocidade da rede para baixo. Exemplo: se você tiver em sua rede um dispositivo com velocidade de 10 Mbps, e o restante em 100 Mbps, a velocidade de sua rede se limitará em 10 Mbps.

A maioria dos *HUBs* possuem de 8 a 32 portas, sendo possível adicionar mais de um *HUB* na mesma rede, ou seja conectar um *HUB* no outro, como se o *HUB* fosse um computador. Desta forma, estamos utilizando o formato de cascamenteo, ou seja, conectando um a outro.

O *Hub* é muito utilizado em redes domésticas ou de pequenas organizações com poucos dispositivos, porém, todos estes devem ter a mesma velocidade, caso contrário, a sua rede irá trabalhar na menor velocidade. Normalmente, estas redes

utilizam a topologia estrela (será melhor descrita no tópico de **TOPOLOGIAS DE REDES**), tendo o *hub* como dispositivo centralizador.

Dentro do *Hub*, temos uma topologia barramento, ou seja, apenas um único canal de comunicação, por isso, ele só envia ou recebe um dado por vez na rede toda.

Em seu lugar, surgiu *hub-switch*, que é uma mescla de *hub* com *switch*. Este dispositivo atua na camada 2 e 3 do modelo OSI⁸ (será melhor descrito na unidade 3 deste livro), enquanto o *hub* atua na camada 1 do modelo OSI, dessa forma, também envia um pacote por vez, porém diferentemente do *hub*, este sabe o endereço do destinatário, não necessitando mais retransmitir para toda a rede, permitindo assim livre tráfego para a rede.

SWITCH

O **SWITCH**, diferentemente do *hub* e do *hub-switch*, é o dispositivo mais utilizado nas redes atuais, atuando na camada 2 e 3 do modelo OSI; porém, é um pouco mais caro do que o *hub* e o *hub-switch*. O *switch* consegue enviar e receber vários pacotes ao mesmo tempo, operando no modo *full-duplex* diferentemente dos outros dispositivos, ou seja, ele tanto transmite quanto recebe, permitindo assim um gerenciamento eficiente da rede.

O *switch* controla todo o tráfego da rede, buscando a melhor rota a ser seguida entre os dois dispositivos, por meio do endereço *MAC*⁹ de cada dispositivo, aumentando assim a velocidade da rede; por exemplo, tomemos dois

⁸ OSI - “Open System Interconnect” - “Foi criada em 1977 pela ISO (*International Organization for Standardization*) com o objetivo de criar padrões de conectividade para interligação de sistemas de computadores às redes de computadores” (CYCLADES, 1999, p. 43).

⁹ MAC – Média Access Control – “É um número único de 48 bits (usualmente representado como um número hexadecimal de 12 dígitos) que é codificado nos circuitos dos dispositivos para identificá-los em uma rede local” (CYCLADES, p. 50).

computadores ou dispositivos de redes, tais como impressoras ou servidores que desejam trocar informações entre si, por sua vez, o *switch* irá reservar um canal de comunicação exclusiva entre os dois computadores conectados em suas portas, evitando assim colisões de pacotes.

O *switch* também consegue controlar cada porta individualmente, ou seja, se tiver dispositivos com velocidades diferentes na sua rede, por exemplo, duas placas *ethernet*, uma com velocidade de 10 Mbps, e outra com 100 Mbps, o *switch* irá criar um canal de comunicação entre os dois, permitindo que apenas neste canal trafegue na menor velocidade, não interferindo na velocidade da rede.



Figura 14 - *Switch*

Existem vários modelos de *switch* no mercado, uns mais baratos e outros mais caros, tudo depende da sua utilidade. Temos *switches* programados via *software*, que torna possível a criação de redes distintas para cada porta do *switch*; nesse caso, precisará de um profissional capacitado para tal configuração. Por exemplo: uma organização possui muitos departamentos, todos os dispositivos de cada departamento estão conectados em um *switch*, que por sua vez se conectam no *switch* principal. Esse *switch* principal é programável e possui uma programação específica em cada porta delimitando os acessos de cada departamento, ou seja, libera para cada departamento apenas o essencial.

ROTEADOR

O roteador é quase igual ao *switch*, porém ele tem mais funções, sendo que seu uso requer mais capacidade técnica em lidar com a configuração. Tudo o que o *switch* faz internamente na sua rede, o roteador faz com interconexões com redes distintas, locais, metropolitanas, ou até geográficas, ou seja, o roteador conecta quantas redes forem necessárias.

Uma outra função básica do roteador é bem simples: ele identifica quando um micro se conecta à rede e então ele define um *IP* para esse micro. Após isso, a tarefa que ele cumpre é de organizar como os dados vão trafegar pela rede.

Atualmente alguns roteadores estão funcionando com modem, e estão roteando o sinal *wi-fi* para a rede de computadores, tanto para uma rede doméstica quanto para uma empresarial.



Figura 15 - Roteador *Wi-Fi*

MEIOS DE TRANSMISSÃO

Neste tópico, iremos abordar alguns conceitos de meios de transmissão, seja ele físico por meio de cabos (coaxial, par trançado e fibra) e pela disposição dos dispositivos por meio das topologias de redes (Barramento, Anel e Estrela). Sendo assim, podemos entender como meio de transmissão, o ato de transmitir dados de um dispositivo para o outro dispositivo. Atualmente temos as seguintes mídias, sendo elas:

Par de cobre trançado	Para redes locais	
Cabos coaxiais	Para links de comunicação	
Fibra Ótica	Para equipamentos de longa distância	
Radiofusão	Para transmissão de dados via ondas de rádio	

Enlace de Micro-ondas	Para conectar localidade onde não existe disponibilidade de cabos de cobre ou par trançado	
Infravermelho	Para conectar dois edifícios próximos e para ambientes internos. Limite de 50 metros	
Transmissão de ondas via satélite	Para localidades remotas onde não existe outro tipo de transmissão	

Quadro 3 - Meios de transmissão

Fonte: os autores

De acordo com Tanenbaum e Wetherall (2011), “Os meios de transmissão podem ser guiados ou não guiados”. Desta forma, temos os meios guiados como meios físicos tais como os cabos (par trançado, o cabo coaxial e a fibra óptica) e os meios não guiados (a rádio, os raios infravermelhos, wireless, satélite, e outros). Iremos descrever com mais detalhes os dois meios.

Cabo Coaxial

O pioneiro meio de transmissão de computadores foi o cabo coaxial, muito utilizado nas placas *ethernet* 10 Mbps. O cabo coaxial foi muito utilizado em redes de computadores em ambientes industriais sujeitos às interferências eletromagnéticas e, principalmente, onde a distância entre os computadores é entre 200

metros. Utilizaram os conectores BNC (“*Bayonet Neill Concelman*” ou *Bristish Naval Connector*) para conectar o cabo nas placas de redes dos computadores e o conector chamado de (T) para conectar os transceptores no cabo. Os padrões mais utilizados foram o 10base5 e o 10base2.

O cabo coaxial 10base5 foi o primeiro a ser utilizado em redes de computadores. Sua estrutura permitia ter uma expansão de no máximo 500 metros diretos conectando até 100 dispositivos. Muito utilizado em redes de *mainframes*, este cabo, na época, era considerado grosso pelo motivo de ter uma Blindagem Dupla. O cabo era pouco flexível, o que dificultava a instalação e tinha um custo razoavelmente alto.

Já o segundo tipo de cabo 10base2 ultrapassou o primeiro na questão de diâmetros, o mesmo ficou mais fino e flexível devido à Blindagem Simples, alcançando 185 metros e conectando até 30 computadores com uma distância de 50 cm entre dispositivos. Uma das vantagens sobre este cabo foi principalmente a facilidade de expansão da rede e melhor custo/benefício.

Ambos eram utilizados na topologia Barramento, em que o mesmo possui um fio central e que são colocados os transceptores que irão perfurar todas as camadas do cabo, chegando até o fio de cobre para transmissão do sinal.

Os dois tipos de cabos trafegavam em uma velocidade de 10 Mbps e utilizavam o padrão *ethernet* de 10 megabits. O último dispositivo desta rede necessita de um terminador encaixado diretamente no conector T do primeiro computador e outro terminador no último computador da rede. Pelo menos um dos terminadores deverá ser aterrado.

Os terminadores tinham a função de terminar com o sinal quando o mesmo chegar ao final da rede, e não encontravam o seu destino, eliminando assim os chamados pacotes sombras, que por sua vez acabavam por atrapalhar o tráfego da rede, causando lentidão.



Figura 16 - Cabo coaxial

O cabo coaxial produz internamente um campo eletromagnético entre o núcleo interno (fio de cobre) e blindagem (malha de metal); com este campo interno o sinal a ser transmitido é melhor, isentando de interferências externas.

Este cabo possui quatro camadas, sendo elas:

- **Jaqueta:** é responsável por proteger o cabo do ambiente externo. Geralmente é de borracha (PVC), ou, raramente, de teflon.
- **Malha de metal:** é o envelope metálico que envolve os cabos, permitindo proteger todos os dados que são transmitidos para não ocasionar em uma distorção dos dados.
- **Isolamento interno:** envolve a parte central sendo formado por um material dielétrico que tem a função de evitar qualquer contato com a blindagem, evitando o contato direto dos cabos caso haja ruptura em algum ponto do cabo, e auxiliando na diminuição do campo magnético produzido pelos próprios cabos.
- **Fio de cobre:** possui a função de transportar os dados, geralmente é formada somente por um fio de cobre ou vários fios entrançados.

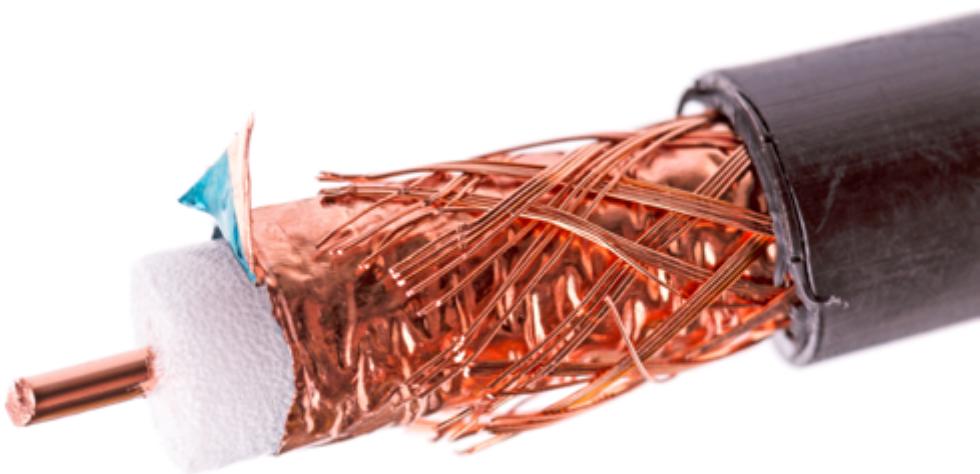


Figura 17 - Estrutura do cabo coaxial

Cabo par trançado

O cabo par trançado (*twisted pair*) foi o primeiro cabo do padrão *ethernet* 10base-T. Esse cabo possui quatro pares de cabos de cores diferentes, cada cabo possui seu correspondente branco, por exemplo, para a cor azul, temos um cabo na cor branca com listras azuis. Esse formato depende do fabricante.

Os cabos vêm trançados entre si de forma a torná-los menos sujeitos ao ruído dentro a capa plástica (capa de vinil), desta forma, reduz o campo eletromagnético externo, que pode ser causado por motores, geradores elétricos, linhas de alta tensão, ou outros equipamentos que produzem este campo magnético.

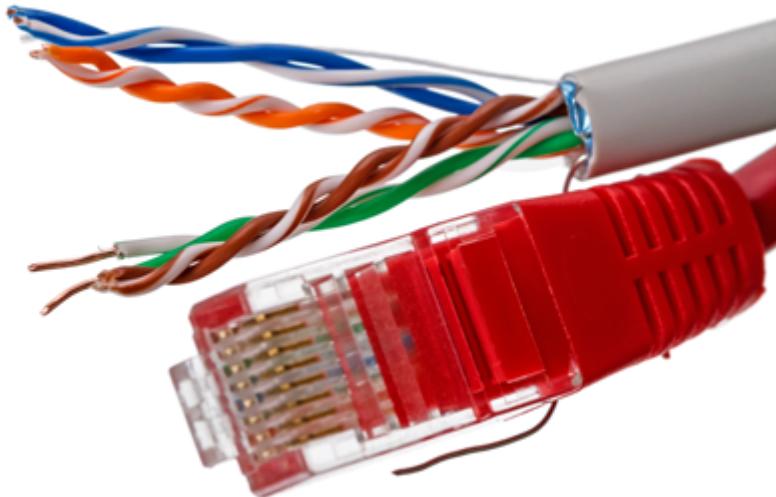


Figura 18 - Cabo par Trançado

Os cabos par trançados possuem as seguintes categorias: Cabo UTP (*Unshielded Twist Pair*), Cabo FTP (*Foiled Twisted Pair*), Cabo STP (*Shielded Twisted Pair*) e Cabo SSTP (*Screened Shielded Twisted Pair*), que iremos estudar em seguida.

Cabo UTP (*Unshielded Twist Pair*):

Esse cabo teve uma evolução constante chegando até o CAT5, passando pelo CAT1, CAT2, CAT3 e CAT4. Porém, todos foram descontinuados. O CAT5 também já não é mais encontrado devido a sua derivação para o CAT5e, que alcança em torno de 100 metros mantendo um bom sinal. Passando desta metragem pode ocasionar perda de sinal.

Caso precise ultrapassar, será necessário colocar repetidores a cada 100 metros, ou a utilização de *hubs* ou *switch*. Possui velocidade variada, dependendo da categoria do cabo, podendo chegar a 1 Gbps. Não tem blindagem, é flexível e de fácil instalação. Também é de fácil conectorização por meio da utilização de conectores RJ45 para a Ethernet e RJ11 para voz. Além disso, esse tipo de cabo possui baixo custo.

O cabo par trançado da **Categoria 6**, apresenta um custo/benefício maior do que o CAT5 para redes de computadores. Esses cabos possuem uma blindagem interna maior do que o CAT5, com o intuito de reduzir as interferências entre os pares de cabos. Para reduzir as interferências utilizam um separador para distanciar os cabos entre si, reduzindo o *crosstalk*.

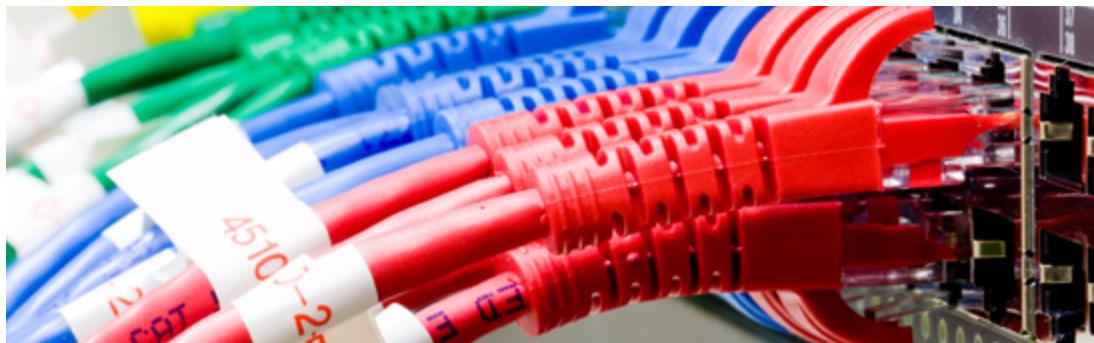
Os sinais enviados do transmissor ao receptor podem estar sujeitos à interferência eletromagnética (ruídos) e à diafonia (*crosstalk*), afetando ambos os fios, e criando um sinal indesejável (FOROUZAN, 2006, p. 178).

Para distanciar os fios é utilizado um espaçador de aproximadamente 3 mm de diâmetro. Consequentemente aumentará o diâmetro do cabo CAT6 em relação ao CAT5, indo de 5.6 mm para 7.9 mm (valores aproximados de fabricante para fabricante). Desta forma a transmissão dos dados pode chegar até 1 GB com uma frequência de 500Mhz. Claro que, para se alcançar esta velocidade toda a rede deve estar alinhada com dispositivos e acessórios para o CAT6. (MORIMOTTO, 2011)

O cabo par trançado utiliza os conectores RJ45 macho em suas pontas, e o conector Jack (fêmea) para espelhos de tomadas, *hubs*, *switchs*, que receberão o cabo com o conector RJ45.

A cor externa dos cabos não interfere em nada no funcionamento da sua rede, a única função é a distinção dos setores físicos. Dessa forma, imagine um *hack* com centenas de cabos, todos da mesma cor, ficaria difícil verificar qual cabo pertence a qual setor, não acha? Por isso, para uma melhor organização e manutenção, é recomendado que cada setor, ou setores específicos, utilizem cores diferentes.

Figura 19 - Organização do Hack



Para realizar a crimpagem do cabo par trançado, você precisará de conectores RJ45, um alicate de bico e um alicate de crimpagem de cabos RJ45, dependendo do fabricante, o alicate já vem com espaçador e o corte.



Figura 20 - Ferramentas de crimpagem de cabos

Os cabos par trançados podem ser blindados ou não, vejamos os seus padrões.

CABO FTP (FOILED TWISTED PAIR)	CABO STP (SHIELDED TWISTED PAIR)	CABO SSTP (SCREENED SHIELDED TWISTED PAIR)
São os que utilizam a blindagem mais simples, por meio de uma folha de aço que envolve todos os pares de cabos, protegendo-os contra interferências externas e entre os pares de cabos.	Vão um pouco além, usando uma blindagem individual para cada par de cabos e melhora a tolerância do cabo com relação a distância.	Combina a blindagem individual para cada par de cabos com uma segunda blindagem externa, envolvendo todos os pares, o que torna os cabos especialmente resistentes a interferências externas.

Quadro 4 - Padrões dos cabos par trançados

Fonte: os autores

Os cabos da categoria 5 não são blindados como os da categoria 6. Por sua vez, estes cabos são mais seguros, porém eles são mais caros e menos flexíveis, devido a sua tecnologia de isolamento ser mais grossa. Para este tipo de cabo, precisamos ter conectores RJ45 para CAT6 e um alicate especial.

Padrões de crimpagem.

EIA/TIA 568A	EIA/TIA 568B
Branco Verde	Branco Laranja
Verde	Laranja
Branco Laranja	Branco Verde
Azul	Azul
Branco Azul	Branco Azul
Laranja	Verde
Branco Marrom	Marrom Branco
Marrom	Marrom

Quadro 5 - Padrões EIA/TIA

Fonte: o autor

Cabo Fibra Ótica

A fibra ótica transmite informações através de sinais luminosos, ou seja, utiliza o fenômeno da refração interna total para refletir feixes de luz a longa distância, em vez de sinais elétricos.

Os cabos de fibra ótica estão substituindo fios de cobre para aumentar a velocidade de transmissão de informação digital, eles possuem um núcleo, um vidro muito fino, sendo feito de sílica, e também coberto por sílica, fazendo com que os feixes de luzes sejam refletidos por longas distâncias. A fibra possui no mínimo duas camadas: o núcleo (filamento de vidro) e o revestimento (material eletricamente isolante). Dessa forma, ela é totalmente imune a ruídos, com isso, a comunicação é mais rápida.

O cabo de fibra ótica garante nível elevado de confiabilidade em nível de transmissão de sinais e dados, voz e vídeo. Para que seja realizada a transmissão pela fibra, é lançado um feixe de luz em uma extremidade da fibra, e esse feixe percorre a fibra por meio de reflexões sucessivas.

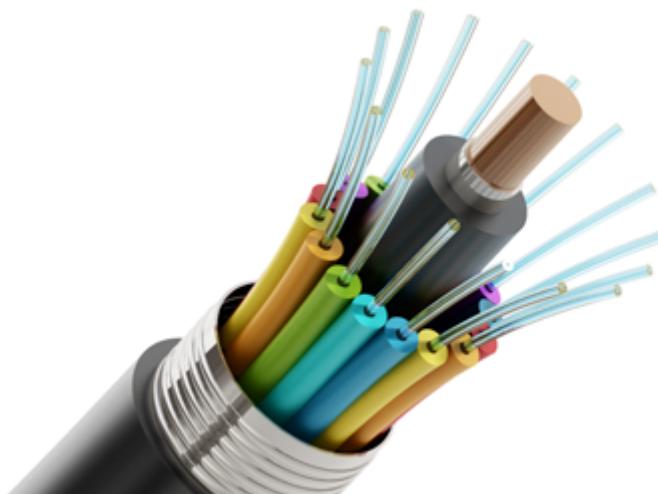


Figura 21 - Fibra ótica

As fibras óticas utilizadas nas redes de computadores de acordo com Tanenbaum e Wetherall (2011) e Ross e Kurose (2005) são classificadas de acordo com a forma que a luz trafega no cabo, sendo elas citadas a seguir:

Na fibra Monomodo, um único sinal de luz é transportado de forma direta no núcleo do cabo. O sinal pode atingir distâncias maiores, sem repetição, desta forma o tráfego da luz quando comparado com a transmissão da fibra multimodo podem atingir 80 quilômetros no padrão 10 Gigabit.

A fibra multímodo tem como característica um feixe de luz que viaja ao longo do seu trajeto, fazendo diferentes refrações nas paredes do núcleo do cabo.

SAIBA MAIS



De acordo com a notícia publicada pelo site “Investimentos e notícias”, em 26 out. 2015, há 160,4 milhões de assinantes conectados no mundo com a fibra ótica.

Leia a matéria na íntegra no link: <<http://www.investimentosenoticias.com.br/noticias/negocios/fibra-optica-160-4-milhoes-de-assinantes-conectados-no-mundo>>. Acesso em 24 set. 2020.

Fonte: Investimentos e notícias (2015, on-line)².

TOPOLOGIAS DE REDES

No tópico anterior estudamos os meios de transmissão, agora abordaremos a estrutura física e a lógica da rede, ou seja, como a rede ficará disposta. Tomemos como exemplo uma planta baixa de um prédio, o projeto arquitetônico onde se localiza cada ponto do edifício. A topologia nada mais é do que mostrar como e onde cada ponto de rede estará disposto.

A topologia de rede descreve fisicamente e logicamente como as redes são desenhadas, dessa forma, podemos ter a estrutura topológica da rede, física ou lógica.

A topologia física é o desenho físico da rede, ou seja, como a rede ficará disposta, enquanto que a lógica descreve o fluxo de dados através da rede.

No decorrer dos anos foram criadas diversas topologias, formando um conjunto de 7 (Sete) Topologias de Rede no total, sendo elas a Ponto a ponto, Anel, Barramento, Estrela, Árvore, Malha e Híbrida.

Vamos focar nas quatro principais e mais utilizadas:

- Ponto a Ponto.
- Barramento.
- Anel.
- Estrela.

Topologia de Rede Ponto a Ponto

Uma conexão ponto a ponto ou *Peer to Peer*, interliga somente dois computadores, por meio de um cabo especial que recebe o nome de *Cross-over*. Essa é a forma mais barata de conectar duas máquinas, basta um cabo par trançado categoria 5 e dois conectores RJ45.

O cabo crossover deve ter uma ponta no padrão **EIA/TIA 568A** e outro no padrão **EIA/TIA 568B**.

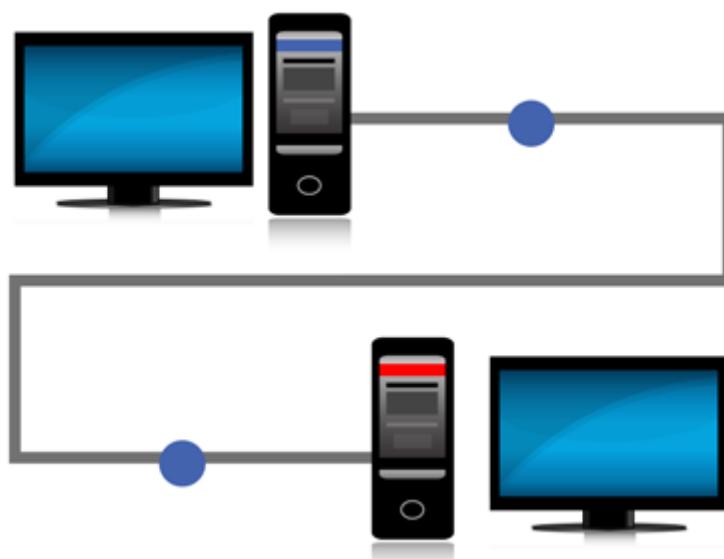


Figura 22 - Conexão direta entre computadores

Topologia Anel

A Topologia Anel foi lançada pela empresa IBM, na qual seus dispositivos são conectados em série, formando um circuito fechado (anel). Os dados são transmitidos em uma única direção, até que o nó ache seu destino. Dependendo do destino, o pacote pode passar por todos os nós da rede. É possível usar anéis múltiplos para aumentar a confiabilidade e o desempenho; caso venha a ocorrer um problema, a rede possui outro anel para retransmitir os pacotes.

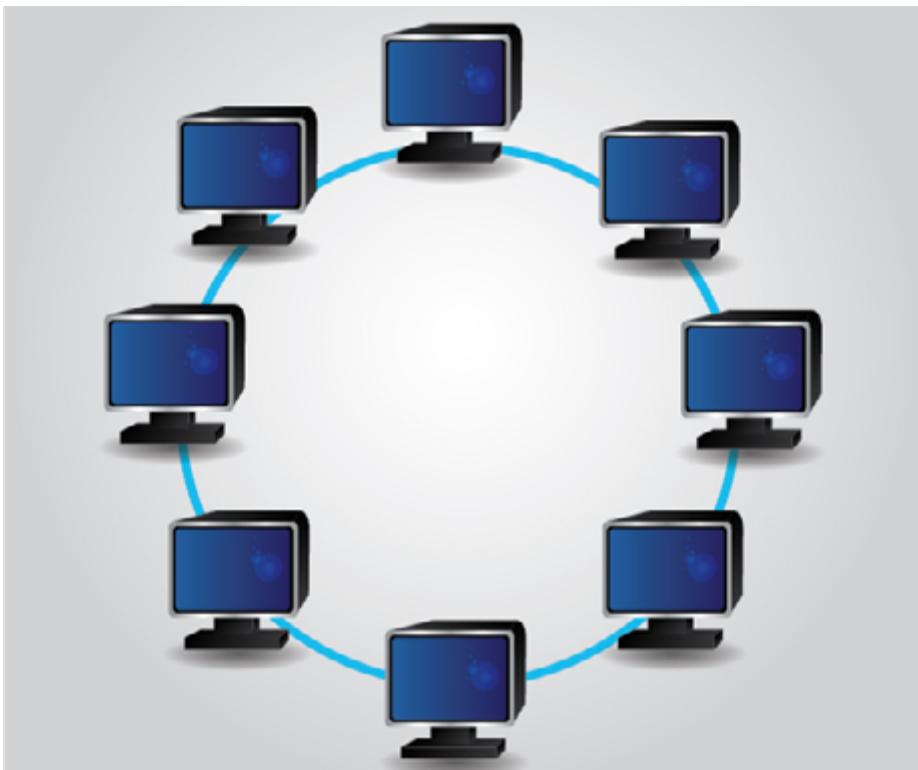


Figura 23 - Topologia Anel

Estrela

Essa topologia é a mais utilizada atualmente, devido a sua facilidade de estruturação, velocidade e custo. Para termos uma topologia em estrela, precisamos ter um dispositivo concentrador, que pode ser: *hub*, *hub-switch*, o *switch* e cabos de par trançado.

Como todos os dispositivos nessa topologia estão conectados no concentrador, se um deles parar de funcionar, apenas este dispositivo irá ficar fora da rede enquanto toda a rede funciona normalmente; e pode-se adicionar outro terminal facilmente desde que tenha uma porta sobrando. Como desvantagem, caso o concentrador apresente problema, toda a rede para de funcionar.

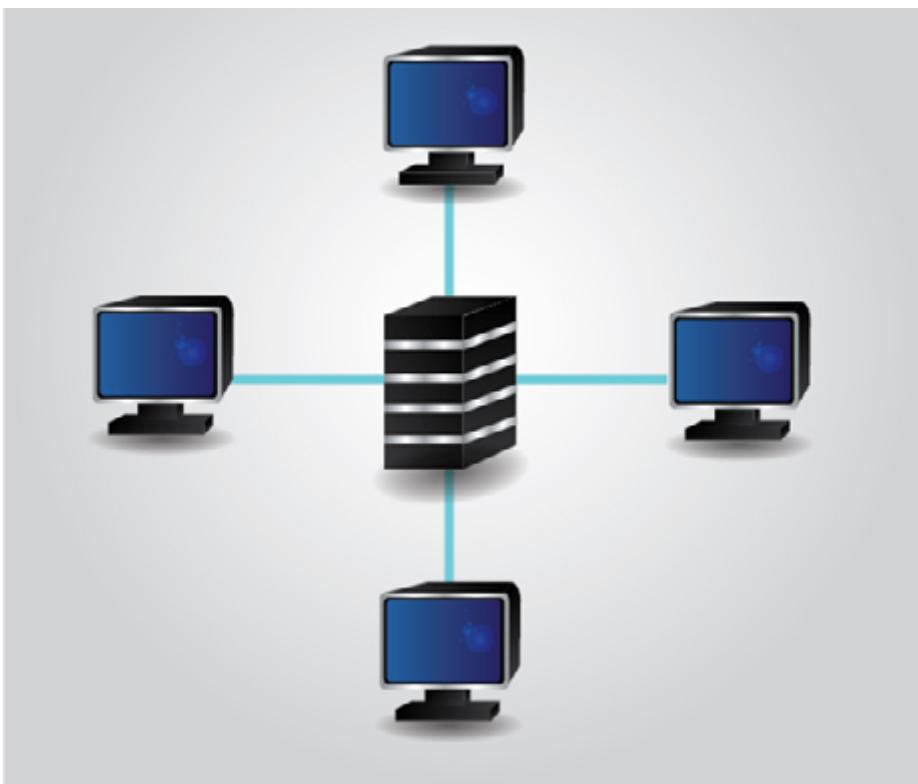


Figura 24 - Topologia estrela

Barramento

A topologia barramento foi a primeira topologia de rede a ser utilizada. Nessa, todos os computadores se conectam ao cabo central por meio do conector do tipo T e um conector do tipo BNC que conecta a placa de rede do computador.

Quando é enviado um pacote, o mesmo passará em todas as máquinas. Porém, cada máquina fica na escuta e apenas o dono que receberá o pacote aceitará. Desta forma, apenas um pacote percorre a rede ao mesmo tempo, caso tenha mais do que um pacote na rede, a transmissão deve ser recomeçada do zero.

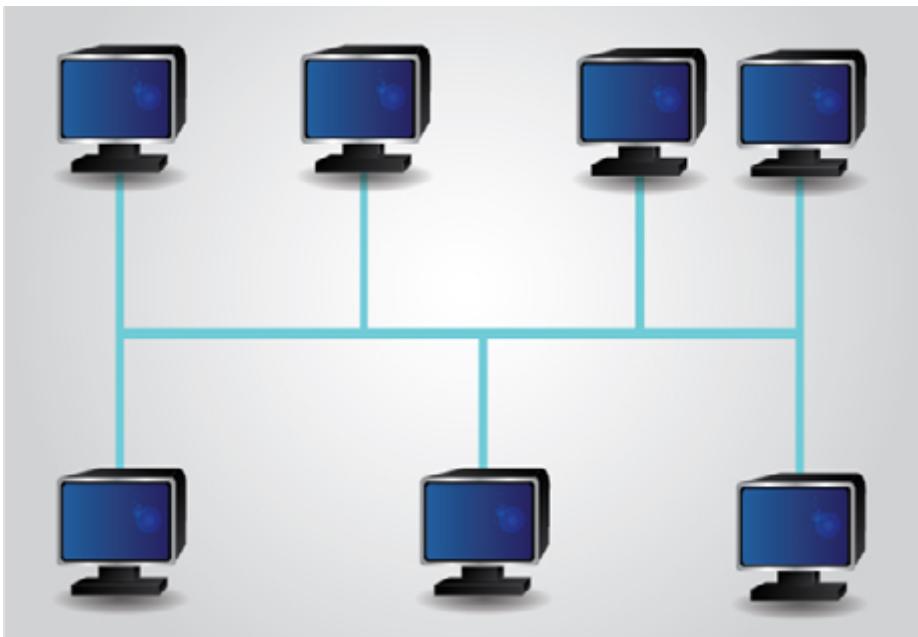


Figura 25 - Topologia Barramento

CONSIDERAÇÕES FINAIS

Nesta primeira unidade do livro, aprendemos no primeiro tópico os principais fundamentos em que consiste uma rede de computadores, desde o seu surgimento até os dias atuais. Ainda nesta unidade vimos a importância de termos as redes de computadores em nossas residências ou em nossas empresas. Aprendemos quais são os possíveis benefícios do compartilhamento de recursos e dispositivos em uma rede de computadores.

Também discutimos no decorrer da unidade a respeito dos tipos de redes de computadores que nos rodeiam, tais como a Internet, a intranet, que auxilia no trabalho no dia a dia de uma organização para a tomada de decisões, reduzindo trabalho desnecessário, e a extranet, como forma de auxiliar em conexões remotas para fornecimento de informações da empresa em tempo real. Foi possível

verificar em nosso estudo a respeito dos serviços que cada tipo de rede dispõe, a sua história e evolução, bem como a classificação dos tipos de redes como sendo: LAN, MAN, WAN, e a rede WIRELESS e suas derivações.

Na sequência de nosso estudo, aprendemos um pouco sobre o padrão ethernet, que regulamenta e padroniza a forma de comunicação, tanto física quanto lógica. Vimos também os dispositivos de rede, como as placas de rede funcionam, as diferenças dos dispositivos concentradores: *hub*, *hub-switch* e *switch*. Aprendemos como classificá-los e a distinguir o uso correto dos dispositivos em uma rede.

Outro tópico discutido foi sobre as mídias de transmissão (os cabos), como são feitos e seus padrões, bem como as suas derivações. Dentro desse tema, foi possível compreender um pouco mais como se deu a evolução das mídias no decorrer do tempo e sua correta utilização.

Encerrando as temáticas propostas para essa unidade, estudamos os comportamentos das topologias de redes, aliadas com as mídias de transmissão, proporcionando uma ampla visão de uma rede de computadores.

Na próxima unidade, vamos estudar os protocolos de comunicação, o Modelo OSI, passando por todas as camadas e o modelo TCP/IP. Deixamos o convite para continuar conosco nessa jornada de estudos!

ATIVIDADES



1. Ao se optar pelo cabo coaxial padrão 10Base2, numa Rede Ethernet, deve-se considerar a distância máxima aproximada de:
 - a) 50 m
 - b) 100 m
 - c) 200 m
 - d) 500 m
2. As redes podem abranger áreas distintas. Por isso, foram criadas algumas designações para classificar as redes. Indique a rede que abrange a internet e a justifique.
 - a) LAN
 - b) MAN
 - c) WAN
3. Qual é a função do DNS?
4. Como é feita a transmissão do sinal em uma topologia bus? O que isso acarreta?
5. Diferencie intranet de extranet.

MATERIAL COMPLEMENTAR



LIVRO

Redes de Computadores - Versão Revisada e Atualizada.

Gabriel Torres

Editora: Novaterra Editora e Distribuidora Ltda.

Sinopse: A espera acabou! Gabriel Torres apresenta a segunda edição de um dos livros de mais referência na área, e amplamente adotado em cursos técnico-profissionalizantes e universidades: Redes de Computadores - Versão Revisada e Atualizada. Gabriel, uma autoridade nacional no assunto, apresenta um conteúdo totalmente atualizado de sua obra, em que o leitor aprenderá, em profundidade, tudo o que precisa saber sobre o tema, seja um estudante, um autodidata, um profissional da área ou mesmo um usuário que deseja aprender a montar uma rede segura por conta própria.



NA WEB

Vamos assistir um vídeo sobre crimpagem de cabos utilizando o cabo par trançado. Disponível em: <<https://www.youtube.com/watch?v=wmxiV0hQUGE>>. Acesso em: 19 maio 2016.





GERÊNCIA DE REDES DE COMPUTADORES - REVISTA INFRA MAGAZINE 3

O artigo trata de trazer uma breve visão sobre boas práticas e desafios de um gerente de redes de computadores em suas atividades diárias, envolvendo equipe, usuários, equipamentos, tipos de software que auxiliam o gerenciamento da rede, políticas de segurança e formas de detectar e resolver problemas nas redes de computadores.

A gerência de redes de computadores é fundamental para garantir a disponibilidade dos serviços, manter o funcionamento da infraestrutura de comunicação e acompanhar seu crescimento ao longo de toda sua existência.

No projeto de implantação existem muitos pontos a serem analisados e que são fundamentais ao bom desempenho da rede, destacando:

- Os serviços que estarão disponíveis, protocolos e suas configurações;
- O valor das informações que trafegarão nesse ambiente;
- A proporção dessa rede, necessidades e prioridades;
- A capacidade média de fluxo de dados para saber a capacidade mínima e desejável dos meios físicos e equipamentos que serão usados;
- Avaliar os custos versus os benefícios;
- Definir a topologia e mapeamento dos equipamentos da rede.

Os itens mencionados compõem uma série de informações necessárias ao planejamento de uma rede, e objetivam minimizar erros de projeto e retrabalho.

Quanto a ampliação de uma rede, há outros pontos que são interessantes de serem observados:

- Os serviços e configurações serão os mesmos?
- Os meios físicos e equipamentos existentes suportarão a demanda de fluxo de dados após a ampliação?
- Qual o horário em que essas modificações serão realizadas?
- Como será atualizado o mapeamento da infraestrutura?

Veja que, até o momento, os itens abordados fazem referência ao planejamento de implantação e/ou ampliação, mas ao decorrer do tempo é bastante comum que o ambiente sofra modificações. A exemplo, a contratação de funcionários que motivam a aquisição de computadores, ou a necessidade de se configurar rede sem fio em salas de reuniões para que coordenadores e gerentes se mantenham conectados nesse ambiente.

Os exemplos citados sobre as pequenas modificações são bastante comuns no cotidia-





no e estão associados a ampliação da rede, ou disponibilização de algum serviço adicional, que por sua simplicidade, são tratados sem a devida importância, culminando em complicações.

Como boa prática o ideal é que toda a documentação referente ao projeto, de implantação ou de ampliação, não seja apenas arquivado e esquecido, mas sim atualizado mesmo quando houver pequenas alterações, pois esse procedimento auxiliará bastante, tanto para um melhor entendimento da infraestrutura, quanto para a identificação de problemas, entre outras situações.

Leia mais em: Santos (2011, on-line)³.

REFERÊNCIAS

- BITTENCOURT, I. I.; ISOTANI, S. **Dados Abertos Conectados**. São Paulo: Novatec, 2015.
- CYCLADES, Brasil. **Guia internet de conectividade**. São Paulo: Editora SENAC, 1999.
- FOROUZAN, B. A. **Comunicação de Dados e Redes de Computadores**. 3 ed. Porto Alegre: Bookman, 2006.
- MORIMOTO, C. E. **Redes de Computadores**: Guia prático. 2 ed. Porto Alegre: Sul Editores, 2011
- ROSS, K.; KUROSE, J. F. **Redes de Computadores e a Internet**: uma abordagem top down. 5 ed. São Paulo: Pearson, 2005.
- TANENBAUM, A.; WETHERALL, D. J. **Redes de Computadores**. 5 ed. São Paulo: Pearson, 2011.

CITAÇÃO DE LINKS

¹ <<http://www.cibersecurity.com.br/70-do-mundo-usara-dispositivos-moveis-em-2020/>> Acesso em: 07 abr. 2016.

² <<http://www.furukawa.com.br/br/rede-furukawa/noticias/fibra-optica:-ja-sao-160,4milhoes-de-assinantes-conectados-no-mundo-1258.html>>. Acesso em 06 dez. 2016.

³ <<http://www.devmedia.com.br/gerencia -de-redes-de-computadores -revista-infra-magazine-3/22926#ixzz3tal2pt9B>>. Acesso em: 19 maio 2016.



GABARITO

1. c
2. c (por ser de alcance geográfico, e o meio de propagação pode ser por rádio e pela internet)
3. DNS (Domain Name Systems – Sistemas de Nome de Domínio), ou seja, é um nome que serve para localizar e identificar sites ou grupos de computadores na Internet.

No Brasil, o site REGISTRO.BR, é o responsável pelo registro de todos os sites e domínios. Para ter um domínio, é necessário ter identificação física e jurídica, e um local de hospedagem, para que quando um usuário insira o endereço do seu site em algum navegador ou sistema de busca, o seu provedor de acesso saiba onde localizar o seu site através deste serviço. Estes domínios podem ser assim classificados: .edu, .net, .gov, .com, .org, .mil etc.

4. Quando é enviado um pacote, o mesmo passa em todos, porém, cada máquina fica na escuta, e apenas o dono que receberá o pacote irá aceitar. Dessa forma apenas um pacote percorre a rede ao mesmo tempo, caso tenha mais do que um pacote na rede, a transmissão deve ser recomeçada do zero.
5. A intranet é uma rede de computadores interna de uma empresa, que não precisa estar conectada com a internet, que tem por objetivo geral, o compartilhamento de informações e de serviços.

Podemos partir do princípio que rede denominada extranet refere-se a uma rede de computadores que é conectada com alguma outra rede de computadores externa, e para que isso seja possível, utilizamos a internet como meio de comunicação.



CONEXÕES, PROTOCOLOS E MODELOS

UNIDADE



Objetivos de Aprendizagem

- Estudar sobre os diversos tipos de conexões existentes: com fio, sem fio, remota, infravermelho, Bluetooth.
- Visualizar a diferença entre as redes móveis 2G, 3G e 4G.
- Apresentar os tipos de protocolos mais utilizados em redes de computadores, como: UDP, TCP, DHCP, FTP, HTTP, SSL, SSH, DNS, SNMP.
- Mostrar o funcionamento do endereço.
- Classificar como são realizados os roteamentos.
- Entender o que são subredes.
- Estudar sobre os protocolos TCP/IP.
- Explicar o Modelo ISO/OSI e realizar uma breve classificação das 7 camadas.

Plano de Estudo

A seguir, apresentam-se os tópicos que você estudará nesta unidade:

- Tipos de Conexões
- Redes Móveis
- Protocolos e Padrões de Rede
- Endereços de IP, Subredes e Roteamento
- Modelos de Referência

INTRODUÇÃO

Na primeira unidade, compreendemos o conceito do que é uma rede de computadores. Conceitos dos quais vão desde os primórdios da Internet, funcionalidades, hardwares, meios de transmissão, até chegar a topologias de redes. Dentre as redes estudadas, definimos Redes WAN, MAN, LAN e várias outras, podendo assim distinguir qual usar em um determinado momento e ambiente.

Aprendemos também que cada tipo de rede pode utilizar um hardware e um software diferente, tudo depende da análise do funcionamento, identificando a viabilidade de cada hardware. Incluem-se nessa análise as topologias utilizadas e, ainda, que tipo de meios de transmissão se utilizar, seja cabos coaxiais, par trançado ou ainda fibra ótica.

Você deve estar se perguntando por que estudou a história e os conceitos preliminares, não é? Lembramos a você que este primeiro estudo é muito importante para darmos continuidade nas próximas unidades. Entender toda a história do surgimento da internet, conceitos e aplicabilidades de redes e topologias proporcionará a você um entendimento mais fácil e, consequentemente, não terá dificuldades em materiais futuros.

Além disso, com essa introdução, você viajará pelo tempo, passando por todas as fases constantes para a Rede de Computadores.

Dando continuidade ao nosso aprendizado, nesta segunda unidade nos aprofundaremos em tipos de conexões, sejam elas com ou sem fio, conexão remota, *Bluetooth*, infravermelho e, claro, não podíamos deixar de fora, as conexões de Redes Móveis, como nossas tecnologias 3G e 4G.

Completando nosso guia de estudo desta unidade, abordaremos também os protocolos de redes, nos quais iremos definir sua importância e o funcionamento de cada um. Conheceremos ainda os Modelos de Referência TCP/IP e OSI, que são uma padronização dos serviços de uma rede, e são muito importantes na organização do fluxo de dados na nossa rede de computadores.

Após essa breve introdução do que vamos aprender, o que acha de nos aprofundar um pouco? Vamos lá?

TIPOS DE CONEXÕES

Conforme a unidade anterior, aprendemos como se deu o início da internet, a grande rede de computadores. Porém, agora vamos começar a descrever as formas de como acontece a conexão dos equipamentos nessa rede.



Figura 1 - Conexão Globalizada

Reprodução proibida. Art. 184 do Código Penal e Lei 9.610 de 19 de fevereiro de 1998.

CONEXÕES COM FIO

Conexão Dial-up

Antes da popularização da Internet, com suas altas velocidades e variados tipos de tecnologias, a conexão acontecia por meio da linha telefônica e de forma discada. Para a conexão, bastava ter um computador equipado com um modem (Modulador e Demodulador de Sinais) conectado a uma linha telefônica e provedores que disponibilizavam um software discador; consequentemente o acesso à internet.



Figura 2 - Placa-mãe com modem integrado

O software discador envia para o provedor de acesso os dados do usuário, como login e senha e, após alguns segundos para autenticação, você estava on-line. O

problema desse tipo de conexão era a baixa velocidade disponibilizada, que atingia a máxima de 56,6 kbps, além de instabilidades, custo benefício e bloqueio da linha telefônica, que ficava ocupada no momento do uso da internet.

Apesar da popularização da internet, ainda é comum o uso desta conexão no Brasil, pelo fato de em alguns locais não ter chegado à tecnologia ADSL ou de outros meios.

CONEXÃO ADSL (ASYMMETRIC DIGITAL SUBSCRIBERLINE)

Atualmente, essa é a tecnologia mais popular quanto à chamada conexão banda larga, que são as conexões de alta velocidade. Surgida em 1989, utiliza-se da linha telefônica para seu funcionamento, assim como a conexão *dial-up*, porém com uma grande diferença: não deixa a linha telefônica ocupada e, em vez de pagar como se fosse uma ligação, o usuário assina um pacote mensal de determinada velocidade.

Para este tipo de conexão, necessita-se, além da linha telefônica, o sinal da operadora e um modem externo (podendo ser com ou sem fio), modem este que dividirá a linha telefônica em três canais: canal de voz, canal de download e canal de upload.

A princípio, os provedores de internet ofereciam velocidades de até 8 Mbps de download e 1 Mbps de upload. Porém, com o passar do tempo, a tecnologia foi evoluindo e foram surgindo novos tipos, como ADSL2 e ADSL2+. Essas tecnologias tiveram um ganho em relação à velocidade e estabilidade; podendo chegar hoje a 150 Mbps dependendo da região e da infraestrutura que é disponibilizada pela operadora.



Figura 3 - Exemplo de Modem ADSL utilizado para as conexões

Segundo Forouzan (2008), ADSL é uma tecnologia adaptativa, na qual a taxa de transmissão dos dados, tanto de download quanto de upload, depende das condições da linha local, distância entre a residência do cliente e a central de comutação, e o tamanho do cabo; afetando em alguns casos a largura da banda. Quanto maior a distância do usuário final para a central, pior é o sinal, prejudicando a velocidade contratada e, ainda, sofrendo cortes de sinal.



SAIBA MAIS

ADSL faz parte de uma família de protocolos que trabalham com o sistema SUBSCRIBER LINE. Além da ADSL, fazem parte da família DSL as conexões do tipo HDSL, SDSL e VDSL. A do tipo HDSL utiliza dois cabos pares trançados para implementar o modelo de trabalho utilizado, o Full Duplex; permitindo taxa de dados de 2 Mbps a uma distância de 5 km. Já a tecnologia SDSL foi desenvolvida para atender as expectativas das empresas, que precisam receber grandes quantidades de dados, seja como download ou upload. Por último, a VDSL, similar à ADSL, porém, admite cabo coaxial, par trançado ou ainda fibra ótica como meio de transmissão em curtas distâncias, podendo alcançar velocidades de download de até 55Mbps e upload de 2,5Mps.

Fonte: Forouzan (2008).

CATV (COMMUNITY ANTENNA TELEVISION)

Como a internet ADSL, a CATV também vem se popularizando. O princípio básico dessa tecnologia é a utilização do próprio cabo da TV a cabo local para se conectar à internet. Um dos motivos da popularização crescente são os pacotes de conexão, que juntamente com os pacotes de TV e telefone, ficam atrativos pelos seus variados preços.

A princípio surgida em meados dos anos 1940, a TV a cabo entrou em funcionamento para atender localidades em que a recepção do sinal era ruim ou ainda, não existia. Para isso, uma gigantesca antena era colocada em uma montanha, e a partir dos cabos, o sinal era distribuído aos usuários. O sistema utilizava a comunicação através de cabos coaxiais, amplificadores, e é unidirecional, devido

à altas taxas de perdas de sinal (TANENBAUM; WETHERALL, 2011).

Com o passar dos anos e a crescente adesão pelos usuários, houve a necessidade de aperfeiçoamento dessa tecnologia, que hoje se utiliza de fibra ótica de alta largura de banda. Com essa evolução, a CATV passou a utilizar uma combinação híbrida de cabo coaxial e fibra ótica, chamado também de HFC (*Hybrid Fiber Coaxial*). Com isso, a comunicação nesse tipo de rede pode ser bidirecional (FOROUZAN, 2008).

O sistema de banda da TV a cabo é dividido em três: uma para vídeo, outra para dados em *downstream*¹ e outra para *upstream*²; e se utiliza de um modem especial para sua conexão.



REFLITA

Você pode encarar um erro como uma besteira a ser esquecida, ou como um resultado que aponta uma nova direção.

Steve Jobs

REDE ELÉTRICA

O sistema de internet pela Rede Elétrica veio como uma alternativa para a conexão em banda larga. Porém, esse tipo de conexão não é muito popular ainda, e não há muitas empresas que disponibilizam esse tipo de conexão no Brasil. Algumas empresas estão em fase de testes e outras já disponibilizam essa tecnologia, porém chegando somente em alguns lugares. Por exemplo, temos a Copel (Companhia Paranaense de Energia Elétrica), que já disponibiliza essa conexão em algumas cidades.

Esse tipo de conexão utiliza o Protocolo PLC (*Power Line Communication*).

¹ *Downstream*: Download (ou downstream) é a velocidade que os dados chegam ao seu computador. Ex: A velocidade de download de um arquivo da internet é de 10Mb.

² *Upstream*: Upload (ou upstream) é a velocidade com que os dados “saem” de seu computador. Ex: A velocidade de upload de um arquivo que vamos “subir” para armazenamento online.

É uma tecnologia mais barata por utilizar uma infraestrutura e mão de obra existente, porém sensível a interferências de até mesmo um eletrodoméstico, que ao serem ligados “sujam” a rede com ruídos. Outros motivos que podemos citar são os elementos da rede elétrica, que na maioria das vezes são antigos e sem manutenção.

Como tudo que é novo sempre apresenta vantagens e desvantagens, podemos citar como vantagem o grande alcance de penetração e o baixo custo na instalação dentre as tecnologias existentes. E como desvantagem, temos a falta de padronização da tecnologia e interferências.

Apesar de tudo, essa tecnologia vem avançando e tendo projetos para várias aplicações, tanto para conexão em banda larga como também para VoIP, utilizando modems PLC, músicas e entretenimento.



SAIBA MAIS

Hoje em dia, podemos dizer que o LI-FI já não é coisa de outro mundo. Está em operação, mas ainda em fase de testes, a LI-FI ou Light Fidelity, a internet de alta velocidade, em que se é conectado por meio de ondas da luz. A tecnologia que vem para substituir o WI-FI e promete produzir velocidades de até 150 Mbps com apenas uma lâmpada de LED equipada com um processador de sinal. Ficou curioso e está querendo uma conexão desta em casa? Conheça mais a respeito a seguir.

Fonte: Dâmaso (2014, on-line)¹.

CONEXÃO SEM FIO

Conexão Via Rádio

Esse tipo de conexão se utiliza de ondas de rádio, onde uma antena transfere os dados para o cliente/usuário. As ondas de rádio são fáceis de gerar, podendo percorrer grandes distâncias e com fácil penetração em ambientes fechados.

Utiliza ondas omnidirecionais, ou seja, o receptor e o transmissor não precisam estar fisicamente alinhados para a troca de informações, pois as ondas viajam em todas as direções.

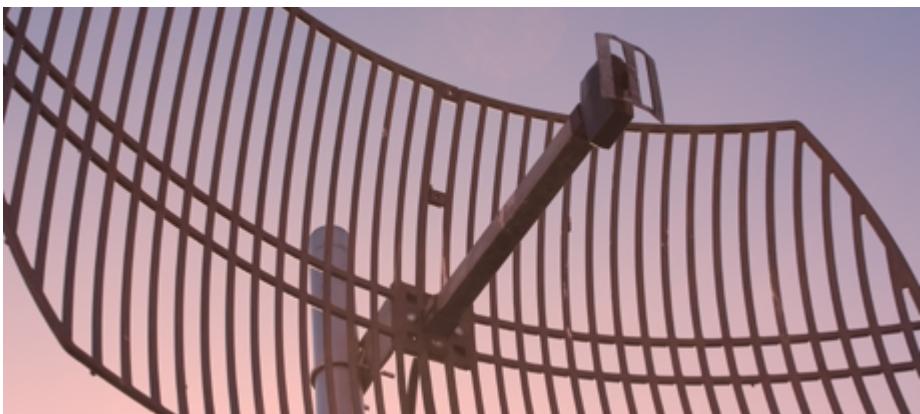


Figura 4 - Antena utilizada para captura de sinal na conexão via rádio

Esse tipo de conexão também atinge grandes velocidades, porém ela está sujeita a interferências, seja por equipamentos elétricos, ou ainda, por obstáculos físicos (como paredes) ou pelo tempo (como em dias chuvosos). Em baixas frequências, atravessam bem os obstáculos, porém a potência cai quanto maior a distância do ponto de origem. Já as ondas de alta freqüência tendem a viajar em linha reta, porém sofrem influência de chuva e outros obstáculos (TANENBAUM; WETHERALL, 2011).

Infravermelho

São usadas em comunicação de curta distância, com frequências que vão dos 300GHz a 400THz. São comumente usados em controle remoto de aparelhos eletrônicos, alguns celulares e PDAs (*Personal Digital Assistants*).

Sua comunicação é relativamente direcional, ou seja, para a troca de informações, os aparelhos devem estar no mesmo campo de visão. Essa tecnologia é econômica, porém tem como fator negativo a baixa qualidade, pois recebem muita interferência, inclusive da luz, e a baixa velocidade de transmissão.

Outro tipo de utilidade dessa tecnologia é para a comunicação de periféricos

sem fio. Alguns fabricantes fornecem uma porta chamada IrDA³, que permite que os periféricos se comuniquem com o PC (FOROUZAN, 2008).

Bluetooth

Surgiu em 1994, por meio da empresa L. M. Ericsson, que tinha o interesse em conectar dispositivos móveis sem a necessidade de conectar cabos, utilizando rádio de curto alcance, baixa potência e baixo custo. A partir daí formou-se um consórcio juntamente com as empresas IBM, Intel, Nokia e Toshiba (TANENBAUM; WETHERALL, 2011).



O Sistema *Bluetooth* funciona como um piconet, ou seja, consistem em um nó mestre e mais sete nós escravos ativos, no qual devem estar em no máximo 10 metros de distância (ROSS; KUROSE, 2013). Ainda, diferentemente do infravermelho, os aparelhos não precisam estar apontados um para o outro para que se dê a conexão e a transmissão dos dados. Este tipo de conexão, como dito, utiliza-se de ondas de rádio, porém é gratuita, sem a necessidade de se conectar à internet para a transferência de dados.

Figura 5 -ícone bluetooth

³ IrDA: Do inglês Infrared Data Association, é uma definição de padrões de comunicação entre equipamentos de comunicação Wireless.

SAIBA MAIS



Em tecnologia, sabemos que sempre há a necessidade de avanços, seja para qualquer tipo de necessidade existente. Com o *Bluetooth* não foi diferente, ele surgiu para auxiliar as pessoas na troca de informações, porém com baixa velocidade de transmissão. Como dito, há uma importância em se atualizar determinado equipamento ou tecnologia para que este não fique defasado ou inutilizado. Nesse intuito, você pode realizar uma breve leitura sobre o avanço da tecnologia *Bluetooth* para os próximos anos em termos de velocidade de transferência de dados no link a seguir.

Fonte: Vieira (2015, on-line)².

Coneção Remota

A conexão remota serve para o auxílio de reparos, instalações de softwares, cópia de arquivos, entre outros; isso para usuários que estão dispostos em locais diferentes do computador cliente, em que se necessita a conexão.

Para o acesso remoto, os computadores deverão estar ligados, com conexão de rede e acesso permitido para conexão e para alterações possíveis. É muito utilizado para manutenção de servidores e para suporte técnico de softwares. Hoje em dia, é possível o acesso remoto tanto de computadores, notebooks, smartphones ou tablets.

Dentre as várias técnicas, a forma mais comum do acesso remoto é por meio da VPN (*Virtual Private Network* ou Rede Privada Virtual), que estabelece diretamente uma ligação entre o computador e o servidor.

Para se conectar por meio da VPN existem duas maneiras, sendo por meio do protocolo SSL, ou ainda, por meio de softwares, os quais são a forma mais usual. Com o SSL, pode-se usar somente um navegador para conexão, porém perde-se em nível de segurança e velocidade de conexão; já os softwares utilizam o Protocolo IPseg, há uma maior segurança e a conexão é mais rápida, dependendo do link ADSL contratado (OLIVEIRA, 2009).

Há vários softwares destinados à conexão remota, dentre eles podemos citar o *TeamViewer*, *LogMeIn* ou *Real VNC*. Esses softwares devem ser instalados tanto na máquina *host*⁴ quanto na máquina cliente, lembrando a necessidade das permissões para acesso. Citando, como consequência do avanço tecnológico, hoje temos versões do LogMeIn e TeamViewer disponíveis tanto para Android e iOS.

REDES MÓVEIS

Sabemos que hoje, mais do que nunca, as redes móveis são utilizadas para tudo que se possa imaginar. Ligações por voz, vídeo-chamadas, navegar na internet e várias outras coisas. Porém, essa tecnologia passou por várias transformações desde o seu surgimento.

Cada transformação, chamada de geração, veio para agregar valores e funcionalidades às redes móveis. A primeira geração (1G), que hoje quase não existe mais, foi desenvolvida em sistemas analógicos especialmente para a comunicação por voz (ROSS; KUROSE, 2013).

Com o passar do tempo, houve uma atualização da 1G, passando a ser conhecida como segunda geração (2G), que também foi projetado para serviços de voz, porém com alta qualidade e sem ruídos. Mais tarde, ela foi atualizada para suportar a navegação por dados, ou seja, a navegação pela internet. Para isso, surgiu o protocolo WAP (*Wireless Application Protocol*), que permitia a comunicação de aparelhos móveis com os servidores por meio de micronavegadores disponíveis nos aparelhos.

Dentro da 2G há quatro sistemas de telefonia, dentre eles estão: D-AMPS, PDC, GSM e CDMA. As duas últimas foram as mais utilizadas na segunda geração, mas a princípio, a tecnologia CDMA (*Code Division Multiple Acces*) não era

⁴ Host: É qualquer máquina conectada a rede, oferecendo informações, recursos, serviços ou aplicações. Em nosso caso, Máquina Host é a máquina do T.I que realizará as atualizações ou operações necessárias para correção de determinado problema na máquina do cliente.

bem aceita, até que pela persistência da empresa Qualcomm, ela amadureceu e hoje é tida como a melhor solução existente, inclusive para base do sistema de terceira geração (TANENBAUM; WETHERALL, 2011).

Hoje a maioria das redes móveis instaladas é da terceira geração (3G), que também suporta voz e dados, porém com uma ênfase na capacidade de trocar dados com uma velocidade maior. Ela surgiu com o intuito de interligar todas as pessoas, e a tecnologia utilizada é a UMTS (Serviço Universal de Telecomunicações Móveis).

Devido a uma combinação de tecnologias que proporcionam uma variedade de serviços, o usuário poderá, além de realizar uma simples ligação, realizar downloads, assistir vídeos on-line, ouvir músicas, rádios, jogar e realizar vídeos conferências a uma velocidade final de aproximadamente 2 Mbps (FOROUZAN, 2008).

Como toda tecnologia sempre tem sua evolução, com a 3G não foi diferente. Com cada vez mais pessoas aderindo, houve a necessidade de expansão, assim surgiu a tecnologia WCDMA, que é conhecida como HSDPA/HSUPA (pacote de acesso de alta velocidade Downlink/Uplink), que na teoria disponibilizava grandes taxas de dados.

A figura 3 demonstra como foi a evolução das redes digitais de telefonia



móvel até chegar na tecnologia 4G:

Figura 6 - Evolução das redes digitais

Fonte: Teleco (2012, on-line)⁴.

4G

Hoje é a tecnologia de maior velocidade em se tratando de redes móveis. No mercado, temos duas tecnologias da quarta geração competindo: a **WIMAX** e a **LTE Advanced**. A WiMAX é utilizada em países como Rússia e Coreia do Sul, e atinge picos de 128 Mbps para download e 56 Mbps para upload.



A LTE (*Long Term Evolution*) é uma evolução da tecnologia HSDPA (3G) e é o primeiro sistema a não diferenciar voz de dados, realizando todas as chamadas por VoIP. Na teoria, ela atinge até 100 Mbps de download e 50 Mbps de upload. Futuramente, espera-se que a LTE atinja a velocidade de 1 Gbps, que é o padrão original da tecnologia.

Além da velocidade, bem maior que a tecnologia da terceira geração, há uma grande mudança nas comunicações entre as torres de telefonia. No caso da 3G, a comunicação entre as torres e a central telefônica é realizada por ondas de rádio, já na 4G, a comunicação é realizada por fibra ótica, o que ocasiona uma maior entrega na velocidade de navegação.

Porém, as redes 4G aqui no Brasil têm uma limitação. Pelo fato da frequência utilizada ser muito alta (2500 MHz ou mais), as ondas que transportam os bits não conseguem penetrar com eficiência em lugares fechados ou com obstáculos.

No entanto, com o fim do desligamento da TV analógica, que está previsto para 2018, as operadoras de telefonia poderão utilizar a frequência na faixa de 700 MHz, que antes eram das TVs análogicas.



SAIBA MAIS

Sabemos que toda tecnologia criada pode ser melhor em um certo país do que em outro, tudo dependendo de interferências físicas ou equipamentos de qualidade utilizados. Recentemente foi realizada uma pesquisa na qual seu principal intuito era mostrar ao leitor os melhores e os piores países em se tratando da tecnologia 4G, seja quanto à cobertura terrestre ou quanto às velocidades finais de conexão. Você se acha curioso(a)? Então acesse o link e leia mais a respeito deste assunto e explore novos horizontes.

Fonte: G1 (on-line, 2015)⁵.

PROTOCOLOS E PADRÕES DE REDE

Neste tópico, estudaremos alguns dos diversos protocolos existentes, dando ênfase aos protocolos mais utilizados. Também falaremos de padrões de rede, como o TCP/IP e o Modelo OSI. Vamos começar?

TCP (*Transmission Control Protocol*)

O TCP é um dos principais protocolos, o qual tem como propósito o envio dos pacotes do emissor até o destino final. É um protocolo orientado à conexão e suas características principais são: transferências dos fluxos de dados, a robustez, o controle de fluxo, ser multiplex, utilizar conexões lógicas e ser *Full duplex* (em que a comunicação poderá ocorrer em as ambas as direções simultaneamente) (RIOS, 2011).

Descrevendo em outras palavras, o protocolo TCP transmitirá um segmento⁵, disparando um *timer*; quando o segmento chega ao seu destino, uma aplicação confirma o recebimento com sucesso dos dados, enviando um número de confirmação igual ao próximo número de sequência que espera receber. Há ainda uma organização dos dados, por parte do receptor, caso os segmentos cheguem fora de ordem. Caso o *timer* do transmissor expire antes da confirmação do recebimento do segmento, o mesmo será retransmitido até estar entregue ao seu destino final (TANENBAUM; WETHERALL, 2011).

Como se trata de um protocolo de transporte, para melhor desempenho da rede, o TCP realiza o controle de congestionamento, no qual utiliza um princípio retirado da física, em que a ideia principal não é injetar um novo pacote na rede até que um pacote chegue ao seu destino, assim desafogando a rede.

Abaixo você pode verificar como são os formatos de endereço IP.

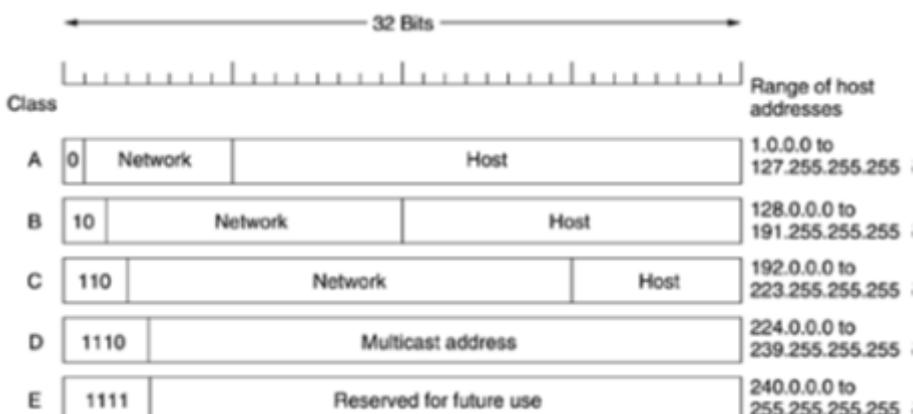


Figura 7 - Formatos de endereço IP

Fonte: Tanenbaum e Wetherall (2011, p. 337)

⁵ Segmento: um segmento TCP nada mais é do que uma mensagem que contém informações relevantes como: porta de destino, número de ordem dos pacotes, aviso de recepção e vários outras informações.

SAIBA MAIS



O protocolo IP nada mais é do que um protocolo de endereçamento, que atribui um endereço de IP a qualquer máquina/equipamento conectado a uma rede. Na internet, cada host e cada roteador tem um endereço IP que codifica seu número, não permitindo, a princípio, que mais de uma máquina tenha o mesmo endereço (TANENBAUM; WETHERALL, 2011).

Para saber mais sobre o funcionamento do Protocolo IP, acesse o vídeo a seguir: Como funciona a Internet? Parte 1: Protocolo IP. <<https://www.youtube.com/watch?v=HNQD0qJ0TC4>> Acesso em: 19 maio 2016. Após, comente sobre o vídeo no tópico de interação da SALA DO CAFÉ, no Ambiente Virtual de Aprendizagem (AVA).

UDP (User Datagram Protocol)

O protocolo UDP não é orientado à conexão, descrito na RFC 768⁶, e não garante a entrega dos segmentos ao seu destino, tornando-se assim um protocolo não confiável, que não elimina possíveis pacotes duplicados e também não realiza controle de rede. Porém, o UDP é uma ótima escolha para o fluxo de dados em tempo real, por ser um protocolo mais rápido e trocando menos informações que o protocolo TCP (ROSS; KUROSE, 2013).

Um exemplo prático de uso do protocolo UDP é a visualização de vídeos, que necessita de uma troca rápida de informações, e na qual a perda de um pacote não irá interferir na sua reprodução. Outro tipo de aplicação são os aplicativos de tecnologia VoIP e os programas P2P (FERNANDES, 2014).

⁶ RFC: Do inglês Request for Comments, são um conjunto de documentos de referência junto da Comunidade da Internet e que descrevem e especificam a maioria das normas, padrões de tecnologias e protocolos ligados à Internet e às redes em geral. A RFC 768 refere-se ao protocolo UDP.



SAIBA MAIS

Sabemos que há diferenças entre os Protocolos TCP e UDP. Sabemos também que mesmo com as diferenças os dois protocolos são utilizados como protocolos de transporte, e muito utilizados na Internet. Para se ter um pouco mais de conhecimentos sobre estes protocolos, acesse e assista o vídeo a seguir. Assim você terá uma breve explicação do funcionamento do protocolo TCP e UDP, auxiliando nas possíveis dúvidas surgidas no decorrer da leitura.

Fonte: os autores.

DHCP (Dynamic Host Configuration Protocol)

Imagine um profissional de TI, em seu largo conhecimento, ter que configurar manualmente o IP de todos os computadores de uma rede. Ele com certeza iria demorar algum tempo para resolver isso, não acha?

Para auxiliar nisso, existe o Protocolo DHCP, que é um protocolo de configuração dinâmica de endereços de rede, adicionados automaticamente a dispositivos ligados na rede, ou seja, quando um computador é ligado à rede, o mesmo não possui um IP, sendo assim, ele solicita uma requisição ao servidor DHCP “informando” que necessita de um endereço IP para se comunicar com outras máquinas da rede; o servidor DHCP envia uma resposta com todos os dados necessários para o acesso deste computador (TANEMBAUM; WETHERALL, 2011).

Como mencionado anteriormente, sabemos que uma rede pode conter várias máquinas, e que a qualquer momento uma nova máquina pode acessar a rede e outra pode se desligar, por esse motivo o servidor DHCP fornece o endereço de rede temporariamente. Durante o período de uso de determinado endereço pelas máquinas, o servidor não disponibilizará o mesmo endereço a qualquer outra máquina; somente ocorrerá quando esta máquina se desligar da rede em questão, podendo, assim, atribuir esse endereço a uma nova máquina (RIOS, 2011).

Normalmente, qualquer dispositivo (cliente DHCP) está preparado para receber as informações do servidor DHCP sem a necessidade de realizar uma configuração mais rigorosa, podendo, assim, se conectar à rede.

FTP (File Transfer Protocol)

Este protocolo permite a transferência de arquivos pela internet e o acesso a arquivos remotos em servidores de arquivos locais em uma empresa. Um exemplo de transferência de arquivos pela internet é o download, na qual o usuário solicita o arquivo pretendido ao Servidor FTP, e como resposta o mesmo começa a transferência dos arquivos para a máquina solicitadora.

Já para acessar arquivos remotos, o usuário deverá entrar com um login e senha para autenticação, neste modo, ele terá acesso ao conteúdo disponível. A imagem abaixo mostra de forma interativa como é realizado o acesso remoto aos arquivos do Servidor FTP.



Figura 8 - Sistema FTP

Fonte: Ross e Kurose (2013)

O cliente pode realizar o acesso ao servidor FTP por diversas maneiras, podendo ocorrer pelo Windows Explorer ou por alguns softwares apropriados, como FileZilla, Free FTP, Cute FTP e outros; ou ainda pelo terminal dos Sistemas Operacionais Windows, Linux e Mac OS.

HTTP (Hypertext Transfer Protocol)

É o protocolo padrão utilizado para o funcionamento de toda WEB, encontra-se na camada de aplicação e é implementada por dois programas: um cliente e outro servidor que conversam por trocas de mensagens HTTP. Este utiliza o protocolo TCP como protocolo de transporte, realizado através de softwares chamados de Browsers (navegadores) (ROSS; KUROSE, 2013).



Figura 9 -Protocolo de comunicação

Dentre os diversos navegadores, podemos citar os mais utilizados como Internet Explorer, Mozilla Firefox e Google Chrome, os quais funcionarão através de uma solicitação ao servidor de uma página da internet, utilizando o protocolo HTTP (RIOS, 2011).



Figura 10 -Navegadores

Em seu surgimento, o HTTP trabalhava somente com texto, porém, com o passar das décadas e o surgimento de novas tecnologias, houve uma atualização significativa nesse protocolo, trabalhando agora com arquivos multimídia, como imagens e vídeos.

Em se tratando de computadores, seja em nível de programação ou redes, sabemos que temos que ter algumas tratativas de erros. Em relação a isso, o protocolo HTTP, quando solicitar a leitura de uma página da internet através do método GET, retornará uma resposta com seu status, podendo realizar sua abertura ou ainda resultar em erros, que são indicados na linha de status através de três dígitos.

O navegador reconhecerá a que pertence o dígito retornado e indicar ao cliente o motivo do erro. Exemplos bem conhecidos são de erros de servidor, ou ainda quando a página que você requisita não existe no servidor de origem.

Dos três dígitos, o primeiro é usado para distinguir as respostas em cinco grupos, que são:

- 1XX – Indica que a informação (requisição) foi recebida e está sendo processada. Normalmente não é usado na prática.
- 2XX – Significa que a requisição foi tratada e o conteúdo está sendo retornado.
- 3XX – Informa ao cliente que procure a página requisitada em outro lugar.
- 4XX – Um dos mais conhecidos, indica que a requisição não pode ser atendida, que faltou devido a um erro do cliente, uma solicitação inválida ou uma página inexistente (Erro 404).
- 5XX – São erros do próprio servidor, seja por erro de programação ou ainda por uma sobrecarga temporária (TANENBAUM; WETHERALL, 2011).



SAIBA MAIS

Com o advento das compras online, tornou-se necessário uma conexão mais segura. A partir daí houve uma atualização necessária ao Protocolo HTTP, partindo-se para o HTTPS (*Hyper Text Transfer Protocol Secure*). Esse tipo de protocolo se utiliza de certificados digitais como o SSL e o TSL.

Normalmente, esse tipo de protocolo é utilizado em sites que realizam transações bancárias, como sites de compras online e serviços bancários, que necessitam de uma segurança extrema.

Para saber mais a respeito desse protocolo, você pode acessar o link em que você poderá ter uma melhor noção sobre o que é e como ele irá te proteger.

Fonte: Alves (2014, on-line)⁶.

SSL (Securty Sockets Layer)

Esse protocolo surgiu com o advento da internet e pelo fato de cada vez mais haver a necessidade de conexões seguras, devido ao grande número de transações bancárias online e compras realizadas com cartões na internet (TANENBAUM; WETHERALL, 2011).

Surgiu em 1995 e foi desenvolvido pelo Netscape, que na época era quem dominava o mercado de navegadores. Hoje, esse protocolo é amplamente utilizado nos navegadores existentes e fica disposto entre as camadas de aplicação e de transporte.

O SSL se utiliza de chaves que criptografam e que decifram os dados enviados, evitando que os mesmos possam ser abertos por qualquer pessoa. Essas chaves são criptografadas com uso de algoritmos complexos como o MD5 e o RSA, e normalmente possuem chaves públicas e privadas de segurança.

Para um melhor entendimento, vamos analisar um estudo de caso. Suponhamos que Amanda deseja comprar roupas pela internet; após escolher suas peças de roupas ela parte para a finalização de seu pedido. No momento em que clica em comprar, o site já ativa o protocolo de segurança de informações, pois o site precisará de alguns dados, como número do cartão crédito, nome completo e outros.

Você pode verificar se o site que está navegando se utiliza deste protocolo, observando a barra de status do navegador utilizado, na qual aparecerá um ícone no formato de um cadeado. Ou ainda, observando que no endereço da loja é adicionado um ‘S’ em http, ficando disposto como ‘https’.

SSH (Security Shell)

O SSH é um protocolo para login remoto, semelhante em funcionalidades ao TELNET, porém com algumas distinções importantes, como comunicação segura, e se utiliza de transferência de dados com algoritmos criptografados.

Como base para seus serviços, o SSH oferece alguns mecanismos, como: autenticação de usuários, na qual o servidor poderá dizer quem está tentando se conectar; confidencialidade e integridade dos dados, dentre outros (RIOS, 2011).

Esse protocolo foi desenvolvido na Universidade de Helsinki em 1955 e hoje basicamente é utilizado na autenticação do login, execução de comandos em máquinas remotamente e para a transferência de arquivos. O SSH se utiliza da porta 22. Das diversas implementações existentes, uma das mais utilizadas é o software PuTTY.

DNS (Domain Name System)

Também conhecido como Sistemas de Nome de domínio, é o protocolo mais utilizado na rede, na qual tem como essência a criação de esquemas de atribuição de nomes de páginas baseados em domínio (o endereço do site), ao invés do IP desta página.



Figura 1: Tipos de domínios

tar o endereço de uma página no navegador, o Servidor DNS realiza a conversão do nome da página em seu endereço de IP. O DNS é composto por dois tipos de domínios, os genéricos, terminados em **.com** (comercial), **.edu** (educacionais), **.gov** (governamentais), dentre outros; e os de países, como, por exemplo, o do Brasil, que é terminado em **.br**. Já os nomes de domínio podem ser absolutos, onde o nome termina com um ponto (ex: eng.sun.com.), que é o contrário do nome relativo, ao qual não existe esse ponto no final (TANENBAUM; WETHERALL, 2011).

Foi criado em 1984 e é um protocolo da camada de aplicação, assim como os protocolos HTTP e FTP. Porém, é um protocolo em que não há uma interação direta com o usuário, sendo fornecida uma função interna que traduz os nomes para seus endereços IPs.

Imagine termos que acessar um determinado site e que o mesmo fosse especificado através de número IP. Seria meio complicado, não acha? Teríamos assim que gravar, ao invés do nome da página, todos os endereços IP. O Protocolo DNS veio para nos ajudar, sendo assim, ao digi-



SNMP (Simple Network Management Protocol)

É um protocolo utilizado para o gerenciamento de redes TCP/IP, em que os administradores podem utilizar para realizar o monitoramento de desempenho da rede, detectar problemas e realizar configurações de correção, sem a necessidade de um software de gerenciamento.

SNMP (Simple Network Management Protocol)

Como arquitetura, o SNMP se baseia em três componentes:

The diagram illustrates the three components of the SNMP architecture:

- Equipamentos Geridos:** Shows a server rack with several network cards and blue human figures representing managed devices.
- Agentes:** Shows a man in a suit holding a laptop, representing the agent application running on a managed device.
- Sistemas de Gestão de Redes:** Shows a man pointing at a network diagram on a large screen, representing the network management system.

Equipamentos Geridos

Também conhecidos como Managed Devices, são os elementos que compõem a rede: Hub, Routers, Pontes ou Servidores. Estes equipamentos são objetos que podem conter informações materiais, parâmetros de configuração ou informações estatísticas.

Agentes

são as aplicações de gestão de rede, na qual residem num periférico e é encarregado de transmitir os dados em formato SNMP.

Sistemas de Gestão de Redes

Figura 12 - SNMP (Simple Network Management Protocol)
Fonte: os autores

ENDEREÇOS DE IP, SUBREDES E ROTEAMENTO

Endereços de IP

Um endereço de IP nada mais é do que um protocolo que atribui a todas as máquinas de uma rede um endereço IP, auxiliando no envio e recebimento de dados. Como um exemplo bem simples, podemos fazer uma analogia ao endereço de nossa residência, onde cada residência tem seu próprio endereço, que facilita a entrega de correspondências aos seus destinatários. Em princípio, duas máquinas nunca devem ter o mesmo endereço IP.

O endereço IP se refere a uma interface de rede. Em geral, eles são compostos por 32 bits, que consistem em um conjunto de quatro sequências de 8 bits separadas por um ponto. Um exemplo é o IP 192.168.1.3, onde cada octeto é formado por números que podem ir de 0 a 255.

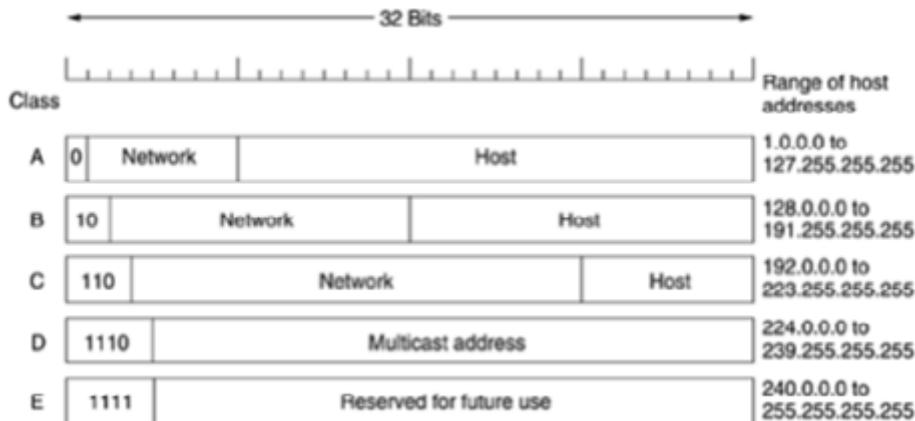


Figura 12 - Formatos de endereços IP

Fonte: Tanenbaum e Wetherall (2011)

Os endereços IP podem ser atribuídos de várias formas nas máquinas. Dentre eles, temos o endereçamento dinâmico, em que o usuário não precisa inserir manualmente as configurações para realizar a conexão a uma rede com serviços DHCP. Outro tipo é o endereçamento estático, que é um número de IP dado permanentemente a um computador, ou seja, seu IP não muda, a menos que seja feita essa mudança manualmente.

SAIBA MAIS



Com o advento da internet, o número de computadores conectados à rede de computadores cresceu substancialmente. Os computadores normalmente são configurados com o protocolo internet IPV4, porém, estamos num momento de transição, onde há a falta de endereços IP para tantos computadores conectados; uma transição para o protocolo internet IPV6. A seguir, selecionamos e disponibilizamos dois vídeos explicativos sobre endereços de IP, nos quais se mencionam sobre o funcionamento e a transição dos protocolos internet.

Como título dos vídeos temos: Os endereços de IP não são todos iguais – Parte 1 - <<https://www.youtube.com/watch?v=jnuHODaLcO8>>. Acesso em: 19 maio 2016. e Os Endereços de IP não são todos iguais – Parte 2 - <<https://www.youtube.com/watch?v=63M61wttuMk>>. Acesso em: 19 maio 2016.

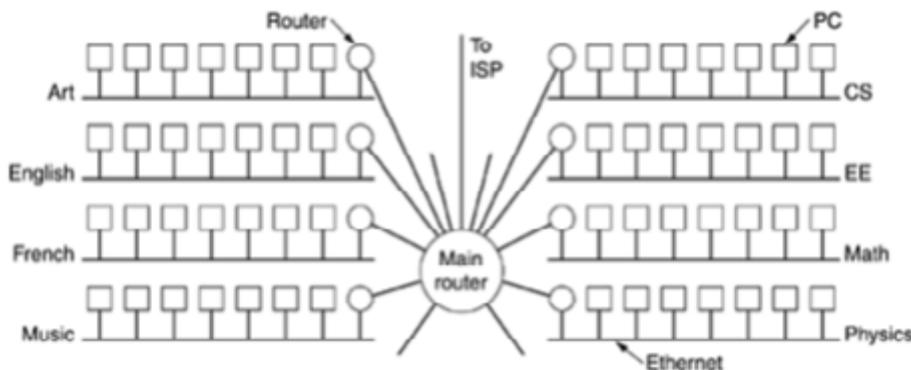
Fonte: os autores

SUBREDES

Podemos dizer que SUBREDES são as partes das redes. Vamos analisar um estudo de caso, retirado do livro de Redes de Computadores, dos autores Tanenbaum e Wetherall (2011, p. 338):

Imagine uma universidade que começou com uma rede da classe B usada pelo departamento de ciência da computação para os computadores em sua Ethernet. Um ano mais tarde, o departamento de engenharia elétrica quis entrar na Internet, e assim comprou um repetidor para estender a rede Ethernet do departamento de ciência da computação até seu edifício. Com o tempo, muitos outros departamentos adquiriram computadores, e o limite de quatro repetidores por rede Ethernet logo foi alcançado. Tornou-se necessária uma organização diferente. Seria difícil obter um segundo endereço de rede, pois os endereços de rede são escassos, e a universidade já tinha endereços suficientes para mais de 60.000 hosts. O problema é a regra segundo a qual um único endereço se refere a uma rede, e não a um conjunto de LANs. À medida que mais e mais organizações se encontravam nessa situação, era feita uma pequena mudança no sistema de endereçamento para lidar com ela.

Conforme estudo de caso, a solução seria a aplicação de subredes, dividindo em diversas partes para uso interno da instituição, ou seja, cada uma das redes teria seu próprio roteador e o mesmo seria conectado ao roteador principal. Nessa

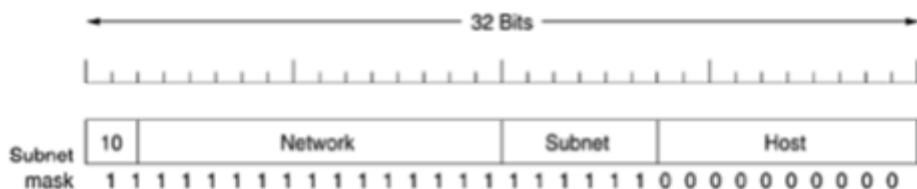


subdivisão, cada rede terá um número de endereço próprio dela.

Figura 13 - Estrutura de como ficaria a REDE

Fonte: Tanenbaum e Wetherall (2011)

Para realizar a divisão de uma rede em subredes, o roteador principal necessita de uma máscara de subrede, na qual ele irá indicar a divisão entre número de rede, subrede e o host. Como exemplo, para melhor entendimento, temos a figura a seguir, que tem uma configuração de como é realizada a máscara de subrede,



que pode ser escrita como 255.255.252.0.

Figura 14 - Uma rede dividida em 64 sub-redes

Fonte: Tanenbaum e Wetherall (2011)

ROTEAMENTO

O roteamento é o mecanismo que auxilia a comunicação das máquinas em uma determinada rede, em que essas máquinas encontram e usam o melhor caminho em uma rede.

O roteamento exerce grande vantagem, dentre elas a escolha de uma melhor rota, de acordo com alguns critérios especificados, tem adaptação à diferentes tecnologias de redes físicas, confiança no envio e controle de acesso e também a reportagem de erros, caso algum pacote tenha chegado com algum erro ao seu destino final (ROSS; KUROSE, 2013).

SAIBA MAIS



O roteamento é a principal forma utilizada na internet para a entrega de pacotes entre hosts (equipamentos de rede de uma forma geral, incluindo computadores, roteadores e outros). No link disponibilizado nas referências consta um artigo que descreve o que é importante saber sobre um roteamento. Nele, há uma breve introdução dos Protocolos de roteamento. Esta leitura ajudará você, aluno(a), em um melhor entendimento dos protocolos e a dar continuidade em nossos estudos nas próximas unidades do livro.

Fonte: Moura (2004, on-line)⁷.

Para que o roteamento funcione de forma adequada e tenha sucesso na entrega dos dados, são utilizadas algumas estratégias em relação ao roteamento. Dentre elas, podemos citar alguns tipos de roteamento:

- 1. Roteamento Estático:** armazena informações de rota realizadas manualmente pelo administrador da rede.
- 2. Roteamento Dinâmico:** armazena atualizações de rota automaticamente em períodos de tempos regulares, para isso ele se utiliza de protocolos de roteamento dinâmico, como exemplo o RIP e BGP.

3. **Roteamento Hierárquico:** é utilizado quando há o aumento substancial das redes e os roteadores não conseguem gerenciar o tráfego da rede. Assim, cada roteador de uma rede “gera” uma tabela de roteamento, sendo cada roteador classificado como uma região.
4. **Algoritmo de Roteamento:** é a parte do *software* da camada de rede responsável pelo caminho que será tomado para a saída e transmissão dos pacotes (TANENBAUM; WETHERALL, 2011).



SAIBA MAIS

Já indicamos a importância de se ter um roteamento em rede de computadores. Para se ter uma ideia, são os roteadores que fazem grande parte do trabalho de envio e recebimento de mensagens, sendo peças essenciais para que as mensagens trafeguem na rede.

A partir disso, vamos assistir o vídeo a seguir, que conta de maneira clara e dinâmica, como é o funcionamento do roteamento. O vídeo está disponível em: <<https://www.youtube.com/watch?v=y9Vx5I-th9Y>>. Acesso em 19 maio 2016. Após assisti-lo, accese a “Sala do Café” no Ambiente Virtual de Aprendizagem e discuta com os colegas sobre o Roteamento de dados nas redes de Computadores.



REFLITA

O maior risco é não correr nenhum risco. Em um mundo que está mudando rapidamente, a única estratégia que certamente vai falhar é não correr riscos.

Mark Zuckerberg

MODELOS DE REFERÊNCIA

TCP/IP

O modelo de referência TCP/IP surgiu por problemas em protocolos existentes, sendo definido em 1974. O nome vem a partir dos protocolos mais utilizados na internet, sendo o protocolo TCP (*Transmission Control Protocol*) e o IP (*Internet Protocol*).

Segundo Tanenbaum e Wetherall (2011), o que propiciou o surgimento foi o fato do Departamento de Defesa dos EUA querer que as conexões permanecessem intactas enquanto os computadores estivessem em pleno funcionamento. Além disso, também era necessário uma arquitetura flexível que realizasse transferências de arquivos e transmissão de dados de voz em tempo real.

O Modelo TCP/IP é dividido em quatro camadas, sendo a Camada de Aplicação, Camada de Transporte, Camada Inter-redes e Camada de *Host/Rede*, que serão descritas a seguir .

Camada de Aplicação

Esta camada é a que se aproxima mais do usuário. Ela contém todos os protocolos de nível mais alto, de acordo com a sua finalidade, como bate papo, videoconferência, e-mail dentre outros. Na tabela 01, alguns protocolos utilizados, com suas respectivas portas utilizadas.

PROTOCOLO	PORTE
<i>Telnet</i>	23
<i>FTP - File Transfer Protocol</i>	21
<i>SMTP - Simple Mail Transfer Protocol</i>	25
<i>DNS - Domain Name System</i>	53
<i>HTTP - Hypertext Transfer Protocol</i>	80

PROTÓCOLO	PORTE
<i>IMAP - Internet Message Access Protocol</i>	143
<i>SSH - Secure Shell</i>	22
<i>DHCP - Dynamic Host Configuration Protocol</i>	67

Tabela 1 - Lista de Protocolos

Fonte: os autores

Camada de Transporte

Nessa camada ocorre o recebimento e a organização dos dados. É onde se terá um controle do fluxo de dados fim a fim, juntamente com um controle de erros. A finalidade da Camada é permitir a comunicação entre a Camada de Aplicação e Camada de Transporte, ou seja, permite que os hosts conversem entre si, independente da distância que eles se encontram.

Essa Camada utiliza dois protocolos importantes, sendo os protocolos TCP (*Transport Control Protocol*) e UDP (*User Datagram Protocol*).

Camada Inter-redes

A tarefa dessa camada é permitir que os hosts adicionem pacotes em qualquer rede e garantir que eles trafegarão independentemente, até seu destino final, mesmo diante de possíveis falhas, e ainda, não importando a ordem que foram enviados, e assim, as demais camadas irão ordená-los corretamente (TANEMBAUM; WETHERALL, 2011).

A Camada inter-redes se utiliza do protocolo IP (*Internet Protocol*), entregando os pacotes onde os mesmos foram solicitados e serão necessários. Além disso, uma questão de muita importância neste protocolo é o roteamento de pacotes, que nada mais é, que o processo de encaminhar pacotes de uma rede para outra.

Camada de Host/Rede

A camada host/rede é responsável por detectar e corrigir possíveis erros no nível físico e controle de fluxo. Ela receberá os pacotes enviados pela camada inter-redes e os enviará/receberá para determinada rede.

O modelo de referência TCP/IP não especifica muito essa camada, somente indica que um determinado host tem que se conectar a uma rede utilizando algum protocolo para que envie os pacotes.

COMPARAÇÃO DO MODELO DE REFERÊNCIA TCP/IP COM MODELO DE REFERÊNCIA OSI	
Modelo de Referência TCP/IP	Modelo de Referências OSI
Aplicação	Aplicação
	Apresentação
	Sessão
Transporte	Transporte
Inter-redes	Rede
Host/Rede	Enlace de Dados
	Física

Quadro 1 - Comparação de Modelo TCP/IP e modelo OSI

Fonte: Tanembaum e Wetherall (2011)

Podemos observar no quadro 1 um breve comparativo do Modelo de Referência TCP/IP com o Modelo de Referência OSI, sendo o modelo OSI mais definido, dividido em 7 camadas, 3 a mais do que o Modelo TCP/IP.

O MODELO OSI (Open Systems Interconnection)

Esse modelo foi desenvolvido como padronização dos protocolos de rede de computadores, pela ISO (*International Standards Organization*) em 1984. É chamado de modelo de Referência, pois se refere à interconexão de sistemas que se comunicam com outros sistemas em uma rede.

A ISO utilizou-se de alguns princípios e conceitos para tornar possível a padronização desta camada. Criou-se então sete camadas, onde cada uma delas deveriam executar funções definidas e, a função da camada, deveria ser escolhida levando-se em conta o protocolo utilizado nela (TANENBAUM; WETHERALL, 2011).

A partir daí, as camadas foram dispostas da seguinte forma:

- Camada Física.
- Camada de Enlace.
- Camada de Rede.
- Camada de Transporte.
- Camada de Sessão.
- Camada de Apresentação.
- Camada de Aplicação.

Em uma breve descrição, dizemos que a **camada física** é responsável pela transmissão de bits por um canal de comunicação, podendo ou não ser realizado em sentidos simultâneos. Já a **camada de enlace de dados** transforma um canal de transmissão bruto em uma linha sem erros de transmissão, não detectados na camada de rede, e também um controle de fluxo de dados. Na **camada de rede**, há um controle de operações da sub-rede, determinando a maneira como os pacotes são roteados até o destino final, superando todos os problemas encontrados.

A **camada de transporte** tem como função aceitar dados da camada acima dela, dividi-los caso necessário e repassá-los à camada de rede, assegurando que todos os dados cheguem corretamente ao seu destino. Já a **camada de sessão** permite que usuários de máquinas diferentes estabeleçam sessões entre elas, oferecendo serviços de gerenciamento de Tokens, sincronização de comunicação e outros.

A **camada de apresentação** está relacionada à sintaxe e à semântica das informações transmitidas, ou seja, tem a função de entregar os pacotes de maneira que sejam entendidos por todas as máquinas e tornar a troca de mensagens entre elas possível. Por último, e não menos importante, temos a **camada de aplicação**, em que nela funcionam vários protocolos conhecidos e realizam a interface com o usuário, para que possam se utilizar dos diversos protocolos (TANENBAUM; WETHERALL, 2011).

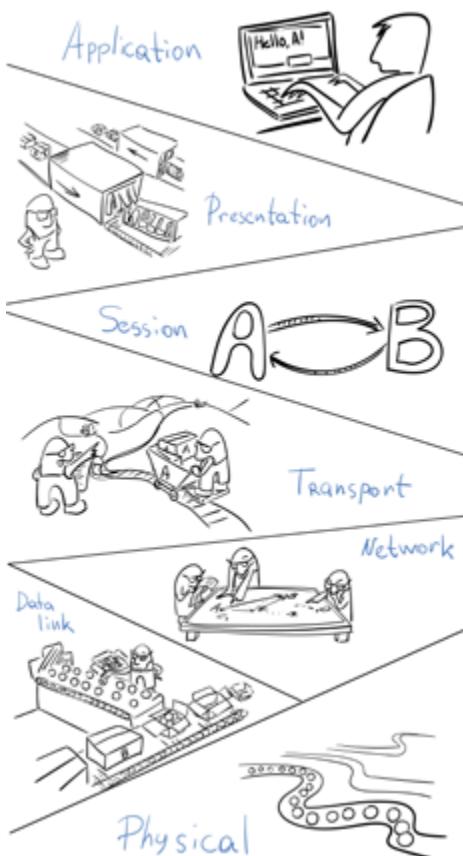


Figura 15 - Mode OSI

CONSIDERAÇÕES FINAIS

Nesta unidade, realizamos um aprendizado acerca dos tipos de conexões existentes, dentre elas, conexões com fio e sem fio. Um estudo de como as conexões com a internet foram evoluindo com o passar do tempo até chegar nos dias de hoje, com suas conexões de alta velocidade por meio de redes de telefonia, satélite, rádio e telefonia móvel. Vimos também, em um dos nossos **Saiba Mais**, que em um futuro bem próximo poderemos utilizar conexões através de lâmpadas de LED, as conexões LI-FI, que nos trazem conexões cada vez mais rápidas. Hoje já podemos observar algumas conexões que se utilizam da energia elétrica da própria residência para a transferência de dados.

Estudamos também o que são os protocolos e sua importância para o funcionamento da rede de computadores, protocolos esses indispensáveis em se tratando de dias atuais. Falamos desde protocolos que nos ajudam no transporte de dados, seja em forma de envio ou recebimento.

Além disso, também foi pontuado a respeito dos protocolos de correio eletrônico, que hoje são um dos mais utilizados mundialmente. Protocolos estes que, para um bom funcionamento, passaram por grandes processos de padronização para que chegassem ao que é hoje. Padronização esta estudada nos Modelos de Referência TPC/IP e suas camadas (Camada de Interface de Redes, Camada Inter Redes, Camada de Transporte e Camada de Aplicação); e uma breve descrição do Modelo OSI.

Em nossa próxima unidade, entraremos mais à fundo no Modelo OSI, entendendo o funcionamento de cada uma das sete camadas que a compõem (Camada Física, Camada de Enlace de Dados, Camada de Rede, Camada de Transporte, Camada de Sessão, Camada de Apresentação e Camada de Aplicação) e quais protocolos são utilizados em cada camada. Sabendo desse contexto, vamos dar seguimento ao nosso aprendizado? Lembre-se que a leitura é fundamental para prosseguirmos com o entendimento dos próximos capítulos!

ATIVIDADES



- 1) Esse protocolo é um dos mais conhecidos na internet, e tem como principal funcionalidade o compartilhamento de arquivos na Internet através de um servidor de arquivos. Dentre as alternativas a seguir, qual é o protocolo que melhor se adequa ao descrito acima?
- a) SMTP
 - b) POP3
 - c) FTP
 - d) NFS
 - e) Telnet
- 2) Com o advento da Internet, o protocolo HTTP precisou ter sua implementação elaborada. A partir daí surgiu o protocolo HTTPS (*HyperText Transfer Protocol Secure*), na qual teve como incorporação uma camada de segurança. O protocolo de segurança originalmente utilizado nessa camada é o?
- a) POP3 (*Post Office Protocol*).
 - b) SMTP (*Simple Mail Transfer Protocol*).
 - c) IMAP (*Internet Message Access Protocol*).
 - d) SSL (*Secure Sockets Layer*).
 - e) SSH (*Secure Shell*).
- 3) Uma empresa multinacional está com planos de se instalar no território brasileiro. Porém, como pré-requisito de instalação, a empresa necessita que a cidade tenha suporte a uma rede móvel que atenda as necessidades dos smartphones distribuídos aos funcionários das empresas, na qual irão precisar encaminhar e receber e-mails com grandes anexos, envio de imagens e vídeos de determinadas situações, e ainda, que quando possível, pudessem realizar vídeo conferências em determinadas localidades. Analisando o que foi dito acima, qual das tecnologias abaixo atende a todos os requisitos informados e que a cidade em questão deverá ter?
- a) GPS
 - b) GSM
 - c) GPRS
 - d) FIXO
 - e) LTE

ATIVIDADES



4) Com a difusão da internet e a evolução das diversas tecnologias, serviços de banda larga estão cada dia mais acessíveis e sendo oferecidos com uma melhor qualidade e com maiores velocidades aos usuários finais. Assinale a alternativa que contém a sigla da tecnologia utilizada para acesso de banda larga residencial.

- a) WLAN
- b) MODEM
- c) ADSL
- d) BGP
- e) ISP

5) É um serviço que permite navegarmos na internet digitando apenas uma URL em formato texto ao invés de endereços IP. Além disso, se utiliza dos protocolos TCP/IP nas instalações de redes de computadores. Dentre os protocolos baixo, qual é melhor definido pelo texto acima?

- a) ARP
- b) DNS
- c) TCP
- d) HTTP
- e) DHCP

6) Na instituição Unicesumar, deseja-se implementar soluções de rede que privilegiam o uso de conexões sem fios. Rafael é quem cuida da gerência de redes e tem a tarefa de fornecer soluções sem fio para 2 diferentes situações:

Situação 1: há diversos equipamentos, como câmera digital, teclado, *mouse*, fone de ouvido etc., que devem ser conectados a um computador, notebook, ou ainda *desktop*.

Situação 2: Deverá ser distribuído aos alunos uma forma de conexão sem fio para que os mesmos consigam realizar pesquisas no Campus da Instituição, por meio de login e senha pelo seu R.A.

ATIVIDADES



As soluções de tecnologia sem fio indicadas corretamente são:

- a) 1 - Bluetooth; 2 - WI-FI.
- b) 1 - Infravermelho; 2 - WI-FI.
- c) 1 - 4G; 2 - Ethernet.
- d) 1 - Bluetooth; 2 - 4G.
- e) 1 – WI-FI; 2 - LAN

7) Sobre os protocolos de transporte do TCP/IP, verifique as afirmativas baixos:

- 1. Por não ser orientado à conexão, o TCP garante a entrega, bem como a taxa de transmissão e o tempo para entrega dos pacotes.
- 2. O TCP possui um mecanismo de controle de congestionamento.
- 3. O socket é uma interface entre o protocolo de aplicação e a camada física.
- 4. O UDP não oferece garantia quanto a atrasos.

Assinale a opção que se aplica aos quatro itens acima:

- a) Todas são verdadeiras.
- b) 4 é falsa.
- c) 1 e 2 são falsas.
- d) 2 e 4 são verdadeiras.
- e) Todas são falsas.

8) Analise as alternativas a seguir e marque a que indica os protocolos presentes na camada de transporte do modelo de referência TCP/IP.

- a) FTP e SMTP
- b) DNS e IP
- c) TCP e UDP
- d) TELNET e SMTP
- e) P2P e HTTP



Estou disponibilizando a você, aluno(a), um artigo interessante a respeito de um comparativo entre as tecnologias WI-FI e LI-FI. Após a leitura, entre em nosso Ambiente de Aprendizagem (AVA) e na Sala do Café, faça uma interação com os colegas sobre essas tecnologias. Você pode ter acesso completo ao artigo no link disponibilizado nas referências.

Segue o artigo:

1. INTRODUÇÃO

Comunicar-se com o mundo sem o uso de qualquer tipo de fiação ou cabo, tem sido uma realidade crescente no cotidiano de qualquer pessoa. Foi-se o tempo em que realizar transação bancária enquanto se passeia com os filhos era ficção de Hollywood. Hoje podemos fazer uma ligação telefônica ou enviar mensagens em praças, shoppings, praias e demais locais públicos. Podemos nos conectar usando *smartphones*, notebooks, *tablets* através da Wi-Fi (*Wireless Fidelity*) ao mundo.

Porém, ao passo que a Wi-Fi cresce surgem novos problemas, e o mais evidente talvez seja interferência entre frequências de rádio. Nos provedores de internet *wireless*, o problema é recorrente devido ao alto número de equipamentos *wireless* espalhados pela cidade. Isso faz com que a empresa tenha que “dançar” entre os canais para conseguir uma conexão íntegra e estável. Temos também questões de segurança; só o fato de uma rede Wi-Fi ser vista por *hosts* vizinhos propicia vulnerabilidades a mesma.

O VLC (*Visible Light Communication*) promete substituir a atual radiofrequência, a começar por redes familiares e/ou corporativas. A tecnologia oferece um novo conceito de comunicação de dados. Funciona através da oscilação de luz, imperceptível a olho nu, emitida através de lâmpadas LED (*Light Emitting Diode*). Ao contrário da radiofrequência, essa tecnologia não tem interferências e não necessita de criptografia grosso modo, já que a mesma não pode ser enxergada por *hosts* vizinhos.

Frequências de rádio são caras, escassas, difíceis de trabalhar e o espectro eletromagnético está saturado. A comunicação via LED já testada em laboratório, tem um custo de instalação e manutenção baixo, não tem interferência e é naturalmente segura. O Li-Fi (*Light Fidelity*) é o padrão para ambientes fechados que promete substituir à atual Wi-Fi. O VLC tem uma série de outras aplicações além da Li-Fi, como comunicação marítima, segurança de trânsito entre outras que serão citadas no decorrer deste artigo.

2. WIRELESS.

2.1. TRANSMISSÕES VIA LUZ

De acordo com Villlate (2005, p. 7) “... a luz, tal como qualquer tipo de matéria, é tanto onda como partícula”. Tanenbaum (2003, p. 107) nos mostra que a mesma passa a ser





visível a uma frequência um pouco mais alta que o infravermelho.

As tecnologias de laser, LED e infravermelho são as existentes no mercado para transmissão via luz. Porém, o padrão que vem surgindo contra a atual Wi-Fi, é o chamado Li-Fi criado pelo professor Haas (2011), tecnologia esta que utiliza LEDs para transmissão sem fio.

2.1.2. LASER

Segundo Tanenbaum (2003), naturalmente, a sinalização óptica que utiliza raios laser é unidirecional, ou seja, o sinal tem só uma direção. Ao contrário, por exemplo, das ondas de rádio que são omnidirecionais, podendo servir para aplicações multipontos também.

Para visualizar melhor o significado dessa afirmação, vamos imaginar um ambiente entre um prédio e outro, os dois se comunicam via laser, cada edifício precisa ter seu próprio comunicador laser e seu sensor fotorreceptor. Esse esquema tem por vantagens, a praticidade, alta largura de banda e principalmente o baixo custo, já que não é necessária uma licença específica para utilização do mesmo.

Se você pensar que, 'Isso é bem útil em dias azuis e ensolarados, mas quando chover ou nevar tudo irá por água a baixo', você errou. Mesmo em belos dias o sistema pode parar de funcionar, principalmente nos dias ensolarados. O calor do sol gerará convecção no ar (comumente chamado de mormaço) entre laser e receptor, fazendo o sinal quase que literalmente dançar.

Outro problema seria a pontaria. Alinhar um laser com 1 mm de largura seria como acertar a cabeça de um alfinete a 500 metros de distância. Fora esses dois problemas anteriores, fatores como vento, tremores e qualquer outro evento que movesse o laser poderia parar o sistema. Por tais motivos, o ponto a ponto via laser é um projeto descontinuado.

2.1.4. LI-FI

Tanenbaum (2003) nos mostra que acima da frequência de infravermelho, temos a nossa tão conhecida luz visível, e é com essa matéria prima que a recém-nascida Li-Fi trabalha. O nome vem com o propósito de substituir o atual Wi-Fi, onde *Wireless* é substituído por *Light*, luz em inglês. Assim temos a "Light Fidelity", ainda não padronizado e não catalogado em nenhuma RFC.

A tecnologia foi criada e apresentada por Harald Haas (2011), professor de engenharia na Universidade de Edimburgo. A apresentação do sistema tirou suspiros e aplausos na TED - *Ideias Worth Spreading* -, feira palco de grandes invenções.



Não serão necessários enlaces de camada 2 para comunicação com roteadores. Segundo Haas (2011) bastará posicionar o notebook, *tablet* ou *smartphone* em baixo da luz e começar a utilizar a internet. Para o usuário será apenas uma lâmpada comum, porém a lâmpada em questão é uma lâmpada de LED.

Como já dissemos anteriormente essa nova tecnologia funciona com uma mudança de paradigma, que seria uma nova aplicação para um princípio antigo. O funcionamento da Li-Fi é basicamente idêntico ao do código Morse, a luz acende e apaga se comunicando com o fotorreceptor. O professor Haas (2011) afirma ainda que o sistema usa um truque matemático chamado OFDM (*Orthogonal Frequency Division Multiplexing*), que permite variar a intensidade da saída do LED em um ritmo muito rápido, invisível ao olho humano.

Neste caso, a luz diminui sua intensidade de 800THz para 400THz, o fotorreceptor recebe a informação e o converte para pulsos eletrônicos. O fotorreceptor em questão pode ser específico de tecnologia proprietária ou um olho eletrônico simples, como uma webcam ou câmera de celular.

As aplicações variam de redes corporativas, comunicações automobilísticas, e até internet e telefonia em aviões. A maior utopia do professor Haas é segundo ele, a completa substituição de todos os aparelhos rádio, incluindo torres e receptores de radiofrequência. Em trecho transcrito para o português, o professor Haas (2011) afirma que o planeta tem 1,4 bilhões de torres de rádio, que demandam muita manutenção e energia elétrica. Tudo isso aliado ao fato das ondas do espectro eletromagnético serem escassas, caras e por vezes burocráticas de se licenciar, tornam a Li-Fi uma solução atraente, principalmente para redes corporativas.

Para escritórios a proposta seria adotar o PLC/VLC (*Power Line Communication* e *Visible Light Communication*), dessa forma a informação transcorre pela rede de energia e é a 'última milha' via LED, através da luz.

Com o limite prática no meio de 10 Gbts, a Li-Fi ainda desconhecida já se mostra uma excelente substituta para a Wi-Fi em todos os seus padrões IEEE.

3. TRANSMISSÃO VIA RÁDIO.

3.3 IEEE 802.16 (WiMAX)

É importante definirmos o porquê do nome WiMAX. Quanto a isso DANTAS (2010) nos deixa claro que o IEEE 802.16 é o padrão e o WiMAX uma implementação do padrão (segue-se a mesma lógica para os demais padrões IEEE 802). Dantas (2010, p. 402) ainda segue dizendo:





A tecnologia WiMAX pode ser compreendida especialmente como uma solução de banda larga sem fio, portanto representando uma alternativa em relação, por exemplo, as tecnologias *cable modem*, DLS e PLC, para acesso à última milha. Acesso a última milha significa o enlace entre o último ponto da operadora de telecomunicação e a residência do usuário.

Segundo Tanenbaum (2003, p.324), o 802.16 fornece serviço para edifícios e, esses não sendo móveis não migram de uma célula para outra com frequência. "Essa diferença significa que o 802.16 pode usar comunicação *full duplex*, algo que o 802.11 evita para manter baixo o custo dos rádios".

Em resumo, Tanenbaum (2003) nos explica que o padrão IEEE 802.16 foi implementado apenas para comunicação *ponto a ponto*, entre estações estacionárias e não móveis. Dantas (2003) afirma que na ligação ponto a ponto, uma estação base origem transmite diretamente a informação para uma estação base destinatário. Porém, o autor também nos mostra que no padrão WiMAX também pode ser utilizada a interoperabilidade entre redes 802.16 e 802.11, combinando *links* ponto a ponto e ponto-multiponto [...]. Para tal largura de banda, o 802.16 trabalha em frequências de 2 à 66GHz.

Segundo Fagundes (2005), a WiMAX poderia substituir o Wi-Fi porém, atualmente muitos provedores de internet wireless sofrem com problemas de interferência nas redes WiMAX. Devido à escassez do espectro esse tipo de problema é possível de ocorrer tanto em redes metropolitanas quanto em wireless locais. Tais problemas não existiram usando-se transmissões via luz.

A empresa ITAOL (2013) da cidade de Itapaci do estado de Goiás nos apresenta um caso muito interessante. Problemas com provedores clandestinos trouxeram uma luta infundável para manter o padrão de qualidade do *link* para seus clientes. A ITAOL (2013) notificou a ANATEL que, depois de um prazo de no mínimo 80 dias tomou as devidas providências. Mas isso não foi suficiente reprimir criminosos que, além de enganarem o consumidor abusam da falta de conhecimento de algumas pessoas para praticar tais crimes. Uma das empresas que teve os equipamentos apreendidos pela ANATEL mudou de nome e continuou com a atividade clandestina, com a tremenda falta de conhecimento, e sem acompanhamento de um engenheiro instalou novas torres, provocando mais ruído e poluindo ainda mais o espectro de 2.4GHz. Dessa forma então, todos os provedores legalizados se veem forçados a mudarem de frequência, preferencialmente adotando frequências de 5.8Ghz acima, e consequentemente tendo que mudar todo o seu parque de equipamentos.

Fonte: Victor (2014, on-line)⁸.

MATERIAL COMPLEMENTAR



LIVRO

Redes de Computadores e A Internet: Uma Abordagem Top-Down

James F. Kurose; Keith W. Ross

Editora: Pearson

Sinopse: seguindo o sucesso da abordagem top-down de suas edições anteriores, 'Redes de computadores e a Internet' tem como foco camadas de aplicação e interfaces de programação, propondo ao leitor uma experiência prática com os conceitos de protocolo e redes de computadores antes de trabalhar com mecanismos de transmissão de informação das camadas inferiores das pilhas de protocolos.



REFERÊNCIAS

- FERNANDES, A. M. **Fundamentos de Redes de Computadores.** Maringá: Centro UniversitárioUnicesumar, 2014.
- FOROUZAN, B. A. **Comunicação de Dados e Redes de Computadores.** 3 ed. Porto Alegre: Bookman, 2008.
- RIOS, R. O. **Protocolos e Serviços de Redes.** Colatina: CEAD / Ifes, 2011.
- ROSS, K. KUROSE, J. F. **Redes de Computadores e a Internet:** uma abordagem top down. 5 ed. São Paulo:Pearson, 2013.
- TANENBAUM, A.; WETHERALL, D. **Redes de Computadores.** 5 ed. São Paulo: Pearson, 2011.

CITAÇÃO DE LINKS

- ¹ <<https://cutt.ly/ngbya3L>>. Acesso em: 19 maio 2016.
- ² <<http://www.tecmundo.com.br/bluetooth/89233-evoluindo-bluetooth-tera-velocidade-alcance-2016.htm>>. Acesso em: 19 maio 2016.
- ³ <<http://www.tecmundo.com.br/windows-vista/2043-acesse-e-controle-um-computador-remotamente.htm>>. Acesso em: 19 maio 2016.
- ⁴ <http://www.teleco.com.br/4g_tecnologia.asp>. Acesso em: 19 maio 2016.
- ⁵ <<http://g1.globo.com/tecnologia/noticia/2015/09/os-melhores-e-piores-paises-para-cobertura-de-4g-brasil-mostra-limitacoes.html>>. Acesso em: 19 maio 2016.
- ⁶ <<http://www.techtudo.com.br/noticias/noticia/2014/02/o-que-e-https-e-como-ele-pode-proteger-sua-navegacao-na-internet.html>>. Acesso em: 19 maio 2016
- ⁷ <<https://memoria.rnp.br/newsgen/9705/n1-1.html>>. Acesso em: 19 maio 2016.
- ⁸ <<http://docsslide.com.br/download/link/artigo-wi-fi-vs-li-fi>> Acesso em: 19 maio 2016.



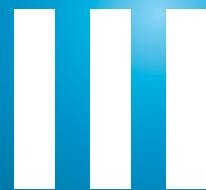
GABARITO

1. C
2. D
3. E
4. C
5. B
6. A
7. D
8. C



INTRODUÇÃO AO MODELO OSI CAMADAS (FÍSICA, ENLACE DE DADOS, REDE, TRANSPORTE, SESSÃO, APRESENTAÇÃO E APLICAÇÃO)

UNIDADE



Objetivos de Aprendizagem

- Estudar as características da Camada Física, comunicação de dados, meios de transmissão e comunicação de rede sem fio e com fio.
- Mostrar as características da Camada de Enlace de Dados, mecanismos de detecção de erros, protocolos de acesso, comutação da camada etc.
- Numerar as características da Camada de Rede, algoritmo de roteamento, controle de congestionamento.
- Entender as características da Camada de Transporte, protocolos de acesso, controle de congestionamento, questão de desempenho.
- Explicar as características e funcionamento da Camada de Sessão.
- Classificar as características e funcionamento da Camada de Apresentação.
- Estudar as características da Camada de Aplicação, protocolos de aplicação, arquitetura cliente/servidor.

Plano de Estudo

A seguir, apresentam-se os tópicos que você estudará nesta unidade:

- Camada Física
- Camada de Enlace de Dados
- Camada de Rede
- Camada de Transporte
- Camada de Sessão
- Camada de Apresentação
- Camada de Aplicação

INTRODUÇÃO

Na unidade II, estudamos os tipos de conexões, com fio e sem fio. Vimos que hoje há uma crescente em estudos de tecnologia a base de conexão via luz e que esta é uma conexão que vem com altas velocidades, incomparáveis com o nosso Wi-fi.

Viajamos também sobre o mundo da rede de telefonia móvel, conhecendo todas as gerações existentes até o momento, desde a primeira geração, passando pela geração digital e suas inovações, até chegar na rede móvel 4G, que hoje é a tecnologia que vem se espalhando mundo a fora.

Descrevemos, no decorrer da unidade anterior, o funcionamento de alguns dos protocolos mais utilizados nas redes, não nos esquecendo dos que mais utilizamos: os protocolos UDP e TCP. Definições importantes que nos ajudarão mais adiante no entendimento do funcionamento do modelo de Referência OSI.

Definimos também subredes, os nossos endereços de IP, que são os nossos endereços na rede mundial de computadores e os roteamentos, que têm uma grande funcionalidade realizando tratativas de congestionamento e de erro de envio de dados.

Aprendemos uma breve introdução a respeito de modelos de referência, tanto o modelo TCP/IP (e suas quatro camadas), quanto o modelo OSI (com suas sete camadas). A partir disso, nesta Unidade, partiremos para um melhor detalhamento de como funciona o modelo OSI e suas sete camadas, identificando a importância que cada uma tem em se tratando de redes.

Citaremos alguns protocolos que são executados em cada camada e suas tratativas, para que sejam executados da melhor forma possível; e, para que os dados sejam encaminhados até o destino final sem causar nenhum transtorno futuro. O que acha de começarmos agora a adquirir novos conhecimentos a respeito das redes de computadores? Vamos lá?

CAMADA FÍSICA

É a camada mais baixa da hierarquia do Modelo de Referência OSI, na qual define como os bits são enviados pelos canais de transmissão. As informações podem ser transmitidas por fios ou fibra ótica, utilizando-se da largura de banda, e que depende da construção, espessura e comprimento que foi utilizado (TANENBAUM; WETHERALL, 2011).

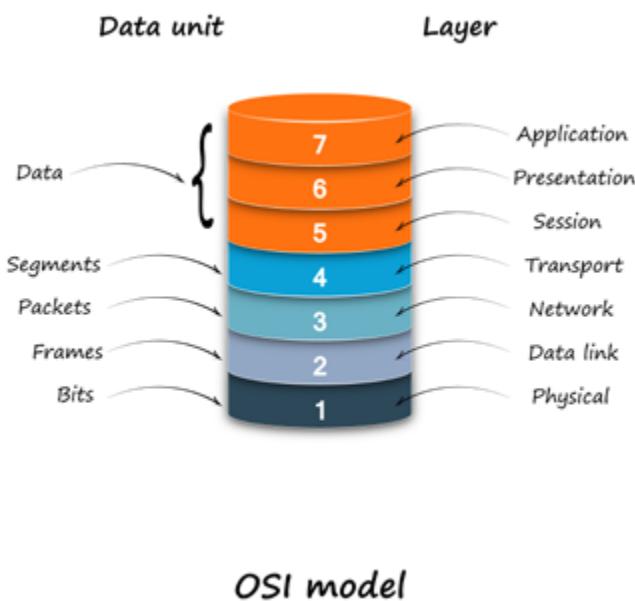


Figura 1 - Sete camadas do Modelo OSI

Em se tratando de largura de banda, engenheiros elétricos e cientistas da computação têm uma definição diferente; na qual, para engenheiros a largura de banda é medida em Hz, já para os cientistas da computação, é a taxa de dados máxima de um canal, e medida em bits.

Sabemos que o objetivo dessa camada é realizar a transmissão de bits de uma máquina para outra, utilizando de meios guiados, como fios de cobre e fibra ótica, e meios não guiados, como redes sem fio, satélites e outros. A partir de agora, iremos distinguir os meios guiados dos não guiados, vamos começar?

Meios de Transmissão Guiados

Em relação aos meios guiados, em nossa primeira unidade aprendemos sobre cabos coaxiais, cabos par trançado e fibra ótica. além desses já definidos, temos também os meios magnéticos e por linhas de transmissão de energia elétrica.

Nos meios magnéticos, uma das formas mais comuns de se transportar dados de uma máquina para outra é por meio de mídias removíveis, ou ainda fitas magnéticas. Lembramos que esse tipo de transporte é muito utilizado, sendo que o usuário pode gravar os dados e transmiti-los a outro computador simplesmente colocando a mídia e realizando a transmissão.

Relembrando um pouco, retornaremos ao cabo par trançado, que é um dos cabos mais antigos e mais utilizado. Podem ser usados em transmissão de dados analógicos e digitais e sua largura de banda depende da espessura do fio e da distância que será percorrida, podendo-se alcançar diversos megabits por segundo em se tratando de taxa de dados. Existem várias categorias de pares trançados, desde os utilizados por linhas telefônicas até os que utilizamos em nossas casas, aquele cabo de rede revestido de uma capa plástica comumente na cor azul.

Já o cabo coaxial tem uma melhor blindagem e pode ser utilizado por uma maior distância e com velocidades mais altas. Temos dois tipos de cabos amplamente utilizados, os empregados na transmissão digital (50 ohms) e os empregados nas transmissões analógicas e também utilizados em TVs a cabo (70 ohms). Um cabo coaxial nada mais é do que um fio de cobre esticado e protegido por um material isolante, no qual se trata de uma malha sólida entrelaçada.

Em relação a fibra ótica, sabemos que é uma das mais rápidas em relação à transmissão de informações. É amplamente utilizada para a transmissão por longa distância nos backbones da rede, LANs de alta velocidade e acesso a internet em alta velocidade.



SAIBA MAIS

Uma fibra ótica nada mais é do que um vidro transparente, fino, com aproximadamente 0,5mm de diâmetro e muito parecido com nosso fio de cabelo. Como forma de entender melhor sobre este assunto, no vídeo a seguir você poderá saber um pouco mais sobre a fibra ótica, uma das tecnologias mais utilizadas no mundo para a transmissão dos dados e voz. <<https://www.youtube.com/watch?v=eVHfET9uDz8>>. Acesso em: 19 maio 2016. Após assistir o vídeo, não deixe de interagir na nossa Sala do Café.

Fonte: os autores

Já citado em nossa segunda unidade, temos também as linhas de energia elétrica, que vêm crescendo como uma alternativa para a conexão em banda larga, porém, só está disponibilizado em alguns lugares do Brasil (veja na Unidade II o tópico sobre os tipos de conexões).

Meios de transmissão não Guiados

Amplamente utilizado por usuários que querem estar conectados sempre em seus smartphones, notebooks, tablets e outros sem precisar estar conectado a um cabo que lhe prenda por determinada distância.

Dentre os meios não guiados temos as transmissões de rádio, que podem percorrer grande distância e penetrar facilmente em residências, viajando em todas as direções possíveis.

Outro tipo é a transmissão por meio de micro-ondas, que ao contrário da transmissão por rádio, não atravessam muito bem obstáculos, tendo em vista que as mesmas viajam em linha reta.

Para a comunicação e transmissão de dados em um curto alcance, e utilizado por notebooks, controle remoto de aparelhos, alguns celulares e outros, temos a transmissão infravermelho, que para realizar a transmissão os aparelhos devem estar direcionados em um mesmo ambiente.

Ainda temos a transmissão via luz, que se utiliza de uma transmissão ótica usando raio laser e de forma unidirecional. Por exemplo, cada prédio precisa de seu próprio raio laser e de seu próprio fotodetector para que se possa realizar a transmissão. Esse tipo oferece uma largura de banda muito alta e segura (TANENBAUM; WETHERALL, 2011).



SAIBA MAIS

Em redes, existe a Comutação, que é a alocação de recursos da rede para a transmissão pelos diversos dispositivos conectados, podendo ser comutação de circuitos, de pacotes e de mensagens. Você pode ter mais informações sobre os tipos de comutação acessando o link nas referências, link este que trata de maneira resumida e fácil a respeito da comutação no modelo OSI.

Fonte: Raulino (2016, on-line)¹.

CAMADA DE ENLACE DE DADOS

Essa camada tem a função de fornecer uma interface de serviços bem definida à camada de rede, lidando com os erros de transmissão e tratando do fluxo dos dados de forma que receptores lentos não sejam atropelados por receptores rápidos.

Serviços oferecidos pela Camada de Enlace

Segundo Ross e Kurose (2013), dentre os serviços que são oferecidos, temos:

- **Enquadramento de dados:** os protocolos encapsulam datagramas da camada de rede dentro de um quadro da camada de enlace antes de transmiti-lo.
- **Acesso ao enlace:** um protocolo de controle de acesso ao meio especifica as regras de como um quadro é transmitido pelo enlace.
- **Entrega confiável e controle de fluxo:** o protocolo da camada de enlace fornece um serviço confiável de entrega, garantindo o transporte sem erro de cada datagrama da camada de rede pelo enlace. Além disso, há um

tratamento em relação ao controle de fluxo, no qual a camada de enlace deve realizar a verificação de quando um receptor está mais lento do que receptores que enviam mais rápido.

- **Detecção e correção de erros:** muitos protocolos desta camada de enlace fornecem mecanismos de detecção e correção de erros no momento da transmissão.

Mecanismos de Detecção e Correção de Erros

A Camada de Enlace de dados disponibiliza técnicas de detecção e correção de erros que permitem a descoberta de ocorrência de erros de bits enviados. Porém, não é um processo 100% garantido, já que mesmo com a utilização desses bits para detecção, pode haver erros de bits não detectados, ou seja, o receptor pode não perceber que a mensagem recebida está corrompida e possui erros (TANENBAUM; WETHERALL, 2011).

Dentre os mecanismos de detecção e correção de erros, observamos três técnicas, sendo elas a **verificação de paridade**, **método de soma de verificação** e **verificação de redundância cíclica**.

Analisaremos a Verificação de Paridade, que é a maneira mais simples de realizar a detecção de erros, utilizando bit de paridade. Como a transmissão é realizada através de bits 0 e 1, o receptor, para verificar a ocorrência de erro, deverá realizar a contagem de quantos “1” ele recebeu e comparar com a quantidade de que foi enviado.

Sendo um único bit de paridade, é simples a verificação pelo receptor, porém, há também erro de bits bidirecionais, que é chamado de **paridade bidirecional**, que são divididos em i linhas e j colunas. A verificação no tipo bidirecional deverá ocorrer pela análise da paridade da coluna e linha, caso as colunas e linhas tiverem um bit modificado, ocasionará o erro (ROSS; KUROSE, 2013).

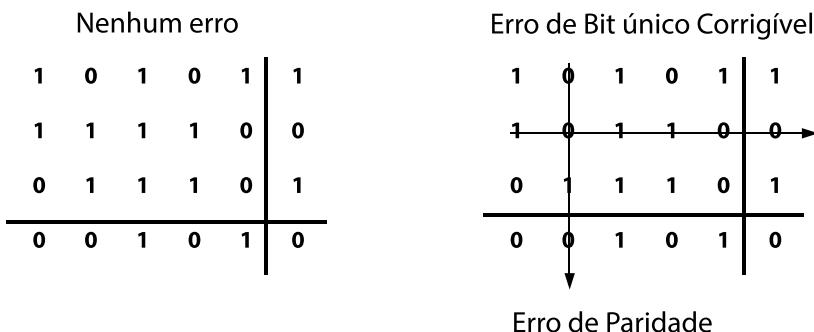


Figura 2 - Paridade par Bidirecional
Fonte: Ross e Kurose (2013)

Protocolos de Acesso Múltiplo

Protocolos de acesso múltiplo são protocolos semelhantes pelos quais os nós (dispositivo de envio e recepção) regulam a transmissão pelos canais de difusão, ou seja, regulam a forma de envio dos quadros de informações para que os mesmos não se percam durante um determinado intervalo de colisão.

Podemos classificar protocolos de acesso múltiplo conforme as seguintes categorias: **protocolo de divisão de canal, protocolo de acesso aleatório e protocolo de revezamento**.

O protocolo de divisão de canal é composto por protocolos que atribuem aos **nós** intervalos de tempo e frequências, permitindo que seus respectivos receptores recebam corretamente os bits codificados pelo remetente. Os protocolos mais utilizados são: TDM (multiplexação por divisão de tempo), FDM (multiplexação por divisão de frequência) e CDMA (acesso múltiplo por divisão de código).

Já o protocolo de acesso aleatório trabalha com um **nó** transmissor sempre transmitindo a taxa total do canal de bits. Nesse protocolo, quando um nó sofre uma colisão, ele é retransmitido repetidamente até que o mesmo passe sem colisão e chegue ao seu destino. Porém, nem sempre isso ocorre, o nó pode esperar um tempo aleatório antes de retransmitir o quadro. Existem vários protocolos de acesso aleatório, dentre eles, podemos citar alguns mais utilizados: o ALOHA e o CSMA (ROSS; KUROSE, 2013).

Ainda, temos o protocolo de revezamento que, como os anteriores, é constituído por dezenas de protocolos. Podemos citar dois mais importantes: o **Polling**, que elimina as colisões e os intervalos vazios, permitindo assim uma eficiência muito maior na entrega; e o protocolo de **Passagem de permissão**, que é descentralizado e tem uma alta eficiência. Este último funciona, como o próprio nome diz, dando permissão aos nós seguintes para serem transmitidos. Por exemplo, o nó 1 poderá enviar a permissão para o nó 2, o nó 2 poderá enviar a permissão para o nó 3, assim por diante, e o nó N poderá enviar uma permissão para o nó 1 (ROSS; KUROSE, 2013).

Protocolos de Enlace de Dados

Existem muitos protocolos de enlace de dados, porém, aqui veremos os protocolos que trabalham nas linhas ponto a ponto da internet (PPP – *Point-to-Point Protocol*), como quando os pacotes são enviados por enlaces de fibra ótica nas redes de longa distância. Na segunda situação, falaremos dos enlaces ADSL, que são os enlaces que conectam milhares de usuários em todo o mundo.

Começamos então a discutir sobre os protocolos ponto a ponto, os quais possuem três recursos principais: um método que delimita o fim de quadro e o início do seguinte; um protocolo de controle de enlace (LPC) que é usado para ativar linhas, testá-las, negociar e desativá-las de forma controlada; e um método com protocolo de controle de rede, no qual deverá negociar as opções da camada de rede de modo independente do protocolo da camada a ser utilizada. O protocolo PPP é o mecanismo que pode transportar pacotes de vários protocolos por muitos tipos de camadas físicas (TANENBAUM; WETHERALL, 2011).

Para exemplificar o enlace ADSL, vejamos a seguinte situação: dentro de casa, um computador envia pacotes IP a um modem DSL usando uma camada de enlace como o Padrão *Ethernet*. O modem envia os pacotes IP para o DSLAM (um roteador conectado a rede). Depois disso, os pacotes IP são extraídos e entram em uma rede ISP, de modo que possam alcançar qualquer destino na internet (TANENBAUM; WETHERALL, 2011).

SAIBA MAIS



Em se tratando de redes de computadores e a internet, temos que saber um pouco mais a respeito das redes ISP, ou ainda, provedor de serviços da internet, que em geral é uma empresa que disponibiliza o acesso à internet mediante o pagamento de mensalidades. Já estudamos alguns tipos de meios de conectar a um ISP, sendo por linha telefônica (dial-up) ou ainda uma conexão banda larga (cablo ou DSL). Além de disponibilizar a conexão com a internet, alguns ISPs disponibilizam também serviços adicionais, como contas de e-mail e domínios para sites.

Fonte: Microsoft (2016, on-line)².

Comutação na Camada de Enlace de Dados

A função da comutação aqui é receber quadros da camada de enlace de dados e repassá-los para enlaces de saída. Utilizando-se de filtragem e repasse, o comutador determina o funcionamento. Sendo que **Filtragem** é a capacidade de um comutador determinar se um quadro deve ser repassado para alguma interface ou deve ser descartado. Já o **Repasse** é a capacidade de um comutador determinar as interfaces para as quais um quadro deve ser dirigido e então dirigir o quadro a essas interfaces.

Podemos observar algumas vantagens com a utilização de comutadores; como a eliminação de colisões, pelo fato do comutador nunca transmitir mais de um quadro em um segmento ao mesmo tempo; há enlaces homogêneos, já que o comutador isola um enlace de outro, diferentes enlaces conseguem operar em diferentes velocidades; e gerenciamento, ao qual o comutador, além de oferecer uma segurança, facilita o gerenciamento da rede.

CAMADA DE REDE

A camada de rede está relacionada à transferência de pacotes da origem para o destino, sendo a camada mais baixa que lida com a transmissão ponto a ponto.

Esta camada deve conhecer a topologia da rede e escolher os caminhos mais apropriados, escolhendo rotas que evitem sobrecarregar roteadores e as linhas de comunicação.

Funções e Serviços da Camada de Rede

A camada de rede possui alguns modelos de serviço de rede, em que define características do transporte, como: entrega garantida dos pacotes ao seu destino, mesmo ocorrendo algum tipo de atraso, entrega de pacotes na ordem em que foram enviados, serviços de segurança, largura de banda mínima garantida e outros (ROSS; KUROSE, 2013).

Ainda nesta questão, a camada de rede fornece serviços orientados à conexão e não orientados à conexão. Caso seja utilizado o serviço não orientado à conexão, os pacotes serão adicionados na rede de forma individual e roteados de modo independente, e esta conexão é chamada de rede de datagramas (TANENBAUM; WETHERALL, 2011).

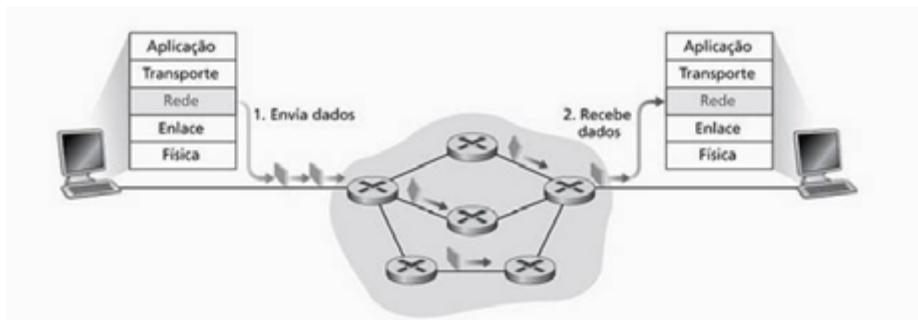


Figura 3 - Rede de Datagramas

Fonte: Ross e Kurose (2013).

Porém, se for utilizado serviço orientado à conexão, deverá estabelecer um caminho desde o roteador de origem até o roteador de destino, antes de enviar qualquer pacote de dados, esta conexão é chamada de rede de circuitos virtuais (TANENBAUM; WETHERALL, 2011).

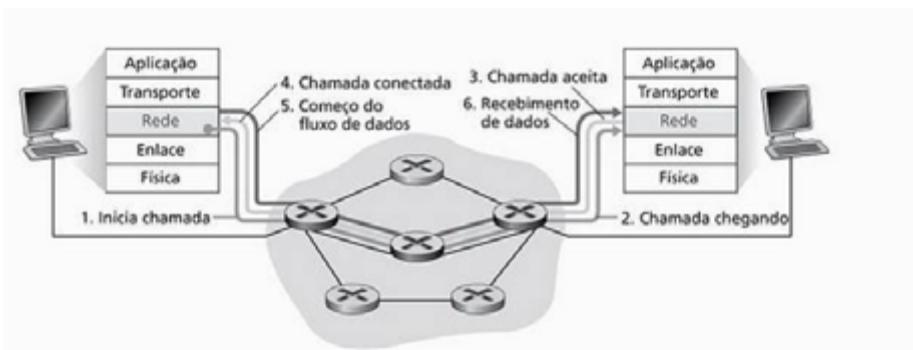


Figura 4 - Estabelecimento de Circuito Virtual

Fonte: Ross e Kurose (2013).

REFLITA



O modo como você reúne, administra e usa a informação determina se vencerá ou perderá.

Bill Gates

Algoritmo de Roteamento

Um algoritmo de roteamento tem como finalidade descobrir o melhor caminho entre o roteador de origem e o roteador de destino. Em se tratando de algoritmo de roteamento, temos vários que auxiliam no melhor transporte das informações. Dentre eles, iremos definir alguns: o Roteamento pelo caminho mais curto, Roteamento por vetor de distância, Roteamento Hierárquico e Roteamento de estado de enlace.

Roteamento pelo caminho mais curto	É a técnica mais simples para calcular os caminhos ideais. A ideia é criar um grafo da rede, em que os nós são os roteadores e os arcos as interfaces de comunicação ou enlace. São conhecidos diversos algoritmos para calcular o caminho mais curto, podemos citar aqui o conhecido Algoritmo de Dijkstra, no qual cada nó é identificado por sua distância a partir do nó de origem.
Roteamento por vetor a distância	É um dos roteamentos mais conhecidos, e tem como função fazer cada roteador manter uma tabela que mostre a melhor distância até o destino, determinando qual o melhor enlace para alcançar o destino final. Também é conhecido por Bellman-Ford .
Roteamento Hierárquico	Este tipo de roteamento é utilizado conforme as redes aumentam de tamanho. Os roteadores são divididos em regiões, na qual cada roteador conecerá os detalhes de como rotear pacotes para outra região.
Roteamento de estado de enlace	É um dos algoritmos mais usados dentro de grandes redes. A ideia é simples e pode ser estabelecida em cinco partes: 1) descobrir quem são os vizinhos e aprender seus endereços; 2) medir quanto de distância tem até os seus vizinhos; 3) criar um pacote na qual recebe as informações que ele aprendeu; 4) enviar esse pacote de informações e receber pacotes de outros roteadores; e 5) calcular o caminho mais curto até cada um dos outros roteadores (TANENBAUM; WETHERALL, 2011).

Quadro 1 - Algoritmos de roteamento

Fonte: os autores.

SAIBA MAIS



Há vários algoritmos de roteamento existentes, podendo ser agrupados conforme funcionamento e características. Alguns algoritmos podem apresentar mais de uma característica, por exemplo, um algoritmo pode ser distribuído e apresentar abordagem pró-ativa. Como forma de aprofundamento em algoritmo de roteamento, estamos disponibilizando nas referências dois links bem interessantes que tratam desse assunto. Após a leitura do texto constante nos links, vá ao seu “ambiente de aprendizagem/sala do café”, e faça um debate com seus colegas sobre os algoritmos de roteamento.

Fonte: Câmara (2001, on-line)³; Teleco (2016, on-line)⁴.

Controle de Congestionamento

Há a necessidade de um controle de congestionamento devido a algumas redes terem pacotes “circulando” em grande quantidade. A presença do congestionamento significa que a carga de pacotes é bem maior que os recursos que a rede pode suportar.

Como auxílio no controle de congestionamento, temos alguns algoritmos que tratam de como evitar o congestionamento da rede. Dentre eles, citaremos o **Roteamento com conhecimento de tráfego** e o **Controle de carga**.

O **Roteamento com conhecimento de tráfego**, no qual o algoritmo realizará uma análise de toda a rede, podendo a rota ser alterada para liberar o tráfego para longe de caminhos muito usados. Como um exemplo para melhor atendimento, imagine um GPS: quando estamos utilizando para nos direcionar a determinada rota, ele nos indica qual a melhor rota, nos livrando de congestionamentos de determinadas cidades.

Outro método utilizado é o **Controle de carga**, podemos dizer também que é a artilharia pesada do controle de congestionamento. Esse método trabalhará da seguinte forma: quando os roteadores estiverem sendo inundados com milhares de pacotes de dados, que não conseguem manipular, ele simplesmente

os descarta. É um método que também é utilizado por concessionárias de energia elétrica, que desligam certas áreas por determinado tempo, para evitar um colapso geral na rede (TANENBAUM; WETHERALL, 2011).



SAIBA MAIS

O Controle de Congestionamento foi proposto por Van Jacobson em 1997 pelo fato de, naquela época e em alguns casos nos dias de hoje, existirem emissores que encaminhavam dados mais do que aceitavam os receptores. Para saber um pouco mais sobre Controle de Congestionamento, disponibilizamos o link nas referências.

Fonte: Ferreira (2008, on-line)⁵.

A camada de Rede na Internet

A internet pode ser vista como um conjunto de subredes conectadas entre si. Sendo que a comunicação se dá com a camada de transporte recebendo o fluxo de pacotes de dados e dividindo-os para que se possam ser enviados como pacotes IP. Os pacotes IP são enviados pelos roteadores IP por um caminho de um roteador para o seguinte, até que o seu destino seja alcançado. A tarefa dos protocolos de roteamento IP é decidir quais caminhos serão usados.

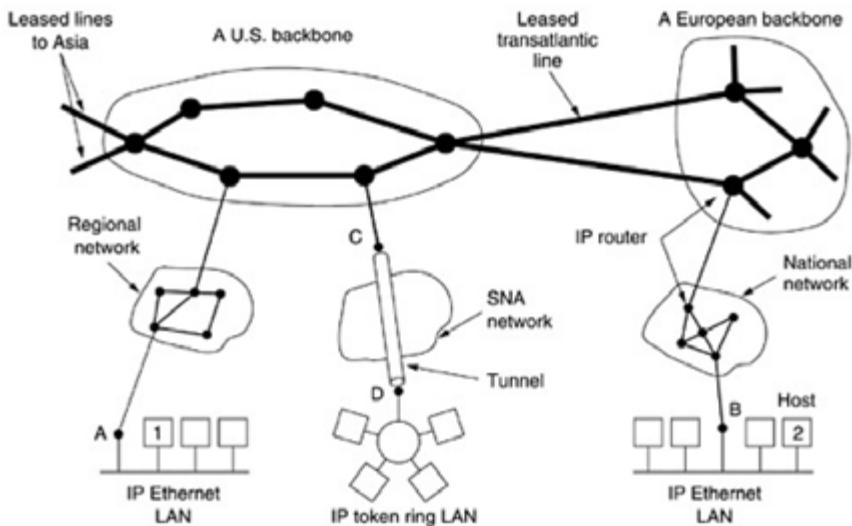


Figura 5 - Coleção interconectada de muitas redes

Fonte: Tananbaum e Wetherall (2011)

A camada de rede da internet utiliza-se de datagramas para a identificação; os chamados protocolos IPV4 e o IPV6. Hoje em dia ainda ocorre a transição do IPV4 para o IPV6, devido à expansão da internet e a necessidade de maior capacidade de endereçamento.

SAIBA MAIS



Neste vídeo, você adquire mais conhecimento a respeito do protocolo IPV6, que surgiu devido ao esgotamento dos endereços de IPs existentes. Ele veio como uma forma de “atualização” do IPV4 para melhor atender a demanda dos dias atuais. O video está no link: <https://www.youtube.com/watch?v=_JbLr_C-HLk>. Acesso em: 19 maio 2016.

Fonte: os autores.

CAMADA DE TRANSPORTE

A camada de transporte é uma das peças centrais da arquitetura de redes, desempenhando papel fundamental de fornecer serviços de comunicação direta. Devido

a essa importância, iremos estudar abaixo como esta camada realiza o transporte dos dados, mencionando suas funções, protocolos utilizados, seu controle de congestionamento e outros. Vamos dar sequência ao aprendizado?

Função de Serviços da Camada de Transporte

O principal objetivo desta camada é oferecer serviços de transporte confiáveis, eficientes e econômicos. Para atingir esse objetivo, a camada de transporte se utiliza de vários serviços oferecidos pela camada de rede.

A Camada de Transporte possui dois serviços parecidos com serviços da Camada de Rede, o **serviço orientado a conexão** e o **serviço não orientado a conexão**. Estes serviços aparecem com o nome **transporte orientado a conexão** e **transporte não orientado a conexão** na Camada de Transporte.

Um protocolo da Camada de Transporte fornece comunicação lógica entre os processos de aplicações, ou seja, do ponto de vista de uma aplicação, tudo se passa como se estivessem conectados diretamente para a realização do transporte.



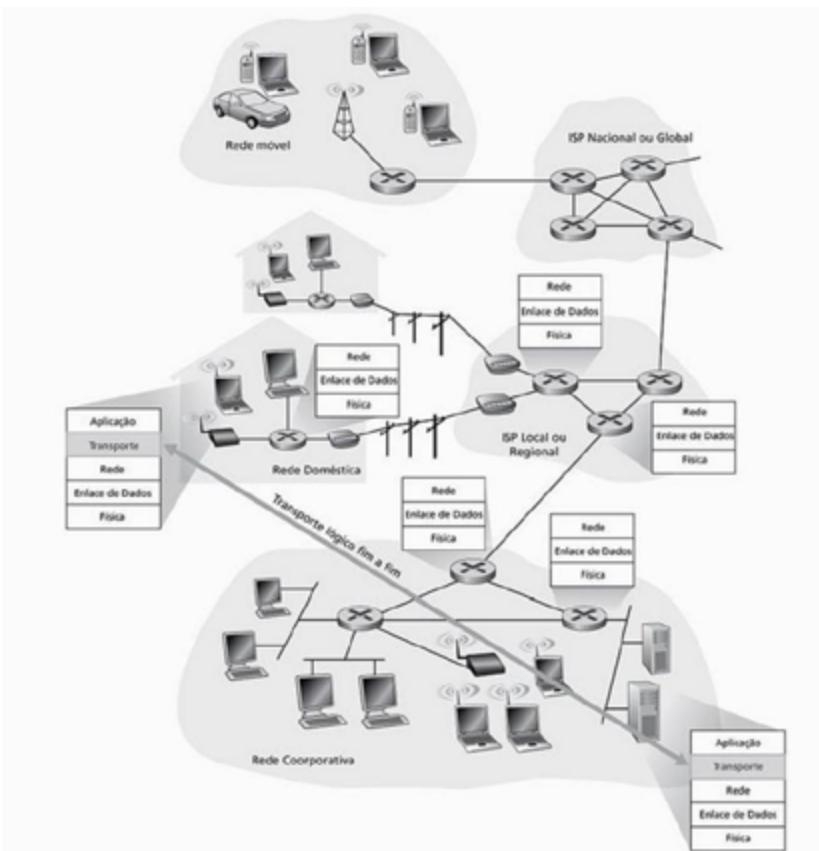


Figura 6 - Comunicação lógica e não física entre processos de aplicações
Fonte: Ross e Kurose (2013).

Protocolos de Transporte

Como já observado, a internet possui dois protocolos principais, são eles o protocolo UDP e TCP, não orientado à conexão e orientado à conexão, respectivamente.

O UDP é um protocolo simples com uso muito importante, como interações entre cliente-servidor, porém o UDP não proporciona uma entrega confiável. Já o TCP foi projetado para oferecer um fluxo de dados fim a fim confiável e projetado para se adaptar dinamicamente às propriedades da rede e ser atento diante de falhas que possam ocorrer (para maiores informações, relembrar a Unidade II, protocolos de redes).

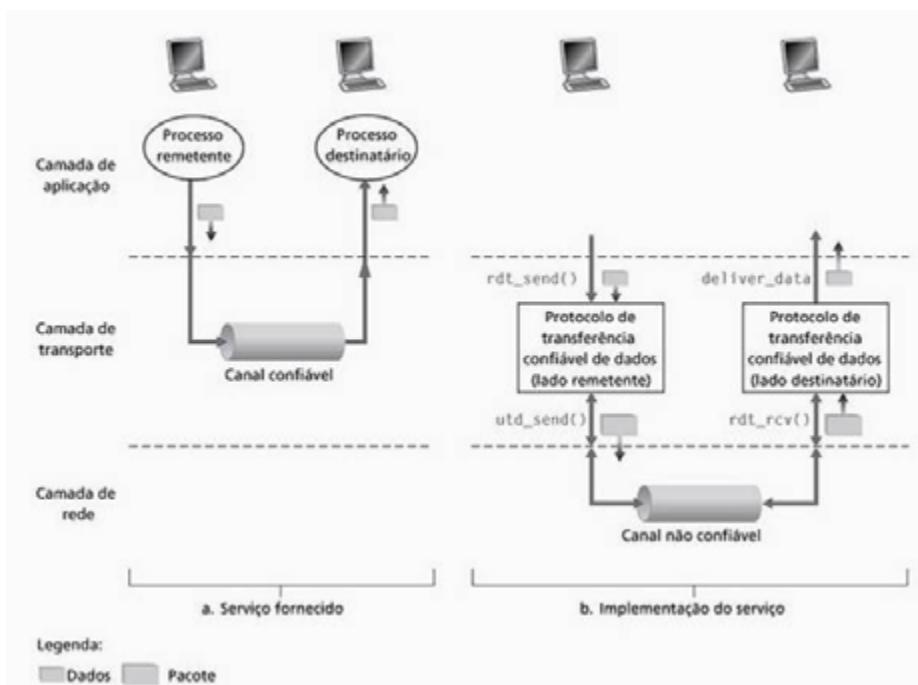


Figura 7 - Modelo de Transferência confiável de dados

Fonte: Ross e Kurose (2013)

Controle de Congestionamento

Sabemos da importância de um controle de congestionamento em se tratando de rede de computadores. Nesse sentido, para um melhor controle, a camada de transporte recebe assistência explícita da camada de rede em alguns casos.

Há alguns mecanismos tratados para o congestionamento, como o controle de congestionamento fim a fim. O que se faz é o protocolo TCP limitar a taxa de envio de dados ao destinatário, caso haja um congestionamento, como uma função do congestionamento percebido, ou seja, caso perceba o congestionamento, ele reduzirá a taxa de envio, caso contrário, ele aumenta a taxa de envio sem causar transtornos até o destinatário (ROSS; KUROSE, 2013).

Mas como regular a taxa de envio? Ela pode ser limitada pelo controle de fluxo caso exista um *buffering* insuficiente no receptor. Outra forma é o congestionamento, caso exista capacidade insuficiente na rede.

Tanenbaum e Wetherall (2011) exemplificam esse ocorrido com a seguinte imagem:

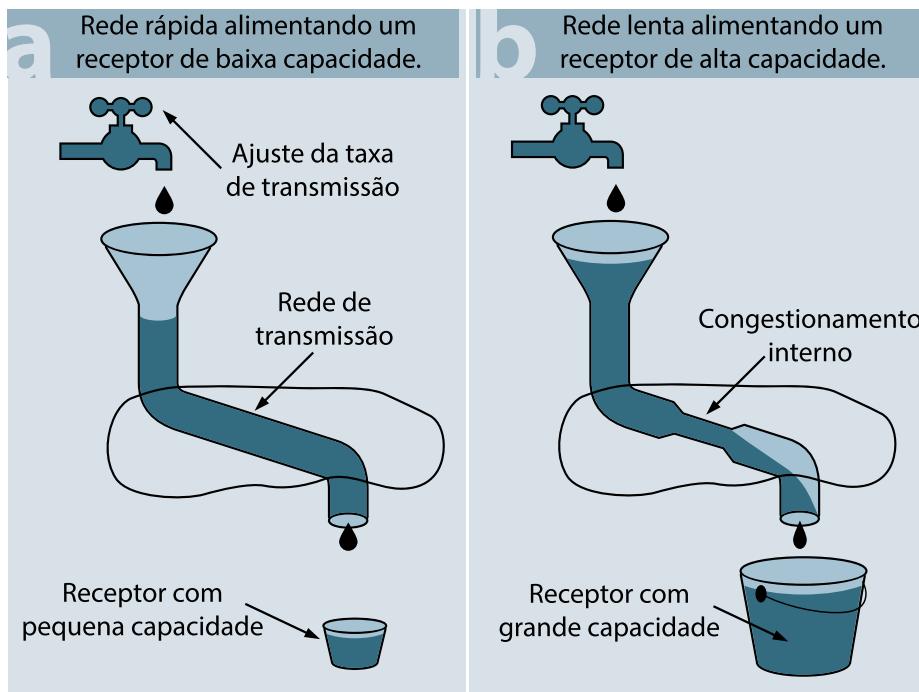


Figura 8 - Congestionamento de dados
Fonte: Tanenbaum e Wetherall (2011).

Sendo tratada como uma situação limitada de controle de fluxo, temos a imagem (a). Já na parte (b) temos como fator limitador a capacidade interna de transporte da rede.

Questão de Desempenho

As questões de desempenho são muito importantes em se tratando de rede de computadores, pelo fato das interações complexas existentes e que trazem consequências imprevistas.

Um destes problemas que podemos citar é o problema de congestionamento que causa sobrecargas temporárias de recursos. Porém, não somente este é o principal vilão do desempenho, temos também a questão do desequilíbrio nos recursos

estruturais, tendo como um exemplo prático uma linha de comunicação com conexão muito alta associada a um PC com poucos recursos, no qual o fraco computador não será capaz de processar os pacotes recebidos com a rapidez necessária, ocasionando a perda de alguns pacotes (TANENBAUM; WETHERALL, 2011).

Normalmente, nós usuários, observamos que uma rede está congestionada devido à lentidão no ato simples de abrir páginas da internet, e na maioria das vezes, sempre reclamamos com os administradores de rede a respeito.

Para solucionar esse problema, os administradores devem descobrir exatamente o que está acontecendo. Para isso, devem realizar medições na rede, que podem ser feitas por meio de contadores que registram a frequência com que algum evento aconteceu.

Lembramos aqui de um velho ditado: prevenir é melhor que remediar. E aplicamos aqui também esse ditado, sendo muito melhor evitar o congestionamento, para que não haja a perda de pacotes. Lembre-se sempre que a velocidade do *host* é mais importante que a velocidade da rede.

CAMADA DE SESSÃO

A camada de sessão admite que haja uma sessão de comunicação entre processos em execução em estações diferentes, definindo como será a transmissão de dados. Há também um suporte de sessão, no qual realiza funções que permitem a comunicação dos processos por meio da rede. Se acaso a rede falhar, os computadores reiniciam a comunicação e transmissão dos dados a partir do último pacote recebido.

Como em toda camada, existem serviços que são disponibilizados. Um exemplo é que a camada de sessão realiza a administração de sessões. Na prática, podemos lembrar do *login* e *logoff*. Também controla a troca de dados, controlando e sincronizando conforme o necessário, podendo abrir conexões para trocar informações *full* e *half-duplex*, ou seja, em um ou nos dois sentidos (FOROUZAN, 2006).

Esta camada permite a transmissão assim como a camada de transporte, porém com alguns melhoramentos, por isso, tem de gerir o modo de comunicação usado por todos os dispositivos.

CAMADA DE APRESENTAÇÃO

Esta camada é responsável pela maneira como os dados serão manipulados na Camada de Aplicação. Compacta os dados reduzindo os bits a serem transmitidos na rede e realiza a criptografia para fins de segurança na transmissão.

Ela resolve problemas de diferença de sintaxes entre os sistemas comunicantes e gerencia a entrada, troca, apresentação e controle dos dados trocados (FOROUZAN, 2006). Exemplos de função da camada de aplicação são aplicações de registros bancários, que também necessitam de uma grande criptografia, e a compressão dos dados no momento do envio para outra aplicação.

SAIBA MAIS



Cada Camada pertencente ao Modelo OSI possui protocolos importantes com suas necessidades bem específicas. A Camada de Apresentação não é diferente. Ela possui diversas funcionalidades que a torna indispensável nas redes de computadores.

Para um melhor entendimento, disponibilizamos o vídeo a seguir que trata a respeito da Camada de Apresentação. De uma forma simples e interativa, explica-se o funcionamento da Camada de Apresentação. O vídeo está disponível em: <<https://www.youtube.com/watch?v=D2HeeVn6Q3E>>. Acesso em 19 maio de 2016.

Fonte: os autores

CAMADA DE APLICAÇÃO

A Camada de Aplicação é a camada em que são encontradas todas as aplicações. Todas as outras camadas têm a função de oferecer serviço de transporte confiável, porém não executam tarefa aos usuários.

Dentre os vários serviços encontrados nessa camada, existem vários que utilizamos diariamente e não percebemos, dentre eles temos o serviço de mensagem eletrônica, acessos remotos, compartilhamento de recursos, terminais de redes virtuais e vários outros (MICROSOFT, 2013)⁶.

Protocolos de Aplicação

São vários os protocolos existentes. Em nosso livro, vamos estudar sobre o DNS (*Domain Name System*), correio eletrônico e WWW (*World Wide Web*).

Sobre o protocolo DNS, já estudamos na Unidade II, porém, vamos relembrar? O DNS tem como essência a criação de esquemas de atribuição de nomes baseados no domínio, usado principalmente para mapear nomes de *hosts* e destinos de mensagens eletrônicas de correios eletrônicos. Quando utilizamos um navegador e digitamos uma página da internet, o servidor DNS “pega” esse endereço em questão e converte para um endereço IP. Após a conversão e, a página ser encontrada, ela é carregada no navegador (TANENBAUM; WETHERALL, 2011).

Já o correio eletrônico, que hoje é muito utilizado, nada mais é do que trocar mensagens pela internet. O sistema de correio eletrônico admite 5 funções:

- **Composição**, que é o processo de criar a mensagem.
- **Transferência**, que se refere ao envio da mensagem do remetente ao destinatário.
- **Geração de relatórios**, que informa ao remetente o que aconteceu com a mensagem, se foi entregue, se ocorreu algum erro, dentre outros.
- **Exibição das mensagens recebidas**.
- **Disposição**, que se refere ao que o destinatário irá fazer com a mensagem após recebê-la.

Alguns protocolos são utilizados no correio eletrônico, dentre eles, temos o SMTP (*Simple Mail Transfer Protocol*), que após estabelecer uma conexão TCP com a porta 25, a máquina que enviar a mensagem espera a comunicação com a máquina que irá receber a mensagem. O servidor começa enviando uma linha de texto na qual consta sua identidade e informa que está tudo certo para receber as mensagens, se houver um retorno de que a máquina existe naquele *host*, dará o sinal para o envio das mensagens (TANENBAUM; WETHERALL, 2011).

Esse tipo de entrega de correio eletrônico funcionou durante décadas, porém, com o advento da internet, ele se tornou não usual pelo fato da necessidade de, tanto o cliente quanto o servidor, estarem ligados para haver a troca de mensagens. A partir daí, criou-se o protocolo POP3, no qual o usuário conseguiria enviar uma mensagem sem a necessidade da máquina cliente e o servidor estarem ligados. Ao enviar a mensagem, as mesmas são copiadas em um Servidor ISP¹, no qual o receptor, após ligar sua máquina e realizar a conexão, receberá sua mensagem. Porém, o POP3 tinha o intuito de que, quando recebesse a mensagem, o usuário deveria excluir a mesma para liberar espaço. Para acabar com esse problema surgiu o IMAP, que pressupõe que todas as mensagens de correio eletrônico permanecerão no servidor por tempo indeterminado e em várias caixas de correio, além de ser um protocolo com muitos recursos e que é executado na porta 143.

Ainda, como tópico de curiosidade, temos o Webmail, como os disponibilizados pelos diversos sites de e-mail (Hotmail, Gmail), que trabalham na porta 25 em busca de conexões de SMTP de entrada.

Outro recurso utilizado na camada de aplicação é a *World Wide Web*, que permite acesso a milhões de documentos chamados de páginas da web. As páginas são visualizadas com o auxílio de navegadores, que buscam a página solicitada e interpretam seu texto e seus comandos de formatação e as exibe ao usuário de forma adequada. É um dos recursos mais utilizados na camada de aplicação devido à popularização da internet.

¹ ISP - Provedor de Serviços de Internet

Com o advento da internet, houve a inclusão de arquivos multimídia, os quais fornecem vídeos sob demanda, músicas, imagens, dentre outros. O acesso à internet banda larga propiciou esse crescimento e cada dia com mais qualidade de acesso, imagens e som. Hoje, pode-se assistir filmes com qualidade de som e



SAIBA MAIS

Sabemos da importância que as Camadas do Modelo OSI têm em Rede de Computadores. A camada de Aplicação é a camada mais próxima do usuário, e a camada que não fornece serviços para nenhuma das outras camadas pertencentes ao modelo OSI.

Com isso, após ter uma grande noção teórica sobre o Modelo OSI, e para seu melhor entendimento, disponibilizamos um vídeo na qual mostra de forma clara e interativa o funcionamento de tal modelo, camada por camada.

Fonte: os autores

imagem digitais, sem a necessidade de realizar a locação de DVDs, sendo tudo realizado pela internet e pelas melhorias que a multimídia nos trouxe.

Arquitetura CLIENTE/SERVIDOR

Uma arquitetura cliente/servidor nada mais é do que um aplicativo, denominado cliente, rodando na máquina local e solicitando um serviço de outro programa aplicativo denominado servidor, rodando em uma máquina remota e que oferece serviços aos clientes.

Dentro da arquitetura cliente/servidor, existem aplicações que podem executar de forma concorrente, sendo de forma cliente ou servidor. Hoje, a maioria dos sistemas operacionais permitem que dois ou mais clientes/servidores rodem ao mesmo tempo, ou seja, podem tanto realizar várias solicitações quanto processar várias solicitações.

Os servidores usam conexões: orientadas à conexão e não orientadas à conexão. Normalmente, as aplicações servidoras que usam UDP (não orientado

à conexão) são interativas, ou seja, processa uma solicitação de cada vez. As aplicações servidoras que se utilizam de TCP (orientado à conexão) são concorrentes, isso significa que o servidor pode servir muitos usuários ao mesmo tempo (ROSS; KUROSE, 2013).

CONSIDERAÇÕES FINAIS

Nesta Unidade, estudamos um pouco mais a fundo sobre o Modelo de Referência OSI, que foi criado pela ISO (Organização Internacional para Padronização) em 1984.

Especificamos a funcionalidade de cada uma das sete camadas que compõem o Modelo OSI, sendo: Camada Física, Camada de Enlace de Dados, Camada de Rede, Camada de Transporte, Camada de Sessão, Camada de Apresentação e Camada de Aplicação.

Passamos pela Camada Física, indicando como se dá a comunicação dos dados, entrando na Camada de Enlace de Dados com seus mecanismos de detecção e correção de erros juntamente com os protocolos que a compõem. Vimos também que a Camada de Rede oferece grandes serviços, como um controle de fluxo de dados para evitar o congestionamento e também algoritmos de roteamento que auxiliam o encontro do melhor caminho para se enviar um determinado pacote.

Na Camada de Transporte, vimos questões de desempenho e os protocolos utilizados para que ocorra da melhor forma o transporte dos pacotes. Por fim, definimos as camadas de Sessão, Apresentação e, por último, a Camada de Aplicação.

Na próxima unidade, você aprenderá que a rede necessita também de uma segurança para a informação, na qual existem vários tipos que podem ser tratados, como assinaturas digitais, algoritmos de criptografia, e os não menos importantes, nossos antivírus e *firewalls*.

Uma questão também muito importante será tratada, a Engenharia Social, que vem crescendo muito no decorrer dos anos. Vamos começar o estudo de como realizar essa segurança?

ATIVIDADES



1) Em nossos estudos, vimos que o modelo de referência OSI possui 7 (sete) camadas. Assinale a alternativa que indica a ordem correta das sete camadas.

- a) Física-Enlace-Transporte-Redes-Sessão-Apresentação-Aplicação.
- b) Física-Enlace-Redes-Transporte-Sessão-Apresentação-Aplicação.
- c) Física-Enlace-Redes-Transporte-Sessão-Aplicação-Apresentação.
- d) Física-Enlace-Transporte-Redes-Sessão-Aplicação-Apresentação.
- e) Física-Enlace-Redes-Sessão-Transporte-Aplicação-Apresentação.

2) Sobre o Modelo OSI, assinale a alternativa que corresponde corretamente à definição do Modelo OSI.

- a) A camada de transporte é uma camada fim a fim.
- b) A camada de enlace de dados se preocupa com as voltagens que serão utilizadas para representar os bits.
- c) A camada de apresentação é responsável por padronizar os protocolos de abertura e fechamento da conexão da camada de transporte.
- d) No modelo OSI, cada camada deve conhecer a implementação das camadas adjacentes.
- e) No modelo OSI, não há distinção entre serviços e protocolos.

3) O IP e o TCP são protocolos de uso na internet. De acordo com o modelo OSI (*Open Systems Interconnection*) de sete camadas, o IP e o TCP são, respectivamente, protocolos das camadas de:

- a) Rede e de transporte.
- b) Rede e de enlace.
- c) Transporte.
- d) Enlace e de aplicação.
- e) De rede.

4) É a Camada que controla fluxo, ordena pacotes e corrige erros. A que camada estamos nos referindo?

- a) Física.
- b) De Transporte.

ATIVIDADES



- c) De Rede.
 - d) De Enlace.
 - e) De Sessão.
- 5) A camada que oferece o controle de “diálogo”, determinando quem deve transmitir em cada momento, gerenciando logins/logouts é a camada de:
- a) Aplicação.
 - b) Apresentação.
 - c) Sessão.
 - d) Transporte.
 - e) Rede.
- 6) Qual das camadas a seguir podemos dizer que não pertence às 7 camadas do Modelo OSI?
- a) Sessão.
 - b) Aplicação.
 - c) Apresentação.
 - d) Transferência.
 - e) Enlace.
- 7) A camada que trata da transmissão de bits brutos por um canal de comunicação é chamada de:
- a) Camada física.
 - b) Camada de rede.
 - c) Camada de transporte.
 - d) Camada de enlace de dados.
- 8) Cite as formas em que o modelo de referência OSI é igual ao TCP/IP e duas que os mesmos são diferentes.



Nesta unidade, aprendemos sobre a importância do Modelo OSI, indicando suas funcionalidades para o acesso e transferência dos dados. A seguir, indicamos uma leitura complementar que nos mostra um pouco mais sobre este modelo.

O Modelo OSI e suas 7 Camadas

Dando sequência ao Modelo OSI, vamos falar e detalhar de forma resumida as 7 camadas que o compõe.

- Aplicação
- Apresentação
- Sessão
- Transporte
- Rede
- Enlace
- Física

Esse é modelo de 7 camadas ISO/OSI.

Ainda não havia citado, mas ISO corresponde a *International Organization for Standardization*, ou Organização Internacional para Padronização, e OSI corresponde à *Open System Interconnection*, ou Sistema de Interconexão aberto. Podemos fazer uma analogia com os *Processos*, ou *POP (Procedimento Operacional Padrão)* como conheço, que a ISO exige das empresas no processo de obtenção do ISO 9001 por exemplo. A ideia é a mesma, “padronizar” para organizar e agilizar os processos.

Como citei na figura, é interessante notar que a ordem numérica das camadas é decrescente, ou seja, o processo começa na camada física, onde os sinais elétricos são convertidos em zeros e uns, e termina na camada de aplicação, onde atuam protocolos como o FTP por exemplo (*File Transfer Protocol*), protocolo para troca de arquivos.

Outra coisa interessante, é qual a PDU (*Protocol Data Unit*, ou Protocolo de Unidade de Dados) cada camada em específico trata. Vou descrever após a breve explicação da camada sequente, qual a PDU correspondente. Após explicar a camada, vou citar sua PDU.

A maioria das literaturas cita o modelo a partir da camada de Aplicação, mas pessoalmente acho mais lógico iniciar pela camada Física, onde é iniciado o processo, imaginando que os dados estão chegando, e não indo.

[...]

Camada Física

Como citei o anteriormente, é onde se inicia o todo processo. O sinal que vem do meio (Cabos UTP por exemplo), chega à camada física em formato de sinais elétricos e se trans-





forma em bits (0 e 1). Como no cabo navega apenas sinais elétricos de baixa frequência, a camada física identifica como 0 sinal elétrico com -5 volts e 1 como sinal elétrico com +5 volts. A camada física trata coisas tipo distância máxima dos cabos (por exemplo no caso do UTP onde são 90m), conectores físicos (tipo BNC do coaxial ou RJ45 do UTP), pulsos elétricos (no caso de cabo metálico) ou pulsos de luz (no caso da fibra ótica), etc. Resumindo, ela recebe os dados e começa o processo, ou insere os dados finalizando o processo, de acordo com a ordem. Podemos associá-la a cabos e conectores. Exemplo de alguns dispositivos que atuam na camada física são os Hubs, tranceivers, cabos, etc. Sua PDU são os BITS.

Camada de Enlace

Após a camada física ter formatado os dados de maneira que a camada de enlace os entenda, inicia-se a segunda parte do processo. Um aspecto interessante é que a camada de enlace já entende um endereço, o endereço físico (MAC Address – *Media Access Control* ou Controle de acesso a mídia) – a partir daqui sempre que eu me referir a endereço físico estou me referindo ao MAC “Address”. Sem querer sair do escopo da camada, acho necessária uma breve ideia a respeito do MAC. MAC address é um endereço Hexadecimal de 48 bits, tipo FF-C6-00-A2-05-D8.

Na próxima parte do processo, quando o dado é enviado à camada de rede esse endereço vira endereço IP.

[...]

A camada de enlace trata as topologias de rede, dispositivos como Switch, placa de rede, interfaces etc., e é responsável por todo o processo de switching. Após o recebimento dos bits, ela os converte de maneira inteligível, os transforma em unidade de dado, subtrai o endereço físico e encaminha para a camada de rede que continua o processo. Sua PDU é o QUADRO.

Camada de Rede

Pensando em WAN, é a camada que mais atua no processo. A camada 3 é responsável pelo tráfego no processo de internetworking. A partir de dispositivos como roteadores, ela decide qual o melhor caminho para os dados no processo, bem como estabelecimento das rotas. A camada 3 já entende o endereço físico, que o converte para endereço lógico (o endereço IP). Exemplo de protocolos de endereçamento lógico são o IP e o IPX. A partir daí, a PDU da camada de enlace, o quadro, se transforma em unidade de dado de camada 3. Exemplo de dispositivo atuante nessa camada é o Roteador, que sem dúvida é o principal agente no processo de internetworking, pois este determina as melhores rotas baseados no seus critérios, endereça os dados pelas redes, e gerencia suas tabelas de roteamento. A PDU da camada 3 é o PACOTE.

Camada de Transporte

A camada de transporte é responsável pela qualidade na entrega/recebimento dos da-



dos. Após os dados já endereçados virem da camada 3, é hora de começar o transporte dos mesmos. A camada 4 gerencia esse processo, para assegurar de maneira confiável o sucesso no transporte dos dados, por exemplo, um serviço bastante interessante que atua de forma interativa nessa camada é o Q.O.S ou *Quality of Service* (Qualidade de Serviço), que é um assunto bastante importante e fundamental no processo de internetworking, e mais adiante vou abordá-lo de maneira bem detalhada. Então, após os pacotes virem da camada de rede, já com seus “remetentes/destinatários”, é hora de entregar-los, como se as cartas tivessem acabados de sair do correio (camada 3), e o carteiro fosse as transportar (camada 4). Junto dos protocolos de endereçamento (IP e IPX), agora entram os protocolos de transporte (por exemplo, o TCP e o SPX). A PDU da camada 4 é o SEGMENTO.

Camada de Sessão

Após a recepção dos bits, a obtenção do endereço, e a definição de um caminho para o transporte, se inicia então a sessão responsável pelo processo da troca de dados/comunicação. A camada 5 é responsável por iniciar, gerenciar e terminar a conexão entre hosts. Para obter êxito no processo de comunicação, a camada de seção tem que se preocupar com a sincronização entre hosts, para que a sessão aberta entre eles se mantenha funcionando. Exemplo de dispositivos, ou mais especificamente, aplicativos que atuam na camada de sessão é o ICQ, ou o MIRC. A partir daí, a camada de sessão e as camadas superiores vão tratar como PDU os DADOS.

Camada de Apresentação

A camada 6 atua como intermediária no processo frente às suas camadas adjacentes. Ela cuida da formatação dos dados, e da representação destes, e ela é a camada responsável por fazer com que duas redes diferentes (por exemplo, uma TCP/IP e outra IPX/SPX) se comuniquem, “traduzindo” os dados no processo de comunicação. Alguns dispositivos atuantes na camada de Apresentação são o Gateway, ou os Traceivers, sendo que o Gateway no caso faria a ponte entre as redes traduzindo diferentes protocolos, e o Transceiver traduz sinais por exemplo de cabo UTP em sinais que um cabo Coaxial entenda.

Camada de Aplicação

A camada de aplicação é a que mais notamos no dia a dia, pois interagimos direto com ela através de softwares como cliente de correio, programas de mensagens instantâneas, etc. Do ponto de vista do conceito, na minha opinião a camada 7 é basicamente a interface direta para inserção/recepção de dados. Nela é que atuam o DNS, o Telnet, o FTP etc. E ela pode tanto iniciar quanto finalizar o processo, pois como a camada física, se encontra em um dos extremos do modelo!

Fonte: Ventura (2012, on-line)⁷.

MATERIAL COMPLEMENTAR



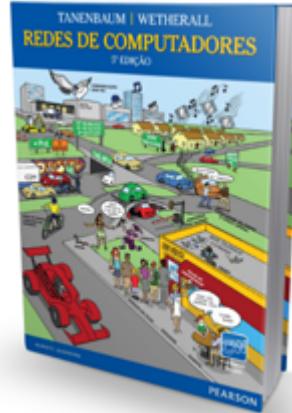
LIVRO

Rede de Computadores

Andrew S. Tanenbaum; David J. Wetherall

Editora: Pearson Education Brazil

Sinopse: Este clássico best-seller foi totalmente atualizado e passa a abordar as redes desenvolvidas a partir de 1990. Entretanto, a partir do ano 2000 também há uma grande quantidade de novos desenvolvimentos. O mais importante é o enorme crescimento das redes sem fio, incluindo 802.11, loops locais sem fio, redes celulares 2G e 3G, Bluetooth, WAP, i-mode e outras. Acompanhando essa tendência, incluímos neste volume uma grande quantidade de material sobre redes sem fio. Outro tópico que se tornou importante recentemente é a segurança; assim, foi acrescentado um capítulo inteiro sobre esse assunto.



REFERÊNCIAS

FOROUZAN, B. A. **Comunicação de Dados e Redes de Computadores.** 3 ed. Porto Alegre: Bookman, 2006.

ROSS, K.; KUROSE, J. F. **Redes de Computadores e a Internet:** uma abordagem top down. 5 ed. São Paulo: Pearson, 2005.

TANENBAUM, A.; WETHERALL, D. **Redes de Computadores.** 5 ed. São Paulo: Pearson, 2011.

CITAÇÃO DE LINK

¹ <<http://docente.ifrn.edu.br/filiperaulino/disciplinas/infra-estrutura-de-redes/aulas/Comutacao.pdf/view>>. Acesso em 24 set. 2020.

²<<http://windows.microsoft.com/pt-br/windows/what-is-internet-service-provider#1TC=windows-7>>. Acesso em: 19 maio 2016.

³ <<http://www.eurecom.fr/~camara/dissertacao/node20.html>>. Acesso em: 19 maio 2016.

⁴ <http://www.teleco.com.br/tutoriais/tutorialredeipec1/pagina_3.asp>. Acesso em: 19 maio 2016.

⁵ <http://www.projetoderedes.com.br/artigos/artigo_controle_de_congestionamento.php>. Acesso em: 19 maio 2016.

⁶ <<https://support.microsoft.com/pt-br/kb/103884>>. Acesso em: 19 maio 2016.

⁷ <<https://www.ateomomento.com.br/o-modelo-osi-e-suas-7-camadas/>>. Acesso em 24 set. 2020.



GABARITO

1. B
 2. A
 3. A
 4. B
 5. C
 6. D
 7. A
8. Os dois modelos de referência OSI e TCP/IP têm muito em comum. Os dois se baseiam no conceito de uma pilha de protocolos independentes. Além disso, as camadas têm praticamente as mesmas funções. Em ambos os modelos, por exemplo, estão presentes as camadas que englobam até a camada de transporte. Nesses modelos, são oferecidos aos processos que desejam se comunicar um serviço de transporte fim a fim independente do tipo de rede que está sendo usado. Essas camadas formam o provedor de transporte. Mais uma vez em ambos os modelos, as camadas acima da camada de transporte dizem respeito aos usuários orientados à aplicação do serviço de transporte.
- Apesar dessas semelhanças fundamentais, os dois modelos também têm muitas diferenças. Algumas delas são: o modelo OSI tem sete camadas e o TCP/IP, quatro. Ambos têm as camadas de inter-rede, transporte e aplicação, mas as outras são diferentes. Outra diferença está na área da comunicação sem conexão e da comunicação orientada à conexão. Na camada de rede, o modelo OSI é compatível com a comunicação orientada à conexão; no entanto, na camada de transporte, o modelo aceita apenas a comunicação orientada à conexão, em que ela de fato é mais importante (pois o serviço de transporte é visível para os usuários). O modelo TCP/IP tem apenas um modo na camada de rede (sem conexão), mas aceita ambos os modelos na camada de transporte, oferecendo aos usuários uma opção de escolha. Essa escolha é especialmente importante para os protocolos simples de solicitação/resposta.



INTERNET E SEGURANÇA DA INFORMAÇÃO

Objetivos de Aprendizagem

- Estudar os conceitos de Criptografia para internet.
- Entender os principais os conceitos de Assinaturas digitais para internet.
- Descrever a segurança em Redes.
- Classificar os tipos de ataques e como se defender.
- Identificar os sistemas operacionais mais utilizados em redes de computadores.

Plano de Estudo

A seguir, apresentam-se os tópicos que você estudará nesta unidade:

- Criptografia e Segurança
- Assinaturas Digitais
- Segurança da Comunicação
- Tipos de ataques
- Sistemas Operacionais para rede

INTRODUÇÃO

Na nossa unidade III, realizamos um estudo minucioso sobre o Modelo OSI. Nesse estudo, relatamos como funciona as suas sete camadas, identificando a importância que cada uma possui em se tratando de redes de computadores.

Descreveremos no decorrer dessa unidade o funcionamento da Segurança em Redes, que é um assunto muito discutido no ambiente corporativo, porque o que está em jogo é o patrimônio, tanto material quanto intelectual. Falhas na segurança podem até mesmo danificar os bens tangíveis e intangíveis, bem como a imagem da organização.

No tópico de criptografia, abordaremos conceito de trocas de mensagens entre destinatários e receptores de forma que, as mensagens só possam ser acessadas e lidas com códigos de acesso específicos.

Em conjunto com a criptografia temos a assinatura digital, que tem se transformado em um dos itens mais importantes na era dos documentos digitais. É uma das técnicas mais utilizadas, pois valoriza qualquer tipo de documento produzido de acordo com padrões de órgãos certificadores.

Entrando na segurança da comunicação, veremos os principais problemas relacionados a forma de comunicação e reportados os índices de acidentes virtuais no Brasil. Esses incidentes ou ataques à segurança de sistemas de informática serão discriminados no decorrer do tópico.

E encerrando esta Unidade, abordaremos o quão importante é a escolha de um Sistema Operacional que dê suporte à conexão em redes, ou seja, para se conectar a uma rede, seja ela a Internet ou uma rede comercial, precisamos de diversos dispositivos, desktops, notebooks, celulares etc., cada aparelho deve possuir um Sistema Operacional.

CRİPTOGRAFIA E SEGURANÇA

Vivemos em uma sociedade contemporânea que gera informações constantemente. Informações estas que transitam pela rede mundial de computadores, desde dados em redes sociais a dados bancários por *internet banking* ou por uma compra em mercado eletrônico. Mas o que impede que esses dados acabem em mãos erradas? Que pessoas possam interceptar os números cartões de créditos e senhas e fazer uso delas? Vamos responder tais dúvidas ao longo deste tópico.

Para Stallings (2008), a criptografia tem como um dos seus objetivos principais prover a troca de mensagens secretas entre duas partes, sem que uma terceira parte a intercepte e a decodifique, ou seja, a criptografia consiste na codificação de uma mensagem onde somente o remetente e o destinatário conheçam a forma de traduzi-la.

Desta forma, utiliza-se de uma chave, a qual contém os parâmetros de conversão de valores de um texto para um modo criptografado e, em contrapartida, existe uma chave correspondente que contém os parâmetros para decriptar essa mensagem, podendo ela ser a mesma do remetente ou até mesmo uma versão inversa.



Figura 1 - Sistemas de Criptografia

Neste contexto, segundo Stallings (2008), os métodos de criptografia atuais são seguros e eficientes, fazendo o uso de uma ou mais chaves de criptografia. Essas criptografias podem ser em duas formas de utilização e distribuição de chaves de criptografia. A primeira utiliza a mesma chave para encriptação e decriptação das mensagens, e a segunda utiliza chaves diferentes. Desta forma, estudaremos os **Sistemas de Criptografia de Chave Simétrica** e **Sistemas de Criptografia de Chave Assimétrica**.

Chave simétrica

Os **algoritmos de chave única** ou **de chave simétrica** caracterizam-se por utilizar a mesma chave tanto para a cifragem como para a decifragem dos dados. Esse método funciona em aplicações bem limitadas, onde o emissor e o receptor possam se preparar antecipadamente para trocar a chave.



Figura 2 - Chave simétrica

Nesse contexto, considere que quando você fosse enviar uma mensagem confidencial para outras pessoas, primeiro, você teria de entrar em contato com cada pessoa individualmente para que pudesse fazer a troca das chaves secretas em separado, ou seja, para cada pessoa deveria ser gerada uma chave secreta.

Consequentemente, você teria que gerenciar este tipo de chave, pois uma chave trocada impedirá a abertura de outra mensagem.

Chave assimétrica

Os **algoritmos de chave pública e privada**, ou **chave assimétrica**, utilizam duas chaves: uma pública e outra secreta. A chave pública pode ser disponibilizada para qualquer pessoa, sendo assim, pode ser disponibilizada universalmente. Já a chave a secreta deve ser conhecida somente por pessoas autorizadas, ou seja, a chave privada deve ser mantida em segredo.

Sendo assim, em um sistema de chave pública, cada pessoa tem duas chaves: uma chave pública e uma chave privada. As mensagens criptografadas com uma das chaves só podem ser descriptografadas com a outra chave correspondente e vice-versa.

Nesse sentido, em uma troca de mensagens entre dois indivíduos ou sistemas, quem for transmitir precisa saber da chave pública da pessoa que receberá a informação. Após a cifragem, os dados são enviados ao destinatário, e como apenas ele possui a respectiva chave privada, realizará a cifragem novamente, retornando a mensagem original.

Reprodução proibida. Art. 184 do Código Penal e Lei 9.510 de 19 de fevereiro de 1998.

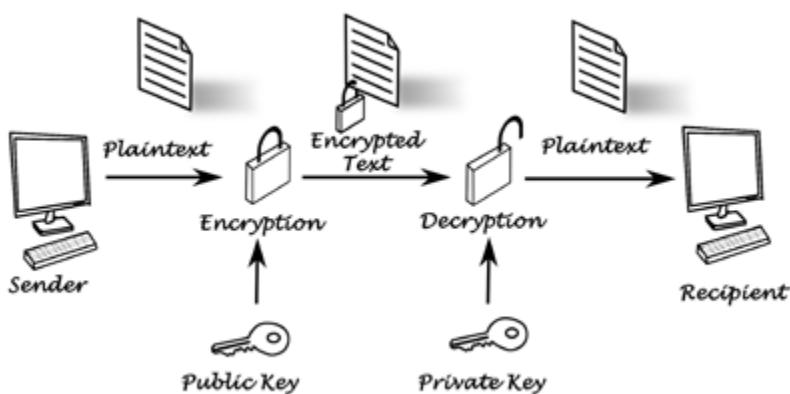


Figura 3 - Chave assimétrica

SAIBA MAIS



A criptografia provê a troca de mensagens secretas entre duas partes sem que uma terceira parte a intercepte e a decodifique. Veja uma introdução à criptografia, sendo assim, assista ao vídeo que explica um pouco mais sobre os estudos de criptografia. Está disponível em: <<https://www.youtube.com/watch?v=wtwlVqEoyyw>>. Acesso em: 19 maio 2016.

Fonte: os autores.

De acordo com Ross e Kurose (2005) e Stallings (2008), a criptografia é muito utilizada para a implementação de várias aplicações como: assinaturas digitais - verificando a autenticidade e a integridade de uma informação ou mensagem; protocolos de segurança - garantindo a segurança, a comunicação dos dados entre os remetentes; certificados digitais - que garantem a autenticidade dos seus donos.

ASSINATURAS DIGITAIS

Neste tópico abordaremos alguns conceitos de segurança que têm se transformado cada vez mais importante à medida que a rede de computadores, em específico a internet, tem se tornado o meio de comunicação de acesso a todas as pessoas.

A autenticação ou assinatura digital é a versão digital da assinatura de punho em documentos físicos. A assinatura digital apresenta um grau de segurança muito superior ao de uma assinatura de punho.

O destinatário de uma mensagem assinada digitalmente pode verificar se a mensagem foi realmente emitida pela pessoa, ou se a mensagem não foi em algum ponto adulterada intencional ou accidentalmente depois de assinada. Mais ainda, uma assinatura digital que tenha sido verificada não pode ser negada. Aquele

que assinou digitalmente a mensagem não pode dizer mais tarde que sua assinatura digital foi falsificada. Em outras palavras, assinaturas digitais habilitam “autenticação” de documentos digitais, garantindo ao destinatário de uma mensagem digital tanto a identidade do remetente quanto a integridade da mensagem.

Conforme Stallings (2008), uma assinatura digital é um mecanismo de autenticação que permite ao criador de uma mensagem anexar um código que atue como uma assinatura. Por sua vez, a assinatura é formada tomando o *hash* da mensagem e criptografando-a com a chave privada do criador. A assinatura garante a origem e a integridade da mensagem.

O principal conceito envolvido na verificação da integridade de uma mídia é o cálculo realizado com a utilização de funções de autenticação unidirecional conhecida como *hash*. Funções *hash* geram a partir de uma entrada digital de qualquer tamanho uma saída de tamanho fixo.

Além da assinatura, temos os protocolos de autenticação mútua que permitem que as partes da comunicação se convençam mutuamente da identidade umas das outras e também para a troca de chaves de sessão. Na autenticação unidirecional, o destinatário deseja alguma garantia de que uma mensagem vem realmente do emissor alegado.

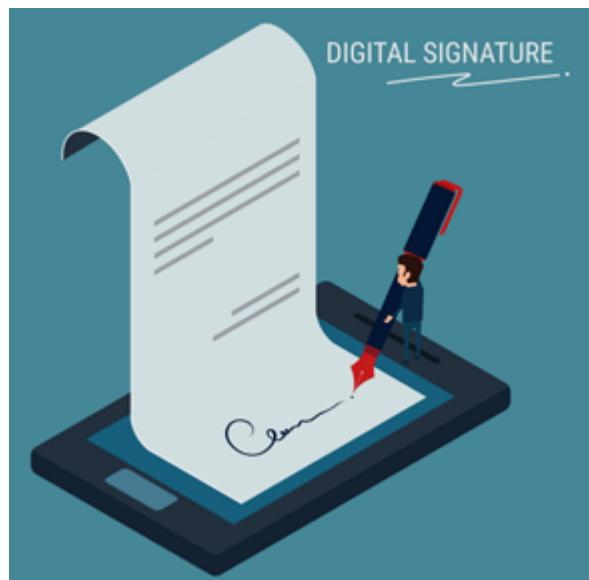


Figura 4 - Assinatura digital

Reprodução proibida. Art. 184 do Código Penal e Lei 9.561 de 19 de fevereiro de 1998.

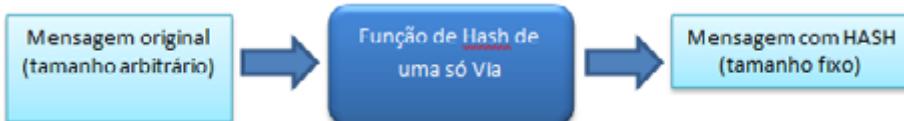


Figura 5 - Mensagem autenticada com a função HASH

Fonte: o autor.

Um exemplo de autenticação unidirecional é a função MD5, por ela ser um *hash* unidirecional, ela não pode ser transformada novamente no texto que lhe deu origem. O método de verificação é, então, feito pela comparação das duas *hash* (uma da mensagem original confiável e outra da mensagem recebida).

A função *hash* transforma uma grande quantidade de bits (informação original) em uma sequência sempre do mesmo tamanho (valor *hash*), não sendo possível recuperar o valor inicial a partir da soma *hash* gerada. Como o tamanho da soma *hash* gerada é limitado, podem haver colisões – valores *hash* iguais para valores de entrada diferentes.

Quando um único bit é alterado em uma informação que foi submetida a uma função hash, o resultado desta informação, ao ser novamente submetida à função hash, não será o mesmo do valor hash anterior à modificação. Vejamos o exemplo abaixo, para melhor entendimento, referente a esta alteração.

1111 -> sha-1 -> 011c945f30ce2cbafc452f39840f025693339c42

1112 -> sha-1 -> 7161a2409087e392cf68559ddac9f1b64b07510c

Neste sentido, existem vários sites¹ disponíveis na internet, que podem utilizar a função hash.

O desenvolvimento mais importante do trabalho em criptografia de chave pública é a assinatura digital. A assinatura digital oferece um conjunto de recursos de segurança que seria difícil implementar de qualquer outra maneira.

A autenticação da mensagem protege duas partes que trocam mensagens contra uma terceira parte. Porém, ela não protege as duas partes uma da outra e diferentes formas de disputas são possíveis entre as duas. Tomemos como exemplo uma troca de mensagens autênticas entre Rafael e a sua esposa Juliana.

Vamos considerar duas disputas que poderiam surgir mediante uma comunicação:

1. Juliana pode forjar uma mensagem diferente e reivindicar que ela veio de Rafael. Juliana simplesmente teria de criar uma mensagem e anexar um código de autenticação usando a chave que Rafael e Juliana compartilham.

¹ Gerador de Hash <<http://www.sha1-online.com/>>. Acesso em 19 maio 2016.

2. Rafael pode negar o envio da mensagem. Uma vez que é possível para Juliana falsificar uma mensagem, não há como provar que Rafael realmente a enviou.

De acordo com os dois cenários acima, podemos ter dois problemas que podem ocorrer. O primeiro pode ocorrer em uma transferência eletrônica de fundos e o receptor aumenta a quantidade de fundos transferidos e afirma que o valor maior chegou do emissor.

Outro problema, pode ocorrer de um e-mail conter instruções para um agente de valores para uma transação que mais tarde resultou desfavorável. O emissor finge que o e-mail nunca foi enviado.

Em situações nas quais não existe confiança mútua e completa entre emissor e receptor, é necessário algo mais do que a autenticação. A solução mais adequada para esse problema é a assinatura digital, que é semelhante à assinatura escrita à mão. Ela deve verificar o autor, a data e hora da assinatura, autenticar o conteúdo no momento da assinatura e ser verificável por terceiros para resolver disputas.



SEGURANÇA DA COMUNICAÇÃO

Neste tópico, iremos abordar alguns conceitos de segurança que têm se tornado cada vez mais importantes à medida que a rede de computadores, em específico a internet, se transforma no meio de comunicação de acesso a todas as pessoas.

A segurança em rede cuida para que essas características estejam na comunicação. Podemos identificar as seguintes propriedades desejáveis da comunicação segura:

Confidencialidade - é um conceito no qual o acesso à informação deve ser concedido a quem tem direito, ou seja, apenas para as entidades autorizadas pelo proprietário ou dono da informação, ou ainda, apenas o transmissor e o receptor desejado devem “entender” o conteúdo da mensagem do transmissor. Exemplo: terminal (A) codifica mensagem e envia ao terminal (B) que é o receptor, que, por sua vez, decodifica mensagem.

Podemos considerar também a confidencialidade como a capacidade de prevenir o vazamento de informações para indivíduos e sistemas não autorizados.

Integridade de mensagem - está ligada à propriedade de manter a informação armazenada com todas as suas características originais estabelecidas pelo dono da informação, tendo atenção com o seu ciclo de vida (criação, manutenção e descarte). Por exemplo: transmissor e receptor querem garantir que a mensagem não seja alterada (em trânsito ou após) sem que isso seja detectado.

Nesse contexto, a Integridade é a capacidade de garantir que um dado não seja modificado sem autorização. A integridade pode ser quebrada por ações maliciosas ou por erros de operação, desta forma, os dados normalmente são modificados e, consequentemente geram resultados incorretos.

Disponibilidade - deve garantir que a informação esteja sempre disponível para uso quando usuários autorizados necessitarem. Podemos encontrar esta disponibilidade em sistema computacional utilizado para armazenar e processar a informação, os controles e protocolos de segurança em *datacenters*, serviços hospitalares, aviação, marinha, entre outros. Normalmente, estes tipos de sistemas possuem mecanismos que previnem a falta de energia elétrica, falha de hardware, falhas de software e ataques contra a disponibilidade da informação, entrando em ação quanto a prevenção ou correção. Sendo assim, os serviços terão disponibilidade por algum tempo.

Autenticação e autorização - transmissor e receptor querem confirmar a identidade um do outro, ou seja, a autenticação é a capacidade de estabelecer ou confirmar se algo ou alguém é autêntico. Esse processo envolve a confirmação da identidade de um usuário ou sistema. A autorização é a validação do usuário após a autenticação, em uma lista de acesso pré-definida, se algo, ou alguém, possui permissões para realizar ações com dados em um sistema da informação.

Segurança operacional - os serviços devem estar acessíveis e disponíveis para os usuários (detecção de invasão, *worms*, *firewalls*, Internet pública).

Uma das principais preocupações com os sistemas de comunicação são os acessos indevidos realizados pelos hackers. Devido a uma grande gama de dispositivos móveis conectados, que por sua vez não possuem segurança, tem chamado a atenção de muitos administradores no tocante à segurança, contra invasão dos hackers. Podemos entender por hacker aquela pessoa que fica tentando conseguir acesso não autorizado em um sistema com intuito de obter lucros, usando a capacidade técnica e a tecnologia para invadir e desativar computadores considerados seguros.

As invasões podem ocorrer por vírus, *softwares* ocultos, programas originais, porém com funções ocultas, ataque DOS, cavalos de Troia, *worms*, *hijackers*, *spywares*, entre outros, causando grandes prejuízos.

O site Cert.br relata sobre os dados crescentes de ataques contra os computadores brasileiros comparados os anos de 1999 e 2014. Utilizando dados atualizados de novembro de 2014, percebemos que os incidentes de ataques tiveram o maior ápice se comparados ao ano de 2012.

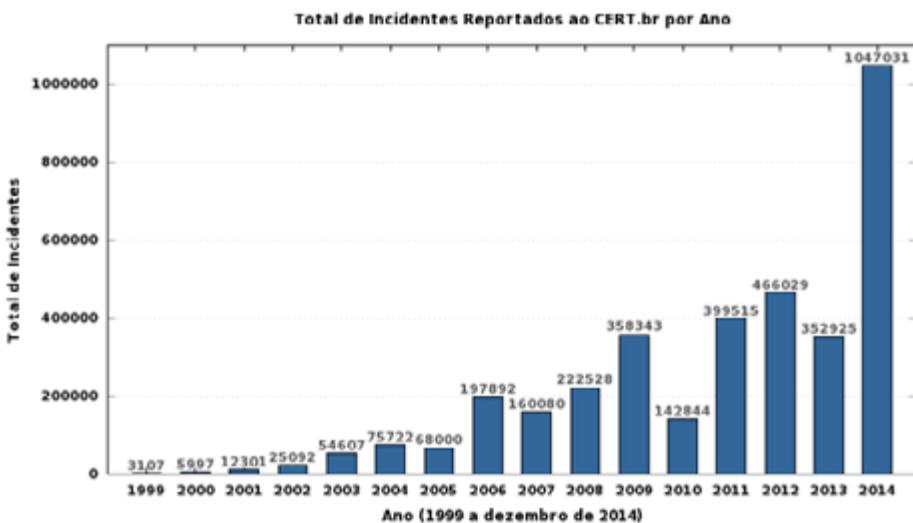


Figura 6 - Total de Incidentes Reportados ao CERT.br por ano

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (20016, on-line)¹.

SAIBA MAIS



"A segurança da informação é a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco para o negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio".

Fonte: NBR ISO/IEC 27002:2005 (DANTAS, 2011, p. 11).

REFLITA



Os dispositivos de segurança que podem ser usados não garantem que um sistema não possa ser invadido, mas garantem que isso não será uma tarefa fácil para o atacante.

Fonte: Carvalho (2005, p. 37)

Os vírus de computador

De acordo com Stallings (2008, p. 445), um vírus é considerado “um software que pode ‘infectar’ outros programas, modificando-os; a modificação inclui uma cópia do programa de vírus, que pode então prosseguir para infectar outros programas.” O vírus é uma forma de invasão de segurança que explora vulnerabilidades de um sistema, mas como veremos ainda nesta unidade, temos outras formas de ataques.

Devemos ter em mente que, um vírus funciona como um arquivo normal, contudo ele pode ser inicializado por meio de uma intervenção do usuário, seja por meio de uma inicialização de um arquivo suspeito, seja por intervenção de um software quando ativado ou por si próprio. Esse tipo de arquivo possui um código fonte executável, que pode ser escondido em arquivos sem que você perceba. Estes são programados para realizar diversas funções e cada uma pode infiltrar e localizar vulnerabilidades, transmitindo informações coletadas para alguém que possui interesses em determinadas informações para possíveis ataques futuros (CARVALHO, 2005; STALLINGS, 2008).

De acordo com Stallings (2008, p. 448), os vírus possuem um tempo de vida classificado em quatro fases, sendo elas:

- **Fase latente:** o vírus está inativo. Ele será ativado por algum evento, como uma data, a presença de outro programa ou arquivo, ou a capacidade do disco de exceder algum limite. Nem todos os vírus têm esse estágio.
- **Fase de propagação:** o vírus coloca uma cópia idêntica de si mesmo em outros programas ou em certas áreas do sistema no disco. Cada programa infectado agora terá um clone do vírus que, por si só, entrará em uma fase de propagação.
- **Fase de disparo:** o vírus é ativado para realizar a função para a qual ele foi planejado. Assim como na fase latente, a fase de disparo pode ser causada por diversos eventos do sistema, incluindo a contagem do número de vezes que essa cópia do vírus fez cópias de si mesma.
- **Fase de execução:** a função é realizada. A função pode ser inofensiva, como uma mensagem na tela, ou danosa, como a destruição de programas e arquivos de dados.

Os vírus de computadores podem ser programados para que se possam reproduzir, ou seja, se espalhar para outros computadores. Consequentemente, cada computador infectado pode infectar outros computadores, de forma programada em determinadas datas, horários, ou durante o uso de determinados sistemas ou softwares, desta forma, os vírus entram em ação.

A propagação dos vírus de computadores estão aumentando de forma desordenada, devido ao grande aumento de dispositivos móveis hoje disponibilizados e conectados à internet. Esta gama de dispositivos são um prato cheio para a propagação desses softwares maliciosos.

A propagação de um vírus não se limita apenas pela internet, mas pode ser transmitida também fisicamente, por meio do carregamento de arquivos via pendrive, cartões de memórias, inter-redes, entre outros. Após a infecção do computador, é necessário que o mesmo seja retirado, para que não se propague pela rede ou por dispositivos físicos citados acima. Para a retirada destes elementos, temos softwares denominadas de antivírus, que podem ser pagos ou gratuitos.

A função de um antivírus é prover a segurança interna do computador por meio de uma base de “vacinas”, que são carregadas e atualizadas quase que diariamente pelos antivírus. Nossa recomendação é que você tenha um antivírus instalado em seu computador, porém, não adianta apenas isso. Este software deve ser atualizado de forma constante, pois, alguns antivírus possuem configurações que, periodicamente, realizam a atualização e a varredura para detectar e recuperar-se do vírus.





SAIBA MAIS

O Symantec, além de prover um ótimo software de antivírus, ferramentas e suporte online, disponibiliza várias informações, que tem como propósito educar o público sobre as novas medidas de segurança antivírus. Confira no site do [symantec.com.](https://www.symantec.com/region/br/avcenter/education/index.html), especificamente no link: <<https://www.symantec.com/region/br/avcenter/education/index.html>> Acesso em 19 maio 2016.

Fonte: os autores

Estas pragas virtuais podem explorar o seu sistema de diversas formas, tais como:



Falhas de segurança - mais conhecidas como *bug*, ou seja, erro de sistemas. Isso ocorre normalmente em sistemas que ainda se encontram na fase beta, ou softwares mal projetados que podem conter falhas.



E-mails - essa é uma das práticas mais exploradas, pois o usuário receberá mensagens que tentam convencê-lo a executar um arquivo anexado e, com isso, contaminar o seu computador.



Downloads - o usuário pode baixar um arquivo de um determinado site sem perceber que este pode estar infectado. Em seguida, este mesmo vírus pode tentar explorar falhas de segurança de outros computadores da rede para infectá-los.

Tabela 1 - Exemplos de pragas virtuais

Fonte: os autores

Cavalos de Troia

Este tipo de ataque é muito antigo, os troianos foram os primeiros a sofrerem este tipo de ataque, ou seja, receberam dos gregos, um presente desconhecido, uma estátua no formato de “cavalo”. Durante a madrugada, os gregos saíram do interior do cavalo abriram os portões para a entrada dos soldados que estavam do lado de fora do reino. Consequentemente os gregos conseguiram o que queriam, dominar Troia e resgatar a esposa de seu rei. (SOUZA, 2016, on-line)².

A partir desta pequena história contado por vários historiadores, é que surgiu o termo de “cavalo de Troia”, que no mundo virtual são mais conhecidos como trojan. São considerados uma praga virtual que permitem acesso remoto ao computador após a infecção, liberando portas para ataques posteriores.

Normalmente, essa praga não se propaga sozinha, quase sempre está vinculada a algum vírus, tendo o objetivo de capturar dados do usuário para transmiti-los a outra máquina por meio de acesso remoto (ou *backdoors*) que permitem conexão ao equipamento infectado. Consequentemente após infiltração faz uso do registro de digitação, principalmente, o roubo de senhas e informações do sistema.



Figura 7 - Cavalo de Troia

Worm

A praga virtual *worms* é uma das que mais se propaga. Podem se espalhar rapidamente para outros computadores - seja pela internet, seja por meio de uma rede local - de maneira automática. Os worms podem infectar o computador de maneira totalmente discreta, explorando falhas em aplicativos ou no próprio sistema operacional. Pode tornar o computador infectado vulnerável a outros ataques e provocar danos apenas com o tráfego de rede gerado pela sua reprodução.

Normalmente, essas pragas são enviadas por meio de algum contato que seja conhecido e de sua confiança, e que possivelmente foi infectado, por exemplo: e-mail ou download que irá procurar explorar alguma vulnerabilidade disponível em um computador, para que possa se propagar.



Figura 8 - Worm

Spyware

Os *Spywares* são programas automáticos de computador que recolhem informações sobre o usuário, ou seja, espionam as atividades dos usuários ou capturam informações pessoais informadas aos sistemas executados nos computadores.

Não muito distantes da propagação dos cavalos de Troia e de vírus, os *spywares* são embutidos em softwares de procedência duvidosa, quase sempre oferecidos como *freeware* ou *shareware*. Consiste em um “sistema”, que recolherá as informações sobre os seus costumes na Internet e, quando infectado, o seu computador começa a capturar dados, como dados de acessos a sites e internet banking, e transmite essa informação a uma entidade externa na Internet, sem o conhecimento e consentimento do usuário.



Figura 9 - *Spywares*

Keylogger

Os aplicativos *keyloggers* são criados e distribuídos de forma oculta em vírus, *spywares* ou *softwares* de procedência duvidosa. Sua principal função é capturar tudo o que o usuário digitar no computador, desde textos até dados de acessos bancários. Além de termos esses programas em formato virtual, os temos também fisicamente, ou seja, em hardware. Neste formato, ele também realiza a mesma

função, captura tudo o que está sendo digitado e clicado em uma máquina. Sua conexão é realizada via USB.

Esse tipo de aplicativo é constantemente utilizado por jogos, pois se necesita monitorar o teclado e saber quando uma combinação de teclas foi acionada durante uma fase.

Para se livrar desse tipo de ameaça, tenha instalado em seu computador um conjunto de ferramentas que ajudam a inibir este tipo de pragas, tais como: firewall, antivírus e um software *antispyware*. Lembre-se que tais aplicativos devem ser constantemente atualizados.



Figura 10 - Keylogger

TIPOS DE ATAQUES

Neste tópico, abordaremos alguns conceitos dos principais tipos de ataques à segurança que têm preocupado os usuários cada vez mais, à medida que a rede de computadores, em específico a internet, tem se tornado o meio de comunicação de acesso a todas as pessoas.



Figura 11 - Tipos de ataques

Reprodução proibida. Art. 184 do Código Penal e Lei 9.610 de 19 de fevereiro de 1998.

Desde então, grandes avanços ocorreram e novas alternativas surgiram, sendo que atualmente grande parte dos computadores pessoais ficam conectados à rede pelo tempo em que estiverem ligados e as velocidades que podem variar de operadora para operadora. Hoje, há grande quantidade de equipamentos com acesso à rede, como dispositivos móveis, TVs, eletrodomésticos e sistemas de áudio.

Portanto, somos sujeitos a várias ameaças e ataques. Uma ameaça pode ser considerada um potencial de interesse para violação da segurança, ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade. As ameaças aproveitam das falhas de segurança da organização, que é considerado como ponto fraco, provocando possíveis danos, perdas e prejuízos aos negócios da empresa (ROSS; KUROSE, 2010, STALLINGS, 2008).

As ameaças são constantes, podendo acontecer a qualquer momento e podendo ser:

- **Naturais:** decorrentes da natureza, tais como fogo, enchentes e terremotos, que podem provocar danos aos ativos.
- **Intencionais:** são provocadas por invasões, fraudes e roubo de informações.
- **Involuntárias:** são causadas por erros de falta de conhecimento ou falta de treinamento, quanto aos equipamentos.

As ameaças exploram os pontos fracos, afetando, assim, a segurança da informação, resultando em infecções por vírus ou até mesmo os acessos indevidos. Dessa forma, é necessário conhecer qualquer tipo de vulnerabilidade que sua organização possui, para que não sejam comprometida a segurança da informação.

A **Vulnerabilidade** de um sistema ou de uma estrutura, seja ela física ou virtual, é considerada um ponto fraco existente, que quando explorado por ameaças, afeta a confiabilidade, a disponibilidade e a integridade das informações de uma pessoa ou organização. Identificando e eliminando os pontos fracos que envolvem a infraestrutura de tecnologia da informação, resultará em um novo dimensionamento dos locais em que estão expostas as vulnerabilidades. Assim, facilitará a definição de uma medida de segurança para fazer a correção, logo, estará evitando, como também prevenindo a concretização de possíveis ameaças (STALLINGS, 2008).



Figura 12 - Vulnerabilidade

Como ocorrido nas ameaças, as vulnerabilidades também podem ser classificadas em (ROSS; KUROSE, 2010; STALLINGS, 2008; TANENBAUM; WETHERALL, 2011):

Armazenamento - as informações são armazenadas em suportes físicos. Suas utilizações inadequadas podem ocasionar uma vulnerabilidade, afetando a integridade, a disponibilidade e a confidencialidade das informações.

Comunicação - está relacionado com o tráfego de informações. O sistema de comunicação escolhido deve ser seguro, de modo que as informações transmitidas alcancem o destino desejado e que não sofram nenhuma intervenção alheia.

Naturais - que podem trazer riscos para os equipamentos e informações (eventos da natureza).

Físicas - são ambientes com pontos fracos de ordem física, ou seja, o local onde são armazenadas ou gerenciados as informações, comprometendo assim a disponibilidade da informação.

Humanas - podem ser de atitudes intencionais ou não, tendo como pontos fracos: uso de senha fraca, compartilhamento de dados de acesso ou falta de treinamentos para o usuário.

Hardwares - são os equipamentos que apresentam defeitos de fabricação, atualização ou configuração, podendo permitir o ataque de vírus ou violações.

Softwares - são os pontos fracos existentes nos aplicativos, permitindo o acesso de indivíduos não autorizados.

Qualquer computador que esteja conectado a uma rede informática, seja ela cabeadas ou sem fio, pode ser considerado um grande potencial alvo de ataque. O

ataque nada mais é que uma exploração de uma falha de um sistema de segurança físicas ou virtuais, para fins que podem ser ou não conhecidos pelo explorador.

Um ataque pode ser considerado um ato ou tentativa deliberada de burlar os serviços de segurança e violar a política de segurança de um sistema. O ataque pode ser ativo ou passivo (STALLINGS, 2008).

O ataque passivo tenta descobrir ou utilizar informações do sistema, mas não afeta seus recursos. O objetivo deste tipo de ataque é obter informações que estão sendo transmitidas por alguma mídia. Este tipo de ataque ainda pode ter facilmente liberação de conteúdo da mensagem e análise de tráfego.

Um ataque ativo tenta alterar os recursos do sistema ou afetar sua operação envolvendo alguma modificação do fluxo de dados ou a criação de um fluxo falso. Podemos ter alguns tipos de ataques, como:

Furto de dados e uso indevido de recursos - informações confidenciais e outros dados podem ser obtidos tanto pela interceptação de tráfego como pela exploração de possíveis vulnerabilidades existentes em seu computador, ou seja, o seu computador pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente coletados e ser usado para a propagação de códigos maliciosos. Além disto, equipamentos de rede (como modems e roteadores) vulneráveis também podem ser invadidos, ter as configurações alteradas e fazer com que as conexões dos usuários sejam redirecionadas para sites fraudulentos. Consequentemente, um atacante pode ganhar acesso a um computador conectado à rede e utilizá-lo para a prática de atividades maliciosas, como obter arquivos, disseminar *spam*, propagar códigos maliciosos, produzir novos ataques e esconder a real identidade do atacante. Nesse caso, recomenda-se utilizar softwares de segurança que lhe irão auxiliar, tais como antivírus e firewall.

Varredura e interceptação de tráfego - um atacante pode fazer varreduras na rede, a fim de descobrir outros computadores e, caso venha a ter acesso à rede, pode tentar interceptar o tráfego e, então, coletar dados que estejam sendo transmitidos sem o uso de criptografia e tentar executar ações maliciosas, como ganhar acesso e explorar vulnerabilidades.

Ataque de negação de serviço - um atacante pode usar a rede para enviar grande volume de mensagens para um computador, até torná-lo inoperante ou incapaz de se comunicar, ou seja, o sistema começa a negar serviços próprios.

Esse tipo de ataque é mais conhecido como Ataques DoS (***Denial of Service***). Um outro tipo de ataque é o DDoS (***Distributed Denial of Service***), é um tipo de ataque DoS de grandes proporções, ou seja, utiliza vários terminais (computadores) para atacar uma determinada máquina, distribuindo a ação entre elas, desta forma, a máquina afetada começa a negar serviço pelo grande volume de requisições.



REFLITA

Não utilizar firewall e antivírus atualizados, representa um risco altíssimo ao seu computador e ao seu sistema operacional.

SISTEMAS OPERACIONAIS PARA REDE

Para se conectar a uma rede, seja ela a Internet ou uma rede comercial, precisamos de diversos dispositivos, desktops, notebooks, celulares etc. Cada aparelho deve possuir um Sistema Operacional que dê suporte à conexão em redes. Neste tópico, abordaremos os sistemas operacionais para rede.

Sistemas Operacionais, ou simplesmente SOs, são os sistemas e softwares responsáveis pelo funcionamento do seu computador. Ele gerencia o funcionamento dos drivers², fazendo com que as placas de som, vídeo e outras funcionem de maneira correta. Nele, instalamos os programas necessários para a utilização do computador, como antivírus, pacotes de escritório, programas de edição de imagens, firewalls e proxys. Sem o Sistema Operacional, o computador seria apenas uma máquina piscante, sem utilidade para usuários comuns.

Dentre os sistemas normalmente utilizados, destacamos o Windows, o Sistema Operacional mais utilizado em todo o mundo, o Linux, sistema estável e preferido dos administradores de redes, o FreeBSD, e o que é considerado o pai de todos os sistemas, o Unix.

² Um driver é um software que permite que o computador se comunique com o hardware ou com os dispositivos. Sem drivers, o hardware conectado ao computador, por exemplo, uma placa de vídeo ou uma impressora, não funcionará corretamente.

Sistemas operacionais para rede são usados para fazer com que computadores ajam como servidores. Eles são softwares que controlam outros softwares e hardwares que rodam em uma rede, além de permitir que vários computadores se comuniquem com um computador principal e entre si, compartilhando recursos, rodem aplicações, enviem mensagens, entre outras funcionalidades. Uma rede de computadores pode ser uma rede sem fio (wireless), rede local (LAN), rede de longo alcance (WAN), ou então uma pequena rede de alguns computadores.

Na rede, é necessária a utilização de um computador central no qual terá uma interface de administração orientada a menus, na qual o administrador da rede poderá realizar uma variedade de atividades, como, por exemplo, formatar discos rígidos, configurar restrições de segurança, estabelecer informações de usuários (logins, acessos etc.), anexar impressoras compartilhadas à rede, configurar o sistema para realizar *backup* automático dos dados, entre outras funcionalidades.

Outro componente de uma rede é o servidor de arquivos, um dispositivo utilizado para armazenar dados usados pelos computadores da rede. Ele pode ser um computador ou um *cluster* de discos rígidos externos. O sistema operacional da rede auxilia no gerenciamento do fluxo de informações entre esse servidor de arquivos e a rede de computadores. Como exemplos consolidados de sistemas operacionais de redes, podemos citar UNIX, Linux, Windows 2000 Server, entre outros.

Os sistemas operacionais de rede podem ser classificados como: *Peer-to-Peer* e Cliente/Servidor.



Figura 13 - Cluster de rede

Os sistemas operacionais de rede *peer-to-peer* permitem que os usuários compartilhem recursos e arquivos em seu computador e também acessem recursos e arquivos compartilhados em outros computadores. Nesses sistemas, não há um servidor de arquivos ou uma fonte

centralizada de gerenciamento. Nesse modelo, todos computadores são considerados iguais, ou seja, todos podem ser servidores ou estações de trabalhos simples.

Em uma rede *peer-to-peer* há um baixo custo por não necessitar de um servidor dedicado e pela facilidade de configuração. Qualquer usuário com conhecimento de sistema operacional consegue compartilhar recursos e arquivos devido aos novos sistemas operacionais já criarem uma rede local automaticamente.

Figura 14 - Sistemas operacionais de rede *peer-to-peer*



Diferentemente do Sistemas Operacionais de rede *peer-to-peer*, o Sistema Operacional de rede Cliente/Servidor permite que os arquivos e funções sejam centralizadas em um ou mais servidores dedicados ou não dedicados. Desta forma o nó, ou a estação principal da rede, passa a ser denominado de “coração” da rede, provendo acesso aos recursos e a segurança na rede.

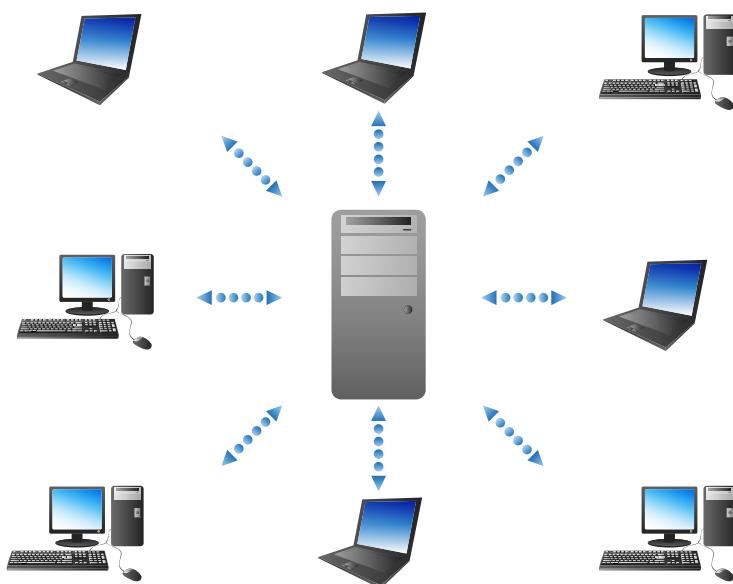


Figura 15 - Sistema operacional de rede Cliente/Servidor

Em uma rede Cliente/Servidor, um servidor dedicado terá um custo mais elevado, caso haja a necessidade de um maior volume de tráfego e de uma maior segurança no alojamento da informação. Justifica-se o seu uso em empresas que necessitem de servidores com estas características, já que tem sempre os seus dados assegurados e disponíveis 24 horas e a uma enorme velocidade de processamento.

Os sistemas operacionais de redes são uma extensão dos sistemas operacionais locais para tornar transparente o uso dos recursos compartilhados com funções de gerenciamento do acesso ao sistema de comunicação e as estações remotas para utilização de recursos de hardware e software remotos. Por sua vez, estes sistemas devem atuar de forma que os usuários possam utilizar o máximo de recursos compartilhados de outras estações da rede como se estivessem operando localmente.

Podemos definir alguns tipos diferentes de servidores: Servidor de Arquivos, Servidor de Banco de Dados e Servidor de Impressão. Vamos estudar a diferença de cada um destes servidores.

Os **Servidores de Arquivos** são usados para distribuir arquivos (como

documentos, arquivos de som, fotografias, filmes, imagens, bases de dados, entre outros) de dados para serem consultados por todos os usuários na rede local. Dessa forma, o servidor de arquivos fornece um ponto centralizado na rede para armazenamento e compartilhamento de arquivos entre os usuários.

Tomemos, como exemplo, um grupo de colaboradores de uma empresa que necessita do armazenamento de arquivos comuns a todos, ou seja, todos podem acessar, criar e alterar os mesmos arquivos, desta forma, o ideal é a configuração desse servidor. Consequentemente, o compartilhamento de informações e o gerenciamento do conhecimento dentro da organização podem ajudar muito no sucesso de uma empresa. Podemos comparar este serviço com os discos virtuais compartilhados em nuvem.

O servidor de arquivos mais utilizado é o Servidor Samba, ele roda na distribuição e permite o gerenciamento e compartilhamento de recursos em redes de computadores Windows. Assim, é possível usar o Linux como servidor de arquivos, servidor de impressão, entre outros, sem que o usuário saiba em qual sistema operacional estão armazenados seus arquivos.

Com o Servidor Samba, é possível compartilhar arquivos, compartilhar impressoras e controlar o acesso a determinados recursos de rede exatamente como em redes Microsoft. Todo trabalho feito pelo Samba é provido de grande segurança, uma vez que há grande rigor nos controles dos recursos oferecidos. Nesse servidor ficam cadastrados todos os usuários da rede e cada usuário terá acesso ou não às pastas do servidor de acordo com a necessidade. Além de ser mais estável que uma solução Microsoft, o Servidor Samba é gratuito e totalmente configurável, trazendo uma grande economia a curto e longo prazo em investimentos de TI.

Os **Servidores de Banco de Dados** são usados para consulta e/ou cadastro de dados. Esse servidor manipula informações contidas em um banco de dados, como, por exemplo, um cadastro de usuários. A interface de visualização pode ser desktop, ou via interface web. Os bancos de dados são de preferência tipo cliente/servidor. Atualmente, cada vez é mais crescente a necessidade das empresas armazenarem de maneira adequada e segura os seus dados. Existem algumas opções para servidores de bancos de dados, como o SQL Server, o Firebird, Mysql, PostgreSQL e o Microsoft Access.

Os **Servidores de Impressão** são máquinas ligadas na rede que têm como principal função gerenciar os arquivos encaminhados a uma impressora ou mais impressoras compartilhadas na mesma rede, pelas diferentes estações de trabalho que compartilham entre si o uso do equipamento de impressão.

O gerenciamento deste tipo de servidor pode incluir desde o simples roteamento dos documentos para as impressoras até o gerenciamento de cotas de papel por usuário por período de tempo, propiciando aos usuários e ao administrador da rede o controle de páginas impressas, permitindo definir ordem de prioridade das solicitações das impressões realizadas a partir dos computadores da sua empresa, seja em impressoras locais ou na rede. Podemos utilizar os sistemas operacionais servidores, tais como Windows 2008, 2003 e Linux.

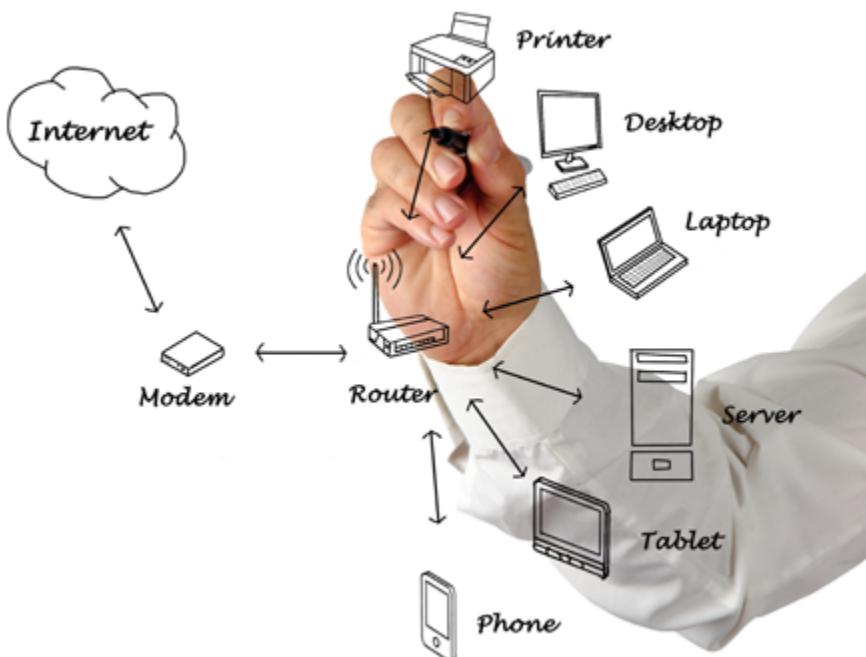


Figura 16 - Impressora em rede

CONSIDERAÇÕES FINAIS

Nesta unidade, estudamos um pouco mais a fundo sobre o funcionamento da Segurança em Redes. Por esse ser um assunto muito discutido no ambiente corporativo, o que está em jogo é o patrimônio tanto material quanto intelectual, pois as falhas na segurança podem prejudicar as organizações.

No primeiro tópico, abordamos como a criptografia pode auxiliá-lo(a) na comunicação segura. Iremos ver que a criptografia consiste na codificação de uma mensagem, em que somente o remetente e o destinatário conheçam a forma de decodificá-la.

No segundo tópico, abordamos o complemento da criptografia, a autenticação ou assinatura digital, que é a versão digital da assinatura de punho em documentos físicos, dessa forma, a assinatura digital apresenta um grau de segurança muito superior ao de uma assinatura de punho.

Em consonância com os tópicos anteriores, nos tópicos 3 e 4 abordamos as propriedades desejáveis da comunicação segura em rede de computadores, vimos os principais tipos de vírus ou pragas virtuais e os tipos de ataques e como se defender dos mesmos, que deixam os administradores de rede de orelha em pé.

E, encerrando esta unidade, abordamos o Sistema Operacional, no tocante ao suporte a redes de computadores, ou seja, para se conectar a uma rede, seja ela a Internet ou uma rede comercial, precisamos de diversos dispositivos, desktops, notebooks, celulares etc., cada aparelho deve possuir um Sistema Operacional.

Na próxima unidade do livro estudaremos a internet das coisas com o estudo da computação nas nuvens, devido a esta tecnologia ter evoluído de maneira progressiva, empresas e indivíduos usam diversos recursos de informação para gerenciarem e controlarem tudo em sua volta, mas o objetivo permanece sempre o mesmo: solucionar e otimizar problemas. Nos vemos na próxima unidade.

ATIVIDADES



1. Sistemas Operacionais são os sistemas e softwares responsáveis pelo funcionamento do seu computador. Sem eles, o computador seria apenas uma máquina piscante, sem utilidade para usuários comuns. Sobre os SOs, podemos afirmar:
 - a) O forte do Linux são as aplicações desktop e a maioria dos servidores web utiliza este sistema com o software Android.
 - b) O Free BSD, assim como Linux, é multiplataforma e suporta diversos tipos de sistemas como Intel, AMD e Power PCs.
 - c) Sendo o pai dos sistemas operacionais, o Unix era um sistema de pequeno porte, criado para os *mainframes* que existiam na época.
 - d) Os sistemas Windows já possuem um Firewall instalado, além de um antivírus gratuito chamado Windows Server.
2. Computadores podem fazer parte de uma rede doméstica, pequena, grande, até mesmo de longo alcance ou sem fio, todas necessitam de segurança. Cavalos de Troia podem abrir uma porta do seu computador para que terceiros possam se conectar. Sobre os Cavalos de Troia, assinale a alternativa correta.
 - a) Backdoors enviam os arquivos infectados para o e-mail dos contatos da lista do contaminado.
 - b) O Keylogger foi criado para registrar tudo que é digitado no computador, inclusive textos, senhas e logins.
 - c) Back Orifice, que possui um cliente e um servidor, fecha a porta do computador para que ela fique acessível a um acesso remoto.
 - d) W32/SirCam recebe os arquivos infectados por e-mail da lista do contaminado.
3. Embora se chame informalmente de vírus todo tipo de ameaça à segurança de confidencialidade, integridade ou disponibilidade, sabemos que existem algumas categorias diferentes de malwares. Leia as afirmativas e assinale a alternativa correta:
 - I. vírus: software que se infiltra e consegue se replicar e infectar outros programas.
 - II. Worm (verme): diferente do vírus, não tem o objetivo de infectar outros programas. Muito presente nos serviços de rede buscando ameaças não corrigidas.
 - III. Cavalo de Troia: programa que engana o usuário prometendo algo, mas permitindo a entrada de worms e rootkit.
 - IV. Exploit: utilizado para detectar as ameaças corrigidas para iniciar um ataque.
 - a) Somente I e II estão corretas.
 - b) Somente I, II e III estão corretas.
 - c) Somente II e III estão corretas.

ATIVIDADES



- d) Somente I, III e IV estão corretas.
 - e) Todas estão corretas.
4. Para se realizar uma ação ilícita com ataques à confidencialidade, integridade ou disponibilidade de dados, softwares conhecidos como malwares se aproveitam de ameaças já identificadas. Leia as afirmativas e assinale a alternativa correta:
- I. *Packet sniffer* (farejador de pacotes) é um software que monitora a rede copiando pacotes.
 - II. *BlackDoor* é um software que abre as portas para futuros ataques.
 - III. *Keylogger* é um software que captura tudo o que foi digitado.
 - IV. *RootKit* é um software que tem por objetivo ocultar a presença de um intruso.
- a) Somente I e II estão corretas.
 - b) Somente II e III estão corretas.
 - c) Somente I, II e IV estão corretas.
 - d) Somente I, III e IV estão corretas.
 - e) Todas estão corretas.



VISÃO GERAL SOBRE O LINUX, O SISTEMA OPERACIONAL QUE É UMA PLATAFORMA UNIVERSAL

Conheça o Linux, um gerador adaptável que serve como base para diversos modelos de uso

Linux está em todo lugar. Se analisar o menor smartphone até a espinha dorsal da Internet ou no maior e mais eficiente supercomputador, você encontrará o Linux. Isso não é algo simples, devido à quantidade de recursos esperada dessas plataformas. Descubra a onipresença do Linux e como ele suporta dispositivos grandes e pequenos e tudo mais que se encontra entre eles.

Linux® atingiu a maioria. Em 2012, Linux completará 21 anos, um sistema operacional maduro com suporte para diversos modelos de uso. Porém, é difícil pensar no Linux como somente um sistema operacional - ele é mais como um camaleão. Sua flexibilidade e kernel modular abordam vários modelos de uso (do maior supercomputador ao menor dispositivo integrado), sendo difícil não classificá-lo uma tecnologia de ativação. Na verdade, o Linux é uma plataforma. É uma tecnologia importante que permite a criação de novos produtos, alguns deles desconhecidos há pouco tempo atrás.

Vamos começar com uma breve exploração do Linux, sua arquitetura básica e alguns de seus princípios mais importantes. Em seguida, veja como o Linux aplica esses princípios a uma diversidade de modelos de uso e por que é uma plataforma e não apenas um sistema operacional.

O que é Linux?

Linux está em uma classe própria no campo da *portabilidade*. O subsistema do driver (que é vasto em seus recursos) suporta módulos carregados dinamicamente sem afetar o desempenho, permitindo a *modularidade* (além de uma plataforma mais *dinâmica*). Linux também inclui segurança no nível do kernel (em diversos esquemas) permitindo uma plataforma *segura*. No domínio de sistemas de arquivo externos, o Linux possibilita uma grande quantidade de array de suporte para sistema de arquivos de qualquer sistema operacional, permitindo, por exemplo, *flexibilidade* por meio da modularidade do design. O Linux implementa não apenas recursos de planejamento padrão, mas também o planejamento *em tempo real* (incluindo garantias sobre a latência de interrupção).

Finalmente, o Linux é *aberto*, o que significa que seu código-fonte pode ser visualizado e aprimorado por praticamente qualquer pessoa. Essa abertura também minimiza as oportunidades de explorações negativas, criando uma plataforma mais *segura*. Muitas empresas colaboram com o Linux, garantindo que ele continuará a abordar vários modelos de uso, enquanto mantém suas propriedades principais.

Esses sete princípios mais importantes não são de forma alguma os únicos atributos fornecidos pelo Linux, mas eles tornam o Linux uma plataforma universal entra uma ampla variedade de modelos de uso. Além disso, o Linux é o mesmo entre esses modelos de uso—não apenas os princípios de design, mas o próprio código. Isso não pode ser dito





de outros sistemas operacionais (como o Windows®— desktop, Server ou integrado— ou Mac OS X ou Apple iOS), que fragmentam suas ofertas para suportar outros modelos de uso.

Desktop e netbook

O Linux apresenta maiores dificuldades na área de desktops e netbooks, em que muitas pessoas usam Linux. Dados recentes de participação no mercado indicam que o Linux captura cerca de 1,5% do mercado de desktops, mas cerca de 32% do mercado de netbooks. Esses números podem parecer baixos, mas, como desenvolvedor, tenho a tendência de ver o Linux com mais frequência do que qualquer outro sistema operacional.

O Linux começou como um sistema operacional experimental simples e, com a introdução do XFree86 em 1994, um gerenciador de janelas mostrou a promessa de um sistema operacional de desktop novato. Hoje, há diversos gerenciadores de janela disponíveis para Linux (tanto uma bênção como uma maldição), permitindo que os usuários padronizem sua personalizada de acordo com suas necessidades. Além disso, o Linux escala automaticamente com recursos de processador (como multicore e multiencadeamento simétrico), planejando de forma eficiente os processos tendo o desempenho em mente.

Versatilidade do Linux

O suporte dos diversos modelos de uso definidos aqui é simplesmente uma opção de pacote para o Linux. As distribuições do Linux englobam os mercados de desktop e servidor, onde as distribuições especializadas se concentram em integrados (como uClinux, se seu dispositivo integrado não tiver uma unidade de gerenciamento de memória). Qualquer pessoa pode pegar um kernel Linux e agrupar um conjunto de aplicativos de usuário para um modelo de uso específico, aproveitando as vantagens dos diversos benefícios do Linux (o array de protocolos de rede e sistemas de arquivo, kernel configurável e dinâmico, interfaces de programação de aplicativo padrão). Esse é um dos motivos para o uso do Linux em plataformas de smartphone de rápido crescimento (com uma interface com o usuário customizada para sua personalidade).

Indo além

Se você comparar o Linux a uma ponte, ele seria uma maravilha da engenharia moderna. Seu modelo de desenvolvimento distribuído desafiou o status quo e o resultado é um dos produtos de software mais flexíveis já criado, envolvendo uma variedade de modelos de uso desde pequenos dispositivos integrados a enormes supercomputadores. O Linux moldou os segmentos de mercado e liderou o caminho da pesquisa de tecnologia de ponta em computação de cluster, sistemas de arquivo, nuvens e virtualização. Qualquer ambiente de computação que surja, o Linux estará lá.

Fonte: Jones (2012, on-line)³.

MATERIAL COMPLEMENTAR



LIVRO

Segurança de Computadores: Princípios e Práticas

Willians Stallings; Lawrie Brown

Editora: Campus

Sinopse: O interesse no aprendizado da segurança de computadores e tópicos relacionados vem crescendo a uma taxa impressionante nos últimos anos. Dessa maneira, o número de cursos sobre segurança de computadores e áreas relacionadas em universidades federais, estaduais, municipais e outras instituições está crescendo. O objetivo deste livro é oferecer um levantamento atualizado dos desenvolvimentos nesse campo. Os problemas centrais que se apresentam aos projetistas e administradores de segurança incluem definir as ameaças a sistemas de computadores e redes, avaliar os riscos relativos dessas ameaças e desenvolver contramedidas que sejam fáceis de usar e efetivas em custo. Vários capítulos incluem uma seção que mostra a aplicação prática dos princípios do capítulo em um ambiente do mundo real. Segurança de Computadores visa o público acadêmico e o público profissional. Como livro didático, é dirigido a cursos de graduação de um ou dois semestres em ciência da computação, engenharia de computadores e engenharia eletrônica. Para os profissionais interessados nessa área, o livro serve como um volume de referência básica e é adequado ao autodidatismo.



LIVRO

Fortaleza Digital

Willians Dan Brown

Editora: Editora Arqueiro

Sinopse: Dan Brown mergulha no intrigante universo dos serviços de informação e ambienta sua história na ultra-secreta e multibilionária NSA.

Quando o supercomputador da NSA, até então considerado uma arma invencível para decodificar mensagens terroristas transmitidas pela Internet, se depara com um novo código que não pode ser quebrado, a agência recorre à sua mais brilhante criptógrafa, a bela matemática Susan Fletcher.

Presa em uma teia de segredos e mentiras, sem saber em quem confiar, Susan precisa encontrar a chave do engenhoso código para evitar o maior desastre da história da inteligência americana e para salvar a sua vida e a do homem que ama.



MATERIAL COMPLEMENTAR



FILME

O Jogo da Imitação

O Jogo da Imitação é baseado na história real do lendário criptoanalista inglês Alan Turing, considerado o pai da computação moderna, e narra a tensa corrida contra o tempo de Turing e sua brilhante equipe no projeto Ultra para decifrar os códigos de guerra nazistas e contribuir para o final do conflito.



MATERIAL COMPLEMENTAR



NA WEB

Recomendamos a consulta ao artigo "Segurança em Redes de Computadores" disponível no link: <<https://brasilescola.uol.com.br/informatica/seguranca-redes.htm>>. Acesso em: 24 set. 2020. O artigo traz de forma bem simples a questão de segurança em redes de computadores.



NA WEB

O Windows 10 veio para ficar, o mesmo já superou o 8.1 e se torna o 2º sistema operacional mais usado no mundo, de acordo com o olhar digital. Para saber mais informações consulte o link: <<http://olhardigital.uol.com.br/noticia/windows-10-supera-8-1-e-se-torna-o-2-sistema-operacional-mais-usado-no-mundo/54504>> Acesso em: 19 maio 2016.



REFERÊNCIAS

CARVALHO, L. G.. **Segurança de Redes**. Rio de Janeiro: Editora Ciência Moderna Ltda, 2005.

Dantas, Marcus Leal. **Segurança da informação**: uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

ROSS, K.; KUROSE, J. F. **Redes de Computadores e a Internet**: uma abordagem top down. 5 ed. São Paulo: Pearson, 2005.

STALLINGS, W. **Criptografia e Segurança de Redes**: Princípios e Práticas. 4 ed. São Paulo: Pearson, 2008

TANENBAUM, A.; WETHERALL, D. **Redes de Computadores**. 5 ed. São Paulo: Pearson, 2011.

CITAÇÃO DE LINKS

¹<<http://www.cert.br/stats/incidentes/>>. Acesso em 19 maio 2016.

²<<http://www.infoescola.com/historia/guerra-de-Troia/>>. Acesso em 19 maio 2016.

³<<http://www.ibm.com/developerworks/br/library/l-linuxuniversal/>>. Acesso em 19 maio 2016.



GABARITO

1. B
2. B
3. B
4. D



CLOUD COMPUTING E VIRTUALIZAÇÃO

UNIDADE

V

Objetivos de Aprendizagem

- Entender como funciona a Computação nas Nuvens.
- Descrever os recursos necessários para o serviço em nuvem.
- Verificar os benefícios da Computação em Nuvem para as empresas.
- Analisar os benefícios da virtualização.
- Conectar os itens usados do dia a dia à rede mundial de computadores.

Plano de Estudo

A seguir, apresentam-se os tópicos que você estudará nesta unidade:

- Princípios da Computação na Nuvem e acesso
- Software, Infraestrutura e Plataforma como serviço
- Sua empresa e a Computação em Nuvem
- Virtualização
- Internet das coisas

INTRODUÇÃO

Chegamos à última unidade deste livro, e vamos dar início ao nosso estudo abordando os principais conceitos de Computação em Nuvem, como que ela proporciona segurança e comodidade em armazenamento e serviços. Esses tipos de serviços são disponibilizados por meio de uma ferramenta tecnológica via web, capaz de reunir todas as informações sem a necessidade de utilizar dispositivos externos de armazenamento.

Após entendermos os princípios que norteiam a computação em nuvem, abordaremos o Software, a Infraestrutura e a Plataforma como serviço. Nota-se que a implantação de um sistema deste porte deve ser planejada e organizada, para que possa ser melhor aproveitada com pouco recurso computacional.

A partir dos princípios apresentados com a evolução do modelo tradicional em que as organizações continham vários dispositivos físicos em suas dependências, o modelo virtual aborda os serviços disponibilizados pela internet por meio da computação em nuvem. A partir desta abordagem, é possível realizar corte de custos operacionais nos departamentos, principalmente o de TI, pois podem reunir esforços e aumentar tempo em melhoramento dos projetos estratégicos, em vez de manter e dar manutenção constante no data center.

Outra forma de poder propiciar benefícios às organizações é com a técnica de Virtualização, esta técnica permite instalar diversos sistemas operacionais em um computador, ou seja, rodar diversos SO em uma única máquina, dando a impressão de que você está utilizando uma máquina real e não virtual.

Diante dessas evoluções tecnológicas, o acesso a informações e serviços é facilitado à sociedade por meio de uma grande variedade de dispositivos eletrônicos. A partir destes serviços, a sociedade tem a possibilidade de captar e gerar novos dados com estes dispositivos e a qualquer hora e local por meio da internet.

PRINCÍPIOS DA COMPUTAÇÃO NA NUVEM E ACESSO

Nesta unidade abordaremos os princípios norteadores da Computação em Nuvem - ou *Cloud Computing* - e também vamos conferir o panorama atual dessa tecnologia, uma vez que é possível encontrar cada vez mais serviços que funcionam a partir de uma conexão com a internet.

A computação em nuvem tem se instituído nos últimos anos como uma importante plataforma de obtenção, compartilhamento, manipulação e exploração de enorme quantidade de dados. Dessa forma, tal tecnologia contribui com esta enorme quantidade de dados, à medida que as empresas e pessoas vão tomando ciência de sua vantagem.



Figura 1 - Computação nas nuvens

Vivemos em uma sociedade geradora de grande quantidade de dados, de forma exponencial, desordenada e desestruturada. Conforme o avanço das tecnologias da informação e da comunicação, em especial a tecnologia mobile, é facilitado, a aquisição e o uso destes aparelhos na sociedade, principalmente pelos jovens e adultos.

Nos tempos atuais, o acesso à internet é facilitado por diversos dispositivos como computadores, smartphones, tablets, entre outros, para várias atividades. Dessa forma, a computação em nuvem apresenta-se como uma ótima opção de

ferramenta tecnológica capaz de reunir todas as informações sem a necessidade de utilizar dispositivos externos de armazenamento.



Figura 2 - Com a nuvem você pode usufruir em qualquer local

REFLITA



O armazenamento na NUVEM veio para substituir o disco virtual? Sabemos que os discos virtuais têm funções de armazenamento e compartilhamento de arquivos e pastas, já substituindo fisicamente o pendrive.

Os sites que disponibilizam o serviço da computação em nuvem comportam programas e aplicativos que não precisam de instalação na máquina local para ser utilizados. Para o acesso a estes sites, é necessário que se tenha acesso à internet e a um navegador instalado em seu computador. Caso queira, é possível instalar

um aplicativo em seu PC para que, quando você esteja sem acesso à internet, seja possível ter uma cópia de seus arquivos. Posteriormente, quando retornar o acesso à internet, automaticamente serão sincronizados com a nuvem.

Existem muitas opções de sites que fornecem o serviço de computação em nuvem, sendo alguns dos mais importantes o Dropbox, Google Drive, OneDrive, entre outros.

	<p>O Dropbox, criado em 2007, atualmente é um dos serviços mais utilizados .</p> <p>Seu grande diferencial é o serviço de indicação, no qual a cada amigo convidado e que cria uma conta, você aumenta a sua capacidade de armazenamento, podendo chegar a 16GB de espaço.</p> <p>Para criar uma conta no Dropbox, acesse <http://dropbox.com>.</p>
	<p>Com o Google Drive é possível armazenar aproximadamente 5GB de arquivos gratuitamente. A vantagem do Google Drive é a velocidade e a integração com o Google Docs, suíte de aplicativos, parecidos com o word, excel, powerpoint etc. Para criar uma conta no Google Drive, acesse: <http://drive.google.com>.</p>
	<p>Da Microsoft, o OneDrive tem vários planos de armazenamento, indo do gratuito ao pago. O plano gratuito tem a sua capacidade de armazenamento de 5GB. Para criar uma conta no OneDrive, acesse: <https://onedrive.live.com/>.</p>

Tabela 1 - Serviços de computação em Nuvem

Figura 3 - Sites em nuvem



Mas, afinal, o que é computação em nuvem? De acordo com Taurion (2009, p.2), a Computação em Nuvem pode ser definida como “um conjunto de recursos como capacidade de processamento, armazenamento, conectividade, plataformas, aplicações e serviços disponibilizados na Internet”. Neste contexto, a computação em nuvem é um modelo de computação composto por processamento, armazenamento e softwares que estão em algum lugar da rede, sendo acessada remotamente.



A computação em nuvem está em todo lugar, como nas redes sociais, tais como blogs e sites de compartilhamento de fotos e vídeos. O acesso a esse tipo de serviço a cada dia é mais facilitado pelas Tecnologias da Informação e da Comunicação (TICs). A sociedade dispõe de uma gama de dispositivos em suas mãos, em busca pelo acesso instantâneo e remoto das informações e arquivos. Esta busca constante é o que impulsiona, de certa forma, o uso de tecnologia em nuvem.

Figura 4 - A nuvem está em qualquer local

Consequentemente, essa demanda proporciona a queda dos custos da tecnologia e um aumento expressivo na qualidade dos serviços prestados (TAURION, 2009).

Nesse contexto, a computação em nuvem funciona de forma centralizada, ou seja, criam-se vários data centers distribuídos geograficamente. Desta forma este serviço também pode ser considerado como um ambiente virtual, ele pode ser alocado em “algum lugar” da Internet e situado fisicamente em algum lugar do globo. É possível alocar hardware sob demanda para o cliente e como exemplo temos as empresas com nomes renomados tais como: IBM, Google e Amazon (OLIVEIRA NETO; FREITAS, 2011; VELTE et al., 2012).

Sendo assim, a computação em nuvem possibilita prover serviços ao usuário, de acordo com a sua demanda e recurso computacional necessário. O usuário tem controle sobre o quanto e quando precisará da demanda de hardware de máquina, e irá pagar somente por aquilo que foi contratado (VELTE et al., 2012).

Outro conceito de *cloud computing* que mais se aproxima de nossa realidade está nos estudos de Oliveira Neto e Freitas (2011, p. 3), que afirma

A computação em nuvens anuncia uma mudança importante na maneira como nós armazenamos informações e executamos aplicações. Em vez de executarmos os programas e as informações em computadores individuais, tudo será armazenado na nuvem. (OLIVEIRA NETO; FREITAS, 2011, p. 3).



SAIBA MAIS

A empresa de TI E-business Conhecimentos Práticos em Gestão de TI disponibilizou um Panorama do Cloud Computing no Brasil, trazendo informações sobre o universo dos profissionais que participaram desta análise, em que 56% afirmaram que aderiram algum tipo de cloud computing. Vejamos melhor esses números no material que está disponibilizado em <https://webinsider.com.br/wp-content/uploads/2012/07/ebusiness_brasil.pdf>. Acesso em 19 maio 2016.

Fonte: adaptado de E-business (2012, on-line)¹.

SOFTWARE, INFRAESTRUTURA E PLATAFORMA COMO SERVIÇO

Como estudamos no tópico anterior, a computação em nuvem surge da necessidade de construir infraestruturas de TI complexas, em que os usuários não têm que realizar instalação, configuração e atualização de softwares. Além disso, recursos de computação e hardware são propensos a ficarem obsoletos rapidamente.

Existem diversos serviços que são atrelados ao conceito e que podem trazer benefícios à operação das empresas, uma vez que podem ser adquiridos na quantidade necessária para cada caso (MOTAHARI-NEZHAD et al., 2009)².

PaaS (Platform as a Service): Esse tipo de serviço tem como função fornecer suporte a todo o ciclo de vida de desenvolvimento de aplicações, desde a sua concepção, execução, debug, teste, implantação, operação e apoio às aplicações Web. Esse serviço também facilita o desenvolvimento de aplicações destinadas aos usuários de uma nuvem, a partir de uma plataforma e uma infraestrutura de alto nível de integração, que possibilita a implementação e os testes de aplicações na nuvem.

DaaS (Database as a Service): Esse tipo de serviço fornece recursos de banco de dados para as aplicações das empresas, sejam internas ou rodando nas nuvens. De acordo com Taurion (2009, p. 128-129), o provedor da nuvem mantém todo serviço de SGDB e o cliente paga somente pelo volume de dados armazenados e transferidos de e para a nuvem.

Taurion (2009, p. 130), sugere alguns usos iniciais para DaaS:

- **Ambiente de desenvolvimento e testes.** Os desenvolvedores podem testar suas aplicações exaustivamente no momento em que precisam, sem a burocracia para ter ambientes disponibilizados.
- **Data archiving.** Sabendo que apenas 20% das informações das empresas estãoativas e, por aderência à legislação, a grande maioria das informações é armazenada em fitas após um período de inatividade. Por meio do DaaS há uma nova alternativa com custos menores para armazenar essas informações inativas.

- **Backup.** O DaaS permite armazenamento de informações com custos menores que em discos próprios, além de fornecer ferramentas para automatizar os *backups*.

IaaS (Infrastructure as a Service): o IaaS traz os serviços oferecidos na camada de infraestrutura, nesses serviços podemos incluir servidores, roteadores, sistemas de armazenamento e outros recursos de computação tais como recursos de hardware, espaço para armazenamento de dados e capacidade de processamento. O IaaS é baseado em técnicas de virtualização de recursos de computação. Tal recurso promove certa economia, pois não será necessário a aquisição de novos servidores e equipamentos de rede para a ampliação de serviços.

SaaS (Software as a Service): são aplicações de software oferecidas como serviços na Internet. Nesse caso, a distribuição de software é *free* e este não precisa ser instalado localmente, mas sim liberado apenas o acesso ao serviço oferecido por este software, sendo este licenciado para a utilização por meio da internet. Os prestadores de serviços disponibilizam o SaaS na camada de aplicação, o que leva a rodar inteiramente na nuvem, trazendo a redução de custos e dispensando a aquisição de licença de softwares.

No modelo tradicional, o cliente deveria adquirir hardware, licenças e realizar a instalação e a manutenção das aplicações em todos os seus equipamentos. Agora com o recurso de Computação em Nuvem, tudo fica disposto na nuvem, ou seja, você não precisa mais adquirir licenças, servidores e manutenção, aqui ela está disponível por meio de um navegador, em qualquer lugar e a qualquer hora.

SUA EMPRESA E A COMPUTAÇÃO EM NUVEM

Neste tópico vamos abordar as vantagens de implantar a computação em nuvem nas organizações.

Na sociedade contemporânea, a informação e o conhecimento são considerados fundamentais para as organizações devido à necessidade de trabalho

coletivo com troca de informações e experiências entre pessoas. O avanço da tecnologia da informação e da comunicação vem desempenhando ao longo dos anos um papel importantíssimo para as organizações (DALKIR, 2005).

Atualmente, a nossa sociedade está passando por frequentes mudanças de paradigma, refletindo no avanço da tecnologia, educação, saúde, política em prol da sustentabilidade de uma economia globalizada. Contudo, esta mudança ainda gera um desconforto para as organizações, pois mudar o que já está funcionando para uma aventura nas nuvens depende de um bom P&D (Planejamento e Desenvolvimento) alinhado com os objetivos estratégicos da empresa.

Taurion (2009, p. 65) afirma que:

Como a computação em nuvem está em um início de sua evolução, o cenário futuro deverá ser diferente e os CIOs devem ter como preocupação a sustentabilidade do negócio dos seus provedores de serviço.

O desafio para a correta tomada de decisões é descobrir como essa tecnologia será inserida no contexto dos negócios e quais vantagens competitivas ela trará. Existem muitos riscos a serem avaliados: riscos de mercado, riscos de viabilidade técnica e os próprios riscos organizacionais.



Figura 5 - Cloud Computing nas organizações

De acordo com o autor Taurion (2009), temos algumas ações que as empresas devem ter em suas preliminares para a adoção da instalação dos serviços em nuvem:

Observar e aguardar: Ação sugerida quando a empresa prefere esperar que a tecnologia amadureça. Essa estratégia não deve tomar tempo demais, pois a empresa pode estar perdendo oportunidade competitiva com o uso estratégico da tecnologia.

Acreditar e liderar: Quando a oportunidade é muito promissora e a empresa pode começar a explorá-la de maneira pioneira.

Com o aumento desta qualidade de serviço, a *cloud computing*, possibilita alcance geográfico maior, além de uma interação mais ágil, eficaz e veloz de armazenamento e transferência do conhecimento entre fornecedores, colaboradores e competidores.

De acordo com Velte et al. (2012), uma das funções da computação em nuvem é cortar custos operacionais nos departamentos, principalmente no de TI, pois podem reunir esforços e aumentar tempo em melhoramentos dos projetos estratégicos em vez de manter e dar manutenção constante no data center.

Complementar a isso, conforme Taurion (2009), os principais benefícios da utilização de uma plataforma com recursos computacionais disponíveis na Internet estão relacionados ao custo e à elasticidade. Dentro do custo, temos dois vieses: o primeiro é relacionado ao investimento inicial, ou seja, a aquisição de maquinário de grande porte como servidores. E, o outro é relacionado à contratação de funcionários dedicados a manter aqueles serviços funcionando.

O outro benefício proposto por Taurion (2009), a elasticidade, é responsável pelo provisionamento automático de aumento ou da diminuição da capacidade de armazenamento e processamento dos servidores. Dessa forma, a elasticidade possibilita o aumento ou diminuição da capacidade de forma automática.

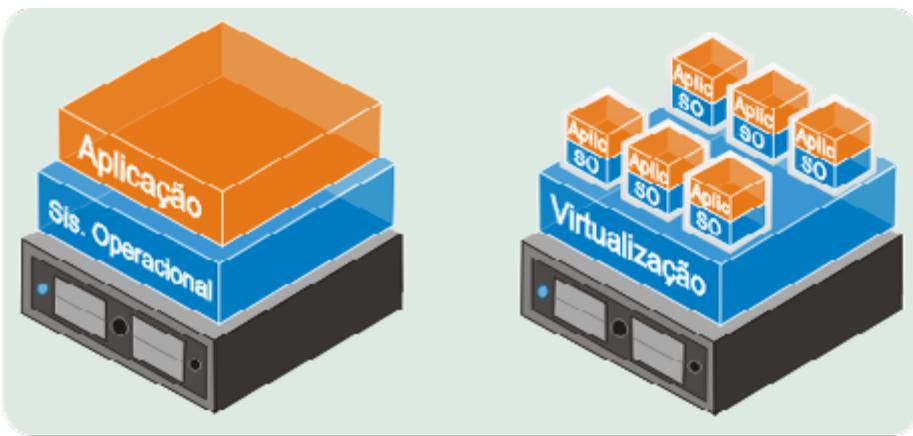
VIRTUALIZAÇÃO

Neste tópico, serão abordados os princípios norteadores das técnicas de virtualização, passando pelas virtualizações de hardware, apresentação, aplicativos, até a computação em nuvem como uma das técnicas mais utilizadas.

Uma máquina virtual ou virtual machine (VM) funciona como um “emulador” de um ou vários sistemas operacionais no mesmo computador. Desta forma, na máquina virtual criada, você pode instalar diversos sistemas operacionais, que ficarão isolados entre si.

Para cada máquina virtual criada, a mesma oferece um ambiente completo, de forma quase que idêntica a uma máquina física instalada. Dessa forma, cada máquina virtual pode ter seu próprio sistema operacional e, nele, ter instalados e configurados aplicativos e serviços de rede, interconectando (virtualmente) cada uma dessas máquinas através de interfaces de redes, switches, roteadores e firewalls virtuais e de VPN (*Virtual Private Networks*) (CARISSIMI; VERAS, 2015).

A partir desse contexto, a virtualização pode proporcionar mais portabilidade e flexibilidade, permitindo assim que várias aplicações e sistemas operacionais diferentes executem em um mesmo hardware simultaneamente. Sendo assim, tomemos a virtualização como sendo uma vantagem para os data centers, pois a diminuição de máquinas físicas implicará na redução de custos de infraestrutura física como espaço, energia elétrica, cabeamento, refrigeração e suporte e manutenção de vários sistemas.



Arquitetura Tradicional x Virtualização

Figura 6 - Arquitetura Tradicional x Virtualização

Fonte: Jandl Junior (2015, on-line)³.

Vamos reforçar os conceitos. Vamos pensar em um computador configurado como um servidor de FTP: mesmo que o disco rígido seja plenamente utilizado, não se pode dizer o mesmo sobre sua capacidade de processamento: enquanto ela pode chegar ao ápice em horários de pico, pode também se aproximar da ociosidade durante alguns momentos. Com isso, existem momentos que o servidor está “inoperante”, ou seja, “com sobra de processamento”. Nessa ocasião, outro aplicativo poderia estar sendo executado em outra máquina virtual no mesmo computador.

De acordo com Carissimi e Veras (2015), a virtualização usa softwares que simulam a existência de hardwares, criando desta forma um sistema de computadores virtuais, resultando assim em uma economia em escala e mais eficiência. Ainda de acordo com os mesmos autores, a virtualização pode ser classificada em: virtualização de servidores, virtualização de apresentação, virtualização de armazenamento, virtualização de aplicação e virtualização de redes. Vamos agora descrevê-las e veremos como cada uma delas se comporta

Virtualização de servidores: esse tipo de virtualização consiste em rodar vários sistemas operacionais na mesma máquina. Para que esta virtualização possa ocorrer, é necessário o uso de programas específicos que geram máquinas virtuais (*Virtual Machines*, ou *VMs*), que, por sua vez, emulam os componentes físicos de um PC, possibilitando que um sistema operacional diferente seja

instalado em cada uma delas. Temos dois grandes papéis na virtualização de servidores: usuários e servidores. A primeira possibilita eliminar a incompatibilidade entre aplicativos e sistemas operacionais. Como, por exemplo, sabe aquele jogo que só roda no Windows XP, e agora com o Windows 10, ele não funciona mais? Basta então instalar uma máquina virtual com o Windows XP e o seu jogo irá rodar normalmente.



Figura 7 - Virtualização de Sistemas Operacionais
Fonte: Redes e Servidores Blog (2011)⁴.

Quanto aos servidores, sua virtualização permite que, ao invés de se ter diversos subservidores físicos, passam a ter vários servidores virtuais, compartilhando do mesmo hardware, reduzindo a quantidade de mão de obra técnica, o espaço para alocar as máquinas e o gasto com eletricidade.

Virtualização de Apresentação: também conhecida como virtualização de desktop. Essa virtualização consiste na configuração dos desktops em uma infraestrutura centralizada virtualmente. Muitos usuários ainda possuem os seus programas instalados em seus computadores, porém, essa barreira está sendo quebrada com o uso da virtualização da apresentação, que possibilita o acesso a um ambiente computacional sem a necessidade de estar em contato físico com ele.

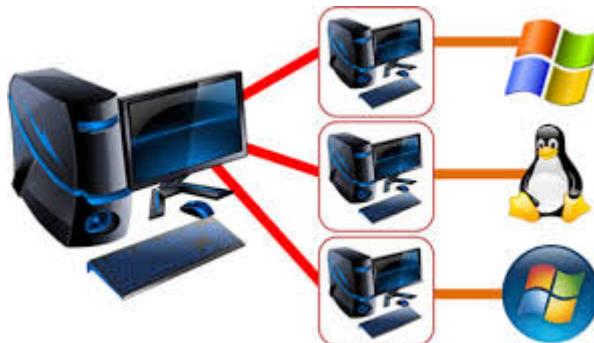


Figura 8 - Virtualização de apresentação

Fonte: Usuário Root (2013, on-line)⁵.

Sendo assim, essa virtualização possibilita a utilização de um sistema operacional completo (bem como de seus aplicativos) de qualquer local do planeta, como se estivessem instalados no seu PC. O conceito é bem parecido com o de acesso remoto, com a diferença de que vários usuários podem se beneficiar do mesmo sistema simultaneamente (sem interferir uns aos outros).

Virtualização de armazenamento: devido à grande quantidade de dados que organizações e sociedade estão criando e armazenando, necessita-se cada vez mais de tecnologias que possam corroborar a crescente demanda por armazenamento seguro destes dados, via local ou via web. Uma das saídas que muitos encontram são os clássicos backups, feitos regularmente em outras mídias e guardadas em locais distintos para evitar a perda do original. Normalmente estes dados possibilitam que vários terminais possam encontrar e acessar os mesmos dados.

Reprodução proibida. Art. 184 do Código Penal e Lei 9.510 de 19 de fevereiro de 1998.



Figura 9 - Virtualização de armazenamento

Fonte: Implico (2011, on-line)⁶.

Dessa forma, muitos acessos a uma mesma máquina física pode criar um estrangulamento, podendo até ficar inoperante. Por estas razões, os dados foram movidos para a virtualização. As empresas utilizam armazenamento centralizado (armazenamento virtualizado) como forma de evitar problemas de acesso a dados. Além disso, a mudança para o armazenamento de dados centralizado pode ajudar as organizações a reduzir custos e melhorar a eficiência da gestão de dados.

Virtualização de aplicação: a técnica dessa virtualização consiste em ter uma cópia de determinado aplicativo (editores de textos, planilhas, entre outros), instalada em um servidor de forma virtual. Os usuários que desejarem ter acesso a este aplicativo podem fazê-lo diretamente, sem a necessidade que ele também esteja instalado na máquina física.

Virtualização de redes: esse tipo de virtualização consiste na reprodução completa de uma rede física. Todavia, esta rede será de forma virtual, ou seja, lógica. Os aplicativos são executados na rede virtual exatamente como se estivessem em uma rede física. Esta virtualização também permite a configuração de sistema de redes (*switches*, roteadores, *firewalls*,平衡adores de carga, VPNs e outros), compartilhando a infraestrutura em comum.

Atualmente no mercado brasileiro temos várias soluções de softwares para virtualização, entre elas: VMWare, Hyper-V, Xen, KV, entre outras. Dentre todos os softwares listados acima, quem mais se destaca é o Vmware. Esse aplicativo é uma ferramenta poderosa, provendo as organizações em diversos recursos avançados para o gerenciamento e administração de um ambiente totalmente virtualizado, possibilitando até a migração de outras máquinas virtuais. Temos outros benefícios desse software, tais como: recursos de alta disponibilidade, tolerância a falhas e *storage* (armazenamento).

INTERNET DAS COISAS

Continuando nossos estudos, abordaremos agora sobre um assunto que tem sido amplamente pontuado na atualidade: a **Internet das Coisas**. Sobre o tema, veremos informações a respeito de onde a encontramos, quais suas vantagens e qual tecnologia é empregada.

Diariamente somos bombardeados de dados e informações e muitas vezes nem sabemos de onde vem e para onde vai. Porém, podemos fazer uso de alguns desses dados e informações. Consequentemente, está ocorrendo uma revolução de equipamentos eletrônicos que permitem captar e gerar novos dados, por meio da internet.

Lacerda e Marques (2015), afirmam que esta tecnologia está sendo chamada por toda a comunidade de **A Internet das Coisas ou Computação Ubíqua**. Essa tecnologia tem como objetivo conectar os itens usados do dia a dia à rede mundial de computadores, de forma a capturar, processar, armazenar, transmitir e apresentar informações.

Para Zambarda (2014)⁷, são muitos os equipamentos que estão (ou estarão) conectados, como geladeiras, óculos, elevadores e carros. Dessa forma, as informações podem fazer parte da atuação das pessoas no mundo.

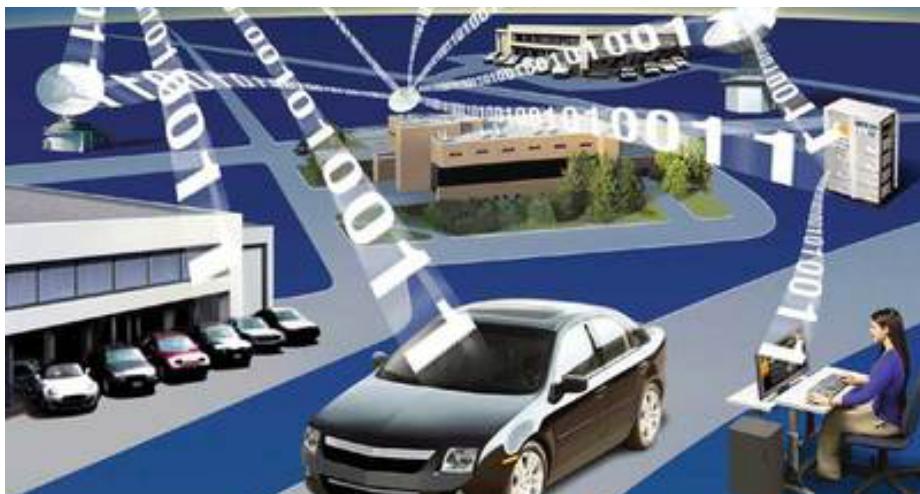


Figura 10 - Internet em diversos dispositivos

Fonte: Correia, Silveira, Venancio e Virtudes (2011, on-line)⁸.

A partir desta interconexão entre os dispositivos, está cada vez mais fácil procurar informações, já que toda esta tecnologia está disponível a qualquer momento por meio de qualquer objeto que utilizamos frequentemente. Assim, nosso cotidiano ficará muito mais produtivo, pois teremos várias facetas para obtermos uma notícia por meio de objetos mais próximo de forma mais simplificada e agradável. A reflexão a seguir permite pensarmos sobre este cenário que estamos vivendo:

Informações estão sendo incorporadas em objetos de uso comum em toda parte. Isto muda fundamentalmente a maneira de compreender a Arquitetura da Informação, a forma de lidar com suas questões científicas e, definitivamente, a forma de praticá-la (LACERDA; LIMA-MARQUES, 2014, p.7).

Desde a criação da internet por Tim Berners Lee, ela vem tornando-se cada vez mais fundamental para a sociedade. Atzori et al. (2010) e Zambarda (2014)⁷ concordam que atualmente a Internet das Coisas vem ganhando grande destaque no cenário das telecomunicações. Tal cenário, por sua vez, está sendo considerado a revolução tecnológica que pretende representar o futuro da computação e comunicação.

Vejamos um exemplo de internet das coisas. Um veículo transitando em uma rodovia estadual ou federal, sem precisar parar no pedágio, pois existe em seu interior um dispositivo que, ao se aproximar da cancela, transmite as informações do carro e de cobrança do motorista para o sistema de recepção instalado na guarita. É uma situação que já vivenciamos em nosso dia a dia e que, muitas vezes, pode passar despercebida.





SAIBA MAIS

Será que a internet das coisas poderá um dia estar no universo dos alimentos? Por exemplo, uma geladeira poderá reconhecer o prazo de validade dos produtos e já transmitir a informação para a central de logística do supermercado, que fará a entrega do produto mediante autorização do proprietário, que receberá a informação via app do celular.

A partir desta revolução, a tecnologia busca conectar equipamentos como eletrodomésticos, meios de transporte, roupas e outros dispositivos conectados à Internet. Para Moreiras (2014)9, esta conexão está acontecendo de forma integrada ao dia a dia das pessoas, disfarçada nos objetos do cotidiano, que, às vezes, passa despercebido.

Fonte: Adaptado de Moreiras (2014).

CONSIDERAÇÕES FINAIS

Chegamos ao final dos nossos estudos. Para fechar os assuntos, nesta unidade, estudamos um pouco mais sobre a tecnologia de computação em nuvem. Por meio da Computação em Nuvem, podemos usar outras ferramentas em qualquer lugar, independente de plataforma, por meio da internet com a mesma facilidade de tê-las instaladas em nossos próprios computadores.

Por meio da computação em nuvem é proporcionado a você, sendo um usuário comum ou avançado, recursos de armazenamento em discos virtuais, os quais podem auxiliar no controle e gerenciamento de seus arquivos, mantendo-os sempre atualizados e acessíveis. Esse serviço possibilita as empresas, além de armazenar na nuvem seus arquivos e backups, contratar espaço de processamento de servidores, eliminando hardware e reduzindo mão de obra.

Além da computação em nuvem, visualizamos que temos a virtualização, que está proporcionando às organizações a redução de custos e complexidade com o ambiente de TI, no tocante à aquisição e manutenção do mesmo. O serviço de virtualização tem se tornado um componente importante para o desenvolvimento de uma estratégia eficiente para a resolução dos desafios enfrentados

nos data centers, aproveitando ao máximo a capacidade do hardware, que muitas vezes fica ociosa em determinados períodos.

Dessa forma, esse aproveitamento possibilita fornecer ambientes de execução independentes a diferentes usuários em um mesmo equipamento físico. Nesse sentido, teremos uma economia de mão de obra de técnicos em informática que mantinham os data centers. Visualizamos também que existem vários tipos de virtualização, mas a função principal dessa tecnologia é separar aplicação e sistema operacional dos componentes físicos.

E, no último tópico, abordamos o conceito sobre a internet das coisas que a cada tempo proporciona à sociedade um novo serviço ou um novo dispositivo. A internet das coisas tem o intuito de que, cada vez mais, o mundo físico e o digital se tornem um só, indissociável e imperceptível, por meio de dispositivos que se comunicam entre si. Nos dias atuais, são muitos os objetos conectados, como geladeiras, óculos, elevadores e carros, mas temos a certeza de que a cada tempo teremos novos dispositivos, pois a cada dia a tecnologia apresenta inovações.



ATIVIDADES



1. A virtualização nada mais é que a simulação de algo virtual em um ambiente real, físico. Existem três tipos de virtualização: de hardware, de apresentação e de aplicativos. Assinale a alternativa correta:

- I. Para a virtualização de hardware é necessária uma máquina virtual e programas utilizados para esse fim.
 - II. Com a virtualização de aplicativos, as pessoas podem acessá-los sem ter a preocupação com bibliotecas ou drivers instalados.
 - III. Os programas mais utilizados para a virtualização são o VWWare, VirtualBox, Virtual P e Hyper-V para ambientes Unix.
 - IV. Um sistema operacional ou software pode ser instalado em um servidor e utilizado por várias pessoas, seria a virtualização de apresentação.
- a) Somente a I e II estão corretas.
 - b) Somente a II e III estão corretas.
 - c) Somente a I, II e IV estão corretas.
 - d) Todas estão corretas.

2. Computação nas nuvens ou *cloud computing* é um tema muito discutido atualmente. Seria a capacidade de se acessar arquivos e aplicativos por meio da internet em qualquer local que você estiver. Sobre a computação nas nuvens, assinale a alternativa correta.

- a) Pode-se utilizar um editor de documentos de texto bastando acessar a internet, não necessitando que seu computador tenha ele instalado.
- b) A computação nas nuvens não consegue compartilhar pastas, fotos, artigos ou trabalhos com outras pessoas.
- c) Não existe invasão de privacidade, já que tudo isso fica armazenado em um servidor na internet.
- d) Quando modificamos algum arquivo em nosso computador e, o mesmo precisa ser acessado pela computação das nuvens, ele não é atualizado corretamente.

ATIVIDADES



3. A virtualização pode proporcionar mais portabilidade e flexibilidade, permitindo assim que várias aplicações e sistemas operacionais diferentes executem em um mesmo hardware simultaneamente. Sendo assim assinale a alternativa incorreta:

- a) **Virtualização de servidores:** esse tipo de virtualização consiste em rodar vários sistemas operacionais na mesma máquina.
- b) **Virtualização de Apresentação:** também conhecida como virtualização de framework. Essa virtualização consiste na configuração dos desktops em uma infraestrutura centralizada virtualmente.
- c) **Virtualização de armazenamento:** devido à grande quantidade de dados que organizações e sociedade estão criando e armazenando, necessita-se cada vez mais de tecnologias que possam corroborar com a crescente demanda por armazenamento seguro destes dados, via local ou via web.
- d) **Virtualização de aplicação:** a técnica dessa virtualização consiste em ter uma cópia de determinado aplicativo (editores de textos, planilhas, entre outros), instalada em um servidor de forma virtual.
- e) **Virtualização de redes:** esse tipo de virtualização consiste na reprodução completa de uma rede física. Todavia, esta rede será de forma virtual, ou seja, lógica.

4. Em computação, a virtualização é uma forma de esconder as características físicas de uma plataforma computacional dos utilizadores, mostrando outro hardware virtual, emulando um ou mais ambientes isolados. Desta forma, assinale a alternativa correta de acordo com as afirmativas abaixo.

- I. Gerenciamento centralizado.
- II. Instalações simplificadas.
- III. Facilidade para a execução de backups.
- IV. Suporte e manutenção simplificados.
- V. Acesso controlado a dados sensíveis e à propriedade intelectual mantendo-os seguros dentro do data center da empresa.

- a) Apenas I e II estão corretas.
- b) Apenas II e III estão corretas.
- c) Apenas I está correta.
- d) Apenas II, III e IV estão corretas.
- e) Todas as alternativas estão corretas.

ATIVIDADES



5. A virtualização é um conceito que vem sendo muito aplicado ultimamente. Há diversos fatores que a tornam um diferencial, um exemplo prático é em relação a montar um Servidor ou até um data center. Independente do tamanho físico ou na nuvem, as máquinas virtuais estão ganhando cada vez mais espaço, transformando o panorama de TI e mudando a forma como as pessoas usam tecnologia. **Sobre o assunto, é correto afirmar que:**

- () As máquinas virtuais são obrigadas a operar sobre o mesmo tipo específico de hardware da máquina física.
- () O sistema operacional da máquina física fica comprometido em questões de segurança durante a virtualização.
- () Várias máquinas virtuais, com diferentes sistemas operacionais, podem funcionar simultaneamente sobre apenas uma máquina física.
- () Máquina física e máquina virtual devem utilizar o mesmo sistema operacional para evitar determinados conflitos.
- () A velocidade do processamento de uma máquina física é prejudicada consideravelmente durante o processo de virtualização o que torna inviável todo esse processo.



CINCO RISCOS DA CLOUD PÚBLICA QUE SUA EMPRESA NÃO PODE IGNORAR

Estamos sendo constantemente confrontados com os três tipos de riscos: o que sabemos que sabemos, o que sabemos que não sabemos, e o que desconhecemos.

Um dos maiores empecilhos para a adoção de computação em nuvem pública é o cálculo dos riscos conhecidos e desconhecidos. Passei os últimos anos contemplando essas questões, tanto como provedor de nuvem pública e quanto como usuário.

Aqui está uma lista de cinco riscos que qualquer empresa enfrenta como cliente de um serviço de nuvem pública.

1. Acesso compartilhado

Um dos princípios fundamentais da computação em nuvem pública é o modelo multitenancy, de uma única instância lógica compartilhada por centenas ou milhares de clientes. Em outras palavras, a típica arquitetura que permite a otimização de recursos de infraestrutura e software através de compartilhamento, mantendo os inquilinos, empresas/clientes, logicamente separados. É comum os clientes compartilharem os mesmos recursos de computação: CPU, armazenamento, espaço, memória, etc.

Pois bem, multitenancy é um desconhecido conhecido para a grande maioria de nós. Ou seja, algo que sabemos que não sabemos. Não só pelo risco de nossos dados privados vazando acidentalmente para outros inquilinos, mas também por conta dos riscos adicionais do compartilhamento de recursos. Vulnerabilidades multitenancy são muito preocupantes, porque uma falha pode permitir que outro inquilino ou atacante veja todos os outros dados ou assuma a identidade de outros clientes.

Várias novas classes de vulnerabilidades derivam da natureza comum da nuvem. Pesquisadores já foram capazes de recuperar dados de outros inquilinos no que era para ser um novo espaço de armazenamento. Outros pesquisadores já foram capazes de se intrometer na memória de outros inquilinos e em espaços de endereço IP. E alguns poucos foram capazes de assumir totalmente os recursos de outro inquilino simplesmente prevendo os endereços IP ou MAC que foram atribuídos a eles.

Questões de segurança multitenancy só agora estão se tornando importantes para a maioria de nós, com as vulnerabilidades começando a ser exploradas.

Arrisco dizer que multitenancy será um grande problema de segurança no longo prazo.

2. Vulnerabilidades virtuais

Cada provedor de serviços de cloud é um enorme usuário de virtualização. E cada camada de virtualização representa uma importante plataforma na infraestrutura de TI, com vulnerabilidades embutidas que podem ser exploradas. Servidores virtuais estão sujeitos aos mesmos ataques que atingem os servidores físicos, assim como novas ameaças estão explorando falhas do hypervisor.





Na minha opinião, há quatro principais tipos de riscos de exploração virtuais: apenas no servidor, "guest to guest", "host to guest", e "guest to host". Todos eles desconhecidos e não calculados na maioria das estimativas de risco.

Quando converso com provedores de nuvem sobre esses risco virtuais, muitos arregalam os olhos. A maioria afirma que os riscos são exagerados. Eu costumo dizer-lhes para verificar a lista de patches de seus fornecedores de software. Não são bonitas.

3. Autenticação, autorização e controle de acesso

Obviamente, os mecanismos de controle de autenticação, autorização e acesso do seu provedor de nuvem é fundamental. Quantas vezes ele procura e remove contas obsoletas? Quantas contas privilegiadas podem acessar seus sistemas - e seus dados? Que tipo de autenticação é necessária para os usuários privilegiados? A sua empresa compartilha um espaço comum com o vendedor e/ou com outros inquilinos?

Namepaces compartilhados e autenticação para criar experiências single-sign-on (SSO) podem aumentar a produtividade, mas também aumentam os riscos, substancialmente.

Certifique-se que os prestadores dos serviços de cloud computing limitam o acesso dos funcionários e as autorizações para o que seja estritamente necessário para a realização de sua tarefas.

Proteção de dados é outra grande preocupação. Se a criptografia de dados é usada e aplicada, as chaves privadas são compartilhadas entre os inquilinos? Quem e quantas pessoas na equipe do fornecedor de nuvem pode ver os seus dados? Onde os seus dados estão armazenados fisicamente? Como seu dado é tratado quando deixa de ser necessário?

Não tenho certeza de quantos fornecedores de nuvem estariam dispostos a compartilhar respostas detalhadas a estas perguntas, mas você tem que pelo menos perguntar se quiser saber o que é conhecido e desconhecido.

4. Disponibilidade

Quando você é um cliente de um provedor de nuvem pública, redundância e tolerância a falhas não estão sob seu controle. Geralmente o que é fornecido e como é feito, não são divulgados. São completamente opacos. Todo serviço de nuvem alega ter tolerância a falhas e disponibilidade fantásticas, ainda que, mês após mês, vejamos o maior e o melhor cair por terra, com interrupções de serviço por horas ou mesmo dias.

Uma preocupação ainda maior são os poucos casos em que os clientes perderam dados, devido a problema com o provedor de nuvem ou com ataques maliciosos. O fornecedor de nuvem geralmente afirma fazer backups dos dados dos clientes. Mas mesmo com os backups garantidos, clientes já perderam de dados - e de forma permanente. Se possível, a sua empresa deve sempre fazer o backup dos dados compartilhados na nuvem por conta própria. Ou se resguardar, em contrato, estabelecendo as responsabilidades do provedor por perdas de dados.





Tem mais. Alguns provedores de cloud computing dependem de terceiros para prestar determinados serviços. Um potencial cliente precisa saber identificar as interdependências potencialmente problemáticas. Considere um modelo de governança em que um fornecedor detém a responsabilidade global para as interrupções e as falhas de segurança.

[...]

Para saber mais veja o artigo na íntegra.

Fonte: ComputerWorld (2016, on-line)¹⁰.

MATERIAL COMPLEMENTAR



LIVRO

Cloud Computing – Computação em Nuvem

Cesar Taurion

Editora: Brasport

Sinopse: O termo Cloud Computing surgiu em 2006 em uma palestra de Eric Schmidt, do Google, sobre como sua empresa gerenciava seus data centers. Hoje Cloud Computing, ou Computação em Nuvem, se apresenta como o cerne de um movimento de profundas transformações no mundo da tecnologia.

Com a Computação em Nuvem a Internet passa a ser o repositório de arquivos digitais e as pessoas podem criar seus documentos, fotos e arquivos sem precisar instalar qualquer software em sua máquina.

A proposta deste livro é explorar e debater os principais aspectos de uso da Computação em Nuvem, suas potencialidades e restrições, suas tecnologias e aplicabilidades. O livro vai concentrar sua atenção nas aplicações e no uso prático no contexto dos usuários corporativos e seus desafios frente a este novo modelo computacional.

A Computação em Nuvem ainda tem muito a evoluir. Estamos todos aprendendo e este é o momento de conhecer um pouco mais seu conceito, suas tecnologias e suas formas de uso.



MATERIAL COMPLEMENTAR



NA WEB

Impacto que a Internet das Coisas terá nas nossas Vidas. Vamos conferir em dois vídeos que demonstram o impacto da internet das coisas, para a sociedade global. O primeiro, denominado como **The Social Web of Things** está disponível no link <<https://www.youtube.com/watch?v=i5AuzQXBsG4>>. Acesso em: 19 maio 2016. O segundo vídeo tem como título **Microsoft Office Labs Vision 2019**. E está disponível em: <https://www.youtube.com/watch?v=CfEi14_FQY>. Acesso em: 24 set. 2020.



NA WEB

Confira no site da Microsoft as recomendação que permitem você implantar uma ampla gama de soluções de computação de forma ágil. Disponível em: <https://azure.microsoft.com/pt-br/services/virtual-machines/?wt.mc_id=BR_ABG_EM_PD_SEM_GWT.srch=1&WT.mc_ID=SEM_jnG2lzt2>. Acesso em: 19 maio 2016.



NA WEB

Confira a entrevista de *Cesar Taurion* feita por Flávia Freire: ameniza as tempestades de questionamento sobre *Cloud Computing*. A entrevista está disponível no link: <<https://docplayer.com.br/463883-Cezar-taurion-ameniza-as-tempestades-de-questionamentos-sobre-cloud-computing-cezar-taurion.html>>. Acesso em: 24 set. 2020.



NA WEB

O site *computerworld* lista 19 serviços gratuitos de armazenagem em nuvem. Vale a pena conferir. O material esta disponível em <<http://computerworld.com.br/19-servicos-gratuitos-de-armazenagem-em-nuvem>>. Acesso em: 19 maio 2016.



NA WEB

Este vídeo dá uma compilação sobre a interface gesto, incluindo tela de toque, acelerômetro, luva virtual e sensor de visão. Eles são representados tanto na imaginação e realidade. Um fato surpreendente é que essa é uma interface que não se atreveria a imaginar há alguns anos e agora, se tornou realidade. O vídeo está disponível em <<https://www.youtube.com/watch?v=Pb0prRaJOqg&list=PL31EEA850C57ACF3C>>. Acesso em: 19 maio 2016.

REFERÊNCIAS

- ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: A survey. **Computer Networks.** v. 54, 2010, p. 2787–2805.
- CARISSIMI, A.; VERAS, M. **Virtualização de Servidores.** Rio de Janeiro: Escola Superior de Redes, 2015.
- DALKIR, K. **Knowledge Management in Theory and Practice.** Boston: Elsevier, 2005.
- LACERDA, F.; LIMA-MARQUES, M. Information architecture as a discipline: a methodological approach. In: RESMINI, A. (Org.) **Reframing Information Architecture.** Human–Computer Interaction Series. Switzerland: Springer, 2014.
- _____. Da necessidade de princípios de Arquitetura da Informação para a Internet das Coisas. **Perspectivas em Ciência da Informação.** V. 20, n.2, abr./jun. 2015, p.158-171.
- OLIVEIRA NETO, O.; FREITAS, R. C. **Computação em nuvens, visão comparativa entre as principais plataformas de mercado.** Trabalho de Conclusão de Curso. (Graduação em Sistemas de Informação). 24 f. Faculdade Integrada Estácio: Ceará, 2011.
- TAURION, C. **Cloud computing – computação em nuvem:** transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009.
- VELTE, A. T.; VELTE J. T.; ELSEMPER, R. **Cloud Computing:** Computação em Nuvem: Uma abordagem prática. Rio de Janeiro: Alta Books, 2012.

CITAÇÃO DE LINKS

¹<https://webinsider.com.br/wp-content/uploads/2012/07/ebusiness_brasil.pdf>. Acesso em: 19 maio 2016.

²< <http://www.hpl.hp.com/techreports/2009/HPL-2009-23.pdf>>. Acesso em: 19 maio 2016.

³<<http://pt.slideshare.net/pjandl/soii2015202virtualizacao>>. Acesso em: 19 maio 2016.

⁴<<http://redes-e-servidores.blogspot.com.br/2011/10/virtualizacao-iii.html>>. Acesso em: 19 maio 2016.

⁵<<http://www.usuarioroot.com.br/2013/01/o-que-e-virtualizacao.html>>. Acesso em: 19 maio 2016.

⁶<<http://www.fr.implico.com/BMV-Mineraloel-Versorgungsgesellschaft-mbH-optimise-ses-processus-de-distribution-et-d'administration/684.news.htm>>. Acesso em: 19 maio 2016.



REFERÊNCIAS

⁷<<https://www.techtudo.com.br/noticias/noticia/2014/08/internet-das-coisas-entenda-o-conceito-e-o-que-muda-com-tecnologia.html>>. Acesso em: 02 out. 2020.

⁸<<http://ssti1-1112.wikidot.com/ainternet-das-coisas>>. Acesso em: 19 maio 2016.

⁹<<http://cio.com.br/tecnologia/2014/02/04/ipv6-um-desafio-tecnico-para-a-internet/>>. Acesso em: 19 maio 2016.

¹⁰<<http://computerworld.com.br/cinco-riscos-da-cloud-publica-que-sua-empresa-nao-pode-ignorar>>. Acesso em: 19 maio 2016.



GABARITO

1. C
2. A
3. B
4. E
5. C



CONCLUSÃO

Enfim, concluímos nossa jornada de estudos. No decorrer do nosso livro, procuramos levar a você, dados e informações sobre os Fundamentos de Redes de Computadores, de forma a proporcionar o entendimento de como funciona uma rede, suas topologias, dispositivos, protocolos, modelos e camadas, segurança e computação nas nuvens. Esperemos ter esclarecido suas dúvidas e despertado em você a curiosidade e vontade de colocar o conteúdo em prática.

Para compreender melhor esse processo, na Unidade I, estudamos os fundamentos que circundam as redes de computadores existentes no mercado de trabalho, assim como suas topologias, com a finalidade de classificá-las quanto ao meio de transmissão.

Na sequência de nosso material, chegando à Unidade II, dedicamos os estudos sobre as conexões existentes, sejam elas com fio, sem fio, remota, infravermelho ou por bluetooth, bem como os tipos de protocolos mais utilizados em redes de computadores, como: UDP, TCP, DHCP, FTP, HTTP, SSL, SSH, DNS, SNMP. Para finalizarmos o tópico, trouxemos a você, uma introdução ao Modelo ISO/OSI com uma breve visualização das 7 camadas.

Completando os protocolos e modelos, na Unidade III, foram apresentadas as funcionalidades por completo das 7 camadas do Modelo OSI, sendo elas: Camada Física, Camada de Enlace de Dados, Camada de Rede, Camada de Transporte, Camada de Sessão, Camada de Apresentação e Camada de Aplicação.

Em nossa Unidade IV, abordamos a respeito dos principais conceitos de segurança em redes de computadores, passando pela criptografia, assinaturas digitais, tipos de ataques e como se defender. E, para finalizar esta unidade, discutimos um pouco a respeito de sistema operacional de redes.

E, como último tópico, na Unidade V abordamos sobre a computação em nuvem como serviço ou armazenamento, os tipos de virtualização e a famosa internet das coisas. Iniciamos uma discussão sobre a quebra do modelo tradicional de informática, saindo do mundo “físico” de enormes data centers para o mundo “virtual”, reduzindo custos com equipamentos e pessoas.

Com este material esperamos ter contribuído com informações que possam ajudá-lo na sua formação. Lembre-se que é muito importante manter-se atualizado sobre tais assuntos, visto que a dinâmica do mundo da tecnologia é extremamente veloz. Desejamos que você seja muito feliz profissionalmente utilizando os conceitos apresentados aqui e, se pudermos ajudar de alguma forma, estamos a sua disposição.

