ADMINISTRAÇÃO DE REDES LINUX

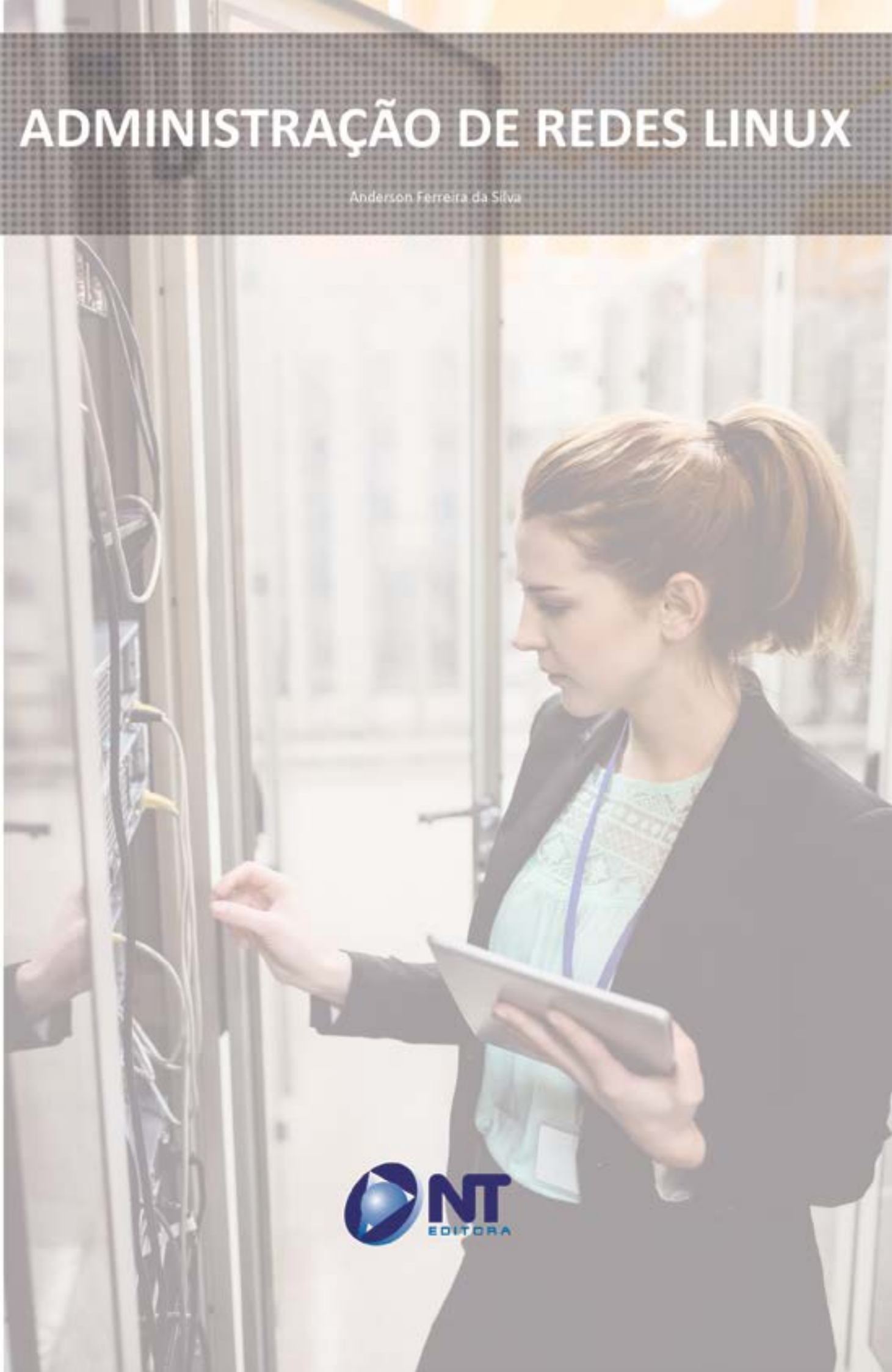
Anderson Ferreira da Silva

INFORMAÇÃO E COMUNICAÇÃO

NT EDITORA

ADMINISTRAÇÃO DE REDES LINUX

Anderson Ferreira da Silva



INFORMAÇÃO E COMUNICAÇÃO

NT EDITORA

Autor

Anderson Ferreira da Silva

Bacharel em Ciência da Computação pela Universidade Federal de Alagoas (UFAL) e Técnico em Informática pela Escola Técnica Federal de Alagoas (ETFAL, antiga CEFET, hoje IFAL). Possui especialização em Gestão de Segurança da Informação pela Universidade de Brasília (UnB) e em Banco de Dados pela Universidade Federal de Goiás (UFG), além de vários cursos na área de TI. Trabalha com sistemas Linux desde 1998, atuando como administrador de redes, em projetos com software livre na indústria e no governo federal e no desenvolvimento e na segurança da informação. Ministra, ainda, aulas de software livre, Linux e LibreOffice em indústria e órgãos públicos.

Design Instrucional
Luan Amoras Silva

Revisão
Filipe Lopes
Renata Kuhn

Editoração Eletrônica
Valter Luis Corrêa
Kaleo Amorim

Projeto Gráfico
NT Editora

Capa
NT Editora

Ilustração
Jésus André Santos

NT Editora, uma empresa do Grupo NT
SCS Quadra 2 – Bl. C – 4° andar – Ed. Cedro II
CEP 70.302-914 – Brasília – DF
Fone: (61) 3421-9200
sac@grupont.com.br
www.nteditora.com.br e www.grupont.com.br

Silva, Anderson Ferreira da.

Administração de redes Linux / Anderson Ferreira da Silva – 1. ed. reimpr. – Brasília: NT Editora, 2019.

268 p. il. ; 21,0 X 29,7 cm.

ISBN 978-85-8416-686-2

1. Administração de redes. 2. Servidores Linux.

I. Título.

ÍCONES

Prezado(a) aluno(a),
Ao longo dos seus estudos, você encontrará alguns ícones na coluna lateral do material didático. A presença desses ícones o(a) ajudará a compreender melhor o conteúdo abordado e a fazer os exercícios propostos. Conheça os ícones logo abaixo:

Saiba mais
Esse ícone apontará para informações complementares sobre o assunto que você está estudando. Serão curiosidades, temas afins ou exemplos do cotidiano que o ajudarão a fixar o conteúdo estudado.

Importante
O conteúdo indicado com esse ícone tem bastante importância para seus estudos. Leia com atenção e, tendo dúvida, pergunte ao seu tutor.

Dicas
Esse ícone apresenta dicas de estudo.

Exercícios
Toda vez que você vir o ícone de exercícios, responda às questões propostas.

Exercícios
Ao final das lições, você deverá responder aos exercícios no seu livro.

Bons estudos!

Sumário

APRESENTAÇÃO

Caro(a) aluno(a),

Seja bem-vindo(a) à **Administração de Redes Linux!**

A administração de uma rede de computadores abrange a tarefa de projetar, planejar, documentar, instalar e atualizar *softwares* e *hardwares* necessários para manter com segurança e eficiência os diversos serviços oferecidos pela rede de computadores.

Na execução de todas essas atividades, está o administrador de rede, que precisa ter um conhecimento de várias áreas (infraestrutura, *data center,* segurança, operação, rede LAN/WAN, entre outras) da computação. A depender da organização, essas várias áreas podem ser divididas, deixando um profissional de TI responsável por cada uma delas. No entanto, quando se trata de pequenas empresas, observa-se que apenas um administrador estará responsável pela chefia de todas essas áreas.

Quase todas as redes de computadores funcionam num misto de várias tecnologias, fazendo uso de diversos sistemas operacionais, em que alguns serviços e aplicações são executadas em Linux e outras no sistema operacional Windows, Unix, MacOS etc. Nesse cenário, é necessário que o profissional administrador de redes possua conhecimento sobre as várias tecnologias e serviços de infraestrutura de redes, bem como sobre a programação de computadores, para que tenha maior destaque no mercado de trabalho e facilidade no planejamento e na execução de suas atividades.

Dessa forma, neste livro, você conhecerá as principais aplicações e serviços a serem administrados em uma rede de computadores com sistema operacional Linux. Assim, será capaz de planejar, projetar e implantar uma rede de computadores com sistema operacional Linux e os *softwares* e serviços necessários para o seu funcionamento.

Isso se torna fundamental porque grande parte das redes de computadores de várias empresas faz uso do sistema operacional Linux em seus servidores. Muitas das aplicações que oferecem serviços de comunicação entre dispositivos em uma rede são executadas com esse sistema operacional Linux, como: serviço de distribuição de números IPs (DHCP), serviço de resolução de nomes (DNS), serviço de compartilhamento de arquivos (NFS e outros), serviço de aplicações *web*, entre outros. Muitos desses serviços são categoricamente adotados e recomendados pelos profissionais quando o assunto é administração de redes, sendo, portanto, fundamental conhecê-los.

Pensando nisso, elaboramos, para este material, parâmetros curriculares para que você possa:

- estudar os conceitos básicos e arquiteturas de redes de computadores para ter entendimento básico sobre os serviços e o funcionamento de uma rede;
- mostrar distribuições Linux que foram desenvolvidas prioritariamente para atuarem como servidor de rede para poder evitar ao máximo a customização trabalhosa de uma distribuição Linux como servidor de rede;
- instalar corretamente serviços de rede em plataforma Linux para manter uma rede segura e eficiente;
- explicitar os servidores de aplicações em plataforma Linux para gerenciar e manter sistemas *web* e outros, funcionando com rapidez e segurança;
- apresentar serviço de diretório com uso de ferramentas Linux para conseguir realizar diversas atividades que envolvem o uso de serviço de diretório, como autenticação de sistemas, dispositivos e outros;
- introduzir conceitos básicos e uso de aplicações em infraestrutura ágil para poder oferecer uma infraestrutura de TI, com sistema Linux, capaz de entregar *software* e serviços com agilidade, produtividade e confiabilidade.

Bons estudos!

DHCP: *Dynamic Host Configuration Protocol* é um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de *host*, máscara de sub-rede, *gateway* padrão, número IP de um ou mais servidores DNS, sufixos de pesquisa do DNS e número IP de um ou mais servidores WINS. Esse protocolo é o sucessor do BOOTP.

Ágil: é uma expressão que define um conjunto de novas metodologias utilizadas no desenvolvimento de *software* e infraestrutura de rede.

1 LINUX PARA SERVIDORES

Veremos, agora, o que são redes de computadores e suas classificações, mostrando diferentes tipos de conexões e seus protocolos. Aprenderemos sobre o vínculo entre servidores e usuários de rede, bem como sobre alguns *softwares* e *hardwares* para servidores.

Objetivos

Ao finalizar esta lição, você deverá ser capaz de:

- compreender os conceitos básicos e as arquiteturas sobre redes de computadores;
- conhecer a pilha de protocolos TCP/IP;
- entender o endereçamento IP;
- compreender os serviços de redes básicos fornecidos por sistemas operacionais Linux;
- conhecer distribuições Linux para servidores de rede.

1.1 Introdução às redes de computadores

Iniciaremos nosso estudo mostrando alguns conceitos sobre redes de computadores. É importante para o profissional responsável pela administração de uma rede de computadores conhecer e estar seguro sobre os conceitos básicos e fundamentais relacionados às redes de computadores.

Esse conhecimento, entre outros procedimentos e problemas que podem ser facilmente e rapidamente resolvidos quando o profissional de tecnologia da informação possui bons fundamentos teóricos, permite ao administrador:

- projetar de forma correta e eficiente uma rede de computadores;
- configurar corretamente determinado serviço ou *hardware* de rede;
- identificar e solucionar rapidamente problemas ocorridos na rede;
- interpretar corretamente *log*s e relatórios de tráfegos de rede.

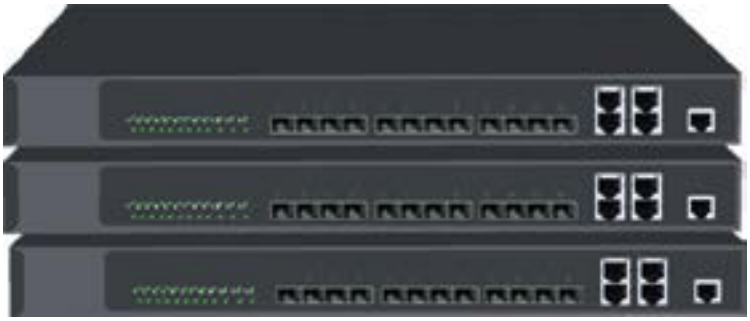
Aqui, faremos um resumo dos conceitos básicos sobre redes de computadores e das estruturas e tecnologias que as compõem.

Iniciando com o conceito de rede de computadores, podemos dizer, de forma resumida, que se trata de dois ou mais computadores que estão conectados por meio de alguma tecnologia (fibra ótica, cabo metálico, ondas eletromagnéticas e outras) e compartilham dados e/ou oferecem serviços e outros recursos entre si.

Cabo metálico: em redes de computadores, são usados cabos metálicos como meios de transmissão de dados.

Ondas eletromagnéticas: propagam-se em dois campos variáveis: um elétrico e outro magnético. Ao contrário das ondas mecânicas, as ondas eletromagnéticas, podem se propagar no vácuo.

Switch: é um dispositivo utilizado em redes de computadores para reencaminhar pacotes (*frames*) entre os diversos nós.



Segundo Tanenbaum (2011), redes de computadores são formadas por computadores autônomos que trocam informações entre si. A conexão entre esses computadores pode ser realizada por diversas formas: fios de cobre, fibra ótica e ondas de rádio. Ainda de acordo com Tanenbaum, nessas estruturas, são utilizados equipamentos concentradores denominados *switches* e outros para interligação dos computadores em uma rede, que podem ser do tipo cliente-servidor, o qual distribui as tarefas entre fornecedores de um recurso (servidores) e os requerentes dos serviços (clientes). Essas estruturas contam com uma forma lógica para se comunicar, denominada protocolo de comunicação.

Broadcast: refere-se a enviar um pacote que será recebido por todos os computadores ou qualquer ativo daquela rede.

A seguir, faremos uma classificação de redes quanto a vários aspectos, dos quais muitos deles você talvez já tenha lido a respeito, que são: extensão geográfica, topologia, meio de transmissão e compartilhamento de dados.

Camada de rede : a camada de rede do modelo OSI é responsável por controlar a operação da rede de um modo geral.

Extensão geográfica

A extensão geográfica considerada em uma rede de computadores é quando os dispositivos interconectados se encontram concentrados em uma mesma área geográfica. Como exemplos dessas redes, podemos citar:

- *Lan Area Network* (LAN), ou apenas rede local – são as redes de alcance local, consideradas as redes internas, como a rede de uma empresa instalada em um único edifício ou mesmo a rede de um pequeno campus universitário. Algumas literaturas colocam um alcance máximo para uma LAN, como de até 10 km. Já outros autores, como Kurose (2013), consideram que uma LAN é uma rede na qual seus nós (o mesmo que computadores ou outros dispositivos interconectados) compartilham um canal de *broadcast*, sem a intervenção de roteamento de camada de rede para interconexão desses nós locais;
- *Metropolitan Area Network* (MAN), ou apenas rede metropolitana – são consideradas as redes que se interligam em áreas geográficas maiores que as LANs, de forma a se encontrarem em regiões metropolitanas diferentes. Por vezes, é comum administradores de rede tratarem LAN e MAN como um mesmo tipo de rede ou apenas uma LAN;
- *Wide Area Network* (WAN), ou apenas rede de longa distância – são as redes de grande extensão, interligando diversas redes independentes e, em geral, de alcance mundial. O melhor exemplo de uma WAN é a internet, uma rede de computadores que interconecta milhares de dispositivos computacionais ao redor do mundo.

Saiba mais

Dos três tipos de redes citados acima, atualmente, já podemos dizer que temos as três variantes dessas para as redes sem fio, que seriam: WLAN, WMAN e WWAN. O W acrescentado na sigla de todas essas redes quer dizer *wireless*, ou sem fio, em português.

No sistema operacional Linux, temos o comando *ifconfig* (do pacote net-tools, disponível nas distribuições Debian até a versão 8.0), que é usado, geralmente, para configurar os dispositivos de rede cabeada. Para configuração de dispositivos de rede sem fio, o Linux disponibiliza o comando *iwconfig* e outros, do pacote wireless-tools (*iwconfig*, *iwevent*, *iwgetid*, *iwlist*, *iwpriv* e *iwspy*.).

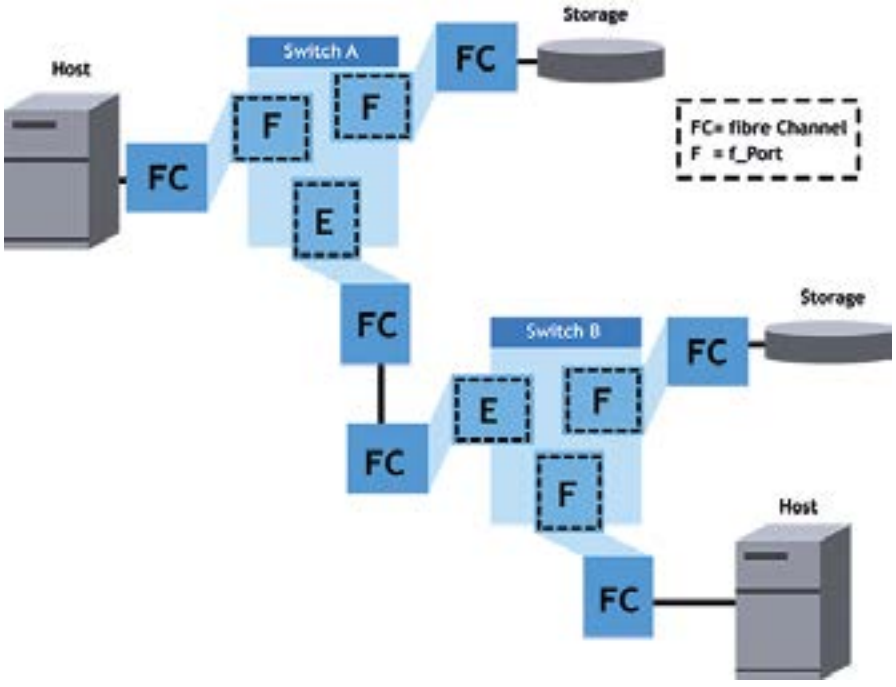
O padrão de rede sem fio instituído pelo *Institute of Electrical and Eletronics Engineers* (IEEE) é o 802.11. É importante para o administrador de rede conhecer alguns desses números, padrões da IEEE, das principais e mais atuais tecnologias, pois isso agiliza a busca de informações, bem como o seu entendimento sobre o assunto.

A seguir, veja outros tipos de redes:

- *Personal Area Network* (PAN), ou apenas rede de área pessoal – são redes nas quais seus dispositivos estão interconectados dentro de uma distância bastante reduzida, como redes que funcionam com tecnologia *bluetooth*.
- *Storage Area Network* (SAN), ou rede de área de armazenamento – são redes destinadas, em geral, à interconexão de servidores de redes (ou outros dispositivos) com servidores de armazenamento (*storage*). Em geral, empresas que possuem *storage* em seu *data center*, a depender do tamanho do seu parque tecnológico, fazem uso de uma rede SAN para ganho de eficiência, desempenho, flexibilidade, disponibilidade e escalabilidade entre seus servidores de rede e o *storage*, uma vez que muitas desses redes são construídas e implementadas com arquitetura de *fibre channel* (RFC 4044, 3643, 2837 e 2625). Essa tecnologia foi desenvolvida exclusivamente para sistemas de armazenamento em rede SAN, interligando servidores com *switches*, *storage* e outros dispositivos. A arquitetura *fibre channel* possui uma série de conceitos e padrões, como diversas topologias próprias (*point-to-point* – FC P2P; *arbitrated loop* – FC AL; *switched fabric* – FC SW), protocolos (FCP, FCIP, iFCP, FCoE e iSCSI) e várias outras características.

Apesar da grande quantidade de empresas que estão migrando seus *data centers* para um ambiente em nuvem, ainda existe bastante demanda de profissionais que possuam bons conhecimentos, certificados e experiência em trabalhar com vários tipos de redes, como a rede SAN, tanto para pequenas empresas quanto para grandes corporações que oferecem serviço de computação em nuvem, especificamente em armazenamento.

Arquitetura *Fibre Channel* de uma rede SAN



***Bluetooth*:** tecnologia usada para conectar e trocar informações entre dispositivos próximos.

***Storage*:** é um equipamento que armazena os dados da rede local de uma empresa ou residência, podendo ser um simples HD até um sistema de armazenamento com vários *petabytes*.

***Data center*:** é um local físico onde ficam, geralmente, os servidores de rede, *storage*, sistemas de telecomunicações e outros ativos de rede de uma empresa ou organização.

Topologia

A topologia de uma rede refere-se a como os dispositivos estão organizados fisicamente e logicamente. Na topologia física, temos o layout da rede, que é a sua configuração espacial e como verdadeiramente ela está organizada. Na topologia lógica, por outro lado, temos como os dados estão trafegando através da rede ou de seus meios de comunicação.

Os principais tipos de topologias podem ser, assim, descritos:

- barramento – é o tipo de topologia mais simples e praticamente em desuso nas redes de computadores. Sua organização constitui-se unicamente de uma linha de transmissão para todos os computadores, em geral por meio de um cabo coaxial. Essa topologia apresenta fácil instalação, mas bastante vulnerável, pois, caso algum ponto falhe, toda a rede será afetada;
- anel – aqui, os dispositivos estão organizados em forma de anel se comunicando um de cada vez e formando um circuito fechado. Nesse tipo de topologia, a comunicação é gerenciada entre os computadores e realizada de modo unidirecional, em uma só direção, passando de computador a computador até atingir o destino;
- estrela – refere-se à topologia em que os computadores estão conectados a um dispositivo central, denominado concentrador, que pode ser um *switch*, roteador ou outros. Esse é o tipo de topologia mais usada atualmente, pois esse tipo de organização facilita a manutenção da rede, podendo adicionar ou remover facilmente um nó da rede, além de que, caso um ponto falhe, este não afetará o resto da rede;
- malha ou *mesh* – é considerada uma evolução da rede em estrela, em que, na topologia em malha, vários computadores ou concentradores passam a se comportar como uma única grande rede, correspondendo a várias conexões ponto a ponto.

Ethernet: é uma arquitetura de interconexão para redes locais - Rede de Área Local (LAN) - baseada no envio de pacotes.

Token Ring: é um protocolo de redes que opera na camada física e de enlace (ligação de dados) do modelo OSI dependendo da sua aplicação.

As topologias apresentadas acima referem-se especialmente à topologia física. Lembrando que a topologia lógica diz respeito a como os dados são transmitidos ao longo da rede, assim, numa determinada organização de uma rede, teremos sua topologia física e lógica. Para a topologia lógica, podemos citar as mais conhecidas: ethernet, *Token Ring* e FDDI. Para cada uma dessas topologias, têm-se várias características, como tratamento de erros, princípio de transmissão, tipos de colisões, tipos de cabos usados para transmissão e velocidades.

O padrão ethernet (IEEE 802.3) é a topologia mais conhecida e, ainda, a mais usada. Na arquitetura de ethernet, os computadores estão interconectados na rede com base no envio de pacotes. Na comunicação dos computadores em uma rede ethernet, os pacotes estão sujeitos a protocolos de controle de acesso ao meio.

Existe uma variedade de tipos de rede ethernet, que podem ser quanto à velocidade, ao alcance e aos tipos de cabos usados. Desde o início, com as redes 10 Mbps; em seguida, com as redes *fast* ethernet, com velocidades de 100 Mbps; e, posteriormente, as redes *gigabit* ethernet (1000 Mbps) e as 10-gigabit ethernet, com velocidades de até 10 Gbps e que podem suportar até 40 km com uso de fibra monomodo.

10 Mbps: padrão da Ethernet, que especifica uma velocidade do dispositivo de 10 megabits por segundo.

Meios de transmissão

Como componente essencial para funcionamento das redes, temos os meios de transmissão, nos quais os mais comuns, por muito tempo, foram os cabos, mas, hoje, as ondas de rádio têm sido bastante usadas, principalmente em pequenas redes, devido à sua fácil instalação e à eliminação de cabeamento.

Como meios de transmissão, podemos citar:

- cabo coaxial;
- cabo de fibra óptica;
- cabo par trançado, que pode ser blindado (STP) ou normal (UTP);
- redes por radiação eletromagnética, que podem ser ondas de rádio, micro-ondas, infravermelho e outras.

Fast ethernet: é um termo para vários padrões da Ethernet que levam o tráfego de dados à taxa nominal de 100 Mbps, contra a taxa de transmissão de 10 Mbps da Ethernet original.

Compartilhamento de dados

Quanto ao tipo de compartilhamento, os dois principais tipos de rede são:

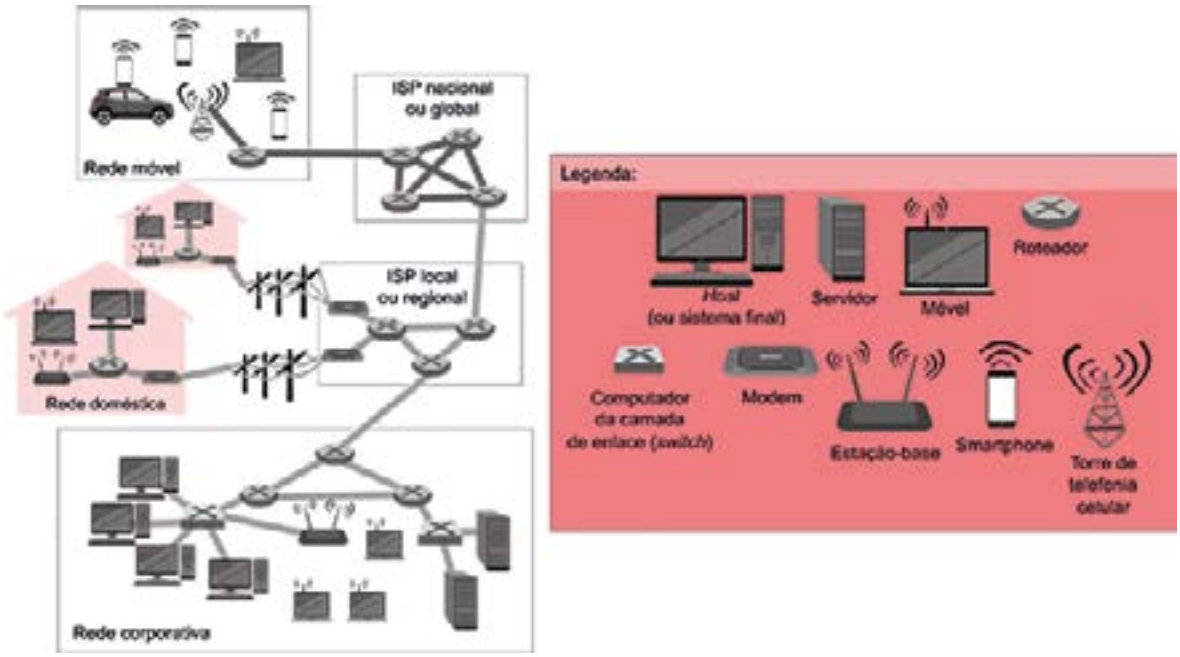
- cliente-servidor – é o tipo de rede mais usado nas empresas. Nesse tipo de rede, têm-se um servidor e as estações ou mesmo outros servidores, considerados clientes, que fazem uso dos serviços ou compartilhamentos do servidor;
- *peer-to-peer* – é o tipo de rede em que o compartilhamento de informações entre os computadores é realizado por meio de uma rede ponto a ponto.

STP: *Spanning Tree Protocol* é um protocolo para equipamentos de rede que permite resolver problemas de *loop*, auxiliando na melhor performance da rede.

Importante

Nesta lição, buscamos abordar, de forma resumida, alguns dos principais e mais usuais conceitos de redes de computadores. Alguns outros tópicos e conceitos básicos sobre redes de computadores serão abordados nas próximas lições, sempre que for necessário. Um estudo mais profundo e completo sobre o vasto mundo das redes de computadores, os tipos, as estruturas, as organizações e as demais características fogem do escopo desde livro.

A seguir, é mostrada uma figura que ilustra bem os vários tipos de redes, meios de transmissão e componentes, conforme o que descreve Kurose (2013).



A figura mostra exatamente como hoje todos nós estamos conectados à internet, seja quando estamos no ambiente de trabalho (rede corporativa), em nossa residência (rede doméstica) ou, ainda, passeando ou fazendo compras (rede móvel). Todas essas redes, para acesso à internet, estarão sempre conectadas a um *Internet Service Provider* (ISP), ou provedor de serviço de internet.

Na primeira nuvem acima, considerando de cima para baixo, temos uma rede móvel, na qual os aparelhos móveis (celular, notebook, smartphone e outros) recebem o sinal de internet diretamente de uma torre de telefonia de celular, a qual, por meio de um comutador de camada, que pode ser um *switch* camada 3 ou um roteador, conecta-se a um ISP nacional ou global. Perceba que o meio de transmissão entre o computador e o primeiro comutador da rede ISP parece ser uma fibra ótica, e esta demonstra ser lançada de forma subterrânea, diferentemente da rede doméstica, que também parece usar cabo (provavelmente fibra ótica) lançado em modo aéreo com o uso de postes.

Na torre de telefonia de celular, na rede móvel mostrada na figura, poderia também ser implementada a tecnologia WiMax, ou seja, uma rede sem fio de longo alcance usada, geralmente, para ambientes externos. Nesse caso, na torre de telefonia de celular, deveríamos ter antenas de transmissão de ondas de rádio para irradiar o sinal do serviço de internet para os dispositivos móveis, algo semelhante ao que fazem as antenas de celular, mas, no caso da rede WiMax, você ou sua empresa poderiam implementar de forma mais fácil e barata, sem necessidade de contrato com uma operadora de celular.

ISP: *Internet Service Provider* (em português, Provedor de Serviço de Internet), é uma organização que oferece serviços de acesso, participação ou utilização da internet.

Comutador de camada: dispositivo utilizado em redes de computadores para reencaminhar pacotes (*frames*) entre os diversos nós.

WiMax: especifica uma interface sem fio para redes metropolitanas (WMAN).

Na rede doméstica, temos uma LAN com mais alguns outros dispositivos, como modem, e uma estação base, que pode ser um *access point* e um roteador. Em geral, atualmente, o que temos nas residências, em especial dos centros urbanos, é um só equipamento substituindo o roteador, o modem e o *access point*, em que todas essas três tecnologias passam a ser embutidas em um só aparelho.

Por fim, na rede corporativa mostrada na figura, temos dois principais novos dispositivos, que são os *switches* de enlace (*switch* de camada 2 ou L2) e os servidores de rede. Os *switches* são justamente para organizar nossa rede, de forma fácil e eficiente, e garantir que todos os dispositivos da rede possam ter acesso ao serviço de intranet e internet. Já os servidores de rede podem oferecer vários serviços à rede e compartilhá-los, como a distribuição de endereçamento IP e serviços de correio eletrônico, de armazenamento de dados, de serviço de diretório e outros que serão discutidos mais adiante neste livro.

Exercitando o conhecimento

Informe que tipo de topologia física e lógica, respectivamente, pode-se definir na nuvem das figuras, a anterior e a seguir, na parte em que mostra o *switch* L2 (*layer* 2) conectado nas estações de trabalho.

a) Anel e *Token ring*.

b) Árvore e FDDI.

c) Estrela e ethernet comutada.

d) Barramento e ethernet compartilhada.

Rede corporativa

Comentário: a alternativa correta é a letra "c". A topologia física em estrela e os dispositivos, ou nós, estão ligados a um concentrador, seja *switch*, roteador ou outro. Já na topologia lógica, a resposta poderia ser apenas ethernet. Como as alternativas citaram ethernet comutada e compartilhada, a correta é a comutada, pois esse tipo de rede é diferente da compartilhada, principalmente pelo uso de *switch* e não *hub*, em que o uso de *switch* reduz o número de colisão entre os pacotes transmitidos, obtendo uma melhor eficiência na rede.

FDDI: redes que adotam uma tecnologia de transmissão idêntica às das redes *Token Ring*, mas utilizando cabos de fibra óptica como meios de transmissão.

***Hub*:** é um concentrador de rede pelo qual se transmite ou difunde determinada informação para muitos receptores ao mesmo tempo (*broadcast*).

1.2 Protocolos TCP/IP

Neste tópico, iremos trazer alguns dos principais protocolos usados no modelo de referência de protocolo de controle de transmissão/protocolo da internet (TCP/IP). O intuito é partimos para a parte mais prática sobre os protocolos e serviços de rede, passando de forma breve sobre a teoria dos modelos de referência, o TCP/IP e a interconexão de sistemas abertos (OSI). Ambos os modelos referem-se a como um determinado dispositivo de rede funciona ao se comunicar numa rede de computadores. Daremos preferência ao modelo TCP/IP para explicação sobre os protocolos e serviços.

Protocolos

Protocolo pode ser definido como o conjunto de regras e instruções bem definidas que possibilitam a conexão e comunicação entre dois ou mais ativos de redes.

Alguns protocolos de rede

Protocolo	Descrição
DHCP	*Dynamic Host Configuration Protocol* é um protocolo que possibilita a configuração dinâmica de *hosts*, com a atribuição de endereços IP de outros parâmetros de configuração para os clientes de rede.
NTP	*Network Time Protocol* é um protocolo para sincronização dos relógios dos *hosts*, definindo parâmetros para que os computadores sincronizem seus relógios, baseados em uma fonte confiável de tempo.
SMTP	*Simple Mail Transfer Protocol* é o protocolo usado para envio de e-mails.
POP3	*Post Office Protocol* é um protocolo usado para acesso remoto a uma caixa de correio eletrônico.
IRC	*Internet Relay Chat* é um protocolo utilizado para conversação (chat) e troca de arquivos, possibilitando a conversa em grupo ou privada.
FTP	*File Transfer Protocol* é um protocolo usado para transferência de arquivos.
HTTP	*HyperText Transfer Protocol* é um protocolo de comunicação utilizado para sistemas de hipermédia distribuídos e colaborativos.

FTP: *File Transfer Protocol*, é um protocolo para transferência de arquivos, que funciona na porta 20 e 21.

***Middleware*:** *software* de computador que fornece serviços para aplicações de *software* além daqueles disponíveis pelo sistema operacional.

Serviços

Serviço em rede de computadores é definido aqui como determinada tarefa sendo executada por uma aplicação entre dois ou mais ativos de rede. Por exemplo, um computador executando uma aplicação de DNS fornece o serviço de DNS para vários clientes, possibilitando a resolução de nomes em endereços IPs.

Esses serviços são formados, em geral, pelas seguintes partes:

- servidor – *host* que executa a parte principal do serviço;
- cliente – aquele que solicita e faz uso do serviço de rede, por exemplo, um navegador *Web* que acessa os serviços de páginas da internet;
- protocolo – o serviço de fato, como explicado anteriormente, é o protocolo, com seus conjuntos de instruções, que define a operação a ser realizada em dois ou mais ativos;
- *middleware* – suporte que permite a execução e comunicação do serviço, garantindo o encaminhamento dos pedidos do cliente ao servidor e vice-versa.

Existem vários tipos de serviços de rede para as mais diversas finalidades. Eles usam, em geral, os protocolos TCP e/ou UDP como suporte de comunicação. Ainda, os serviços possuem uma determinada porta de comunicação para operarem, embora os números das portas possam ser alterados em suas configurações, estes possuem números predefinidos, conforme a tabela que segue.

Serviços, portas e suporte de comunicação

Serviço	Porta	Transporte
Servidor FTP (porta de dados e de controle)	20 e 21	TCP
Servidor DNS	53	UDP

Servidor *Telnet*	23	TCP
Servidor HTTP	80	TCP
Servidor SSH	22	TCP
SNMP	161 e 162	UDP
Servidor *BOOTP*/DHCP	67	UDP
Servidor NTP	123	TCP/UDP

Modelos de referência da arquitetura de rede

No modelo OSI, temos sete camadas. É um modelo de referência que pode ser adotado para definirmos os serviços de rede em camadas de determinado equipamento, como no caso de redes corporativas, em que são usados um *switch* L2 ou *layer* 2 – referindo-se a um equipamento que funcione até a camada 2 (*enlace*) do modelo OSI.

Essa divisão em camadas é adotada devido a várias vantagens, uma vez que essa estrutura, segundo Silva (2017):

- decompõe os ativos de rede em partes menores e mais simples;
- padroniza os ativos de rede, desenvolvidos por vários fabricantes;
- facilita o aprendizado e a compreensão do funcionamento das redes e seus ativos, estando divididos em partes menores (camadas);
- mostra como tipos diferentes de *hardware* e *software* de rede conseguem se comunicar facilmente.

Ainda, as camadas do modelo OSI são divididas em: aplicação, apresentação, sessão, transporte, rede, enlace e física. No modelo TCP/IP, a pilha de protocolos ou camadas se divide em cinco [ou quatro, segundo alguns autores, pois excluem a física], que são: aplicação, transporte, rede, enlace e física. As funções de várias dessas camadas são semelhantes às do modelo OSI.

A seguir, é mostrada a tabela comparativa entre os dois modelos, suas camadas, seus protocolos e alguns equipamentos e *softwares* que trabalham na referida camada.

Comparativo modelo OSI e TCP/IP

Modelo OSI	TCP/IP	Protocolos	Equipamento ou *software*
Camadas 7, 6 e 5	Aplicação	DNS, DHCP, NTP, SNMP, HTTPS, FTP, SSH, *Telnet*, HTTP, POP3 e outros	Servidores *Web*, Servidores de correio eletrônico, *browser* ou navegadores de internet e outros.
Camada 4	Transporte	TCP e UDP	*Gateway* e outros
Camada 3	Rede	IP, ICMP, IGMP e outros	Roteador, *Firewall*, *Switch* L3 e outros
Camada 2	Enlace	ARP (MAC), RARP e outros	*Bridge*, *Switch L2 e* outros
Camada 1	Física	Ethernet, *token ring* e outros	*HUB*, *USB*, *Bluetooth* e outros

SSH: protocolo de rede criptográfico para operação de serviços de rede de forma segura sobre uma rede insegura

OSI: o modelo OSI permite a comunicação entre máquinas heterogêneas e define diretivas genéricas para a construção de redes de computadores.

TCP/IP: conjunto de protocolos de comunicação entre computadores em rede.

IGMP: *Internet Group Management Protocol* é um protocolo cuja função é controlar os membros de um grupo de *multicast* IP, controlando a entrada e a saída de *hosts* deles.

Vamos, agora, ver uma breve explicação das camadas mostradas na tabela anterior, considerando o modelo TCP/IP.

RJ45: é um conector modular usado em terminações de telecomunicação e são usados normalmente em cabo par trançado.

IPv6: é a versão mais atual do protocolo de internet (IP)

Camada física

A camada física, ou camada 1, refere-se a tensão, sinais elétricos e conexões mecânicas. A maioria das redes, atualmente, faz uso de cabos UTP de categoria 5 ou superior e conectores RJ45.

Dispositivos como repetidores e *hubs* fazem parte dessa camada. Em geral, não é possível usar um *software* para verificar um repetidor ou *hub* na rede. A única coisa que esses dispositivos estão realizando é a amplificação de sinais elétricos em cabos.

Existem os *hubs* passivos, que são amplificadores multiportas de um sinal elétrico para todas as outras conexões, e os *hubs* ativos, que fazem isso lendo e retransmitindo bits, sem interpretar qualquer significado desses bits.

Camada de enlace

Cada camada possui um nome específico para os dados que são trabalhados. Na camada de enlace, temos os quadros. Na camada 2, encontramos tecnologias como a ethernet, em que cada placa de rede é identificável por um endereço MAC exclusivo de 48 bits.

Nessa camada, possuímos ainda dispositivos como pontes (*bridges*) e *switches*. Uma ponte é mais inteligente do que um *hub*, uma vez que pode tomar decisões com base no endereço MAC de placas de redes (ou *interface* de rede). Um *switch* também entende endereços MAC.

Camada de rede

Na camada de rede, ou camada 3, ou ainda camada de internet, temos os pacotes IP. Essa camada fornece a cada dispositivo de rede um endereço IP exclusivo de 32 bits.

O *Internet Protocol*, ou protocolo de internet (IP), não é o único protocolo nessa camada, pois existem, também, ICMP, IGMP, IPv6 e outros. Num sistema Linux, uma lista completa de protocolos pode ser encontrada no arquivo */etc/protocols*.

Nessa camada, encontramos dispositivos como roteadores e *switches* de camada 3 (L3) que reconhecem [e possuem] endereços IPs.

Camada de transporte

A camada de transporte, ou camada 4, é responsável por receber os dados da camada de aplicação (próxima camada a ser vista) e enviá-los para camada de internet (camada acima). Nessa camada, temos os protocolos TCP, responsáveis por um transporte seguro de pacotes entre origem e destino, e o UDP, responsável por um transporte inseguro.

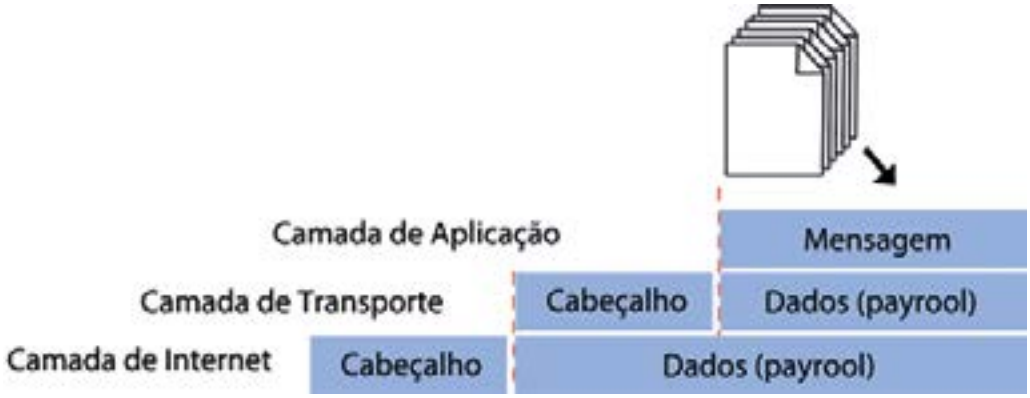
Saiba mais

TCPs são os protocolos sob os quais a internet é baseada. Ele é complementado pelo protocolo da internet, sendo normalmente chamado de TCP/IP. O UDP, por sua vez, é o protocolo da camada de transporte que permite que a aplicação envie um datagrama encapsulado num pacote IPv4 ou IPv6 a um destino sem qualquer garantia de que o pacote chegue corretamente (ou de qualquer modo).

Camada de aplicação ou camadas 7, 6 e 5 (no modelo OSI)

A camada de aplicação no modelo TCP/IP refere-se às três últimas camadas do modelo OSI (seção, apresentação e aplicação). Essa camada permite o desenvolvimento e a utilização de aplicações pelo usuário, possuindo vários protocolos e serviços, como: SMTP (para correio eletrônico), FTP (para transferência de arquivos), DNS (para resolver nomes), HTTP (para serviço *web*), entre outros.

No sistema Linux, você poderá encontrar vários serviços, protocolos e número da porta no arquivo */etc/services*.



Dos protocolos citados acima, reforçamos os principais que o administrador de rede deve melhor conhecer:

- IP – o *Internet Protocol* define o encaminhamento de pacotes de dados de um comutador para outro (RFC 791). Considerando a pilha de protocolos TCP/IP, o IP está definido na camada de rede, portanto, a maioria dos equipamentos de rede consegue entender os pacotes IPs. Endereçamento IP será algo bastante trabalhado por um administrador de rede. Em quase todos os serviços de rede, iremos precisar atribuir ou realizar algum procedimento com endereçamento IP, seja na sua versão 4 (mais usada) ou na versão 6. Ainda nesta lição, veremos mais detalhes sobre endereçamento IP;
- ICMP – o *Internet Control Message Protocol* é o protocolo que define vários tipos de suporte de baixo nível para o IP, incluindo mensagens de erro, assistência de roteamento e ajuda de depuração (RFC 792). Talvez você já deva ter "pingado" uma máquina, ou seja, executado o comando *ping* para verificar se determinado computador estava ligado ou usando certo endereço de IP. Saiba que, ao realizar um comando *ping*, você está enviando pacotes ICMP na rede;

Ping: utilitário que usa o protocolo ICMP para testar a conectividade entre equipamentos.

ARP: protocolo de resolução de endereços, que mapeia um endereço de um endereço físico.

Datagrama: unidade de dados de protocolo de um bloco de dados da camada de rede no modelo OSI.

Full-duplex: tipo de comunicação com dispositivo transmissor e receptor, podendo transmitir dados simultaneamente em ambos os sentidos (transmissão bidirecional).

SMTP: programa que envia e-mails de um computador local para um *host* de correio configurado (*mailhub*).

- ARP – o *Address Resolution Protocol* converte os endereços IP em endereços de *hardware* (endereço físico ou MAC) (RFC 826). Lembra-se do *switch* L2? Esse equipamento funciona até a camada de enlace (modelo TCP/IP ou OSI) com o encaminhamento de pacotes, na LAN, de acordo com o endereço MAC. Esse *switch* não conseguirá trabalhar com protocolos de camadas superiores, como os TCP, DHCP, DNS e outros. Assim, quando tiver que instalar um equipamento concentrador em uma rede, em que este precise realizar roteamento e distribuição de IP (serviço de DHCP), você logo descartará um *switch* L2, pois este só funcionará até a camada de enlace;
- UDP – o *User Datagram Protocol* implementa a entrega de dados não orientados à conexão (RFC 768). O UDP é um protocolo da camada de transporte e bastante simples, além disso, não fornece controle de erros (o que citamos como um protocolo não orientado à conexão) nem garantia de que as mensagens serão entregues, mas é considerado um protocolo rápido e, por isso, é usado em muitos sistemas que necessitam de *performance*. Ele não se preocupa tanto com a entrega completa dos dados, como aplicações de vídeo e áudio, uma perda mínima de pacotes não prejudicará o entendimento da mensagem. Alguns protocolos que funcionam com UDP são: DNS, DHCP, SNMP e outros.

Importante

Lembre-se de que o protocolo UDP é da camada de transporte, e, quando citamos que outros protocolos fazem uso do UDP para se comunicarem na rede, queremos dizer que sua mensagem será "encapsulada" dentro desse protocolo de transporte, para, então, ser enviada. Por exemplo, uma mensagem de DNS é enviada dentro de um datagrama UDP, na porta 53. Tendo esse entendimento claro sobre o funcionamento do tráfego na rede, isso o ajudará a resolver problemas, aplicar procedimentos e configurações, bem como a ter uma leitura clara de registros de *dumps* sobre dados de rede.

- TCP – o protocolo de controle de transmissão implementa uma comunicação confiável na rede, com controle por fluxo e orientado à conexão (RFC 793). Diferentemente do UDP, o TCP fornece o controle de erros nas trocas de mensagens na rede e garante o envio da mensagem. É um protocolo considerado confiável e *full-duplex*, usado quando se deseja ter a certeza da entrega da mensagem, mesmo que ocorra um pouco da perda de eficiência. Alguns dos protocolos que usam prioritariamente TCP são: FTP, *Telnet*, SMTP, HTTP, IMAP, POP3 e outros.

Saiba mais

Veja a definição de algumas dessas siglas:

- *Telnet* – é um protocolo de rede utilizado na internet ou nas redes locais para proporcionar uma facilidade de comunicação baseada em texto interativo bidirecional usando uma conexão de terminal virtual;
- SMTP – *Simple Mail Transfer Protocol*, ou protocolo de transferência de correio simples, é o protocolo padrão para envio de e-mails através da internet;
- IMAP – *Internet Message Access Protocol*, protocolo que gerencia o correio eletrônico. Utiliza, por padrão, as portas TCP 143 ou 993;
- POP3 – *Post Office Protocol*, ou protocolo dos correios, versão 3, é o protocolo utilizado no acesso remoto a uma caixa de correio eletrônico.

Como administrador de rede, se trabalhar com *firewall*, muito provavelmente deverá realizar algumas políticas de bloqueio de tráfego, tendo que bloquear ou liberar pacotes que trafegam tanto em UDP quanto em TCP.

Endereço IP

O endereço IPv4 (IP versão 4) ainda é o método padrão para atribuir um endereço único de um ativo de rede na internet ou intranet (rede interna). O IPv4 é um endereço de 32 bits, composto de quatro campos de 8 bits, divididos por um ponto. Os primeiros campos identificam o endereço da rede e restante o dispositivo de rede. Com o IPv4, podemos ter 4,29 bilhões de endereços diferentes.

Exemplo de endereço IPv4 e sua forma binária:

10.98.1.1 = 00001010.01100010.00000001.00000001

Existem 5 classificações de redes definidas pelos endereços IP. Essa classificação é dividida em classes, conforme mostra a tabela seguinte.

Classes dos endereços IPv4

Classe do endereço	Faixa do endereço IP
A	0.0.0.0 a 127.255.255.255
B	128.0.0.0 a 191.255.255.255
C	192.0.0.0 a 223.255.255.255
D	224.0.0.0 a 239.255.255.255
E	240.0.0.0 a 247.255.255.255

Essa versão 4 do IP já não está sendo suficiente para endereçamento de todos os ativos existentes, considerando que atualmente todos os aparelhos eletrônicos podem ser conectados em uma rede, como celulares, tablets, impressoras, televisores e, até mesmo, geladeiras, cafeteiras e outros aparelhos. Pensando nesse esgotamento de endereços IPv4, várias tecnologias estão sendo desenvolvidas para solucionar o problema, como o NAT (*Network Address Translation*, ou endereço de rede), o CIDR (*Classles Inter-Domain Routing*, ou roteamento de interdomínio sem classes) e, ainda, a versão 6 do IP, ou IPv6, que é um endereço IP com 128 bits, separados em 16 octetos.

Com o IPv6, já disponível para uso, é possível termos 2^{128} ou $3{,}42 \times 10^{38}$ endereços únicos. Nesta lição, os comandos e as ferramentas no Linux farão uso de endereços IPv4, e não IPv6, pois atualmente ainda é muito raro encontrarmos redes funcionando unicamente com IPv6.

NAT: reescreve os endereços IP de origem de um pacote de maneira que um computador de uma rede interna tenha acesso ao exterior ou Rede Mundial de Computadores (rede pública).

Endereço IP privado e NAT

Os endereços IPs privados são aqueles atribuídos aos dispositivos que estão dentro de organizações, escolas, laboratórios e qualquer outro local que não seja a internet. Isso mesmo que você leu! O IP da interface de rede da sua máquina que está conectada agora na internet não é o IP visto pelo mundo. São os endereços privados usados nas chamadas intranets ou redes locais. A criação dos endereços IPs privados foi uma das primeiras soluções encontradas para evitar o esgotamento dos endereços IPv4, pois os endereços privados podem se repetir em intranets diferentes.

Importante

Lembre-se de que o endereço de IP é atribuído à interface de rede e não ao computador, ou seja, seu computador pode ter várias interfaces de rede e, logo, mais de um endereço IP. Muito provavelmente seu notebook tem a interface de rede cabeada e a sem fio, então, no mínimo, já podemos dizer que tem dois endereços IPs, quando devidamente configurado. Nesta lição, ao falarmos "IP da máquina", estaremos considerando aquele da interface de rede que está sendo usada para comunicação na rede.

Proxy: servidor (sistema de computador ou aplicação) que age como um intermediário para requisições de clientes, solicitando recursos de outros servidores.

Quando a sua máquina, com IP privado em determinada interface, conecta-se à internet, esta precisa de um IP válido, roteável, e aí surge a solução de NAT, que traduz o endereço privado da intranet para um IP de internet, através de um processo chamado *gateway* de tradução de endereço de rede ou um servidor proxy para possibilitar a conectividade na internet.

Classes de endereços privados do IPv4

Classe do endereço	Faixa do endereço IP
A	10.0.0.0 a 10.255.255.255
B	172.16.0.0 a 172.31.255.255
C	192.168.0.0 a 192.168.255.255

Máscaras

Antes de explicar o CIDR, precisamos entender o conceito de máscara ou máscara de sub-rede. Como já vimos, um endereço IPv4 tem duas partes: uma que identifica sua rede (ou, melhor dizendo, sub-rede) e a outra, o *host*. O limite entre essas duas partes, de rede e de *host*, é um endereço IP, chamado de máscara de sub-rede (ou *netmask*). Esse endereço da máscara de sub-rede também é um número de 32 bits especificado com quatro segmentos de 8 bits.

Na tabela a seguir, mostramos as máscaras de sub-redes categorizados pelas classes A, B e C dos endereços de IPv4.

Classes A, B e C das máscaras de sub-redes

Classe	IP forma decimal	IP forma binária	Descrição
A	255.0.0.0	11111111.00000000.00000000.00000000	Endereço de rede de 8 bits e endereço de *host* de 24 bits.
B	255.255.0.0	11111111. 11111111.00000000.00000000	Endereço de rede de 16 bits e endereço de *host* de 16 bits.
C	255.255.255.0	11111111. 11111111. 11111111.00000000	Endereço de rede de 24 bits e endereço de *host* de 8 bits

Perceba que, na tabela anterior, para saber o número de bits de cada parte, basta contar a quantidade de "1" para endereço de rede e a de "0" para endereço de *host*.

Essa quantidade de "0" também nos fornece o número máximo de *hosts* que podemos ter numa rede. Por exemplo, supondo que você tenha uma rede que receba IPs 192.168.1.1, 192.168.1.2 etc.,

e que, nessa rede, a máscara é 255.255.255.0. Diante dessas informações e pela tabela apresentada, você sabe que o número de *hosts* é de 8 *bits*, então teríamos:

```
192.168.1.1 = 11000000.10101000.00000001.00000001
192.168.1.2 = 11000000.10101000.00000001.00000010
192.168.1.3 = 11000000.10101000.00000001.00000011
...
192.168.1.255 = 11000000.10101000.00000001.11111111
```

Ou seja, teríamos 255 *hosts*, que você poderia ter calculado rapidamente apenas convertendo de binário para decimal a quantidade de bits reservada para os *hosts*, no caso 8 bits, que equivale a 255.

Importante

No exemplo anterior, na verdade, deveríamos ter 2^8 *hosts*, o que daria 256 endereços, pois temos que contar também o endereço 192.168.1.0. Entretanto, na prática, os endereços 192.168.1.0 e 192.168.1.255 não podem ser atribuídos em uma interface de rede, porque são considerados os endereços de rede e *broadcast*, respectivamente. Esses são os endereços para justamente delimitar nossas sub-redes e podem ser descobertos a partir de cálculos simples, com operações lógicas de AND. Portanto, a quantidade real de *hosts* que podemos ter no exemplo acima é 254.

Além das classes predefinidas (A, B e C) de máscaras de sub-redes, podemos ter vários outros valores de máscara, bastando apenas mover para direita ou esquerda, no endereço IP, um bit, permitindo, assim, termos mais ou menos sub-redes.

Por exemplo, adicionando um bit à máscara de sub-rede classe C em seu endereço IP, teríamos um endereço de rede de 25 bits e endereço de *host* de 7 *bits*:

```
255.255.255.128 = 11111111.11111111.11111111.10000000
```

Considerando a rede 192.168.1.0, se tivermos uma máscara para esta rede com valor 255.255.255.128, seria possível dividir essa rede (192.168.1.0) em duas, com a faixa de IP de 192.168.1.0 a 192.168.1.127 e outra de 192.168.1.128 a 192.168.1.255. Logo, cada uma dessas redes estaria com 27 – 2 *hosts* (lembre-se de que estamos excluindo o número de IP de rede e o de *broadcast*, por isso, menos 2).

A seguir, a tabela mostra alguns detalhes de sub-redes com alterações de uma máscara classe C.

Detalhes de sub-redes IP de máscara classe C

Máscara de sub-rede	Bits adicionados	Número de sub-redes	Endereço de rede	Endereço de *broadcast*	Endereço de IP mínimo	Endereço de IP máximo	Número de *hosts*
128	1	$2^1 = 2$	0	127	1	126	126
			128	255	129	254	126
192	2	$2^2 = 4$	0	63	1	62	62
			64	127	65	126	62

			128	191	129	190	
			192	255	193	254	62
224	3	$2^3 = 8$	0	31	1	30	30
			32	63	33	62	30
			64	95	65	94	30
			96	127	97	126	30
			128	159	129	158	30
			160	191	161	190	30
			192	223	193	222	30
			224	255	225	254	30

Uma vez entendidas máscaras e sub-redes, voltamos ao CIDR (roteamento interdomínio sem classes), que nada mais é do que uma forma de especificar as máscaras de sub-rede. A notação do CIDR usa o formato endereço/prefixo, em que o prefixo se refere ao número de bits que será usado pela máscara de sub-rede. Por exemplo, o IP 192.168.1.27 que está em uma rede de máscara de sub-rede 255.255.255.0 pode ser representado na notação CIDR da seguinte maneira: 192.168.1.27/24.

A notação CIDR possibilita personalizar as máscaras de sub-rede, criando-as além das limitações impostas pelas classes.

TCP/IP: conjunto de protocolos de comunicação entre computadores em rede.

Saiba mais

Como vimos neste tópico, o modelo de referência TCP/IP (também chamado de arquitetura de protocolo da internet) implementa uma série de protocolos distribuídos em camadas. Esses protocolos formam uma pilha de protocolos de comunicação sobre a qual a internet e grande parte das redes funcionam. Os protocolos TCP e IP compõem o nome desse modelo de referência devido ao fato de terem sido os primeiros protocolos a serem definidos.

Existe uma discussão sobre qual o número correto de camadas no modelo TCP/IP. Alguns autores citam 4 (aplicação, transporte, internet, *host*/rede ou *link* ou acesso à rede), e outros, 5 camadas (aplicação, transporte, rede, enlace e física), conforme a figura a seguir. Alguns ainda falam que o modelo sofreu uma melhora, tornando-se um modelo híbrido e que, por isso, passou de 4 para 5 camadas. Outros ainda citam que as 5 camadas são, na verdade, um modelo de abstração, resultado da "junção" do modelo OSI com o modelo TCP/IP de 4 camadas.

Modelo de arquitetura de rede TCP/IP com 4 e 5 camadas

Até mesmo em questões de concursos públicos existe a confusão e diferentes interpretações sobre o tema, como os exemplos a seguir.

UEM - 2018 - UEM - Técnico em Informática

Na realidade, o _____ é um conjunto de protocolos. Esse grupo é dividido em quatro camadas: aplicação, transporte, rede e interface. Cada uma delas é responsável pela execução de tarefas distintas. Essa divisão em camadas é uma forma de garantir a integridade dos dados que trafegam pela rede.

a) TCP/IP

b) *PROXY*

c) HTTPS

d) LINUX

e) POP3

Gabarito oficial: letra A.

HTTPS: é o HTTP usando uma camada de segurança com TLS/SSL.

CESPE - 2018 - Polícia Federal - Escrivão de Polícia Federal

Acerca das características de internet, intranet e rede de computadores, julgue o próximo item.

O modelo de referência de rede TCP/IP, se comparado ao modelo OSI, não contempla a implementação das camadas física, de sessão e de apresentação.

Certo

Errado

Gabarito oficial: Certo.

Nessa questão, perceba que foi considerado um modelo de 4 camadas para o TCP/IP, pois, quando o gabarito oficial considerou a resposta como certa, confirmou, de acordo com enunciado, que a camada física não existe no modelo TCP/IP, e a questão não foi anulada, portanto, o candidato deveria conhecer de fato sobre o entendimento da banca para "acertar" a questão.

CESPE - 2016 - TRE-PI - Técnico Judiciário - Operação de Computadores

Considerando que o conjunto de protocolos TCP/IP é constituído de cinco camadas: física, enlace de dados, rede, transporte e aplicação, assinale a opção correspondente à combinação correta entre camada e seus protocolos.

a) Camada de transporte: SMTP, TCP e UDP.

b) Camada de rede: IP, ICMP e ARP.

c) Camada de aplicação: SMTP, FTP e RARP.

d) Camada física: *Telnet*, Ping e *Bluetooth*.

e) Camada de enlace: DNS, SCTP e IPSec.

Gabarito oficial: letra B.

A mesma banca, Cespe, que, na questão anterior, considerou o modelo de 4 camadas, agora, nessa outra questão, já afirma que o modelo é de 5 camadas. Além disso, a banca considerou que o ARP também pode atuar na camada de rede, quando, na verdade, vimos que é um protocolo predominante da camada de enlace.

Para tentar amenizar a polêmica sobre o número de camadas do TCP/IP, podemos verificar o que dizem algumas RFCs e o entendimento de autores que tratam do assunto:

- a RFC 1122, a partir da página 8, no item "1.1.3 Internet Protocol Suite", descreve a arquitetura da internet em 4 camadas: aplicação, transporte, Internet e link;
- a RFC 1392, na página 29, no item "layer", deixa claro que o modelo TCP/IP possui 5 camadas e o OSI é composto por 7;
- Kurose (2010), em seu livro "Redes de computadores e a internet", nas páginas 37 e 38, deixa claro que a pilha de protocolos da internet é composta por 5 camadas;
- Nemeth (2018), em seu livro "Unix and Linux Administration Handbook", descreve o modelo TCP/IP em 5 camadas, dizendo que esses protocolos são organizados em uma hierarquia ou pilha, com os protocolos de nível superior fazendo uso daqueles que estão logo abaixo. O TCP/IP é convencionalmente descrito como um sistema de 5 camadas, mas os protocolos TCP/IP reais fazem uso de apenas 3 dessas camadas.

Portanto, parece não existir um entendimento único sobre o número de camadas no modelo TCP/IP. No entanto, este livro adota o modelo em 5 camadas por considerá-lo mais bem definido e abordado na maioria das obras literárias dos autores e pesquisadores mais conhecidos no mundo, como Kurose e Tanenbaum. Entretanto, não consideramos prejudicial (com exceção para certas questões de concurso) essas diferentes interpretações sobre o número de camadas para o entendimento sobre o funcionamento da arquitetura e dos protocolos de uma rede de computadores, pois as concepções sobre o modelo de 4 camadas, aparentemente, atribuem a característica da camada de nível mais baixo ao conjunto de características e funcionamento das camadas de enlace e física no modelo de 5 camadas.

Fibre Channel: é uma tecnologia de comunicação de alta velocidade que é utilizada em armazenamento de dados em rede.

Cliente-servidor: é uma estrutura de aplicação distribuída que distribui as tarefas e cargas de trabalho entre os fornecedores de um recurso ou serviço.

Exercitando o conhecimento

Um modelo de arquitetura de rede, dividido em camadas, no qual, em sua camada de número 3, implementa serviços ou funções auxiliares, tais como *multicast*, é:

a) OSI.

b) *Fibre Channel*.

c) TCP/IP.

d) Ethernet.

Comentário: a alternativa correta é a letra "b". Como citado resumidamente, no tópico anterior, sobre o uso da tecnologia *Fibre Channel* (FC) em redes SAN, a arquitetura FC também possui um modelo dividido em camadas, num total de 5, que são codificadas em uma sequência numérica de 0 a 4 (FC-0, FC-1, FC-2, FC-3 e FC-4), em que FC-3 é a camada que implementa funções auxiliares, tais como: *striping*, *hunt groups* e *multicast*.

1.3 Servidores de rede básicos

Servidor de rede é mais um ativo de tecnologia da informação (TI) que um administrador de rede terá contato durante grande parte de suas atividades. Todo servidor está destinado a oferecer algum serviço de rede, e aqui não estamos considerando apenas a arquitetura de cliente-servidor, mas de qualquer estrutura, seja o servidor *hardware* ou *software* que possa oferecer algum tipo de serviço na rede, e num modelo cliente-servidor, P2P (par-a-par) ou outro.

Um único servidor de rede pode oferecer diversas funcionalidades ou serviços na rede, como:

- serviço de diretório;
- serviço de nomes;
- serviço de distribuição de endereços IPs;
- serviços de compartilhamento de arquivos;
- serviço de tempo.

Um bom exemplo de servidor de rede que oferece todos esses serviços de rede é um servidor *Active Directory* da Microsoft, no qual, numa instalação padrão, todos esses e outros serviços podem ser oferecidos. Um único servidor com sistema operacional Linux também pode oferecer vários serviços de rede, mas é claro que, num ambiente de rede, com uma quantidade grande de usuários, o ideal é distribuir alguns serviços entre vários servidores. Mesmo em um servidor com um poder de processamento e memória altos, alguns serviços apresentam melhor desempenho quando executados em vários servidores.

Em um *data center*, você encontrará os servidores geralmente dispostos em um rack. Entre os vários tipos de formatos físicos de servidores, nesses racks, os principais que poderão existir são servidores do tipo *blade* (ou lâmina), de rack ou de torre, apresentados nas imagens a seguir.

Os três tipos de servidores físicos ilustrados são os mais encontrados nas empresas.

***Blade*:** é um tipo de computador/servidor, geralmente usado em *data centers*, projetado para ocupar menos espaço, reduzir o consumo de energia e simplificar o seu funcionamento.

Os servidores *blades* são dispostos em um chassi ocupando de 4U a 6U. Esse tipo de servidor é composto de um único chassi e várias lâminas (*blades*), em que cada uma possui apenas um microprocessador, uma memória principal e barramentos. Outros itens do servidor, como fonte de alimentação, ventoinhas de refrigeração, *switch* redundante e interfaces de armazenamento, são compartilhados entre as lâminas.

4U ou 6U: refere-se à medida de um rack (*rack unit*), equivalente a 1,75 polegada ou 44,45 mm.

Entre suas vantagens estão:

- preço mais barato que o de seus concorrentes;
- menor consumo de energia;
- ocupam pouco espaço;
- simples de operar;
- apresentam poucas falhas.

Servidores de rack possuem um design parecido com um computador de mesa de gabinete horizontal, com todos os seus componentes de *hardware* (memória, disco rígido, processador, fonte de alimentação e outros) em um único chassi. Esses servidores podem ocupar 2U ou 4U e, em geral, são empilhados, proporcionando uma economia de espaço.

CPU: em inglês, *Central Processing Unit*, é a unidade central de processamento, a parte de um sistema computacional e tem papel parecido ao cérebro no computador.

Os servidores torre têm seu formato semelhante aos computadores desktop de gabinete verticais, mas com a grande diferença em seus componentes de *hardware* interno, com processadores de grande desempenho, às vezes mais de uma CPU, maior quantidade de memória e outras tecnologias superiores a um computador de uso doméstico. Um inconveniente desses servidores é que ocupam bastante espaço em um *data center*, além de difícil transporte. São servidores mais indicados para pequenas empresas ou escritórios.

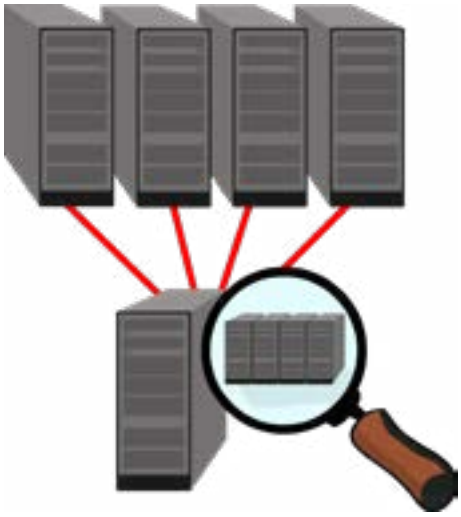
Mesmo com a adesão cada vez maior de serviços em nuvem, muitas empresas, órgãos públicos ou mesmo pequenos escritórios ainda possuem seus servidores físicos. Mais que a computação em nuvem, a virtualização de servidores tem sido vista em quase todo *data center*.

Memória RAM: a memória de acesso aleatório (*Random Access Memory*) é um tipo de memória que permite a leitura e a escrita, utilizada como memória primária em sistemas eletrônicos digitais.

Virtualização

Atualmente, é muito improvável termos uma quantidade grande de servidores físicos desempenhando um ou vários serviços de rede. As empresas instalam em seus servidores físicos um sistema operacional capaz de criar vários servidores ou máquinas virtuais, em um processo chamado de virtualização, em que é possível obter uma grande economia de recursos computacionais, além de outras vantagens – daí termos os servidores de virtualização.

Imagine, por exemplo, que sua empresa precise implantar vários serviços de rede e que muitos desses precisarão de uma quantidade de memória RAM e processamento, o que o obrigaria a distribuir esses serviços em vários servidores. Se optar por comprar vários servidores físicos, além do custo maior, você precisará de mais espaço no seu *data center*, maior consumo de energia e aquecimento dos equipamentos, maior tempo de manutenção e backup de todos os servidores físicos, entre outras operações necessárias para cada servidor. Mas, caso opte pela virtualização, você poderá adquirir apenas um único servidor físico de grande porte e, nele, instalar um sistema operacional capaz de virtualizar recursos, podendo, assim, criar todas as máquinas virtuais de que necessita para seus serviços de rede.



Com a virtualização, você terá um único servidor físico para manutenção e backup, com um consumo de energia reduzido, grande economia de espaço físico em seu *data center* e fácil gerência dos servidores, podendo rapidamente criar ou excluir as máquinas virtuais, além de outras vantagens.

Destacamos, aqui, os principais fornecedores de tecnologias de virtualização:

- VMware (SO ESXi): www.VMware.com;
- Citrix *Hypervisor*: www.citrix.com;
- Microsoft Hyper-V: https://www.microsoft.com/en-us/evalcenter/evaluate-hyper-v-server-2019;
- XenServer: xenserver.org.

Existem vários outros fornecedores de tecnologias de virtualização. As citadas acima são as principais do mercado. Algumas possuem também solução para uso doméstico, como o VirtualBox (http://www.virtualbox.org) e a *VMware Player* (https://www.VMware.com/tryvmware/?p=player&lp=1), as quais você pode já ter usado.

Uma empresa que já possui seu parque de servidores com tecnologia de virtualização devidamente implantada e gerenciada tem mais facilidade para uma fácil migração para um ambiente em nuvem.

Vários outros tipos de virtualização podem existir em um *data center*, como virtualização de *storage*, de rede, de aplicação e outros. Ainda, existem diversos outros conceitos sobre o entendimento de como funciona a virtualização. No entanto, esses e outros assuntos de virtualização não serão tratados neste livro.

VMware: permite a execução de um ou mais sistemas operacionais simultaneamente num ambiente isolado, criando computadores virtuais dentro de um computador físico possibilitando rodar um sistema operacional totalmente distinto.

Virtualbox: *software* de virtualização que visa criar ambientes para instalação de sistemas distintos.

Saiba mais

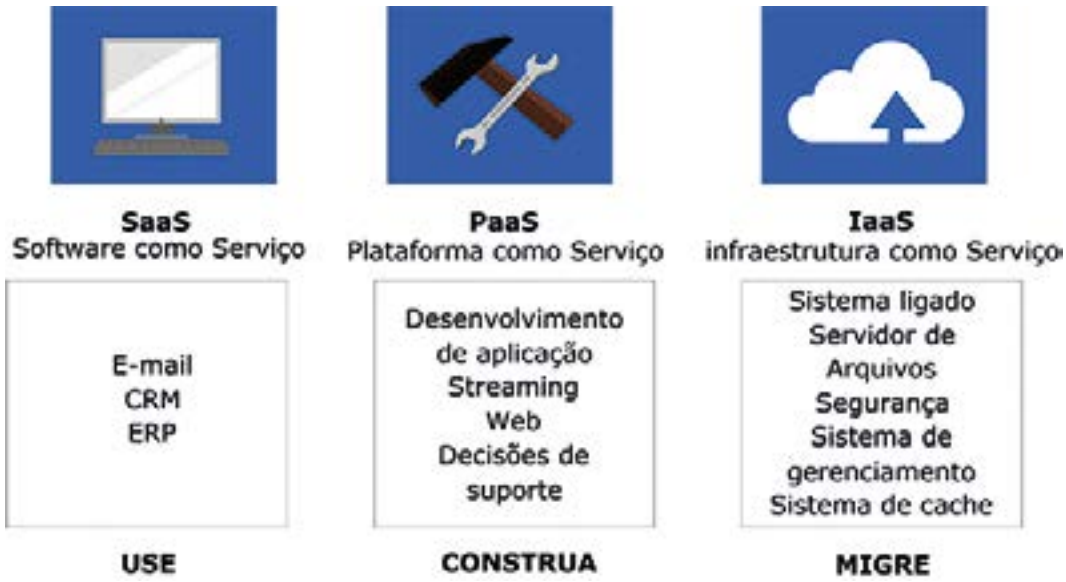
Já ouviu falar de um servidor *bare metal*? Esse é um termo usado para identificar um servidor dedicado em uma infraestrutura como Serviço ou IaaS. Serve para descrever ambientes de TI em que o sistema operacional é instalado diretamente no *hardware*, em vez de uma camada de sistema hospedando diversas VMs, como é realizado em ambientes virtualizados.

Nos serviços em nuvem, podemos ter três principais categorias:

- infraestrutura como serviço (IaaS), na qual os usuários solicitam recursos de computacionais, como memória, rede e armazenamento. Esses são normalmente entregues na forma de servidores privados virtuais, também conhecidos como VPS. Em IaaS, os usuários são responsáveis por gerenciar tudo acima do *hardware*: sistemas operacionais, redes, sistemas de armazenamento e seus próprios *softwares*;
- plataforma como serviço (PaaS), na qual os desenvolvedores enviam seus aplicativos empacotados em um formato especificado pelo fornecedor. O fornecedor, então, executa o código em nome do usuário. Nesse modelo, os usuários são responsáveis por seus próprios códigos, enquanto o fornecedor gerencia o sistema operacional e a rede;
- *software* como serviço (SaaS), a categoria mais ampla, na qual o fornecedor hospeda e gerencia *software* e os usuários pagam uma taxa de assinatura para terem acesso. Os usuários não mantêm nem o sistema operacional nem o aplicativo. Atualmente, muitos aplicativos hospedados na *Web* (Wix, Wordpress, Joomla, Drupal e outros) se enquadram na categoria SaaS.

Existem outras categorias que podem ser consideradas apenas subcategorias das citadas acima, como: desenvolvimento como serviço (DaaS); comunicação como serviço (CaaS); banco de dados como serviço (DBaaS); e, segurança como serviço (SECaaS). E o conjunto de todas elas seria "Tudo como Serviço" (EaaS), em que, para alguns consultores e especialistas em TI, o futuro tem caminhado para esse cenário, no qual os benefícios de agilidade, economia financeira e de espaço físico, atualização e modernidade são essenciais para empresas em um mundo cada vez mais digital.

Atualmente, as plataformas em nuvem mais usadas, e que oferecem os vários serviços citados são: Amazon Web Services; DigitalOcean; Google Cloud Platform; IBM Softlayer; Microsoft Azure; OpenStack; Rackspace e VMware vCloud Air.



Exercitando o conhecimento

As redes de computadores possibilitam uma estrutura em duas camadas, por meio das quais computadores de usuários se conectam a computadores servidores de rede para efetuarem requisições de serviços e coleta de informações. Sabendo disso, assinale o nome da arquitetura que implementa a estrutura em duas camadas utilizando a rede de computadores.

a) Cliente-servidor.

b) *Web*.

c) P2P.

d) Distribuída.

Comentário: a alternativa correta é a letra "a". Em uma arquitetura cliente-servidor, há um hospedeiro sempre em funcionamento, denominado servidor, que atende a requisições de muitos outros hospedeiros, denominados clientes. Estes podem estar em funcionamento às vezes ou sempre (no enunciado da questão são os computadores de usuários). No caso da alternativa "b", *Web* seria apenas um tipo de serviço oferecido por um servidor de rede e não um tipo de arquitetura. Já, na alternativa "c", tem uma outra arquitetura, a P2P ou par-a-par, na qual quase sempre não há necessidade de um servidor dedicado para atender a clientes. No P2P, a aplicação poderá realizar a comunicação entre hospedeiros de forma direta, entre pares. Exemplos de aplicações que fazem uso de uma estrutura em P2P são BitTorrent, Skype, IPTV e outras, que, geralmente, possuem um tráfego intenso. E, por fim, a alternativa "d" está mais relacionada aos tipos de sistemas distribuídos, podendo usar vários servidores ou aplicações para seu melhor funcionamento, e não a um tipo de arquitetura de rede.

1.4 Distribuições Linux para servidores

Neste último tópico, mostraremos alguns exemplos de distribuições Linux específicas para uso como servidores de rede.

Saiba que qualquer distribuição Linux poder ser usada como um servidor de rede, bastando, para isso, instalar os serviços de rede que você deseja. Entretanto, quando uma distribuição Linux já é preparada e construída para determinado propósito, é recomendado que a use, pois isso facilitará bastante a busca, configuração e instalação de *softwares* específicos para tal finalidade, além de, em alguns casos, o kernel está devidamente modificado para o propósito a que se destina o uso da distribuição Linux.

Exemplo disso é a família de distribuições Linux do Ubuntu, como o Ubuntu Studio (http://ubuntustudio.org/download/), uma versão modificada para uso na edição de multimídia, com um kernel diferente da versão padrão do Ubuntu, para melhor desempenho das placas de som e vídeo, otimizando *softwares* de edição de imagem, vídeo, som e modelagem 3D.

Outra variação do Ubuntu é a versão Server (https://www.ubuntu.com/download/server), que pretendemos mostrar em outras distribuições. No Ubuntu Server, suportes a LVM, RAID, Vlans, *bonds* e outros já são devidamente habilitados em seu kernel. E aplicações como Nginx, PHP, Apache e outros serviços de rede importantes e mais atuais já estão disponíveis na versão Ubuntu Server.

Kernel: núcleo de sistema operacional.

Nginx: é um servidor *web* rápido, leve, e com inúmeras possibilidades de configuração para melhor *performance*.

PHP: *Personal Home Page* é uma linguagem interpretada livre, capaz de gerar conteúdo dinâmico na *World Wide Web*.

Saiba mais

Veja o significado de algumas das siglas mencionadas:

- LVM – *Linux Logical Volume Manager*, ou gerenciador de volume lógico, é um mapeador de dispositivos que fornece gerenciamento de volume lógico para o kernel do Linux;
- RAID – *Redundant Array of Inexpensive Drives*, ou conjunto redundante de discos econômicos, é um meio de se criar um subsistema de armazenamento composto por vários discos individuais;
- Vlan – uma rede local virtual, logicamente independente. Várias VLANs podem coexistir em um mesmo computador (*switch*), de forma a dividir uma rede física em mais de uma rede (virtual), criando domínios de *broadcast* separados;
- *Bond* – ou *nic bonding*, refere-se à possibilidade de combinar múltiplas interfaces de rede em uma única interface lógica.

Debian GNU/Linux

É uma distribuição usada prioritariamente como servidor de rede e uma das mais aceitáveis pelas empresas para esse fim. Usa rigorosamente o kernel Linux padrão e suas aplicações básicas, todas com licença GNU/Linux. Muitas outras distribuições têm o debian como base.

Site oficial: <https://www.debian.org/>.

Wiki: *website* no qual utilizadores modificam colaborativamente conteúdo e estrutura diretamente do *web browser*.

Fedora

Mantido pelo Projeto Fedora, tem como base a distribuição RHEL, inclusive é patrocinada pela empresa *Red Hat*. O Fedora pode ser utilizado tanto em desktop quanto em servidor, possuindo as duas versões prontas para download. Na versão *server* (https://getfedora.org/en/server/), o sistema destaca aspectos como a modularidade, que traz um novo repositório modular que fornece versões adicionais de *software* em ciclos de vida independentes; a aplicação *cockpit*, que permite administrar o sistema com simplicidade de uma interface moderna e poderosa, visualizando e monitorando o desempenho e status do sistema, podendo implementar e gerenciar serviços baseados em *container*; e um solução completa de domínio corporativo, permitindo gerenciamento avançado de usuários, DNS, serviços de certificados, integração com domínio proprietário da MS Windows com a ferramenta.

Site oficial: <https://fedoraproject.org/>.

***Desktop*:** parte da interface gráfica de sistemas operacionais que exibe, no vídeo, representações de objetos usualmente presentes nas mesas de trabalho.

openSUSE

Mantida pela comunidade do Projeto openSUSE, é o sistema mais usado em servidores. Em seu site, está disponível a versão *Tumbleweed* e *Leap*, sendo esta última mais indicada para servidores, com pacotes prontos para instalação fácil de serviços de rede, como servidor de impressão, controlador de domínio, servidor *web*, de arquivos e outros. Em sua wiki (https://pt.opensuse.org/HCL/Servers), a openSUSE disponibiliza uma lista de compatibilidade de *hardware* para servidores (HCL).

Site oficial: <https://www.opensuse.org/>.

SUSE

É a versão paga da distribuição Linux, tanto para versão desktop quanto server. Existem vários tipos da versão servidor, na versão padrão, tem o SUSE Linux Enterprise Server, que se destaca por um

sistema operacional moderno e modular que ajuda a simplificar a TI multimodal, tornando a infraestrutura de TI tradicional eficiente e fornecendo uma plataforma envolvente para desenvolvedores. Ainda segundo informação no *site* oficial da distribuição, a versão servidor do SUSE permite facilmente implantar e fazer a transição de cargas de trabalho críticas para o negócio em ambientes de nuvem pública e no local.

Site oficial: <https://www.suse.com/>.

Red Hat Enterprise Linux – RHEL

Considerada a distribuição como líder de mercado nos Estados Unidos, foi criada e é mantida pela empresa de mesmo nome, Red Hat. Seu sistema é muito usado em servidores de redes. Atualmente, a distribuição RHEL está mais voltada para o mercado empresarial. Possui vários tipos na versão servidores, até mesmo versão específica para Storage, Virtualização e Diretório. Em outubro de 2018, a *Red Hat* foi vendida para a IBM.

Site oficial: <www.redhat.com>.

CentOS

Mantida pelo Projeto CentOS, é uma distribuição gratuita e derivada do *Red Hat* Enterprise Linux. O CentOS é a distribuição usada como base da plataforma de virtualização XenServer e outras.

Site oficial: <https://www.centos.org/>.

Slackware

É a distribuição Linux mais antiga em atividade. Mantida ainda pelos desenvolvedores e mantenedores espalhados em todo mundo, sendo o seu criador, Patrick Volkerding, responsável também principalmente pela integração, pelo empacotamento e pelo gerenciamento dos *softwares* para distribuição. É considerada uma distribuição bastante estável, segura e com certa neutralidade em relação à instalação de aplicativos, uma vez que é realizada diretamente pelos arquivos fontes dos *softwares*, sem depender de gerenciadores de pacotes.

Site oficial: <www.slackware.com>.

ClearOS

É uma distribuição Linux baseada no CentOS e Red Hat Enterprise Linux – RHEL. Essa distribuição sucede o antigo Linux ClarkConnect. O ClearOS foi desenvolvido para trabalhar como *gateway* de rede e também como servidor de rede, possuindo a aplicação *WebConfig* usada para administração do servidor, por meio de uma interface *web*.

Serviços e suporte para o ClearOS podem ser adquiridos pelo ClearCenter, empresa privada, sediada na Nova Zelândia, que desenvolve *softwares* para o ClearOS e também outros produtos, como virtualização (ClearVM), *hardware* (ClearBox) etc.

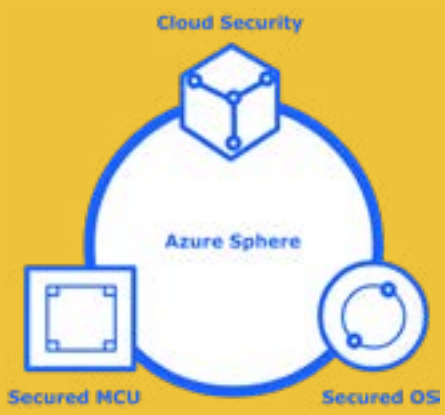
Existe também a versão livre do ClearOS desenvolvida pela comunidade da internet e disponível livre para download. Atualmente, a ClearCenter em parceria com a HPE (Hewlett Packard Enterprise) têm ofertado o ClearOS em servidores HPE ProLiant. O HPE ProLiant integrado ao ClearOS oferece uma experiência simples, acessível e segura.

Site oficial: <https://www.clearos.com/>.

RSA: é um dos primeiros sistemas de criptografia de chave pública e é amplamente utilizado para transmissão segura de dados.

Saiba mais

Pensando na computação em nuvem e, principalmente, na internet das coisas (IoT), em 16/04/2018, na RSA *Conference* 2018, em São Francisco, na Califórnia, a Microsoft anunciou o Azure Sphere OS, um sistema operacional com kernel Linux personalizado. Sim, isso mesmo, a Microsoft possui agora uma distribuição Linux. A Microsoft informou que a solução Azure Sphere possui três componentes principais para garantir que os dispositivos da IoT possam ter melhor proteção, entre eles, os microcontroladores Azure Sphere, o Azure Sphere Security Service baseado em nuvem e o Azure Sphere OS.



Exercitando o conhecimento

Imagine que você é um administrador de redes Linux a ser contratado por uma empresa que trabalha com computação em nuvem em várias plataformas com sistemas operacionais Linux. Quais certificações citadas a seguir poderiam agregar valor ao seu currículo para aumentar as suas chances de contratação?

a) *Red Hat Certified OpenStack Administrator.*

b) MCSA Linux on Azure.

c) *AWS Certified Solutions Architect*.

d) Todas as certificações anteriores.

Comentário: a alternativa correta é a letra "d". Na alternativa "a", temos a plataforma da Red Hat de computação em nuvem, o OpenStack, que tem como base o Red Hat Enterprise Linux. Umas das certificações atuais mais exigidas aos profissionais de TI. Além da certificação de nível administrador do OpenStack, tem também a de engenheiro (*Red Hat Certified Engineer in Red Hat OpenStack*). A alternativa "b", MCSA Linux on Azure, refere-se à certificação para profissionais que desejam trabalho com a plataforma de computação em nuvem da Microsoft, o Azure. Essa certificação atesta que o profissional possui capacidade para projetar, arquitetar, implementar e manter soluções complexas para nuvem do Linux que aproveitam os recursos do Microsoft Azure. Ela também comprova que o profissional possui habilidades de administração do sistema Linux. E, por fim, a alternativa "c", a *AWS Certified Solutions Architect,* atualmente, é uma das certificações mais desejadas e valorizadas por profissionais de TI.

Resumindo

Nesta lição, vimos uma introdução à rede de computadores, mostrando não só os principais tipos de redes que atualmente são projetados, mas também os equipamentos usados, os meios de transmissão e os demais ativos de TI que, em geral, um profissional administrador de rede irá se deparar constantemente em suas atividades.

Falamos, ainda, dos protocolos de rede mais usados, com base principalmente no modelo de arquitetura de rede TCP/IP. Além disso, citamos o endereçamento IP, com fase na versão 4, e vimos como se constituem os endereços IP, a máscara de rede, as classes de endereços e os demais conceitos que são trabalhados constantemente pelo administrador de rede.

Sobre os servidores de rede, vimos os principais modelos físicos de servidores que ainda são usados em *data centers* de empresas e a tendência da virtualização e da computação em nuvem que as empresas têm adotado. Por fim, estudamos as principais distribuições Linux que atualmente são usadas como servidores de rede.

Veja se você se sente apto a:

- descrever os conceitos básicos e as arquiteturas de redes de computadores;
- avaliar o tipo de rede, equipamentos de interconexão e meios de transmissão necessários para estabelecimento da rede;
- aplicar corretamente configurações de protocolos, serviços e IP em uma rede;
- indicar o tipo de servidor que melhor se adéqua a um *data center*;
- recomendar a virtualização para emprego de servidores de rede virtuais;
- buscar soluções em computação em nuvem para atender a serviços de tecnologia da informação, seja de infraestrutura, desenvolvimento ou *softwares*;
- avaliar se uma distribuição Linux é ideal para atuar como um servidor de rede.

Exercícios

Parabéns, você finalizou esta lição!

Agora responda às questões ao lado.

Questão 1 – Qual o padrão IEEE designado para uma rede sem fio ou *WLAN*?

a) Ethernet.

b) *Wireless*.

c) 803.11.

d) 802.11.

Questão 2 – Os tipos de rede digital podem ser classificados em função dos seus alcances geográficos. A rede que cobre uma área física maior, como o campus de uma universidade, nas configurações dos roteadores para se referir à rede externa, é conhecida como:

a) *WLAN*.

b) PAN.

c) MAN.

d) LAN.

Questão 3 – Com relação aos conceitos básicos sobre computação em nuvem (c*loud computing*), assinale a alternativa correta.

a) No modelo de implantação de nuvem comunitária, a infraestrutura de nuvens é disponibilizada para o público em geral, sendo acessada por qualquer usuário que conheça a localização do serviço.

b) Os modelos de computação em nuvem são: nuvem privada, nuvem pública, nuvem mista e nuvem comunitária.modprobe xpto e sudo modprobe - r xyz.

c) Algumas plataformas de nuvens públicas oferecem o serviço de PaaS. Entre essas, temos as plataformas Eucalyptus, Nimbus, OpenNebula e OpenStack.

d) A computação em nuvem é um modelo para acesso conveniente, sob demanda e de qualquer localização, a uma rede compartilhada de recursos de computação que possam ser rapidamente provisionados e liberados com mínimo esforço de gerenciamento ou interação com o provedor de serviços.

Questão 4 – Sobre a virtualização, é correto afirmar que:

a) a camada de virtualização, ou monitor de virtualização, é que constrói as interfaces reais a partir da interface real.

b) uma máquina virtual é um computador real feito de *hardware*.

c) o sistema real, ou sistema hospedeiro, é que executa sobre o sistema virtualizado.

d) o sistema real, ou sistema hospedeiro, é que contém os recursos reais de *hardware* e de *software* do sistema.

Questão 5 – Assinale a alternativa que apresenta a topologia que possui as vantagens de fácil instalação e, quando comparada a outras topologias, exige menor quantidade de cabos, mas que, por outro lado, tem como desvantagem o difícil isolamento de falhas na rede.

a) *Mesh*.

b) Barramento.

c) Estrela.

d) *Token ring*.

Questão 6 – Na pilha de protocolo TCP/IP, existe o serviço de transporte sem conexão e não confiável utilizado em aplicações que não implementam controle de fluxo nem manutenção da sequência das mensagens enviadas, o qual é denominado:

a) TCP.

b) RARP.

c) ICMP.

d) UDP.

Questão 7 – "Para atender a uma maior capacidade de endereçamento, um novo protocolo IP, o _____, foi desenvolvido. O IPv4 foi projetado em uma época em que a internet era utilizada, primordialmente, entre pesquisadores de redes mutuamente confiáveis. Porém, hoje, essa segurança é preocupação primordial, tanto que foram desenvolvidos protocolos que oferecem serviços de segurança e um deles é o _____."

Assinale a alternativa que completa correta e sequencialmente a afirmativa anterior.

a) IPv6 / ICMP.

b) IPv4 / IPSec.

c) IPv6 / IPSec.

d) IPv10 / ICMP.

Questão 8 – Muitas empresas têm mudado sua organização interna para adotar modelos de computação em nuvem (*cloud computing*). A respeito desse conceito, e respectivas vantagens e desvantagens, é correto afirmar que:

a) a computação em nuvem é sempre aplicada com nuvens privadas que estão disponíveis para apenas uma organização.

b) a computação em nuvem é aplicada somente no modelo IaaS (*Infrastructure as a Service*).

c) uma das desvantagens da computação em nuvem é, geralmente, aumentar problemas de manutenção de infraestrutura.

d) uma das vantagens da computação em nuvem é facilitar a escalabilidade da solução de computação.

Questão 9 – Qual máscara de rede deve ser aplicada para delimitar exatamente 62 *hosts* à rede?

a) 255.255.255.240.

b) 255.255.255.252.

c) 255.255.255.100.

d) 255.255.255.192.

Questão 10 - Uma empresa vai instalar uma arquitetura de redes locais para trabalhar com fibra ótica. As redes devem trabalhar com anel duplicado e atuar com dados gerados pelo protocolo TCP/IP. A arquitetura montada deve ser do tipo:

a) ATM.

b) MPLS.

c) FDDI.

d) Appletalk.