

Aula 00 - Profs. Diego Carvalho e Renato da Costa

*TRANSPETRO (Profissional de Nível
Médio - Ênfase 1: Administração e
Controle) Noções de Informática - 2026*
Autor:
(Pós-Edital)
**Diego Carvalho, Equipe
Informática e TI, Renato da Costa**

14 de Agosto de 2026

Índice

1) Internet - Conceitos Básicos, Protocolos e Serviços - Teoria	3
2) Internet - Conceitos Básicos, Protocolos e Serviços - Resumo	58
3) Internet - Conceitos Básicos, Protocolos e Serviços - Questões Comentadas - CESGRANRIO	70
4) Internet - Conceitos Básicos, Protocolos e Serviços - Lista de Questões - CESGRANRIO	90



TÓPICOS DA AULA

Tópicos da Aula	3
Internet.....	5
Contexto Histórico	5
Conceitos Básicos	7
PAN (Personal Area Network).....	7
LAN (Local Area Network).....	8
MAN (Metropolitan Area Network).....	9
WAN (Wide Area Network).....	11
Web (WWW).....	13
Web 0.0.....	13
Web 1.0.....	14
Web 2.0.....	14
Web 3.0.....	14
Deep Web e Dark Web	16
Internet das Coisas (IoT).....	19
Tecnologias de Acesso	21
Protocolos de Comunicação	24
Conceitos Básicos	24
Modelo OSI/ISO.....	25
Arquitetura TCP/IP.....	28
Protocolos da Camada de Rede	29
Protocolos da Camada de Transporte.....	33
Protocolos da Camada de Aplicação	36
Serviço VoIP	53



Glossário	55
-----------------	----



INTERNET

Contexto Histórico

INCIDÊNCIA EM PROVA: MÉDIA

A Internet surgiu como um sistema de redes interconectadas, desenvolvida principalmente para fins militares dos EUA durante a Guerra Fria, visando a comunicação segura em caso de guerra nuclear. Iniciada nos anos 50, a criação da **ARPA (Advanced Research Projects Agency)** foi um marco, buscando manter os EUA na vanguarda tecnológica militar, especialmente após a URSS lançar o Sputnik.

A **ARPANET**, precursora da Internet, começou nos anos 60 ligando universidades. Era uma rede de comutação por pacotes, uma inovação comparada à antiga comutação por circuito usada em telefonia. Na comutação por pacotes, a informação é dividida em blocos (pacotes) que viajam independentemente pela rede, tornando a comunicação mais eficiente e robusta contra falhas, ao contrário da comutação por circuito, que reservava uma linha dedicada para cada comunicação.

Esse método permite um uso mais eficiente dos recursos da rede, evitando que canais fiquem reservados quando não estão sendo usados. Por exemplo, enviar um arquivo grande é como dividir um relatório volumoso em vários envelopes para enviar pelos correios. Cada pacote pode seguir uma rota diferente e chegar em ordem distinta, sendo remontado na ordem correta no destino.

Com o crescimento da ARPANET, surgiu o desafio de manter listas atualizadas de endereços de computadores na rede. Em 1973, optou-se por um registro central de endereços na Universidade de Stanford, facilitando a organização e o encaminhamento de pacotes. As diversas redes emergentes usavam formatos diferentes para pacotes, criando um desafio de compatibilidade. **A solução foi adotar um conjunto comum de protocolos de comunicação chamado TCP/IP.**

Esse conjunto de protocolos que padroniza a forma como os dados são transmitidos e recebidos, garantindo a comunicação eficaz entre diferentes redes e dispositivos. Dessa forma, a interconexão de redes usando o TCP/IP evoluiu para a moderna Internet. Atualmente, a internet oferece uma infinidade de serviços disponibilizados! Dentro os principais serviços ou aplicações, os mais conhecidos são:

SERVIÇOS	DESCRIÇÃO
WORLD WIDE WEB (WWW)	Trata-se do serviço de visualização de páginas web organizadas em sites em que milhares de pessoas possuem acesso instantâneo a uma vasta gama de informação online em hipermídia que podem ser acessadas via navegador – é o serviço mais utilizado na Internet. Em geral, esse serviço utiliza protocolos como HTTP e HTTPS.
CORREIO ELETRÔNICO	Trata-se do serviço de composição, envio e recebimento de mensagens eletrônicas entre partes de uma maneira análoga ao envio de cartas – é anterior à criação da Internet. Utiliza tipicamente um modo assíncrono de comunicação que permite a troca de mensagens dentro de uma organização. Em geral, esse serviço utiliza protocolos como POP3, IMAP e SMTP.
ACESSO REMOTO	Trata-se do serviço que permite aos usuários facilmente se conectarem com outros computadores, mesmo que eles estejam em localidades distantes no mundo. Esse acesso remoto pode ser feito de forma segura, com autenticação e criptografia de dados, se necessário. Em geral, esse serviço utiliza protocolos como SSH, RDP, VNC.
TRANSFERÊNCIA DE ARQUIVOS	Trata-se do serviço de tornar arquivos disponíveis para outros usuários por meio de downloads e uploads. Um arquivo de computador pode ser compartilhado ou transferido com diversas pessoas através da Internet, permitindo o acesso remoto aos usuários. Em geral, esse serviço utiliza protocolos como FTP e P2P.



WIKI	Wikis são plataformas colaborativas online que permitem que múltiplos usuários editem, criem e organizem conteúdo de forma conjunta. Qualquer pessoa pode modificar ou adicionar informações, facilitando a construção de conhecimento coletivo. Um exemplo famoso é a Wikipedia, onde o conteúdo é constantemente atualizado e expandido por sua comunidade de usuários.
FERRAMENTAS DE BUSCA	Ferramentas de busca são plataformas que permitem aos usuários pesquisar informações na web por meio de palavras-chave. Eles utilizam algoritmos para indexar e classificar páginas da internet, exibindo resultados relevantes em poucos segundos. Exemplos populares incluem Google, Bing e Yahoo, que ajudam a localizar websites, imagens, vídeos e outros conteúdos digitais.
REDES SOCIAIS	Redes sociais são plataformas digitais que conectam usuários, permitindo a criação e o compartilhamento de conteúdo como textos, imagens, vídeos e links. Elas facilitam a interação entre indivíduos e comunidades através de curtidas, comentários e mensagens. Exemplos incluem Facebook, Instagram e Twitter, que possibilitam a troca de informações em tempo real.
GRUPOS DE DISCUSSÃO	Grupos de Discussão são espaços virtuais onde pessoas com interesses comuns se reúnem para trocar informações, debater ideias e compartilhar experiências sobre um tema específico. Esses grupos podem ser organizados em fóruns online, listas de e-mails ou plataformas sociais, facilitando a comunicação e a colaboração entre os participantes em torno de tópicos variados.
COMPUTAÇÃO EM NUVEM	Computação em nuvem é a tecnologia que permite o armazenamento, processamento e gerenciamento de dados e aplicativos pela internet, em vez de servidores ou dispositivos locais. Os recursos de TI são fornecidos sob demanda, permitindo que empresas e usuários acessem dados remotamente, escalem operações e reduzam custos de infraestrutura física.
PORTAIS WEB	Portais Web são plataformas que centralizam e organizam uma vasta gama de informações e serviços em um único local online. Eles oferecem acesso a conteúdos diversos, como notícias, e-mails, fóruns, e-commerce e mais. Funcionam como uma porta de entrada para a navegação na web, facilitando o acesso a recursos variados em um só lugar.

Importante: a internet funciona em uma arquitetura cliente/servidor, organizando a comunicação de forma eficiente entre dispositivos. O cliente é o dispositivo que faz solicitações (como navegar em um site) e o servidor é o responsável por processar essas solicitações e fornecer os recursos, como páginas web ou arquivos. Essa separação permite que servidores centralizem e gerenciem os dados, enquanto clientes acessam remotamente, garantindo escalabilidade e compartilhamento de recursos na rede.



Conceitos Básicos

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

A Internet é uma rede de computadores, logo é importante entender a definição de redes de computadores:

"Uma rede é um conjunto de terminais, equipamentos, meios de transmissão e comutação que interligados possibilitam a prestação de serviços".

Eu gosto de uma definição mais simples que afirma que uma rede é um conjunto de dispositivos (normalmente conhecidos como nós) conectados por links de comunicação. Em uma rede, um nó pode ser um computador, uma impressora, um notebook, um *smartphone*, um *tablet*, um *Apple Watch* ou qualquer outro dispositivo de envio ou recepção de dados, desde que ele esteja conectado a outros nós da rede.

As primeiras redes de computadores surgiram dentro de organizações – como uma empresa ou um laboratório de pesquisa – para facilitar a troca de informações entre diferentes pessoas e computadores. **Esse método era mais rápido e confiável do que anterior, que consistia em pessoas carregando pilhas e pilhas de cartões perfurados ou fitas magnéticas de um lado para o outro dentro de uma organização.**

Um segundo benefício das redes de computadores é a capacidade de compartilhar recursos físicos. Por exemplo: em vez de cada computador possuir sua própria impressora, todos em um departamento poderiam compartilhar apenas uma impressora conectada à rede de computadores. Outro uso comum era compartilhar dispositivos de armazenamento, que na época eram muitos caros e não era viável ter um para cada computador.

Como nós podemos resumir tudo isso? **Bem, uma rede de computadores basicamente tem como objetivo o compartilhamento de recursos, deixando equipamentos, programas e principalmente dados ao alcance de múltiplos usuários,** sem falar na possibilidade de servir como meio de comunicação entre pessoas através da troca de mensagens de texto, áudio ou vídeo entre os dispositivos.

As redes de computadores podem ser classificadas quanto à dimensão, tamanho ou abrangência de área geográfica em PAN, LAN, MAN e WAN:

PAN (Personal Area Network)

INCIDÊNCIA EM PROVA: BAIXA

A **Rede de Área Pessoal** é definida como uma rede de computadores utilizada para conectar e transmitir dados entre dispositivos localizados em uma área pessoal. Pode ser chamada também de WPAN (Wireless Personal Area Network), uma vez que seu principal meio de transmissão é o Bluetooth. Em suma, ela é basicamente uma rede de computadores ou dispositivos que abrange um espaço pequeno (em geral, alguns metros).



DISTÂNCIA

ALGUNS CENTÍMETROS A POUCOS METROS

Sabe aquele domingo que você leva sua caixinha de som para ouvir uma música na beira da piscina e a conecta ao seu *smartphone*? **Pois é, isso é uma PAN!** Sabe quando você vai dar aquela corridinha



segunda-feira e leva seu fone de ouvido sem fio conectado ao seu smartphone para ouvir uma música? **Isso também é uma PAN!** Enfim... entenderam, não é? Cuidado: PAN nem sempre é tratada em questões como uma classificação padrão!

CARACTERÍSTICAS	DESCRIÇÃO
DEFINIÇÃO	Rede pessoal que cobre uma área pequena, geralmente cerca de alguns metros.
COBERTURA	Alguns centímetros a poucos metros.
FINALIDADE	Conectar dispositivos pessoais de curto alcance.
VELOCIDADE	Geralmente de alta velocidade devido à proximidade dos dispositivos.
TECNOLOGIAS	Em geral, Bluetooth, Wi-Fi, USB.
SEGURANÇA	Geralmente mais segura devido à proximidade física.
COMPLEXIDADE	Menos complexa devido à simplicidade da conexão.
ISOLAMENTO	Fácil de isolar problemas devido à proximidade.
APLICAÇÕES	Conexão de dispositivos pessoais (Ex: fones de ouvido sem fio, teclados, etc).

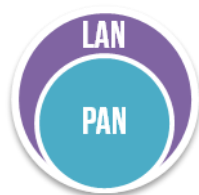
(INSTITUTO VERBENA / IFG - 2022) Uma classificação para os tipos de redes de comunicação de dados, ou redes de computadores, e que é muito adotada na literatura técnica dessa área, leva em conta o alcance máximo de transmissão, seja por meio de cabo, seja sem fio. Considerando o critério acima mencionado, a tecnologia de rede sem fio denominada Bluetooth® é um exemplo de classificação do tipo:

- a) Local Area Network (LAN).
- b) Wide Area Network (WAN).
- c) Personal Area Network (PAN).
- d) Metropolitan Area Network (MAN).

Comentários: o bluetooth é comumente associado a redes de curto alcance (Personal Area Networks), que são projetadas para conectar dispositivos em uma área pessoal próxima, geralmente dentro de alguns metros de alcance (Letra C).

LAN (Local Area Network)

INCIDÊNCIA EM PROVA: ALTÍSSIMA



DISTÂNCIA

DE ALGUMAS CENTENAS DE METROS A ALGUNS QUILOMETROS

A **Rede de Área Local** é definida como uma rede de computadores utilizada para conectar e transmitir dados entre dispositivos localizados em uma área de abrangência local. *Quem aí já foi a uma Lan House?* O nome já dá a dica, trata-se de uma LAN. A rede da sua casa também, assim como a rede do andar de um prédio ou a rede de um órgão localizado em um único espaço físico também são redes locais.

Dessa forma, podemos dizer que uma LAN é uma rede de computadores que abrange uma área geográfica relativamente pequena, como um escritório, uma residência, um prédio ou um campus. **Ela é projetada para a interconexão de dispositivos próximos, geralmente dentro de um único local geográfico.** Ela permite a troca de informações, a comunicação eficaz entre os dispositivos conectados e o compartilhamento de recursos (como impressoras e arquivos).



As redes de área local oferecem uma velocidade de comunicação relativamente alta, permitindo uma rápida transferência de dados entre dispositivos, podendo ser configuradas em várias topologias, como barramento, anel ou estrela (mais comum). Além disso, elas podem ser cabeadas ou não. **Em geral, esse tipo de rede possui baixa ocorrência de erros por serem redes pequenas e contidas em um local específico.**

CARACTERÍSTICAS	DESCRIÇÃO
DEFINIÇÃO	Rede local que abrange uma área geográfica limitada (Ex: edifício ou campus).
COBERTURA	De algumas centenas de metros a alguns quilômetros.
FINALIDADE	Facilitar a comunicação dentro de uma organização local.
VELOCIDADE	Alta velocidade dentro da rede local.
TECNOLOGIAS	Em geral, Ethernet e Wi-Fi.
SEGURANÇA	Pode ser configurada com medidas de segurança, como firewalls.
COMPLEXIDADE	De complexidade moderada, dependendo do tamanho da rede.
ISOLAMENTO	Problemas podem ser isolados com relativa facilidade.
APLICAÇÕES	Uso em escritórios, escolas e redes corporativas locais.

(AMEOSC / Prefeitura de São João do Oeste-SC - 2023) "No contexto da informática, uma rede consiste em diversos processadores que estão interligados e compartilham recursos entre si". (Tanenbaun, 2014). Os principais tipos de redes de computadores são: LAN, MAN, WAN, WLAN. Assinale a seguir a alternativa que fala corretamente sobre as redes tipo LAN:

- a) As LANs são redes de computadores que abrangem uma área restrita, como um escritório, uma escola ou um prédio, permitindo a comunicação entre dispositivos próximos.
- b) As LANs são redes de computadores que utilizam apenas tecnologias sem fio (Wi-Fi) para conectar dispositivos dentro de uma área restrita, como um escritório ou uma casa.
- c) As LANs são redes de computadores que conectam dispositivos em longas distâncias, utilizando cabos submarinos e satélites para comunicação global.
- d) As LANs são redes de computadores que abrangem uma ampla área geográfica, como um país inteiro, permitindo a conexão entre diferentes regiões.

Comentários: (a) Correto, ela realmente é projetada para abranger uma área geograficamente restrita, como um escritório, uma escola, um prédio ou uma residência, permitindo a comunicação entre dispositivos próximos; (b) Errado, elas podem empregar tanto tecnologias com fio quanto sem fio, dependendo das necessidades e da infraestrutura do ambiente; (c) Errado, redes de longas distâncias são chamadas de WAN (Wide Area Network); (d) Errado, Elas abrangem áreas restritas e não têm a capacidade de conectar diferentes regiões ou países (Letra A).

MAN (Metropolitan Area Network)

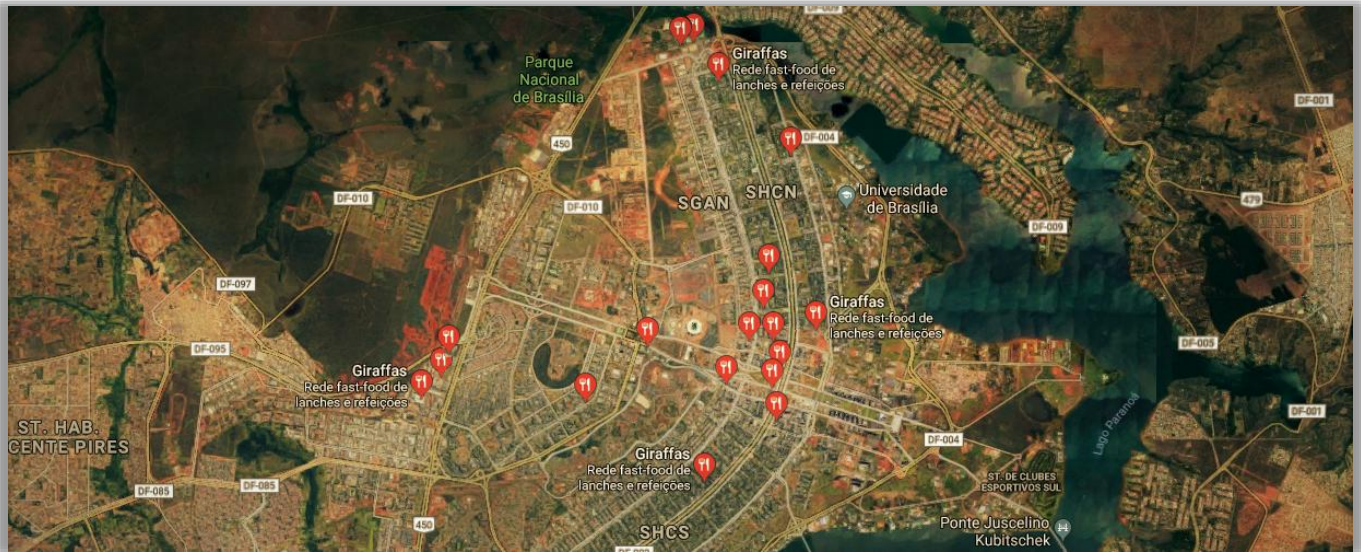
INCIDÊNCIA EM PROVA: ALTÍSSIMA



DISTÂNCIA

ALGUMAS DEZENAS DE QUILOMETROS





A **Rede de Área Metropolitana** é definida como uma rede de computadores utilizada para conectar e transmitir dados entre dispositivos localizados em locais distintos. Elas possuem abrangência maior que a de uma rede local e menor que a de uma rede extensa - que veremos a seguir. Normalmente uma rede metropolitana resulta da interligação de várias redes locais em uma cidade, formando assim uma rede de maior porte.

Na imagem, temos uma foto aérea de Brasília! Eu não sei se vocês sabem, mas foi aqui que foi criada a Rede de Fast-food Giraffas! Na imagem, temos a localização de dezenas de filiais dessa empresa em uma mesma cidade: **essas filiais podem se conectar formando uma única rede de área metropolitana espalhada em diferentes locais dentro de uma mesma cidade ou metrópole** a uma distância maior que a de uma rede local e menor que a de uma rede extensa.

CARACTERÍSTICAS	DESCRIÇÃO
DEFINIÇÃO	Rede metropolitana que abrange uma cidade ou uma área metropolitana.
COBERTURA	Algumas dezenas de quilômetros.
FINALIDADE	Conectar redes locais dentro de uma área metropolitana.
VELOCIDADE	Velocidade variável, dependendo da infraestrutura da rede.
TECNOLOGIAS	Em geral, Ethernet e fibra óptica.
SEGURANÇA	Maior risco devido à extensão geográfica, exigindo segurança adicional.
COMPLEXIDADE	Moderadamente complexa por conta da complexidade da infraestrutura.
ISOLAMENTO	Pode ser desafiador isolar problemas devido à extensão geográfica.
APLICAÇÕES	Integração de redes locais em uma área metropolitana.

(VUNESP / ALESP - 2022) O aspecto principal que distingue as tecnologias de rede do tipo A das tecnologias de rede do tipo B é a escalabilidade, pois uma rede do tipo A deve ter a capacidade de crescer o quanto for necessário para permitir a conexão de uma grande quantidade de sites espalhados a grandes distâncias geográficas, com muitos computadores presentes em cada site. A e B são, respectivamente:

- LAN (Local Area Network) e WAN (Wide Area Network).
- LAN (Local Area Network) e MAN (Metropolitan Area Network).
- WAN (Wide Area Network) e LAN (Local Area Network).
- PAN (Personal Area Network) e WMAN (Wireless Metropolitan Area Network).



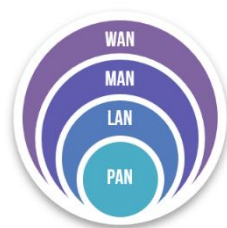
e) PAN (Personal Area Network) e WAN (Wide Area Network).

Comentários: escalabilidade é a capacidade de um sistema, rede, aplicativo ou recurso de expandir sua capacidade para acomodar um aumento crescente na carga de trabalho ou no volume de dados. Em termos mais simples, significa que um sistema escalável é capaz de crescer e lidar com demandas crescentes sem perder desempenho ou eficiência.

As redes WAN são projetadas para abranger grandes distâncias geográficas e interconectar sites distribuídos globalmente, o que requer escalabilidade para suportar muitos computadores em cada site. Por outro lado, as LANs são redes locais que normalmente abrangem uma área geográfica restrita, como um escritório, escola ou prédio, e geralmente não precisam suportar a mesma escala que as WANs (Letra C).

WAN (Wide Area Network)

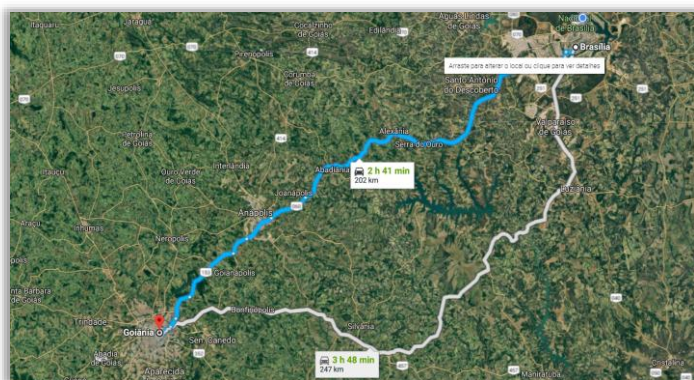
INCIDÊNCIA EM PROVA: ALTÍSSIMA



DISTÂNCIA

CENTENAS A MILHARES DE QUILOMETROS

A **Rede de Área Extensa** é definida como uma rede de computadores utilizada para conectar e transmitir dados entre dispositivos localizados em uma grande área geográfica. E quando eu digo grande, é grande mesmo – podendo ser entre cidades, entre países ou – até mesmo – entre continentes diferentes. O Programa Antártico Brasileiro (PROANTAR) – por exemplo – realiza pesquisas nesse continente e envia os dados para o Brasil por meio de uma rede extensa.



Quando uma empresa possui filiais em cidades ou países diferentes, ela pode criar uma Rede WAN. *Aliás, vocês sabem qual é o melhor e mais clássico exemplo de WAN? A Internet! Sim, a Internet é uma WAN – conforme mostra a imagem ao lado. Outro exemplo seria uma rede entre filiais de empresas localizadas em Brasília e Goiânia – como apresentado na imagem acima. Essa rede formaria o que nós chamamos de rede de área extensa.*

CARACTERÍSTICAS	DESCRIÇÃO
DEFINIÇÃO	Rede de grande área que pode abranger cidades, países ou até continentes.
COBERTURA	Centenas a milhares de quilômetros.
FINALIDADE	Conectar redes em diferentes locais geograficamente distantes.
VELOCIDADE	Geralmente menor velocidade devido a longas distâncias.
TECNOLOGIAS	Frame Relay, MPLS, Internet.
SEGURANÇA	Requer medidas rigorosas devido ao alcance e à exposição a ameaças.



COMPLEXIDADE	Em geral, complexa devido à escala global e aos diferentes tipos de tecnologia.
ISOLAMENTO	Requer ferramentas avançadas para isolar problemas em redes extensas.
APLICAÇÕES	Comunicação em escala regional, nacional ou global.

(QUADRIX / CFT - 2021) A Internet, que é uma rede global, é um exemplo de rede WAN (Wide Area Network).

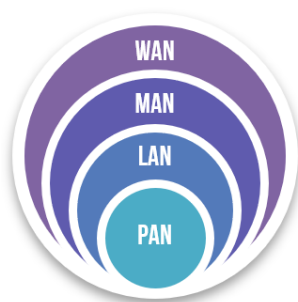
Comentários: a Internet é um exemplo clássico de uma rede WAN (Wide Area Network). Uma WAN abrange uma grande área geográfica, conectando dispositivos em diferentes locais, como cidades, países ou mesmo continentes. A Internet é a maior rede WAN do mundo, conectando bilhões de dispositivos em todo o planeta, permitindo a troca de dados e comunicação entre eles (Correto).

(AOCP / UFFS - 2019) Para que possa ser implementada uma correta e adequada interconexão de redes de computadores, é muito importante definir que tipo de rede será construída e utilizada para a comunicação. Dentro desse cenário, a rede a ser desenvolvida possui as seguintes características: deve cobrir áreas geograficamente dispersas, abrangendo uma grande área; deve possuir a interconexão de várias sub-redes de comunicação; e deve conter inúmeras linhas de transmissão. Com base nas características apresentadas, qual é o melhor tipo de rede para implementação?

- a) MAN (Metropolitan Area Networks).
- b) LAN (Local Area Networks).
- c) WAN (Wide Area Networks).
- d) PAN (Personal Area Networks).
- e) VLAN (Virtual Local Area Networks).

Comentários: o melhor tipo de rede para implementação é o WAN - ela é projetada para cobrir áreas geograficamente dispersas e permite a interconexão de várias sub-redes de comunicação. Também é caracterizada por utilizar inúmeras linhas de transmissão para possibilitar a comunicação em larga escala, geralmente em âmbito nacional ou internacional (Letra C).

TIPO	SIGLA	DESCRIÇÃO	DISTÂNCIA
PERSONAL AREA NETWORK	PAN	Rede de computadores pessoal (celular, tablet, notebook, etc).	De alguns centímetros a alguns poucos metros.
LOCAL AREA NETWORK	LAN	Rede de computadores de lares, escritórios, prédios, entre outros.	De algumas centenas de metros a alguns quilômetros.
METROPOLITAN AREA NETWORK	MAN	Rede de computadores entre uma matriz e filiais em uma cidade.	Cerca de algumas dezenas de quilômetros.
WIDE AREA NETWORK	WAN	Rede de computadores entre cidades, países ou até continentes.	De algumas dezenas a milhares de quilômetros.



Essas classificações apresentadas possuem uma classificação correspondente quando se trata de um contexto de transmissão sem fio (wireless). Em outras palavras, há também WPAN, WLAN, WMAN e WWAN. Por outro lado, as questões de prova nem sempre são rigorosas na utilização desses termos (Ex: é comum enunciados tratando de redes locais sem fio como LAN e, não, WLAN). Infelizmente, desencanem na hora de resolver questões de prova.



Web (WWW)

INCIDÊNCIA EM PROVA: BAIXA

Web é uma contração do termo World Wide Web (WWW). Ah, professor... você tá falando de internet, não é? Não! Muito cuidado porque são coisas diferentes! **A internet é uma rede mundial de computadores que funciona como uma estrutura que transmite dados para diferentes aplicações.** A Web é apenas uma dessas aplicações – uma gigantesca aplicação distribuída rodando em milhões de servidores no mundo inteiro usando navegadores.

Vamos entender isso melhor por meio de uma analogia: a Internet pode ser vista como uma vasta rede rodoviária que conecta cidades, estados e países. Essas estradas permitem que você vá de um lugar para outro, independentemente de qual seja o seu destino. Nessa rede rodoviária, você pode dirigir um carro, andar de bicicleta, caminhar, pegar um ônibus ou usar qualquer outro meio de transporte que desejar. **A estrutura das estradas e rodovias é o que torna tudo isso possível.**

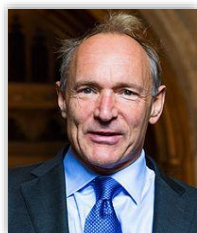
Agora, pense na web como lojas, casas, escritórios e pontos de interesse que você encontra ao longo das estradas da Internet. Cada loja ou local representa um site da web, e você pode visitá-los para obter informações, fazer compras, se divertir, etc. Os sites da web são destinos ao longo da estrada. Em suma: a web é composta por uma vasta coleção de documentos e recursos interconectados, que são acessados por **meio de navegadores da web.**

COMPONENTES DA WEB	DESCRIÇÃO
HIPERTEXTO	A Web é baseada em documentos que contêm links (hiperlinks) para outros documentos relacionados. Isso permite que os usuários naveguem de uma página para outra, seguindo os links.
URL	Cada documento ou recurso na Web é identificado por um URL exclusivo, que é um endereço usado para acessar o recurso em um navegador.
NAVEGADORES DA WEB	São aplicativos que permitem aos usuários visualizar e interagir com documentos da Web. Exemplos populares de navegadores incluem o Google Chrome, Mozilla Firefox, Microsoft Edge e Safari.
PROTOCOLOS DE COMUNICAÇÃO	A Web utiliza protocolos de comunicação, como HTTP (Hypertext Transfer Protocol) e HTTPS (HTTP Secure), para transferir dados entre navegadores e servidores web.
SERVIDORES WEB	São computadores que hospedam documentos e recursos da Web. Eles respondem às solicitações dos navegadores e fornecem os conteúdos solicitados.
PÁGINAS DA WEB	São documentos criados usando linguagens de marcação, como HTML (Hypertext Markup Language). As páginas da web podem conter texto, imagens, links e outros elementos interativos.
MOTORES DE BUSCA	São ferramentas que ajudam os usuários a encontrar informações na Web, indexando e classificando páginas da web com base em palavras-chave.

Agora vamos falar um pouco agora sobre as gerações da web (note que elas não se excluem, elas se sobrepõem). Vamos vê-las em detalhes...

Web 0.0





Em março de 1989, a World Wide Web teve a primeira especificação composta pelo Protocolo HTTP e a Linguagem HTML lançada por Tim Berners-Lee. Sim, se utilizamos a web atualmente, devemos agradecer a esse senhor aqui do lado! Até então, a web era uma fonte de acesso a informações, onde páginas de hipertexto (textos com links), de conteúdo estático, escritas por jornalistas e outros profissionais eram publicadas em Servidores Web e podiam apenas ser lidas pelos demais usuários. *Galera, vocês querem conhecer a primeira página web da história? Segue o link:*

[HTTP://INFO.CERN.CH/HYPertext/WWW/THEPROJECT.HTML](http://info.cern.ch/Hypertext/WWW/TheProject.html)

Em 1991, a página web acima era a única do mundo; em 1994, já havia 2.738 páginas web - inclusive o **Yahoo!**; em 1998, já havia 2.410.067 páginas web - inclusive o **Google**; em 2001, já havia 29.254.370 páginas web - inclusive a **Wikipedia**; em 2005, já havia 64.780.617 páginas web - inclusive o **Youtube**; em 2008, já havia 172.338.776 páginas web - inclusive o **Dropbox**; e em 2018, temos 1.805.260.010 páginas web - inclusive o **Estratégia Concursos!**

Web 1.0

A Web 1.0 é a primeira fase da internet, caracterizada por sites estáticos, com conteúdo fixo e pouca ou nenhuma interação dos usuários. Nessa época, as páginas eram basicamente informativas, apresentando textos e imagens sem a possibilidade de colaboração ou personalização. Os usuários eram apenas consumidores de conteúdo, e a comunicação era unidirecional, com pouca interatividade entre o criador e o visitante.

Web 2.0

A Web 2.0 refere-se à segunda geração da internet, caracterizada pela interatividade e colaboração dos usuários. Diferente da Web 1.0, que era estática e unidirecional, a Web 2.0 permite a criação e compartilhamento de conteúdo em plataformas como redes sociais, blogs e wikis. Os usuários deixam de ser apenas consumidores e passam a ser também criadores de conteúdo, com destaque para a evolução de interfaces mais dinâmicas e amigáveis.

Web 3.0

A Web 3.0, também chamada de Web Semântica, é a evolução da internet que visa tornar os dados mais inteligíveis para máquinas, permitindo uma navegação mais personalizada e conectada. Baseada em tecnologias como inteligência artificial, blockchain e descentralização, a Web 3 permite que os usuários tenham maior controle sobre seus dados e interajam com aplicativos sem intermediários, promovendo segurança, transparência e interoperabilidade.

CARACTERÍSTICAS	WEB 1.0	WEB 2.0	WEB 3.0
INTERATIVIDADE	Baixa	Alta	Muito Alta
CONTEÚDO	Estático e somente leitura	Dinâmico, com feedback do usuário	Inteligente, com semântica
USUÁRIOS	Consumidores passivos	Produtores de conteúdos	Participantes ativos
SOCIALIZAÇÃO	Ausente	Integração de redes sociais	Integração com IA e Internet das Coisas



EXPERIÊNCIA DO USUÁRIO	Limitada	Melhorada e personalizada	Altamente personalizada
TECNOLOGIA	HTML	AJAX, APIs e RSS	IA e Aprendizado de Máquina
EXEMPLOS	Sites estáticos de início da web	Redes sociais, blogs e wikis	Assistentes virtuais
PRINCIPAIS APLICAÇÕES	Sites informativos e institucionais	Redes sociais e colaboração online	Assistentes virtuais e Internet das Coisas



Deep Web e Dark Web

INCIDÊNCIA EM PROVA: MÉDIA

A web é dividida em diferentes camadas, sendo a Surface Web apenas cerca de 4% dela. Ela é composta por sites e páginas que podem ser indexados por mecanismos de busca comuns (Ex: Google ou Bing), e acessados sem autenticação. Por exemplo, páginas abertas em redes sociais como Facebook são parte da Surface Web. Os outros 96% compõem a Deep Web, que inclui páginas não indexáveis por mecanismos de busca padrão e protegidas por autenticação.

SURFACE WEB	DESCRIÇÃO
ACESSIBILIDADE	Facilmente acessível por meio de mecanismos de busca e navegadores padrão.
CONTEÚDO PÚBLICO	Compreende sites, páginas e conteúdo que são acessíveis ao público em geral.
INDEXAÇÃO POR MECANISMOS DE BUSCA	Os motores de busca, como Google e Bing, indexam e exibem o conteúdo da Surface Web em resultados de pesquisa.
INFORMAÇÕES AMPLAMENTE VISÍVEIS	Notícias, blogs, lojas online, fóruns públicos e outros tipos de sites podem ser encontrados na Surface Web.
SEM RESTRIÇÕES SIGNIFICATIVAS	Os usuários podem navegar e acessar conteúdo sem a necessidade de credenciais ou permissões especiais.
EXEMPLOS	Páginas de notícias, blogs, lojas online e outros sites acessíveis ao público em geral.

Um exemplo disso é a Intranet, acessível somente a servidores autorizados, o que a coloca na Deep Web. **Embora não visível para quem não tem autorização, não é completamente segura em termos de privacidade.** A comunicação entre computadores e servidores deixa rastros, que podem ser usados para identificar usuários e suas atividades na web. Isso levanta preocupações sobre privacidade, especialmente em países com regimes repressivos ou censura.

DEEP WEB	DESCRIÇÃO
CONTEÚDO NÃO INDEXADO POR MOTORES DE BUSCA	O conteúdo da Deep Web não é indexado pelos mecanismos de busca tradicionais, o que o torna invisível nas pesquisas comuns.
REQUER AUTENTICAÇÃO	Muitos sites da Deep Web exigem credenciais ou autenticação para acessar, tornando o conteúdo acessível apenas a usuários autorizados.
INFORMAÇÕES CONFIDENCIAIS	Inclui informações privadas, como dados de empresas, registros médicos, sistemas de gerenciamento de bibliotecas e muito mais.
NÃO ACESSÍVEL POR LINKS COMUNS	Você não pode simplesmente clicar em um link para acessar o conteúdo da Deep Web; geralmente, precisa de informações de login ou URLs específicas.
VARIEDADE DE CONTEÚDO	A Deep Web abrange uma ampla gama de informações, desde bancos de dados privados a sistemas de gerenciamento de conteúdo corporativo.

A Dark Web, uma subseção da Deep Web, oferece maior privacidade e anonimato. Ela não é indexada por mecanismos de busca e requer o uso de redes e navegadores especiais para ser acessada. A mais conhecida dessas redes é a Tor, originalmente um projeto militar dos EUA para comunicação segura. O navegador Tor permite acessar a Surface Web, Deep Web e Dark Web, sendo uma ferramenta crucial para pessoas em países com restrições de acesso à Internet. Não confunda Dark Web com Darknet:



a segunda é a infraestrutura de rede anônima utilizada para comunicação privada; e a primeira são os sites, serviços e conteúdos hospedados dentro dessa rede.

DARK WEB	DESCRIÇÃO
ACESSÍVEL COM SOFTWARE ESPECÍFICO	A Dark Web é acessada por meio de redes criptografadas, como o Tor (The Onion Router), que requerem software especial para acesso.
CONTEÚDO ILEGAL E OSCURO	Inclui sites que hospedam atividades ilegais, como tráfico de drogas, armas, venda de informações roubadas e outros conteúdos obscuros.
ANONIMATO É VALORIZADO	Os usuários da Dark Web muitas vezes valorizam o anonimato, pois os serviços são frequentemente anônimos e transações são criptografadas.
RISCOS À SEGURANÇA	A Dark Web é um ambiente de alto risco, onde os usuários podem ser vítimas de fraudes e ataques cibernéticos.
NÍVEIS PROFUNDOS DE ANONIMATO	Diferentemente da Deep Web, a Dark Web oferece um nível mais profundo de anonimato e criptografia, tornando difícil rastrear usuários.

O Navegador Tor direciona as requisições de uma página através de uma rota que passa por uma série de servidores proxy da Rede Tor operados por milhares de voluntários em todo o mundo, **tornando o endereço IP não identificável e não rastreável**¹. Vocês não precisam entender como isso funciona, vocês só precisam entender que os dados passam por uma série de camadas de encriptação de modo que seja praticamente impossível identificar de onde veio a requisição.

Conforme eu disse anteriormente, pode-se acessar páginas da Surface Web por meio desse navegador. Nesse caso, não é possível identificar quem está acessando, mas é possível identificar qual serviço está acessando (Ex: Google). Por outro lado, há algumas páginas da Dark Web que realmente só existem dentro da Rede Tor. Nesse caso, é absolutamente impossível identificar quem está acessando, quando está acessando, o que está acessando, etc – é completamente anônimo.

Galera, você pode encontrar usuários negociando entorpecentes e armas, contratando matadores de aluguel, planejando atentados terroristas, enviando vídeos de suicídio, compartilhando fotos de pedofilia, vazando documentos de empresas ou governos, trocando fotos de nudez, exibindo fotos/vídeos de torturas, estupro e homicídios de pessoas e animais, conteúdos racistas e xenófobos, canibalismo, esquisitices, falsificação de documentos, entre outros.

Eu sei que essa aula atiga a curiosidade de várias pessoas, mas eu já adianto que não recomendo que vocês acessem esses sites. Saibam que se trata de um ambiente em que é possível encontrar um bocado de hackers, cibercriminosos e outros profissionais desse tipo. Eu já recebi perguntas de alunos perguntando sobre “hipóteses” de atividades não muito legítimas. **Para terminar, vamos apenas falar um pouco sobre a relação entre a Dark Web e Criptomoedas.**

Em 2013, o site Silk Road, acessado pela Dark Web, permitia a venda de produtos ilícitos como drogas. Em vez de cartões de crédito, que deixam rastros, as transações eram feitas com Bitcoin, uma criptomoeda que não passa pelo sistema financeiro tradicional e oferece anonimato. No entanto, o dono do site foi preso após usar seu nome verdadeiro em um fórum da Surface Web, permitindo ao FBI conectá-lo a atividades ilícitas e condená-lo a prisão perpétua.

Por fim, vamos resumir tudo o que vimos na tabela apresentada a seguir e, por fim, uma analogia para finalmente consolidar o entendimento sobre esse conteúdo.

¹ O nome **Tor** vem de **The Onion Router** (O Roteador Cebola) porque os dados passam por diversas camadas de encriptação como em uma cebola.



CARACTERÍSTICAS	SURFACE WEB	DEEP WEB	DARK WEB
ACESSIBILIDADE	Acessível por mecanismos de busca e navegadores comuns.	Requer credenciais específicas ou URLs exclusivas.	Acessível apenas por redes criptografadas, como o Tor.
CONTEÚDO COMUM	Contém informações e sites disponíveis publicamente.	Inclui conteúdo não indexado por mecanismos de busca, como bancos de dados privados.	Contém conteúdo obscuro e frequentemente ilegal.
ANONIMATO	Não oferece anonimato especial para usuários.	Pode exigir credenciais de login, mas não enfatiza o anonimato.	Valoriza altos níveis de anonimato e segurança.
CONTEÚDO COMERCIAL	Amplamente usado para negócios, educação, entretenimento e informações públicas.	Inclui recursos protegidos por senha, como e-mails, serviços bancários online e redes corporativas.	Muitas vezes associada a atividades ilegais e conteúdo obscuro.
EXEMPLOS	Sites de notícias, blogs, redes sociais, sites de compras online.	E-mails privados, intranets corporativas, bancos de dados de bibliotecas.	Sites de venda de drogas, mercados negros, fóruns de hackers.



Internet das Coisas (IoT)

INCIDÊNCIA EM PROVA: BAIXA

A transformação digital é o processo em que empresas e sociedades integram tecnologias digitais inovadoras para melhorar operações, resolver problemas e entregar mais valor aos clientes. Isso envolve uma mudança estrutural e cultural, com a tecnologia desempenhando um papel central no sucesso e resiliência dos negócios. Com a crescente adoção de dispositivos inteligentes, a conectividade global se expande rapidamente.

A pandemia de COVID-19 acelerou essa transformação, forçando empresas a adotar o trabalho remoto e reconfigurar operações para atender às novas demandas. A digitalização tornou-se essencial para enfrentar desafios econômicos e operacionais, consolidando-se como um pilar para o futuro das empresas e da sociedade. **Dito isso, vamos falar um pouco sobre uma tecnologia que vem para acelerar ainda mais o processo de transformação digital...**

INTERNET DAS COISAS

Trata-se de uma revolução tecnológica que se refere à conexão de dispositivos físicos e objetos do mundo real à internet. Esses dispositivos, também chamados de "coisas" na IoT, são integrados com sensores, software e outras tecnologias para coletar e trocar dados com outros dispositivos e sistemas pela internet.

A Internet das Coisas (IoT) se refere à conexão de dispositivos diversos à internet, além dos comuns como smartphones e computadores. Itens como câmeras de segurança, Smart TVs e videogames já fazem parte dessa rede, e em países mais desenvolvidos, até geladeiras e máquinas de lavar estão conectadas. A ideia é tornar esses dispositivos mais eficientes em suas funções específicas.

A IoT tem aplicações além das residências, como em setores como agricultura, pecuária, hospitais, escolas e indústrias, aumentando a eficiência e automação em diversas áreas. Com o avanço do 5G, a conectividade entre esses objetos se tornará ainda mais comum, acelerando a transformação digital e ampliando as possibilidades de uso em diferentes contextos. IoT não é uma tecnologia monolítica -seus componentes principais podem variar bastante. Vejamos:

COMPONENTES	DESCRIÇÃO
DISPOSITIVOS	São os elementos físicos que compõem a IoT, como sensores, atuadores e outros dispositivos conectados, como câmeras, medidores inteligentes, veículos e eletrodomésticos. Eles coletam dados do mundo real e podem executar ações com base nesses dados.
TECNOLOGIAS DE COMUNICAÇÃO	São os meios pelos quais os dispositivos IoT se comunicam entre si e com a nuvem. Isso pode incluir Wi-Fi, Bluetooth, 3G/4G/5G, Zigbee, LoRa, entre outros. As redes de comunicação são responsáveis pela transferência de dados dos dispositivos para a nuvem e vice-versa.
SENSORES E ATUADORES	Os sensores coletam informações do ambiente, como temperatura, umidade, localização, movimento e muito mais. Os atuadores são responsáveis por tomar ações, como ligar ou desligar um dispositivo. Eles são os olhos e as mãos da IoT.
NUVEM (CLOUD)	A nuvem é onde os dados coletados pelos dispositivos IoT são processados, armazenados e disponibilizados para acesso. Plataformas de nuvem fornecem recursos de computação, armazenamento e análise de dados em grande escala, tornando possível o processamento de grandes volumes de informações.

Imagine uma casa que tem monitoramento de segurança, controle de temperatura ambiente e gerenciamento de iluminação integrados. Os dados de câmeras, alarmes contra incêndio, aparelhos de



ar-condicionado, lâmpadas e outros itens são enviados para um sistema que controla cada aspecto. **Esse sistema pode ser um serviço em nuvem, garantindo acesso a ele a partir de qualquer lugar.**

Lembrando que o IPv6 (evolução do IPv4) permitiu a oferta de um número absurdamente gigantesco de endereços, logo a quantidade de dispositivos e sensores não deverá ser um problema por um bom tempo. É importante destacar também que a comunicação é um elemento essencial para a transmissão de dados entre dispositivos, sensores e sistemas de IoT. Vejamos algumas das principais tecnologias e protocolos de comunicação utilizados na IoT:

TECNOLOGIAS DE COMUNICAÇÃO	DESCRIÇÃO
WI-FI (802.11)	Trata-se de uma das tecnologias de comunicação sem fio mais amplamente utilizadas e oferece alta largura de banda. É adequado para dispositivos que têm acesso a redes locais de alta velocidade e energia suficiente.
BLUETOOTH (802.15)	Trata-se de uma tecnologia de comunicação sem fio de curto alcance, adequada para dispositivos pessoais, como fones de ouvido sem fio e dispositivos vestíveis. O Bluetooth Low Energy (BLE) é uma variante de baixo consumo de energia.
ZIGBEE	Trata-se de um padrão de comunicação sem fio de baixa potência projetado para redes de sensores e dispositivos IoT em ambientes domésticos e industriais.

Poxa, Diego... IoT só tem coisas boas! Calma, não é bem assim! **Os dispositivos podem eventualmente estar vulneráveis a ataques de segurança e privacidade.** Existe uma infinidade de riscos associados à IoT, tais como: riscos de um dispositivo permitir o acesso não autorizado e o uso indevido de informações pessoais; riscos de facilitar ataques em outros sistemas, escalonando privilégios ao invasor; riscos de os dispositivos servirem de escravos em botnets; entre outros.

VANTAGENS	DESVANTAGENS
Varejistas podem fornecer bônus de fidelidade para clientes preferenciais.	A dependência de compras online pode custar empregos.
As cidades podem avaliar as necessidades futuras de transporte.	Os varejistas podem saber tudo o que você está comprando.
Indivíduos podem reduzir os custos de energia e dos sistemas de aquecimento residenciais.	Os indivíduos podem receber mais e-mails de spam.
Fabricantes podem reduzir a inatividade prevendo as necessidades de manutenção dos equipamentos.	Uma falha da rede pode ser catastrófica.
Os governos podem monitorar o ambiente.	As empresas que criam dispositivos vestíveis têm muitas informações pessoais sobre os usuários.

É importante mencionar que a IoT - em geral - utiliza uma tecnologia chamada Long-Range Low-Power Wide Area Network, isto é, um tipo de rede sem fio de longa distância que permite comunicações com baixa taxa de transmissão de dados e baixo consumo de energia. A ideia do IoT é transmitir dados a grandes distâncias e, inclusive, a partir de dispositivos à bateria. **Apenas para comparação, o Bluetooth é uma tecnologia Short-Range Low-Power Personal Area Network.**

Finalmente, a IoT poderia ser definida, portanto, como uma tecnologia que permite que uma malha de dispositivos - **tais como dispositivos móveis, wearables (tecnologias para vestir), sensores, aparelhos eletrônicos de consumo e domésticos, dispositivos automotivos e dispositivos ambientais** - possam ser integrados para acessar aplicativos e informações ou para a interação com pessoas, redes sociais, governos e empresas.



Tecnologias de Acesso

TECNOLOGIAS DE ACESSO À INTERNET

Referem-se aos métodos e infraestruturas utilizados para conectar dispositivos, como computadores, smartphones e outros equipamentos, à Internet. Essas tecnologias permitem que os dispositivos acessem os serviços e recursos disponíveis na World Wide Web e em outros serviços online. Existem várias tecnologias de acesso à Internet (Ex: Dial-Up, ADSL, HFC, Fibra Óptica, PLC, Rádio, Satélite e Telefonia Móvel), e a escolha depende das necessidades e da disponibilidade em uma determinada região.

Até o início dos anos 90, a internet era conhecida principalmente por pesquisadores e profissionais ligados a universidades, governo ou indústria. **Com o surgimento da Web, a internet se tornou acessível a milhões de usuários com diferentes interesses.** Este crescimento explosivo foi impulsionado por Provedores de Serviços da Internet (ISPs), que permitiram a conexão de usuários individuais à internet, transformando-a em um serviço de utilidade pública, semelhante à telefonia.

A infraestrutura de rede da internet, conhecida como Backbone, desempenha um papel crucial nesse processo. Composta por satélites, ondas de rádio e de cabos de fibra óptica terrestres e submarinos, essa rede interliga diferentes países e continentes, sendo responsável por cerca de 80% de toda a comunicação global. Os backbones são construídos e administrados por provedores de serviço de internet, incluindo companhias telefônicas de longa distância e governos nacionais.

Esses troncos de rede de alta velocidade e desempenho fornecem acesso à internet para várias outras redes. Os ISPs, como NET/CLARO, GVT/VIVO e SKY, são os responsáveis por vender o acesso à internet a provedores menores e usuários finais. Os backbones, que podem ser terrestres ou submarinos, formam uma rede essencial que sustenta a comunicação e o acesso à internet em todo o mundo. **Existem três níveis de provedores de acesso:**

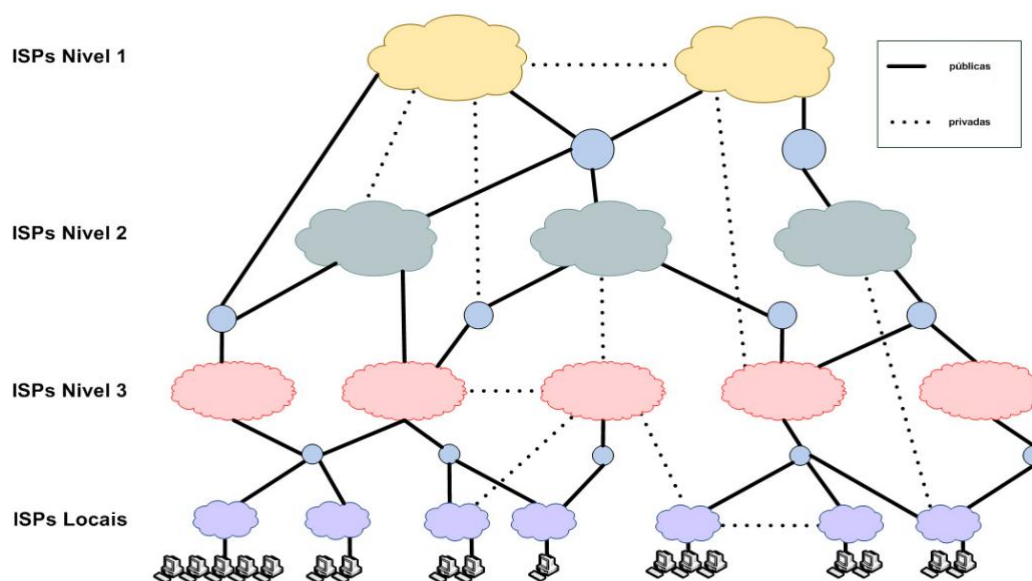
NÍVEIS	DESCRIÇÃO
ISP NÍVEL 1	São os provedores de acesso à internet de nível mais alto na hierarquia. Eles não precisam comprar acesso à internet de outros provedores, pois possuem uma rede global de alta capacidade e trocam tráfego diretamente uns com os outros. Exemplos de provedores de Nível 1 incluem AT&T, Verizon, NTT Communications e CenturyLink. Eles têm uma presença global e fornecem acesso à internet em escala internacional. Imagine ISPs de Nível 1 como rodovias federais, como a Rodovia Presidente Dutra (BR-116). Essas rodovias cruzam continentes e países sem precisar pagar pedágio a outras estradas menores. Os provedores de Nível 1 constroem e mantêm essas "rodovias da internet" e interconectam-se diretamente para permitir um tráfego rápido e eficiente.
ISP NÍVEL 2	Estes são provedores de acesso à internet que não possuem redes globais como os Nível 1, mas ainda têm uma rede significativa em uma área geográfica específica. Eles geralmente compram acesso à internet de Nível 1 ISPs e podem vender serviços a ISPs de nível inferior ou a empresas e consumidores diretos. Exemplos de provedores de Nível 2 incluem Cogent, Orange, Charter, Deutsche Telekom, entre outros. ISPs de Nível 2 podem ser comparados a rodovias estaduais. Eles atendem a áreas geográficas maiores, como estados ou regiões inteiras. Essas rodovias estaduais se conectam às autoestradas globais (Nível 1) e podem cobrar pedágio por permitir que o tráfego flua entre essas grandes autoestradas e áreas locais.
ISP NÍVEL 3	São provedores regionais ou locais que não possuem redes globais. Eles compram acesso à internet de provedores de Nível 1 ou 2 para fornecer conectividade a empresas



e consumidores em áreas geográficas específicas. Esses ISPs podem se concentrar em uma única cidade, região ou país. Alguns provedores de Nível 3 podem ser ISPs de acesso final, que fornecem serviços diretamente a residências e empresas locais.

ISPs de Nível 3 são como as estradas locais e ruas em cidades. Eles atendem áreas geográficas muito específicas, como uma cidade ou bairro. Essas estradas locais se conectam às rodovias regionais (Nível 2) ou diretamente às autoestradas globais (Nível 1) e permitem que o tráfego alcance destinos locais.

ISPs Locais normalmente se enquadram como ISPs de Nível 3. Eles são responsáveis por fornecer conectividade à Internet para áreas locais específicas e são mais próximos dos usuários finais.



Dito isso, os enlaces que conectam as redes de acesso residenciais aos ISP Nível 3 ou Locais podem ser de diferentes tecnologias. Todo computador que se conecta à internet, seja via cabo ou Wi-Fi, precisa de uma placa de rede (também chamada de NIC - Network Interface Card), que pode ser uma placa de rede Ethernet (para conexões cabeadas) ou uma placa de rede Wi-Fi (para conexões sem fio). Vamos conhecer as principais tecnologias de acesso:

TECNOLOGIAS DE ACESSO	DESCRIÇÃO
DIAL-UP	Dial-Up é uma conexão à internet via linha telefônica convencional, onde a transmissão de dados é feita utilizando o tom de discagem. A velocidade é baixa, geralmente até 56 Kbps, e a linha telefônica fica ocupada durante o uso, sendo uma tecnologia obsoleta em comparação com as alternativas atuais.
ADSL	ADSL (Asymmetric Digital Subscriber Line) usa a linha telefônica comum para transmitir dados em alta velocidade, sem interromper as chamadas telefônicas. A velocidade de download é maior que a de upload, ideal para uso doméstico, com velocidades típicas de até 24 Mbps dependendo da qualidade da linha e da distância da central.
HFC	HFC (Hybrid Fiber-Coaxial) combina fibra óptica e cabos coaxiais para transmitir dados. A fibra é usada até uma certa distância, sendo complementada por cabos coaxiais até o usuário final. Comum em serviços de TV a cabo, permite velocidades de internet rápidas, dependendo da infraestrutura local.
FIBRA ÓPTICA	FTTH (Fiber to the Home) é uma tecnologia que utiliza fibra óptica diretamente até a residência do usuário, proporcionando conexões de alta velocidade, estáveis e com



	baixa latência. É uma das tecnologias mais avançadas para acesso à internet, suportando velocidades simétricas de upload e download.
PLC	PLC (Power Line Communication) usa a rede elétrica para transmitir dados de internet. É uma solução que permite a distribuição de sinal de internet por meio da infraestrutura de energia, sendo útil em áreas com baixa cobertura de outras tecnologias. A velocidade pode variar conforme a rede elétrica local.
RÁDIO	A tecnologia de rádio transmite sinal de internet sem fio por meio de torres de rádio, sendo uma opção para áreas rurais ou de difícil acesso. A velocidade e a estabilidade da conexão dependem da proximidade com a torre e das condições climáticas, sendo uma alternativa viável onde não há cabeamento.
SATÉLITE	Satélite permite o acesso à internet em áreas remotas, transmitindo dados via satélites em órbita. Apesar de ser uma solução para locais onde outras tecnologias não chegam, tem maior latência e menor velocidade em comparação a soluções terrestres, sendo influenciada por condições climáticas.
TELEFONIA MÓVEL	A Telefonia Móvel usa redes celulares 3G, 4G ou 5G para fornecer acesso à internet. A cobertura depende da infraestrutura de torres de telefonia, e a velocidade varia conforme a geração da rede. É amplamente utilizada devido à sua mobilidade, permitindo conexões em qualquer lugar com sinal disponível.

Observação: nem sempre um computador precisa de um modem diretamente para se conectar à internet. O modem é um dispositivo que converte os sinais digitais do computador em sinais adequados para transmissão via linhas telefônicas (ADSL), cabos coaxiais (cabo), fibra óptica, ou sinal de rádio (3G/4G/5G), dependendo da tecnologia de internet usada. Em muitas redes, especialmente em redes domésticas e corporativas modernas, o roteador já inclui um modem integrado, e os computadores apenas se conectam ao roteador via Wi-Fi ou cabo Ethernet.



PROTOCOLOS DE COMUNICAÇÃO

Conceitos Básicos

INCIDÊNCIA EM PROVA: BAIXA

PROTOCOLOS DE COMUNICAÇÃO

Protocolos são conjuntos de regras e convenções que especificam como os dispositivos em uma rede devem se comunicar. Eles definem os formatos dos dados, a sequência de mensagens, a detecção e correção de erros, o controle de acesso e muitos outros aspectos necessários para a comunicação eficaz entre computadores em uma rede. Esses protocolos desempenham um papel fundamental na garantia de que diferentes dispositivos de rede, com hardware e software diversos, possam se comunicar e trocar informações de maneira consistente.

Andrew Tanenbaum define um protocolo como um acordo que estabelece como a comunicação ocorrerá, enquanto Behrouz Forouzan o descreve como um conjunto de regras que controlam a troca de dados. Já Diego Carvalho compara protocolos a idiomas, explicando que, em uma rede, os protocolos organizam e representam os dados, assim como as gramáticas e estruturas dos idiomas facilitam a comunicação entre pessoas de diferentes línguas.

Os protocolos de comunicação definem como os dados são formatados, transmitidos e interpretados em uma rede, permitindo que diferentes dispositivos, como computadores e roteadores, possam se comunicar. Assim como usamos regras de idioma para nos comunicar em um país estrangeiro, os dispositivos de rede seguem regras de protocolo para entender e trocar informações entre si, independentemente das suas diferenças de hardware ou software.

O conjunto de protocolos TCP/IP é o padrão da internet e permite que dispositivos em redes diferentes se comuniquem de forma eficaz. Independentemente do sistema operacional ou da arquitetura do dispositivo, se ele estiver conectado à internet, está utilizando o TCP/IP, que fornece as regras necessárias para garantir a comunicação global entre máquinas de diversas plataformas.



Modelo OSI/ISO

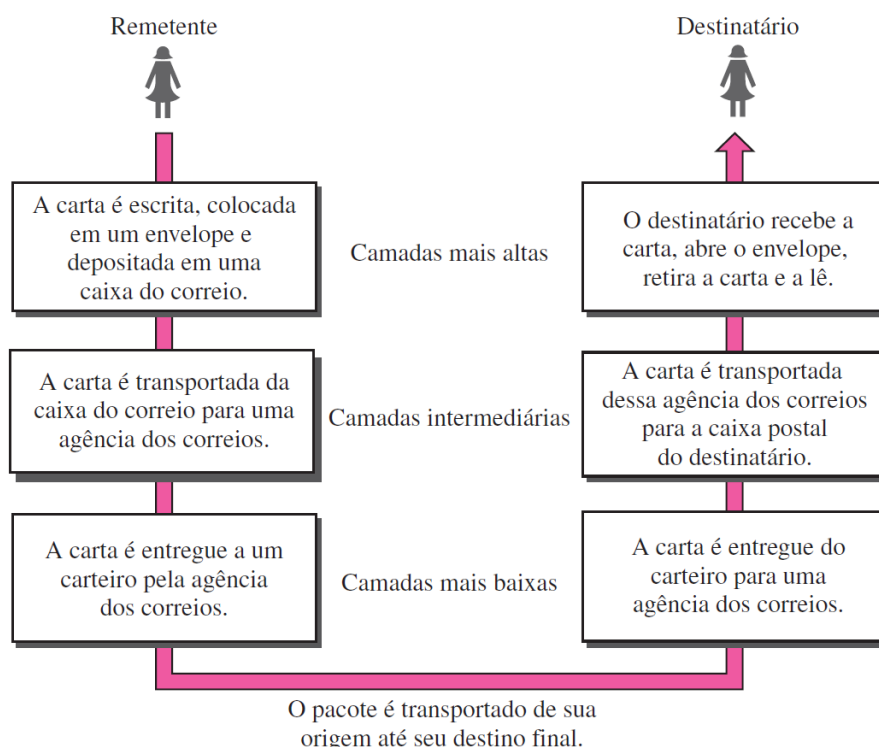
INCIDÊNCIA EM PROVA: MÉDIA

MODELO OSI/ISO

O Modelo OSI (*Open Systems Interconnection / International Organization for Standardization*) é um modelo de referência utilizado para entender como os protocolos de rede funcionam e interagem. Ele divide as funções de comunicação em uma rede de computadores em sete camadas, cada uma com um propósito específico. Essas camadas são organizadas hierarquicamente e servem como um guia para o desenvolvimento e a compreensão de protocolos de comunicação em redes.

Nós já sabemos que uma rede é uma combinação de hardware e software que envia dados de uma localidade para outra. **Para que dados possam trafegar de um ponto a outro, é necessário que tanto hardware quanto software realizem algumas tarefas.** Pessoal, vocês já se perguntaram como um e-mail enviado para um amigo que mora do outro lado do mundo consegue chegar até o computador dele? Tudo acontece tão rápido que até parece simples, mas não é!

Falando especificamente do contexto de softwares, a atividade de enviar um e-mail pode ser dividida em várias tarefas, cada uma das quais realizada por uma camada de software diferente. Professor, não estou entendendo bulhufas! Imaginem dois amigos se comunicando por cartas! O processo de enviar uma carta a um amigo seria complexo se não existisse nenhum serviço disponível das agências dos correios, concordam? Vejamos...



A comunicação em redes pode ser organizada em camadas, onde cada uma realiza uma tarefa específica e usa os serviços da camada inferior. Isso permite que o processo de transmissão de dados seja dividido em etapas menores e mais fáceis de gerenciar. Cada camada é responsável por uma parte da comunicação, e a sequência correta entre elas garante que os dados sejam enviados e recebidos adequadamente.



As camadas se comunicam através de interfaces que especificam os serviços a serem fornecidos à camada superior. Isso permite que cada camada seja independente, podendo ser alterada ou substituída sem afetar as outras, desde que suas funções sejam mantidas. Esse design modular simplifica a manutenção e o desenvolvimento de sistemas complexos, garantindo eficiência e flexibilidade.

Esse conceito de dividir a comunicação em camadas é amplamente utilizado em redes de computadores. A organização em camadas facilita a interoperabilidade entre diferentes sistemas e tecnologias, promovendo a compatibilidade entre dispositivos de diferentes fabricantes. Além disso, a padronização das camadas garante que a comunicação ocorra de maneira consistente e eficiente, independentemente das diferenças entre os sistemas.

Isso possibilita a criação de redes em que dispositivos de diferentes fabricantes possam funcionar em conjunto de forma harmoniosa, seguindo as especificações do Modelo OSI.

NÚMERO	CAMADA	DESCRIÇÃO	PROTOCOLOS
7	APLICAÇÃO	Camada responsável por habilitar o usuário, seja ele humano ou software, a estabelecer a comunicação entre aplicações e a acessar a rede.	HTTP, SMTP, FTP, SSH, TELNET, SNMP, POP3, IMAP, DNS.
6	APRESENTAÇÃO	Camada responsável por definir o formato para troca de dados entre computadores, como se fosse um tradutor.	AFP, ICA, LPP, NCP, NDR, TOX, XDR, PAD.
5	SESSÃO	Camada responsável por permitir que duas ou mais aplicações em computadores diferentes possam abrir, usar e fechar uma conexão, chamada sessão.	NETBIOS.
4	TRANSPORTE	Camada responsável por organizar dados em segmentos e que eles cheguem ao destino livre de erros (sem perdas, sem duplicações e na ordem correta).	TCP, UDP, NETBEUI.
3	REDE	Camada responsável pelo endereçamento, roteamento e entrega de pacotes individuais de dados desde sua origem até o seu destino, provavelmente através de várias redes.	IP, ICMP, ARP RARP, NAT.
2	ENLACE	Camada responsável por organizar os dados em frames (ou quadros) e por estabelecer uma conexão nó-a-nó entre dois dispositivos físicos que compartilham o mesmo meio físico.	Ethernet, Token Ring, Bluetooth, Wi-Fi.
1	FÍSICA	Camada responsável por definir as especificações elétricas e físicas da conexão de dados.	USB, DSL.

MNEMÔNICO DAS CAMADAS						
F	E	R	T	S	A	A
FÍSICA	ENLACE	REDE	TRANSPORTE	SESSÃO	APRESENTAÇÃO	APLICAÇÃO
FLAMENGO	ENSACOU NA	REDE	TRÊS	SAPECADAS NO	ATLÉTICO E	AVAÍ

O Modelo OSI é basicamente um modelo de referência para conexão e projetos de sistemas de redes que se baseia em camadas sobrepostas. Sendo beeeeeeeem rigoroso, esse modelo não é propriamente dito uma arquitetura de rede, uma vez que não especifica os serviços e os protocolos exatos que devem ser utilizados em cada camada. Em outras palavras, nem sempre será possível “encaixar” um protocolo em uma camada específica do Modelo OSI.





Esse modelo é apenas uma abstração teórica - uma referência conceitual - usado pela academia para representar o que seria um modelo perfeito de rede com suas respectivas descrições de camadas. Ele tem uma função mais didática do que pragmática. Não se trata de um modelo utilizado atualmente em redes de computadores - na prática, a arquitetura utilizada atualmente é o TCP/IP.



Nós sabemos que a comunicação entre dois computadores é extremamente complexa, logo esse modelo sugere dividir essa complexidade em uma estrutura de sete camadas distintas, porém relacionadas entre si, cada uma das quais definindo uma parte do processo de transferência de informações através de uma rede. **Compreender esses conceitos é importante para entender posteriormente a função de cada protocolo.** Nos tópicos seguintes, nós veremos a função de cada uma dessas camadas. Vem comigo... é legal! Eu juro... no fim da aula, tudo fará sentido!



Arquitetura TCP/IP

INCIDÊNCIA EM PROVA: ALTA

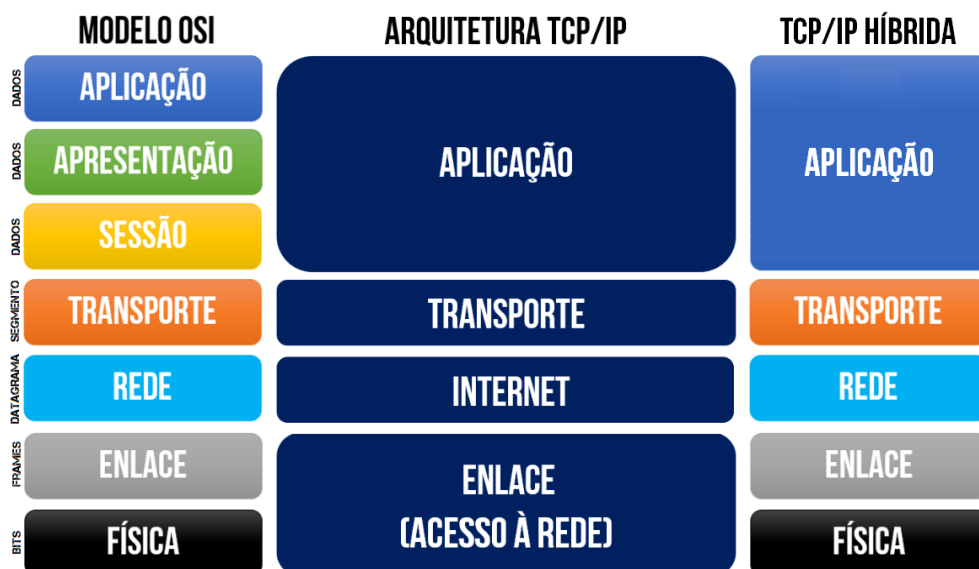
ARQUITETURA TCP/IP

A arquitetura TCP/IP (*Transmission Control Protocol / Internet Protocol*) é um conjunto de protocolos de comunicação que são amplamente utilizados na internet e em redes locais. Ela fornece um conjunto de regras e especificações que permitem que diferentes dispositivos se comuniquem em redes de computadores, independentemente do fabricante ou sistema operacional.

Nós acabamos de ver em detalhes o Modelo OSI e descobrimos que – apesar de ser um modelo conceitual bastante interessante e de facilitar o entendimento da comunicação entre redes – ele é apenas um modelo teórico utilizado didaticamente para mostrar o funcionamento ideal da comunicação de dados em uma rede de computadores. **Ele não é uma tecnologia, nem um conjunto de protocolos, nem um software e só tem utilidade pedagógica.**

Na prática, o que é utilizado é a Arquitetura ou Pilha TCP/IP. Essa arquitetura foi desenvolvida – na verdade – antes do Modelo OSI. Dessa forma, as camadas que nós veremos a seguir não correspondem exatamente àsquelas do Modelo OSI. A Arquitetura TCP/IP é o conjunto de protocolos e camadas utilizados para conectar várias redes diferentes de maneira uniforme – **trata-se do conjunto padrão de protocolos da Internet.**

A quantidade e nome das camadas apresentada acima para a Arquitetura TCP/IP foi baseada na documentação oficial (RFC 1122)². No entanto, alguns autores modelam essa arquitetura com três, quatro ou cinco camadas de nomes bastante diversos. Observem que ela condensa as camadas de aplicação, apresentação e sessão na camada de aplicação. Ademais, ela condensa a camada física e de enlace na camada de enlace e chama a camada de rede de internet.



² O projeto original do TCP/IP prevê quatro camadas (conforme a RFC 1122). Apesar disso, como os modelos TCP/IP e OSI não combinam, há autores que defendem uma arquitetura híbrida de cinco camadas: física, enlace, rede, transporte e aplicação.





Eventualmente, quando um servidor – uma máquina especializada – fornece os serviços de um protocolo, é comum chamar esse servidor pelo nome do protocolo que ele implementa. Isso facilita a compreensão e a identificação de servidores e seus propósitos. Logo, temos que:

- Um **Servidor** que fornece serviços de apresentação de páginas web pode ser chamado de **Servidor HTTP**;
- Um **Servidor** que fornece serviços de envio de e-mails pode ser chamado de **Servidor SMTP**;
- Um **Servidor** que fornece serviços de tradução de domínios pode ser chamado de **Servidor DNS**;
- Um **Servidor** que fornece serviços de transferência de arquivos pode ser chamado de **Servidor FTP**.

Protocolos da Camada de Rede

IP (Internet Protocol)

INCIDÊNCIA EM PROVA: ALTÍSSIMA

INTERNET PROTOCOL (IP)

O IP é a base da comunicação na Internet, sendo responsável por rotear pacotes de dados de origem para destino em uma rede. Cada dispositivo conectado à Internet recebe um endereço IP exclusivo, que é usado para identificar e encaminhar dados para o destinatário correto. Quando um dispositivo deseja enviar dados para outro, ele divide os dados em pacotes. Cada pacote contém informações sobre o remetente, destinatário, dados reais e outros metadados – esses pacotes são então enviados pela rede. O roteamento é o processo pelo qual os pacotes são direcionados do remetente para o destinatário através de vários dispositivos intermediários, como roteadores.

IP significa Internet Protocol (ou Protocolo de Internet). *Vamos traduzir Internet?* **Inter** significa entre e **net** significa rede, logo Internet significa entre redes. Agora vamos juntar tudo isso e dar um significado! IP é um protocolo – um conjunto de normas, padrões e convenções – para comunicação entre redes. **O endereço IP define de forma única e universal a conexão de um dispositivo** (Ex: um computador ou um roteador).

Eles são exclusivos no sentido de que cada endereço define uma única conexão com a Internet – dois dispositivos jamais podem ter o mesmo endereço ao mesmo tempo na mesma rede. Além disso, eles são universais no sentido de que o sistema de endereçamento tem de ser aceito por qualquer host (máquina) que queira se conectar à Internet. Todo dispositivo da internet possui um endereço lógico chamado Endereço IP.

O IP é um protocolo não confiável, de melhor esforço e sem conexão. Isso significa que, quando os pacotes de dados são enviados pela rede, o protocolo não garante que eles chegarão ao destino, que



chegarão na ordem correta ou sem erros. Ele simplesmente tenta entregar os pacotes da maneira mais eficiente possível, sem criar uma conexão contínua entre remetente e destinatário.

Da mesma forma que um carteiro precisa saber o CEP de uma casa, o protocolo IP precisa saber o endereço IP de uma máquina para entregar os dados destinados a ela. E como é esse endereço? Bem, isso depende da versão! Existem basicamente duas versões: **IPv4** (Versão 4) e **IPv6** (Versão 6). Vamos iniciar nosso papo falando sobre o IPv4!

IPv4 (IP Versão 4)

O IPv4 (Versão 4) basicamente possui 32 bits de comprimento. Esses 32 bits geralmente são divididos em 4 octetos. O que é um octeto, Diego? É um conjunto de 8 bits ou 1 byte!

ENDEREÇO IP COM NOTAÇÃO DE OCTETOS BINÁRIOS

10101010

01010101

11100111

10111101

Usar endereço em bits pode acabar incorrendo em erros. Como só tem 0 e 1, se você tem miopia, pode acabar errando. *Puxado, concordam?* **Pois é, mas alguém teve a brilhante ideia de converter esses números do sistema binário para o sistema decimal.** Dessa forma, cada octeto em binário pode ir de 0 a 255 em decimal – você nunca vai encontrar um número que não esteja nessa extensão. Se convertermos os números da tabela acima para decimal, fica assim:

ENDEREÇO IP COM NOTAÇÃO DECIMAL PONTUADA

170

85

231

189



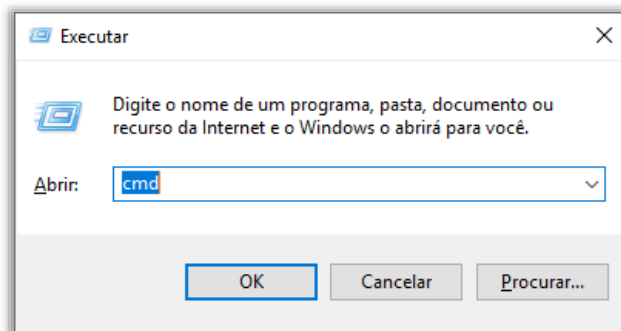
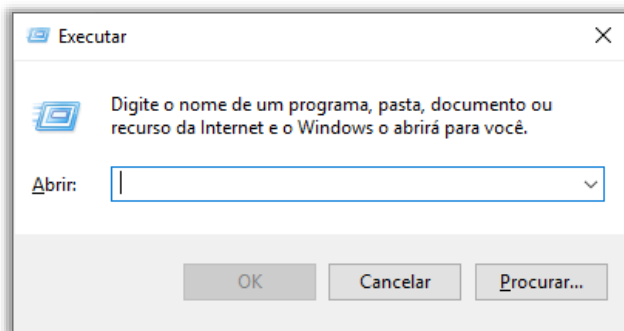
ESCLARECENDO!

Existem diversos sistemas de numeração! Seres humanos utilizam um sistema de numeração decimal, isto é, nós fazemos contas utilizando dez dígitos (0, 1, 2, 3, 4, 5, 6, 7, 8 e 9). Já os computadores utilizam um sistema de numeração binária, isto é, eles fazem contas utilizando apenas dois dígitos (0 e 1) – o nome desse dígito binário é Bit (do inglês, Binary Digit). É possível converter números de um sistema para outro sem nenhum inconveniente. Vejam abaixo o número 123 em outros sistemas numéricos:

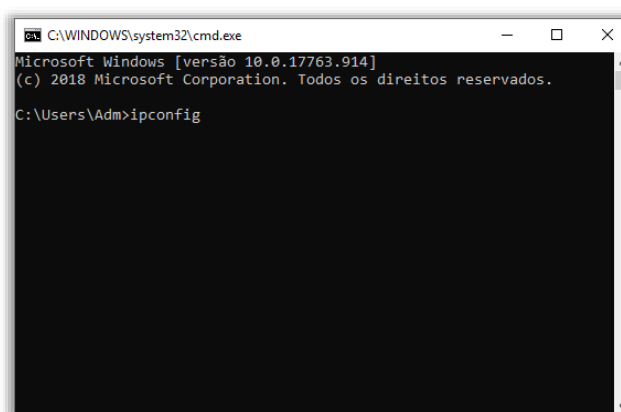
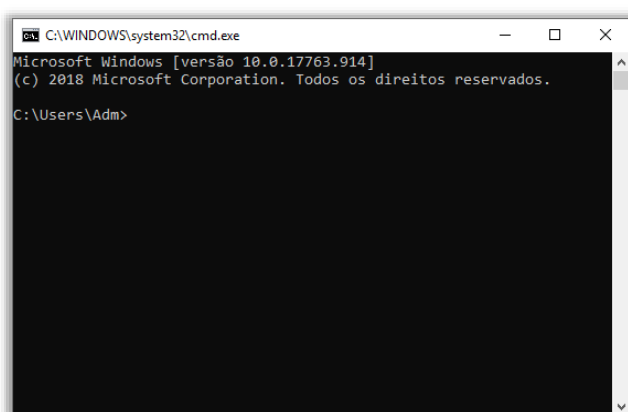
SISTEMA DECIMAL	SISTEMA HEXADECIMAL	SISTEMA OCTAL	SISTEMA BINÁRIO
123	7B	173	01111011

Professor, está tudo muito abstrato! Você pode dar um exemplo? Claro! Para tal, eu vou propor um exercício para vocês: eu quero que vocês pressionem simultaneamente as teclas Win + R.

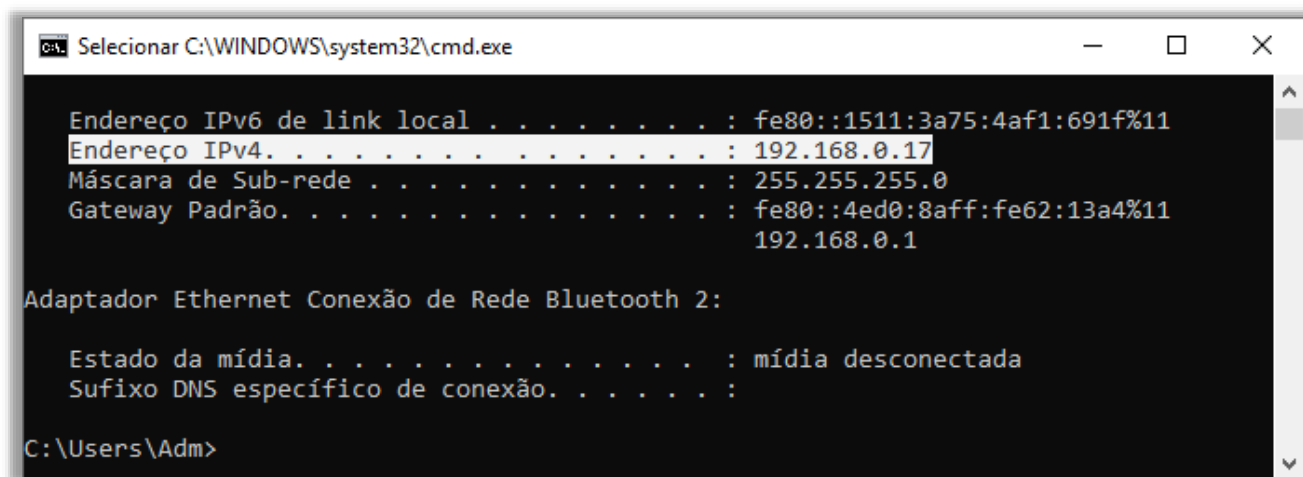




Quando vocês fizerem isso, aparecerá essa imagem da esquerda. Eu quero, então, que vocês escrevam o comando **cmd** e cliquem em OK:



Notem que será exibida essa janela da esquerda. Em seguida, eu quero que vocês escrevam o comando **ipconfig** e aperte ENTER. No meu caso, foi exibido:



Eu destaquei em branco meu Endereço IPv4: **192.168.0.17**! Lembrando que esse é o meu IP privado e, não, público.

IPv6 (IP Versão 6)

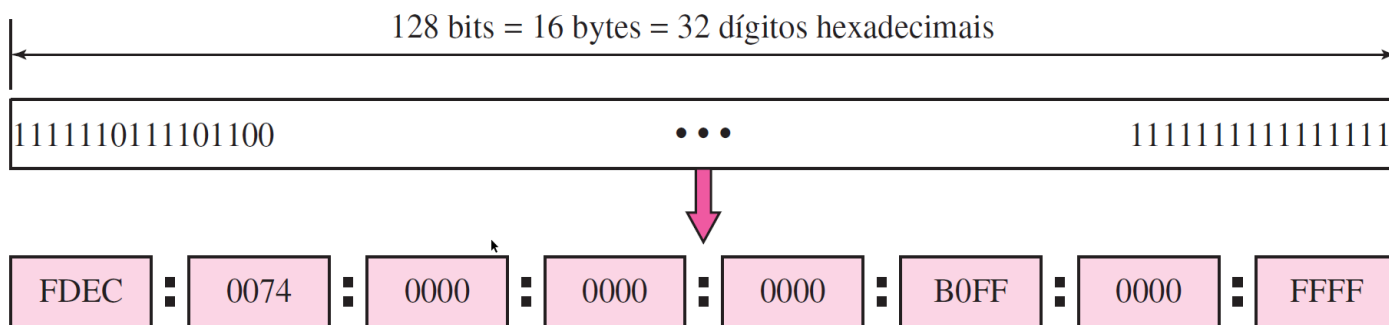


O IPv4 foi implementado em 1983, quando a internet ainda estava engatinhando. Nenhum engenheiro de redes imaginou que teríamos em pouco tempo uma quantidade tão absurda de equipamentos no mundo acessando a internet. Nós estávamos avançando em máxima velocidade ao esgotamento total de endereços IP. **Era evidente: endereços não são infinitos - eles são recursos escassos como qualquer outro...**

Na época, surgiram soluções de curto prazo para ajudar a resolver o problema de esgotamento de endereços. No entanto, a escassez de endereços não era o único problema! Havia outros, tais como a falta de tratamento específico para transmissão de áudio/vídeo em tempo real e a criptografia/autenticação de dados para algumas aplicações. Tudo isso serviu de motivação para a criação de uma nova versão do Protocolo IP: **IPv6 (Versão 6)**.

A nova versão possui 128 Bits, logo temos até **2^{128}** possíveis endereços ou **340 undecilhões** de endereços ou 340.282.366.920.938.000.000.000.000.000.000.000.000 de endereços!

No IPv4, decidiu-se utilizar uma representação decimal de 32 bits para facilitar a configuração! Ainda que fizéssemos isso com o IPv6, teríamos uma quantidade imensa de números. Dessa forma, optou-se por utilizar uma **representação com hexadecimal**, que necessita de todos os números e mais algumas letras: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Dividem-se 128 Bits em 8 grupos de 16 Bits (seção de 4 hexadecimais), separados por dois-pontos.



O IPv6 não possui o conceito de classes e nem endereço de broadcast. Além disso, como o endereço ainda fica grande com o hexadecimal, há algumas formas de abreviar: zeros não significativos de uma seção (quatro dígitos entre dois-pontos) podem ser omitidos, sendo que apenas os zeros não significativos podem ser omitidos e, não, os zeros significativos. Na tabela abaixo, temos um exemplo:

ENDEREÇO ORIGINAL
FDEC:0074:0000:0000:0000:B0FF:0000:FFF0
ENDEREÇO ABREVIADO
FDEC:74:0:0:0:B0FF:0:FFF0
ENDEREÇO MAIS ABREVIADO
FDEC:74::B0FF:0:FFF0

Usando-se essa forma de abreviação, 0074 pode ser escrito como 74, 000F como F e 0000 como 0. Observe que se tivéssemos o número **3210**, por exemplo, não poderia ser abreviado. Outras formas de abreviações são possíveis se existirem seções consecutivas formadas somente por zeros. **Podemos eliminar todos os zeros e substituí-los por um dois-pontos duplo.** Note que esse tipo de abreviação é permitido apenas uma vez por endereço (Ex: não pode 2001:C00::5400::9).

Se existirem duas ocorrências de seções de zeros, apenas uma delas pode ser abreviada. A reexpansão do endereço abreviado é muito simples: devemos alinhar as partes não abreviadas e inserir



zeros para obter o endereço original expandido. É interessante notar que o IPv6 permite também o endereçamento local, isto é, endereços usados em redes privadas. Por fim, o IPv6 não pode se comunicar diretamente com o IPv4, mas existem diversas estratégias indiretas.

ENDEREÇO ORIGINAL
2001:0C00:0000:0000:5400:0000:0000:0009
ENDEREÇO ABREVIADO
2001:C00:0:0:5400:0:0:9
ENDEREÇO MAIS ABREVIADO
2001:C00::5400:0:0:9 OU 2001:C00:0:0:5400::9
NÃO PODE SER ABREVIADO
2001:C00::5400::9

Protocolos da Camada de Transporte

TCP (Transmission Control Protocol)

INCIDÊNCIA EM PROVA: ALTA

TRANSMISSION CONTROL PROTOCOL (TCP)

Protocolo da camada de transporte, considerado confiável e orientado à conexão. Ele utiliza portas para estabelecer conexões, utiliza controle de fluxo para evitar congestionamento na rede, permite a transferência de dados bidirecional e confirma o recebimento de pacotes, retransmitindo os que não são confirmados. Além disso, ele garante que os pacotes cheguem na ordem correta e utiliza a soma de verificação para detectar erros nos dados recebidos. O TCP é amplamente utilizado em aplicações que requerem entrega garantida de dados, como navegadores web e e-mail.

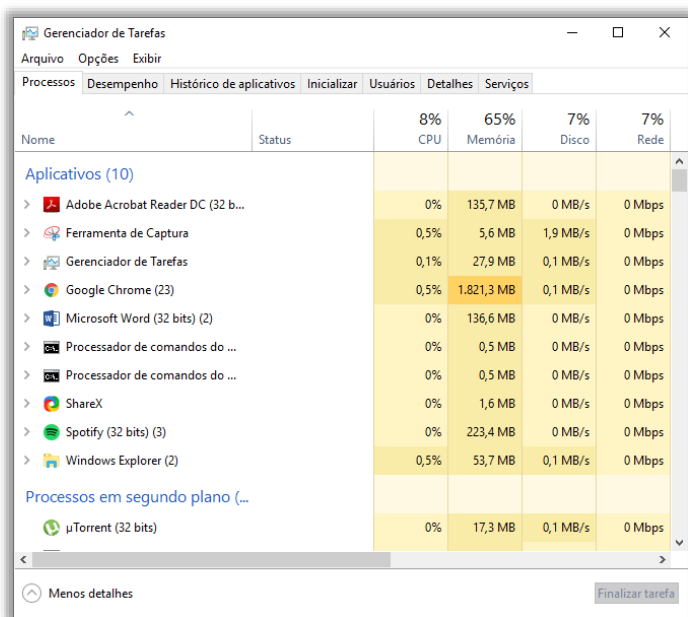
O protocolo TCP (Transmission Control Protocol) é um dos principais protocolos usados na comunicação de dados pela internet. Ele é responsável por garantir a entrega confiável de dados entre dois dispositivos conectados em rede. Diferente do IP, que é um protocolo não confiável, o TCP é orientado a conexões, o que significa que ele estabelece uma conexão entre o remetente e o destinatário antes de começar a transferência de dados.

O TCP divide os dados em segmentos menores, assegurando que cada segmento chegue ao destino corretamente e na ordem certa. Ele usa mecanismos de confirmação para garantir que os pacotes foram recebidos e retransmite aqueles que se perderam ou chegaram corrompidos. Esse controle de erros, junto com o controle de fluxo, torna o TCP ideal para aplicações onde a integridade dos dados é crucial, como transferências de arquivos e navegação na web. Em resumo, o TCP prioriza a confiabilidade e a correção dos dados transmitidos, criando uma camada de segurança sobre o protocolo IP.

Para entender melhor esse protocolo, vamos fazer uma analogia: imaginem que moram cinco pessoas na sua casa. Para que um carteiro lhe entregue um pacote, ele precisa do seu endereço. No entanto, esse endereço é compartilhado por toda a sua família. O carteiro não vai entrar na sua casa, procurar qual é o seu quarto, bater na sua porta e entregar um pacote diretamente para você.

Nesse sentido, podemos dizer que a sua casa possui um único endereço, mas ela possui diversos quartos, cada um com uma porta de modo que cada morador pode utilizar o serviço dos Correios. **Agora me acompanhem: imaginem que um pacote de dados viajou o planeta e, por meio do seu endereço IP, ele chegou ao seu computador.** Só que o seu computador possui dezenas de processos diferentes em execução. *E aí, qual deles é o dono do pacote?*





*Processos, professor? Sim, vamos fazer um teste! Pressionem de forma simultânea as teclas CTRL + SHIFT + ESC! Esse atalho abrirá o Gerenciador de Tarefas do Windows. **Observem que várias abas serão exibidas, sendo que a primeira delas é a aba de processos.***

Nessa aba, estarão listados diversos processos que estão sendo executados atualmente em seu computador. No exemplo ao lado, no meu computador, há dez aplicativos abertos em primeiro plano no momento em que eu escrevo essa aula – cada um executando um ou mais processos.

Logo, um processo é uma instância de uma aplicação em execução em determinado

momento. Se chegam dados a uma máquina, ela não consegue saber quem é o remetente sem saber o número da porta. **Por meio dele, ela consegue entregar os segmentos de dados diretamente ao destinatário correto.** O pacote percorreu o mundo inteiro em rotas terrestres e submarinas, chegou no meu computador e agora precisa saber qual processo deve recebê-lo. Para tal, precisa do número da porta!

Galera, o número da porta de destino é necessário para entrega e o número da porta de origem é necessário para resposta. *Professor, como são esses números?* Cara, são apenas números que variam entre zero e 65535. Cada uma pode ser usada por um programa ou serviço diferente, de forma que – em tese – poderíamos ter até 65536 serviços diferentes ativos simultaneamente em um mesmo servidor (tudo isso em um único Endereço IP)³.

Por exemplo: quando você está acessando uma página web por meio de um navegador, essa página web está armazenada em um servidor em algum lugar do mundo e o navegador está no seu computador. **O navegador é utilizado para acessar a web e o protocolo padrão da web é o HTTP!** Logo, para que o seu computador troque dados com o servidor que armazena a página do Estratégia Concursos, você precisará de uma porta. *Vocês se lembram do porquê?*

Porque um pacote encontrará o computador ou o servidor, mas não saberá qual processo é o dono do pacote. No caso do HTTP, a porta padrão é a 80! *Por que exatamente esse número?* Galera, tem uma organização chamada IANA (Internet Assigned Number Authority) responsável por definir e controlar algumas portas – ela definiu que a porta do HTTP é a 80! Logo, vamos fazer um último teste! Tentem acessar o endereço: **http://www.estrategiaconcursos.com.br:80**.

³ A combinação do Protocolo + Endereço IP + Número da Porta é também chamada de **Socket**.





Não é possível acessar esse site

A página <http://www.estrategiaconcursos.com.br:21/> pode estar temporariamente indisponível ou pode ter sido movida permanentemente para um novo endereço da Web.

ERR_UNSAFE_PORT

Notem que a página do Estratégia Concursos abrirá normalmente. Agora tentem com um número de porta diferente – por exemplo: <http://www.estrategiaconcursos.com.br:21>. Vejam que retornará um erro chamado **ERR_UNSAFE_PORT**. Esse erro é retornado quando você tenta acessar dados utilizando uma porta não recomendada pelo navegador. Em outras palavras, você está utilizando a porta errada!

UDP (User Datagram Protocol)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

USER DATAGRAM PROTOCOL (UDP)

Protocolo da camada de transporte, considerado sem conexão e utiliza portas para comunicação de forma similar ao TCP. Ele não possui controle de fluxo e permite a transferência de dados rápida, mas sem garantias de entrega, ordem ou integridade. Esse protocolo é considerado não confiável porque não é capaz de confirmar o recebimento de pacotes e não retransmite os pacotes perdidos. Ele também não reordena pacotes e realiza apenas verificações básicas de erros nos dados recebidos (mas não os corrige). Por fim, ele não requer estabelecimento de conexão antes da transferência de dados, sendo ideal para aplicações que requerem transmissão rápida, como streaming de vídeo e jogos online.

Protocolo da camada de transporte, ele fornece um serviço de entrega sem conexão e não-confiável (sem controle de fluxo e de congestionamento). Esse protocolo é praticamente o inverso do anterior – ele não adiciona nenhum controle adicional aos serviços de entrega do IP, exceto pelo fato de implementar a comunicação entre processos, em vez da comunicação entre hosts. Ele até realiza alguma verificação de erros de erros, mas de forma muito limitada.

*Professor, se esse protocolo é tão simples assim, por que um processo iria querer usá-lo? Com as desvantagens vêm algumas vantagens! Por ser muito simples, ele tem um baixo overhead (tráfego adicional). **Se um processo quiser enviar uma pequena mensagem e não se preocupar muito com a confiabilidade, o UDP é uma boa escolha. Ele exige menor interação entre o emissor e o receptor do que quando utilizamos o TCP.***

Alguns contextos específicos não se preocupam se um pacote eventualmente for perdido, duplicado ou chegar fora de ordem. Se eu estou conversando com outra pessoa por áudio ou vídeo, perder um ou outro pacote de dados não causa problemas significativos – talvez eu perca uma palavra ou outra quando estou conversando por áudio com alguém; se eu estiver conversando por vídeo, pode ser que eu perca alguns quadros.

No entanto, não faz nenhum sentido tentar reenviar esses pacotes perdidos – como ocorre com o TCP. *Por quê?* Porque nesses serviços *real-time* (tempo real), essas pequenas perdas são insignificantes. **Bacana? TCP e UDP possuem algumas vantagens e desvantagens em relação ao outro dependendo do contexto de utilização.** Para não ter mais confusão, vamos ver uma tabela comparativa entre TCP e UDP...



TCP	UDP
É comparativamente mais lento que o UDP	É comparativamente mais rápido que o TCP
Entregas confiáveis	Entregas não confiáveis (melhor esforço)
Orientado à conexão	Não orientado à conexão
Dados perdidos são retransmitidos	Dados perdidos não são retransmitidos.
Tolera atrasos, mas não tolera perdas	Tolera perdas, mas não tolera atrasos
Bastante utilizada em e-mail, navegação, etc.	Bastante utilizada em VoIP, streaming, etc.

Protocolos da Camada de Aplicação

Protocolos de E-Mail

INCIDÊNCIA EM PROVA: ALTA

Correio Eletrônico (E-Mail) é uma forma de comunicação digital que permite aos usuários enviar e receber mensagens através de redes eletrônicas. O serviço de correio eletrônico é baseado em uma arquitetura cliente/servidor, isto é, uma arquitetura composta de máquinas responsáveis por oferecer serviços (por essa razão, é chamada de servidor) e de máquinas responsáveis por consumir serviços (por essa razão, é chamada de cliente).

No decorrer desse tema, vamos ver diversos termos que vocês estão acostumados, mas que podem gerar dúvidas. Dessa forma, vamos parar um pouquinho para detalhá-los:

CLIENTE DE E-MAIL	Trata-se de uma aplicação instalada em uma máquina local que permite enviar/receber e-mails (Ex: Mozilla Thunderbird, Microsoft Outlook, etc);
SERVIDOR DE E-MAIL	Trata-se de uma máquina especializada que recebe e-mails de um cliente de e-mail ou de um webmail, e os envia para o servidor de e-mail de destino;
PROVEDOR DE E-MAIL	Trata-se de uma empresa ou serviço que hospeda e disponibiliza serviços de e-mail para outras empresas ou usuários finais (Ex: Gmail, Outlook, Yahoo, Uol, etc);
WEBMAIL	Trata-se de uma aplicação hospedada em um servidor remoto que permite enviar/receber e-mails (Ex: Outlook.com, Gmail.com, Yahoo.com, Uol.com, etc).

Os principais protocolos de correio eletrônico são: SMTP, POP e IMAP. Vamos vê-los resumidamente na tabela a seguir e depois entraremos nos detalhes de cada um:

PROTOCOLOS DE E-MAIL	DESCRIÇÃO
SMTP	Protocolo utilizado basicamente para enviar e-mails. Ele transfere mensagens de e-mail de um cliente para um servidor ou entre servidores. Funciona bem para a entrega de mensagens, mas não para recuperá-las.
POP	Protocolo projetado para recuperar e-mails de um servidor. Quando você o utiliza, os e-mails são baixados para o seu dispositivo e geralmente são excluídos do servidor. Isso é útil para acessar e-mails offline, mas pode ser limitante se você usar vários dispositivos, pois as mensagens estão disponíveis apenas no dispositivo onde foram baixadas inicialmente.
IMAP	Também usado para recuperar e-mails de um servidor, mas - diferentemente do anterior - ele mantém as mensagens no servidor. Isso permite que você acesse seus e-mails de vários dispositivos, mantendo tudo sincronizado. As mudanças feitas em um dispositivo (como ler ou excluir uma mensagem) são refletidas em todos os outros dispositivos.



SMTP

ENVIAR

POP3

RECEBER E COPIAR

IMAP

RECEBER E ACESSAR

E-Mail: SMTP

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

Protocolo da camada de aplicação responsável pelo envio de e-mails de um cliente para um servidor ou entre servidores de e-mail. Ele é bastante utilizado por clientes de e-mail e servidores de e-mail para a transmissão de mensagens de correio eletrônico, funcionando por meio de uma arquitetura cliente/servidor. Além disso, é interoperável com outros protocolos de e-mail (Ex: POP3 e IMAP) para uma funcionalidade de e-mail completa.

O SMTP é um protocolo da camada de aplicação utilizado para enviar mensagens de e-mail de um cliente de e-mail para um servidor de e-mail e entre servidores de e-mail em uma rede de computadores. Quando um usuário envia um e-mail, o SMTP cuida de encaminhar essa mensagem do servidor de e-mail do remetente para o servidor de e-mail do destinatário. O SMTP é eficaz para enviar mensagens, mas não para recuperá-las ou armazená-las.

S

SUA

M

MENSAGEM

T

TÁ

P

PARTINDO

Ele também é utilizado para a comunicação entre servidores de e-mail, permitindo que eles passem e-mails de um para o outro até que a mensagem alcance o servidor de e-mail do destinatário final (veremos esse caso específico mais à frente). **O SMTP - em seu uso moderno - inclui mecanismos de autenticação para aumentar a segurança, ajudando a prevenir o abuso do sistema de e-mail, como o envio de spam.** Vejamos alguns cenários de utilização:

a) Cenário 1: troca de e-mails em um mesmo provedor

Vamos supor que Diego deseja enviar um e-mail para Renato e ambos possuem uma conta no mesmo provedor de e-mail, logo utilizarão o mesmo servidor de e-mail. Considere que o e-mail de Diego é *diego@gmail.com* e o e-mail de Renato é *renato@gmail.com*. **Notem que o domínio é o mesmo (gmail.com), logo se trata do mesmo provedor de e-mail, portanto ambos acessam o mesmo servidor de e-mail.**

Quando Diego quiser enviar um e-mail para Renato, a mensagem não será encaminhada diretamente de um para o outro. *Por quê?* Porque o serviço de correio eletrônico é baseado em um modelo cliente/servidor, logo o remetente e o destinatário não se comunicam de forma direta. Dessa forma, a mensagem de Diego deve passar pelo servidor de e-mail antes de chegar a Renato. *E o que o servidor faz?* Ele armazena a mensagem! *Onde ele armazena?* **Na caixa postal de Renato!**

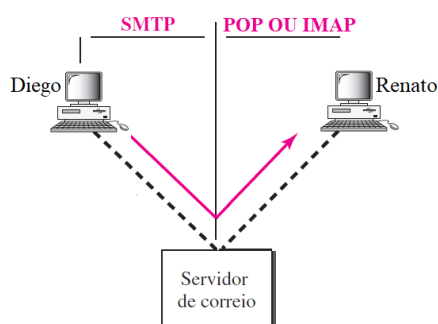




Vamos fazer uma analogia: suponha que você trabalha viajando o país e não possui um endereço físico. Ainda assim, você pode precisar receber correspondências ou encomendas eventualmente. *E agora, o que fazer?* Você pode ir aos Correios e contratar um serviço de Caixa Postal. *O que é isso?* É um recipiente para receber correspondências e encomendas de maneiras prática, sem precisar ter um endereço fixo ou alguém em casa para recebê-los. No contexto de e-mails, a caixa postal tem o mesmo sentido.

A caixa postal de e-mail funciona exatamente assim: o servidor de e-mail armazenará a mensagem enviada por Diego na caixa postal de Renato. Professor, quando o Renato vai ler o e-mail enviado? Isso é irrelevante porque o serviço de e-mail é assíncrono, isto é, a comunicação não exige uma sincronia para ocorrer – ela pode ocorrer de maneira simplesmente dessincronizada. *Ainda não entendi muito bem, professor...*

Galera, um exemplo de serviço síncrono é um chat ou um telefonema: quando um fala, o outro deve estar disponível no mesmo momento para que possa responder à mensagem; caso contrário, a conversa não fluirá. Você não vai ligar para alguém, falar “alô” para ela responder só daqui duas horas! Um serviço assíncrono permite que o destinatário leia e responda quando bem entender (como nós fazemos com mensagem e áudio no Whatsapp). Então, vamos resumir...



Diego compõe uma mensagem no Gmail e a envia para Renato. O SMTP é utilizado para enviar esta mensagem do cliente de e-mail de Diego para o servidor de e-mail do Gmail. Uma vez que o servidor do Gmail recebe a mensagem, ele identifica que o destinatário, Renato, também está no Gmail. O servidor então processa a mensagem internamente, sem a necessidade de enviar a mensagem para outro servidor. A mensagem é colocada na caixa postal de Renato no Gmail, que pode acessá-la posteriormente.

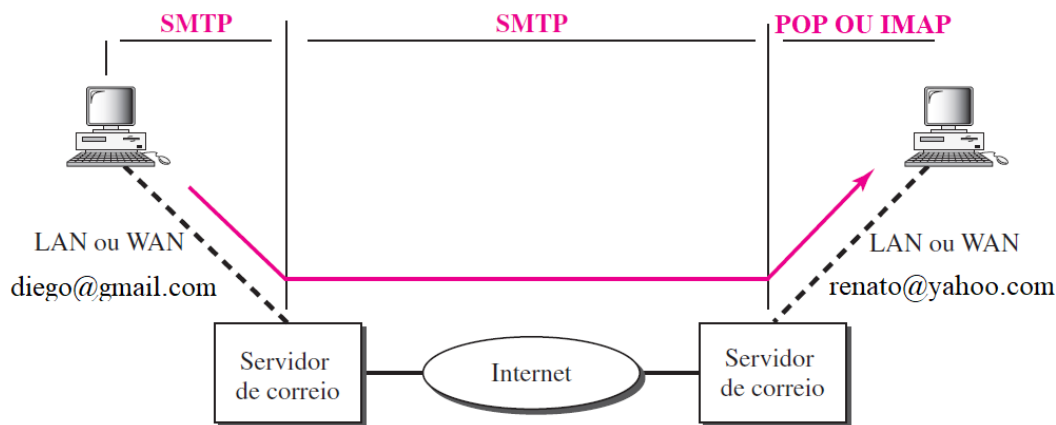
b) Cenário 2: troca de e-mails em provedores diferentes

Suponha agora que o e-mail de Diego é *diego@gmail.com* e o e-mail de Renato é *renato@yahoo.com*. Nesse caso, temos domínios diferentes, logo teremos provedores (e servidores) diferentes entre os usuários. Quando Diego enviar uma mensagem para Renato, a mensagem sai do seu programa cliente de e-mail e chega até o servidor de correio de origem (também chamado de servidor de saída).

O servidor de correio de origem analisa apenas o segmento que se encontra após o símbolo de @ para identificar o endereço de domínio de destino (*renato@yahoo.com*). O servidor de saída – ainda por meio do SMTP – envia a mensagem para o servidor de correio de destino (também chamado de servidor de entrada). O servidor de correio de destino identifica a informação existente antes do símbolo @ (*renato@yahoo.com*) e deposita a mensagem em sua respectiva caixa postal.

Quando Renato quiser, ele utiliza seu programa cliente de e-mail ou webmail para – por meio do POP3 ou IMAP – recuperar a mensagem e/ou armazená-la na máquina local. Vamos resumir...





Diego escreve e envia um e-mail para Renato por meio do Gmail. O SMTP transfere a mensagem para o servidor de e-mail do Gmail. Esse servidor também utiliza o SMTP para enviar a mensagem para o servidor de e-mail do Yahoo, que é o provedor de Renato. Este processo pode envolver a mensagem passando por vários servidores e redes de computadores na internet. Uma vez que o servidor do Yahoo receba a mensagem, ele a processa e entrega na caixa de Renato no Yahoo.

E-Mail: POP

POST OFFICE PROTOCOL (POP)

Protocolo da camada de aplicação responsável por recuperar e-mails de um servidor de e-mail. Em regra, ele baixa os e-mails do servidor para o cliente local e os deleta do servidor, mas há outros modos de funcionamento. O POP3 suporta criptografia via SSL/TLS e autenticação através de usuário/senha, além de permitir a leitura de e-mails offline e controle limitado sobre as mensagens no servidor. Por outro lado, ele não sincroniza o estado da mensagem entre múltiplos dispositivos (lido/não lido, marcado/não marcado). Ele é menos flexível que IMAP, sendo ideal para usuários que acessam e-mail de um único dispositivo.

O protocolo POP3 permite que os usuários façam o download de e-mails de um servidor para suas máquinas locais, facilitando o acesso offline e liberando espaço no servidor. No passado, isso era essencial devido às limitações de armazenamento dos servidores de e-mail. O modo padrão, chamado Delete/Download, remove as mensagens do servidor após o download, liberando espaço, mas dificultando o gerenciamento de e-mails em diferentes dispositivos.

No modo Keep/Notification, o POP3 baixa as mensagens, mas mantém uma cópia no servidor, permitindo maior flexibilidade e proteção contra perda de dados. No entanto, isso podia causar problemas de armazenamento, esgotando o limite do servidor. Apesar de sua utilidade em tempos de acesso limitado à internet, o POP3 mostrou-se problemático com o aumento do uso de múltiplos dispositivos e a necessidade de maior organização.

Com o avanço da tecnologia, o POP3 perdeu popularidade para o IMAP, que oferece funcionalidades mais avançadas, como a sincronização em tempo real entre múltiplos dispositivos, a possibilidade de organizar mensagens no servidor e o acesso a pastas. O IMAP se mostrou mais eficiente para o gerenciamento de e-mails modernos, permitindo acesso contínuo e centralizado ao correio eletrônico.

E-Mail: IMAP

INTERNET MESSAGE ACCESS PROTOCOL (IMAP)

Protocolo da camada de aplicação responsável pelo acesso, gerenciamento e sincronização de e-mails armazenados em um servidor de e-mail. Ele permite ao usuário visualizar e manipular mensagens diretamente no servidor, além de sincronizar o estado das mensagens (lido/não lido, marcado/não marcado) entre múltiplos



dispositivos. Ele suporta criptografia via SSL/TLS e autenticação através de usuário e senha. Esse protocolo é mais flexível que o POP3, sendo ideal para usuários que acessam e-mail de múltiplos dispositivos. As mensagens geralmente permanecem no servidor, permitindo acesso a partir de qualquer dispositivo.

Um usuário pode verificar o cabeçalho de um e-mail antes de baixá-lo; pode procurar pelo conteúdo de um e-mail antes de baixá-lo; pode baixar parcialmente um e-mail – isso é útil se a largura de banda for limitada e o e-mail tiver conteúdos com grandes exigências de largura de banda; um usuário pode criar, eliminar ou renomear caixas de correio no servidor de e-mail; e pode criar uma hierarquia de caixas de correio em pastas para armazenamento de e-mails.

O IMAP é equivocadamente associado a webmails pelo caráter de repositório central que esses serviços oferecem ao permitir amplo acesso a e-mails (mobilidade). No entanto, navegadores (e consequentemente webmails) não suportam IMAP – eles utilizam o HTTP/HTTPS! **O IMAP possui uma versão mais segura chamada IMAPS (IMAP Secure). Nesse caso, ele utilizará a Porta 993 e, não, 143.** Vamos ver uma tabela comparativa:

POP3	IMAP
Post Office Protocol (Version 3)	Internet Message Access Protocol
Não recomendado para acesso em múltiplos dispositivos	Recomendado para acesso em múltiplos dispositivos
Não permite criar e organizar pastas no servidor	Permite criar e organizar pastas no servidor
Não permite verificar o cabeçalho antes de baixá-lo	Permite verificar o cabeçalho antes de baixá-lo
Modificações em um dispositivo não refletidas em outros	Modificações em um dispositivo refletidas em outros
Não permite baixar parcialmente um e-mail	Permite baixar parcialmente um e-mail
Por padrão, mensagens de e-mail são lidas offline	Por padrão, mensagens de e-mail são lidas online
Não permite múltiplas caixas postais	Permite múltiplas caixas postais
Porta 110	Porta 143

E-Mail: WebMail

WEBMAIL

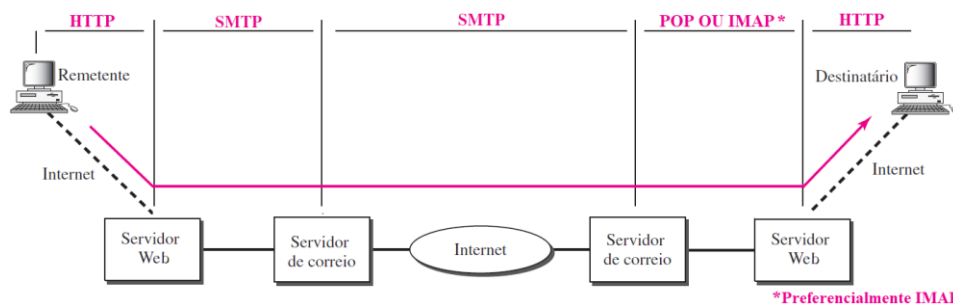
Um webmail é um serviço de e-mail que pode ser acessado e usado através de um navegador da web, em vez de um cliente de e-mail dedicado. Ele funciona como uma interface baseada na web para enviar, receber e gerenciar mensagens de e-mail (Ex: Gmail, Yahoo, Outlook, Hotmail, etc).

Agora vamos falar sobre um Webmail! **Trata-se de um sistema web que faz a interface com um serviço de e-mail hospedado em um Servidor Web!** Armaria, professor... entendi foi nada! Galera, quando vocês acessam a página do Estratégia Concursos, vocês estão acessando – por meio de um browser – uma página que está hospedada (armazenada) em uma máquina especializada chamada Servidor Web. Ocorre de maneira semelhante com e-mail...

Quando vocês acessam – por meio de um navegador – um serviço de e-mail, temos um... webmail! **É como se o cliente de e-mail apresentado no esquema anterior estivesse hospedado em um servidor web**



e você utilizasse um browser para acessá-lo. Logo, a comunicação entre a máquina do remetente e o servidor web de origem se dá por meio do HTTP! Ao final, para recuperar o e-mail do servidor web para a máquina do destinatário também se utiliza o HTTP.



Algumas questões não primam pelo rigor técnico e acabam omitindo o servidor web e tratando ambos – servidor web e servidor de correio eletrônico – apenas como servidor de correio eletrônico.

CARACTERÍSTICAS DE WEBMAIL	DESCRIÇÃO
ACESSIBILIDADE	Webmails podem ser acessados de qualquer dispositivo com uma conexão à internet e um navegador web, oferecendo grande conveniência e mobilidade.
NÃO QUERER INSTALAÇÃO DE SOFTWARE	Ao contrário dos clientes de e-mail que requerem instalação, como Microsoft Outlook ou Mozilla Thunderbird, o webmail opera inteiramente no navegador.
ARMAZENAMENTO NA NUVEM	As mensagens de e-mail são armazenadas no servidor do provedor de e-mail, não no dispositivo local. Isso facilita o acesso a e-mails de diferentes dispositivos.
INTERFACE DO USUÁRIO	Webmails geralmente têm interfaces de usuário ricas, semelhantes a aplicações desktop, com recursos como arrastar e soltar, pastas, e ferramentas de busca avançada.
SEGURANÇA E MANUTENÇÃO	A segurança e a atualização de software são gerenciadas pelo provedor do serviço, reduzindo a necessidade de manutenção por parte do usuário.
INTEGRAÇÃO COM OUTROS SERVIÇOS	Muitos webmails são integrados com outros serviços online, como calendários, gerenciamento de contatos, armazenamento em nuvem e aplicações de escritório.

Protocolo DHCP

INCIDÊNCIA EM PROVA: BAIXA

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Protocolo da camada de aplicação responsável por atribuir automaticamente endereços IP e outras configurações de rede a dispositivos em uma rede. Ele funciona com um modelo cliente-servidor em que o Servidor DHCP atribui IPs dinamicamente aos clientes da rede e suporta alocação dinâmica, alocação automática e alocação estática de endereços IP. O DHCP simplifica o gerenciamento de endereços IP (especialmente em redes grandes), sendo amplamente utilizado em redes domésticas, corporativas e públicas para simplificar a configuração de rede.

O **DHCP (Dynamic Host Configuration Protocol)** é um protocolo da camada de aplicação que permite a alocação automática de endereços lógicos, ou seja, endereços IP. Ele pode atribuir esses endereços de forma estática (fixos) ou dinâmica (variáveis). O endereço lógico é diferente do endereço físico (MAC), que está permanentemente associado ao hardware de um dispositivo. O endereço IP pode ser alterado sem problemas, tornando-o flexível para a conexão de diferentes dispositivos na rede.



Todo dispositivo na internet precisa de um endereço IP único, que pode ser fornecido por um provedor de serviços de internet (ISP). Existem dois tipos de IP: estático e dinâmico. O endereço estático é fixo, ideal para servidores que precisam manter o mesmo IP constantemente. Já o endereço dinâmico, que é mais comum para usuários domésticos, é configurado automaticamente pelo DHCP e pode mudar a cada nova conexão, proporcionando maior segurança e eficiência.

O DHCP facilita a configuração de redes, especialmente em redes grandes, onde seria inviável configurar manualmente cada dispositivo. Ele atribui automaticamente o endereço IP e outras configurações importantes, como máscara de sub-rede e gateway padrão. Isso simplifica o gerenciamento da rede e reduz a chance de erros, especialmente em redes com muitos dispositivos conectados.

Além de simplificar o processo de conexão, o DHCP gerencia a alocação de endereços de maneira eficiente, desalocando um IP quando uma conexão termina para que ele possa ser reutilizado por outro dispositivo. Antes da automação do DHCP, os usuários precisavam configurar manualmente os parâmetros de rede, como o endereço IP e DNS, o que era muito mais trabalhoso e propenso a erros.

Protocolo DNS

INCIDÊNCIA EM PROVA: ALTÍSSIMA

DOMAIN NAME SYSTEM (DNS)

Protocolo da camada de aplicação responsável por traduzir (também chamado de resolver) nomes de domínio legíveis por humanos para Endereços IP. Ele funciona em um modelo de consulta e resposta, sendo estruturado de maneira hierárquica com vários níveis de Servidores DNS. Esse protocolo armazena as respostas recentes para reduzir o tempo de resposta e o tráfego na rede, incluindo extensões de segurança para proteger contra ataques. O DNS é essencial para a navegação na internet, permitindo o uso de URLs em vez de endereços IP numéricos.

D	N	S
DÁ	NOME AO	SITE

DNS: Funcionamento

Galera, quantos números vocês sabem decorados? Eu, por exemplo, tenho uma péssima memória! Eu sei meu CPF, RG, Conta Bancária e Telefone. Fora isso, eu já começo a ter dificuldades de lembrar. Nós sabemos que os computadores na Internet são identificados utilizando endereços IP (Exemplo: 192.168.10.15). **Uma vez que é mais fácil decorar nomes que números, foi criado um sistema capaz de traduzir números em nomes e vice-versa.**

Vamos fazer mais um teste! Dessa vez, eu quero que vocês abram um navegador web qualquer, digitem **216.58.211.14** e vejam o que acontece! **Pois é, abrirá a página do Google!** Professor, como isso é possível? Galera, toda página web está armazenada em algum servidor e nós já sabemos que todo dispositivo na internet precisa ter um endereço lógico exclusivo. Logo, um servidor também precisa de um endereço para ser acessado.

O servidor que armazena o Google tem o endereço lógico 216.58.211.14. Agora vocês já imaginaram se nós tivéssemos que decorar todos os endereços IP de todos os sites que nós acessamos diariamente? Seria completamente inviável! Para resolver esse problema, surgiu o Domain Name System (DNS). **Trata-se de um protocolo cliente/servidor da camada de aplicação responsável por atribuir endereços lógicos aos recursos da rede** - ele é como uma agenda de contatos da Internet!



Professor, falou difícil agora! Galera, endereço léxicos são aqueles formados por palavras ou vocábulos de um idioma, em vez de um número. Em outras palavras, ele busca transformar endereços numéricos em nomes amigáveis, mais compreensíveis para humanos e mais fáceis de memorizar. *O que é mais fácil de decorar: 216.58.211.14 ou Google.com?* Pois é! Notem que, apesar de ser mais fácil para **você** memorizar, o **computador** entende apenas Endereço IP.

Imaginem que um dia você sai de uma balada de madrugada, chama um taxi e simplesmente diz ao motorista: *"Parceiro, me leva na casa do João!"* Ué, galera... o taxista lá sabe quem é João? Taxista conhece endereços e, não, nomes de pessoas. **Nessa analogia, o taxista seria o seu navegador - ele só reconhece endereços e, não, nomes de pessoas.** Professor, como o DNS consegue fazer essa tradução de nome para endereço e vice-versa?

Vocês sabem decorados todos os números de telefone armazenados no smartphone? Eu duvido! Quando vocês querem ligar para alguém, vocês procuram o nome de um contato e o celular disca o número armazenado. E se vocês, por algum acaso, souberem o número, ele faz o caminho inverso e identifica o nome. O DNS funciona exatamente como a agenda telefônica de um smartphone. **A tabela seguinte mostra a correspondência entre URL e Endereço IP:**

DNS (DOMAIN NAME SYSTEM)	
URL	IP
www.google.com	216.58.211.14

DNS: URL

Antes de prosseguir, vamos entender o que é uma URL (*Uniform Resource Locator*)! **Trata-se do endereço de um recurso em uma rede de computadores.** Todo recurso computacional (página web, arquivo, servidor, impressora, computador, documento, entre outros) deve possuir um endereço para que possa ser localizada. Ela oferece uma maneira uniforme e padronizada de localizar recursos na rede. Uma URL é formada pela seguinte estrutura:

URL - SINTAXE ABSTRATA	
PROTOCOLO://IP-OU-DOMÍNIO:PORTA/CAMINHO/RECURSO	
COMPONENTES	DESCRIÇÃO
PROTOCOLO	Também chamado de esquema, trata-se do protocolo utilizado para acessar um recurso.
IP	Número de IP do Servidor (Host) que hospeda um recurso.
DOMÍNIO	Nome do Domínio do Servidor (Host) que hospeda um recurso.
PORTA	Ponto lógico que permite criar uma conexão em um processo.
CAMINHO	Estrutura de diretórios dentro do servidor que armazena um recurso.
RECURSO	Componente físico ou lógico disponível em um sistema computacional.

Pessoal, os componentes de um endereço funcionam para ajudar a encontrar o recurso desejado. Vamos pensar em um endereço fictício: SQN 115 Bloco A Apt 208 - Asa Norte - Brasília/DF (sim, os endereços em Brasília são meio malucos). Eu estou dizendo que - para encontrar esse endereço - você deve ir até o



Distrito Federal, localizar Brasília, se deslocar até a Asa Norte, seguir até a SQN 115, procurar o Bloco A e chegar no Apt 208.

A URL é o endereço virtual de um recurso em uma rede, logo ela está informando que para encontrar o recurso desejado, você deve utilizar um determinado protocolo, informar o endereço lógico ou nome do domínio para encontrar o servidor, depois procurar em uma porta específica, seguir um caminho nos diretórios no disco que armazena esse recurso até finalmente encontrá-lo. Então vamos ver um exemplo:

HTTPS://WWW.ESTRATEGIACONCURSOS.COM.BR/APP/DASHBOARD/CURSOS/AULAS/AULA1.PDF

COMPONENTES	DESCRIÇÃO
PROTOCOLO	https
DOMÍNIO	estrategiaconcursos.com.br (www é apenas um prefixo que pode ser omitido)
PORTA	443 (apesar de ter sido omitida, essa é a porta padrão desse protocolo)
CAMINHO	/app/dashboard/cursos/aulas
RECURSO	Aula1.pdf

Existe uma confusão entre URL e Domínio! Observem que - se eu modifico o nome do recurso da URL anterior para "Aula2.pdf", eu terei uma URL diferente, no entanto o domínio permanecerá o mesmo! Pessoal, nós vimos na página anterior a sintaxe abstrata de uma URL! *Por que dizemos que se trata de uma sintaxe abstrata?* **Porque a sintaxe completa pode conter vários outros componentes como apresentado abaixo:**

URL - SINTAXE COMPLETA

PROTOCOLO://NOME-DE-USUÁRIO@IP-OU-DOMÍNIO:PORTA/CAMINHO/RECURSO?QUERY#FRAGMENTO

Dos componentes apresentados, apenas dois são obrigatórios: **Protocolo** e **Domínio**. Porta, Caminho e Recurso são bastante comuns, mas opcionais. Já na sintaxe completa, é possível ver mais três componentes opcionais bem mais raros: Query (ou QueryString), Fragmento e Nome de Usuário. O primeiro é usado para passar parâmetros de pesquisa; o segundo para ir diretamente para uma parte específica de uma página web; e o terceiro para autenticação de usuários.

COMPONENTES EXTRAS	DESCRIÇÃO
QUERY / QUERYSTRING	Utilizado para passar parâmetros adicionais para o servidor em formato chave-valor.
FRAGMENTO	Utilizado para navegar diretamente para uma seção específica de uma página da web.
NOME DE USUÁRIO	Utilizado em contextos em que é necessária a autenticação para acessar os recursos.

A Query String permite passar parâmetros adicionais para o servidor. Isso inclui dados de formulários, filtros para pesquisas, informações de paginação, ou qualquer outro dado que precise influenciar a resposta do servidor. Ela é iniciada por um ponto de interrogação (?) e é seguida por uma ou mais pares de chave-valor, que são separados por e comercial (&)⁴. Cada par chave-valor é composto pela chave, um sinal de igual (=), e o valor associado.

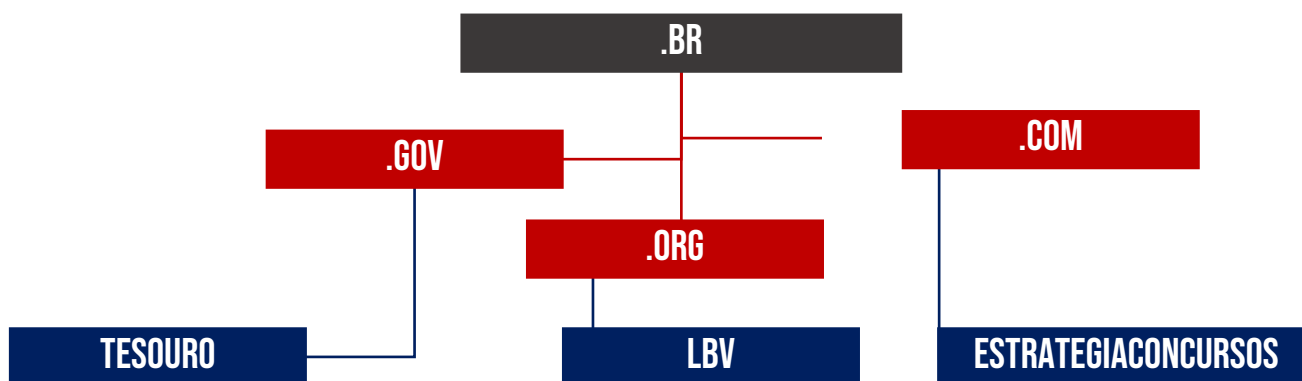
⁴ Note que a URL não permite acentuação gráfica e possui alguns caracteres reservados (Ex: ?, /, \$, :, etc). A codificação de URL converte os caracteres reservados em um formato inteligível por navegadores (Ex: espaço em branco é codificado como "%20").



Já o fragmento (ou âncora) é uma parte da URL que segue o caractere cerquilha (#) e é usada para identificar e direcionar para uma parte específica dentro de um documento. O fragmento não é enviado ao servidor durante uma solicitação HTTP; ele é processado exclusivamente pelo navegador. Por exemplo, em uma página com múltiplos títulos ou seções, é possível acessar diretamente uma seção específica.

DNS: Hierarquia

O domínio é o principal componente de uma URL e, por isso, dizemos que o DNS traduz, transforma, resolve um Nome/Domínio em um Endereço IP e vice-versa. Agora vamos falar mais detalhadamente sobre domínios. **O DNS é um protocolo cliente/servidor que apresenta uma estrutura hierárquica e distribuída, em que seu espaço de nomes é dividido em vários servidores de domínio baseado em níveis.** Vejam a imagem seguinte...



Diego, o que é um espaço de nomes? Para evitar ambiguidades, os nomes atribuídos às máquinas devem ser cuidadosamente selecionados a partir de um espaço de nomes – que nada mais é que um conjunto organizado de possíveis nomes. **Em outras palavras, os nomes devem ser exclusivos, uma vez que os endereços IP também o são.** A entidade que controla o registro e manutenção de domínios em nível global é chamada de ICANN.

Essa entidade define que o domínio .br pertence ao Brasil⁵; o domínio .pt pertence à Portugal; o domínio .jp pertence ao Japão; o domínio .es pertence à Espanha; entre outros. **Já em nível nacional, existe uma outra entidade responsável pelo registro e manutenção de domínios brasileiros chamada Registro.br.** Caso algum dia vocês queiram adquirir e registrar um domínio próprio, vocês provavelmente terão que acessar a página seguinte:

WWW.REGISTRO.BR

Professor, eu não tenho grana para isso não! Galera, fiquem tranquilos porque é bem baratinho. Em um plano de 10 anos, custaria pouco mais de R\$3/Mês.

Além disso, existem algumas subcategorias de domínio .br. Como assim, professor? Se você exerce uma atividade comercial, você poderá ter um domínio .com.br; se você possui uma organização não-governamental sem fins lucrativos, você poderá ter um domínio .org.br. Algumas categorias possuem ainda restrições adicionais por serem direcionadas a empresas de setores específicos, sendo necessária comprovação por meio de envio de documentos.

⁵ Isso significa que um site .br está registrado no Brasil e, não, que ele está hospedado fisicamente no Brasil.



Existem algumas regras que devem ser observadas em um nome de domínio registrado no Registro.br: (1) deve possuir entre 2 e 26 caracteres, não incluindo a categoria. Logo, o domínio *www.x.com.br* é inválido porque possui apenas 1 caractere; (2) deve ser composta por caracteres alfanuméricos. Logo, o domínio *www.123.com.br* é inválido porque não contém letras; (3) não pode começar ou terminar com hífen, mas pode ter acentuação e cedilha desde 2008.



Pessoas Jurídicas

COM RESTRIÇÃO

AM.BR	Empresas de radiodifusão sonora
COOP.BR	Cooperativas
FM.BR	Empresas de radiodifusão sonora
G12.BR	Instituições de ensino de primeiro e segundo grau
GOV.BR	Instituições do governo federal
MIL.BR	Forças Armadas Brasileiras
ORG.BR	Instituições não governamentais sem fins lucrativos

PSI.BR

Provedores de serviço Internet

DNSSEC OBRIGATÓRIO

B.BR	Bancos
DEF.BR	Defensorias Públicas
JUS.BR	Instituições do Poder Judiciário
LEG.BR	Instituições do Poder Legislativo
MP.BR	Instituições do Ministério Público



Genéricos

Para pessoas físicas ou jurídicas

ART.BR	Artes: música, pintura, folclore
COM.BR	Atividades comerciais
ECO.BR	Atividades com foco eco-ambiental
EMP.BR	Pequenas e micro-empresas
NET.BR	Atividades comerciais
ONG.BR	Atividades não governamentais individuais ou associativas



Universidades

EDU.BR	Instituições de ensino superior
---------------	---------------------------------



Pessoas Físicas

BLOG.BR	Web logs
FLOG.BR	Foto logs
NOM.BR	Pessoas Físicas
VLOG.BR	Vídeo logs
WIKI.BR	Páginas do tipo 'wiki'

Protocolos Web

INCIDÊNCIA EM PROVA: ALTÍSSIMA

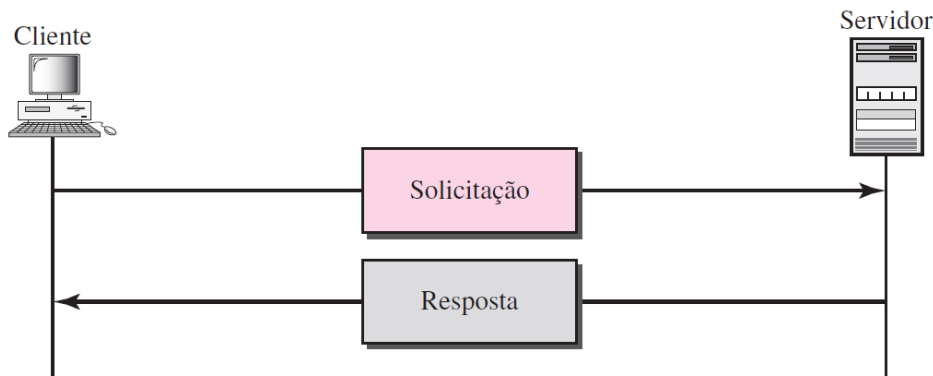
Web: HTTP

HYPERTEXT TRANSFER PROTOCOL (HTTP)

Protocolo da camada de aplicação utilizado para carregar páginas da web, enviar formulários, realizar transações online, obter recursos, entre outros. Trata-se de um protocolo baseado em um modelo de requisição-resposta entre um cliente (Navegador Web) e um servidor (Servidor Web): mensagens enviadas pelo cliente são chamadas de solicitações ou requisições (Requests) e as mensagens enviadas pelo servidor são chamadas de respostas (Responses).



O HTTP (HyperText Transfer Protocol) é um protocolo cliente/servidor da camada de aplicação utilizado por programas de navegação (browsers) para acessar dados na web. Em português, seria traduzido como Protocolo de Transferência de Hipertexto⁶, sendo responsável pela transferência, formatação e apresentação de páginas web com conteúdo multimídia (textos, áudio, imagens, vídeos, etc) entre um servidor e um cliente na Internet.



A imagem anterior ilustra uma transação típica entre um Cliente HTTP e um Servidor HTTP. O cliente inicializa uma transação enviando uma mensagem de solicitação. O servidor responde enviando uma mensagem de resposta. *Como assim, Diego?* Galera, toda página web está armazenada em um servidor web. Logo, quando você acessa qualquer página pelo navegador, você está fazendo uma solicitação ao servidor para acessar aquela página.

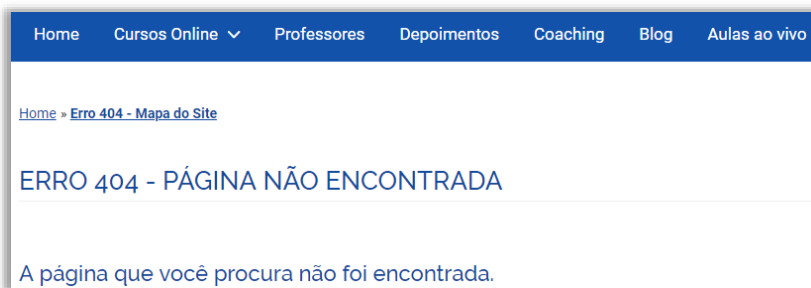
Se você conseguir acessá-la, significa que o servidor web autorizou e te devolveu como resposta a página que você desejava acessar. **Por falar em servidor web, esse é o nome dado ao servidor que hospeda ou armazena páginas ou recursos web** – assim como o servidor que armazena e-mails é chamado de servidor de e-mail. Prosseguindo... toda solicitação ou requisição a um servidor web retorna um código de status de três dígitos e divididos em cinco categorias:

CÓDIGO	CATEGORIA	SIGNIFICADO
1XX	INFORMAÇÃO	100 significa que o servidor concorda em atender à requisição.
2XX	SUCESSO	200 significa que a requisição foi bem-sucedida e 204 significa que a página está sem conteúdo.
3XX	REDIRECIONAMENTO	301 significa que a página foi movida e 304 significa que a página em cache ainda é válida.
4XX	ERRO DO CLIENTE	403 significa que a página é proibida e 404 significa que a página não foi encontrada.
5XX	ERRO DO SERVIDOR	500 significa que houve um erro interno e 503 significa que você deve tentar novamente mais tarde.

Professor, há como explicar melhor o que você quis dizer? Claro que sim! Façam um teste: abram um navegador e digitem: www.estrategiaconcursos.com.br/euamopinkfloyd.

⁶ Hipertexto é basicamente um texto que possui links para outros textos em páginas web. Antigamente, uma página web possuía apenas textos, mas atualmente ela possui texto, áudio, imagem, vídeo, etc. Logo, o termo mais preciso atualmente é hiperídia = hipertexto + multimídia.





Vocês viram que retornou um erro? Pois é, Erro 404! Esse erro é da categoria Erro do Cliente e significa que uma determinada página não foi encontrada. *Por que, professor?* Cara, essa página não foi encontrada basicamente porque ela não existe - eu acabei de inventar apenas para mostrar um código de retorno! **Esse código sempre existirá para qualquer requisição, mas nem sempre será exibido para os usuários (se houve sucesso, não faz sentido exibir).**

5xx Server Error: entenda o erro que tirou WhatsApp, Facebook e Instagram do ar

Erro de servidor faz com que usuários não possam acessar os serviços das plataformas do Facebook nesta segunda-feira (4)

Vocês se lembram quando o Whatsapp, Instagram e Facebook caíram por um dia inteiro? Ao tentar acessar essas páginas, aparecia um **ERRO 5XX**. Ele significa que o problema está sendo ocasionado por uma falha nos servidores. Na prática, ele ocorre quando o servidor (computador central) não consegue completar a solicitação do usuário e, por isso, não tem como exibir a informação desejada.



HTTP é um **protocolo** para transferência ou acesso de hipertexto e HTML é uma **linguagem** para criação de páginas web. **HTTP** é **Protocolo** e **HTML** é **Linguagem**.

Web: HTTPS

HYPERTEXT TRANSFER PROTOCOL SECURE (HTTPS)

Protocolo da camada de aplicação utilizado para carregar páginas da web, enviar formulários, realizar transações online, obter recursos, entre outros, porém com uma camada adicional de segurança entre o cliente e o servidor. Possui recursos para criptografar a comunicação, protegendo a troca de dados contra interceptação e alteração. Esse protocolo requer certificados digitais para autenticar a identidade do servidor e garante que os dados transferidos sejam acessíveis apenas para o destinatário pretendido. Além disso, ele verifica se os dados enviados não foram alterados ou corrompidos durante a transferência e confirma a identidade do site para o usuário.



O HTTPS é um protocolo que tem a mesma finalidade do HTTP. Em outras palavras, ele é responsável pela transferência, formatação e apresentação de páginas web com conteúdo multimídia (textos, áudio, imagens, entre outros) entre um servidor e um cliente. No entanto, ele realiza transferências de forma segura, oferecendo criptografia, autenticação e integridade às transferências de dados de/para um servidor web.

Trata-se de uma implementação do HTTP sobre uma camada adicional de segurança que utiliza um outro protocolo chamado SSL/TLS⁷. Esses protocolos possuem propriedades criptográficas que permitem assegurar confidencialidade e integridade à comunicação. Dessa forma, é possível que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor web por meio de certificados digitais.

Imagine que você está em um Coffee Shop, tomando seu cafezinho com seu notebook e decide comprar um presente para sua mãe online em um site que utiliza apenas o HTTP e, não, HTTPS. Uma pessoa na mesa ao lado pode utilizar métodos maliciosos para interceptar sua transação e descobrir os dados do seu cartão de crédito, uma vez que seus dados estão trafegando em claro (sem criptografia).

Por meio da utilização do HTTPS, a mensagem será criptografada e permanecerá ilegível mesmo que seja interceptada por usuários não autorizados. Imaginemos outro cenário...

Você procura no Google um site bacana para comprar o presente. Entre os links encontrados, você lê rápido e não percebe que, na verdade, acessou a amason.com em vez da amazon.com. Esse primeiro site é igualzinho ao original, mas foi feito por um hacker para você pensar que se trata do mesmo site e roubar os dados do seu cartão de crédito. *E agora, professor?*

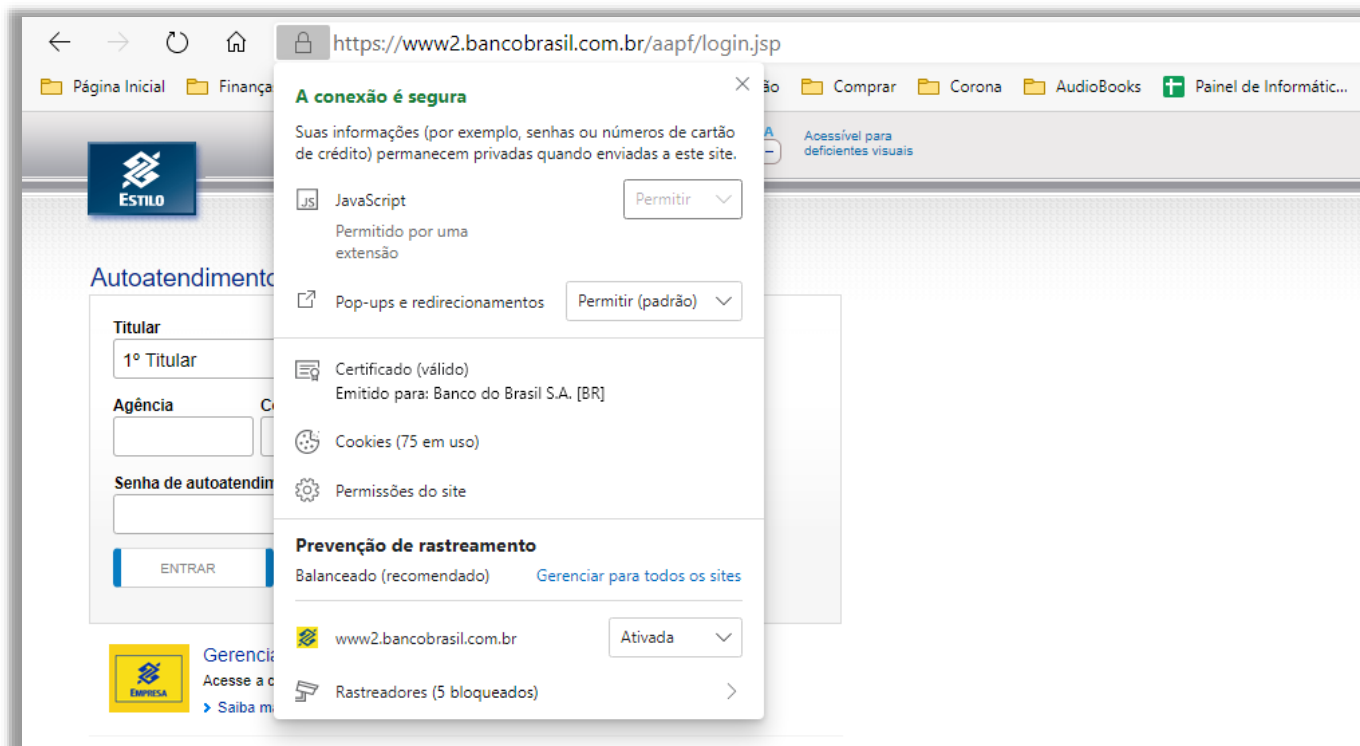
Nesse momento, seu navegador solicitará ao site um documento chamado Certificado Digital. Esse documento é simplesmente uma maneira de validar se um site é realmente quem diz ser, isto é, de uma empresa legítima. **Um site legítimo envia as informações da empresa a uma autoridade certificadora registrada para criar um certificado digital e permitir que usuários acessem sua página de forma segura.**



Após recebê-lo, o navegador consulta diversas autoridades públicas e privadas para verificar se esse certificado é válido - é como se alguém enviasse uma assinatura e você fosse a vários cartórios para

⁷ SSL (Secure Sockets Layer) é mais antigo e o TLS (Transport Layer Security) é mais novo.

conferir se aquela assinatura era legítima ou não. *Sabe quando você tenta acessar uma página e o navegador avisa que o certificado é inválido? Pois é, isso significa geralmente que o certificado não foi encontrado, expirou ou foi revogado.* Logo, tomem cuidado com esse tipo de mensagem!



Exemplo: se você entrar em um site de um Internet Banking, você visualizará o endereço começando com **https://** e um pequeno cadeado do lado esquerdo da barra de endereço indicando que a conexão a essa página é segura. *Por quê?* Porque veja que é informado que o certificado já foi recebido, já foi verificado e foi considerado válido. É claro que isso não é uma garantia absoluta, é apenas uma forma de garantir que a informação trafegada estará segura.



Protocolo FTP

INCIDÊNCIA EM PROVA: ALTÍSSIMA

FILE TRANSFER PROTOCOL (FTP)

Protocolo da camada de aplicação baseado no modelo cliente/servidor utilizado para a transferência de arquivos entre sistemas. Ele pode transferir uma variedade de tipos de dados (incluindo arquivos binários e de texto), além de permitir upload e download de arquivos, além de suporte a comandos para manipulação de diretórios. Ademais, requer autenticação (nome de usuário e senha) para acesso, embora possa ter acesso anônimo. O FTP é amplamente utilizado para distribuição de arquivos, backup e transferência de dados entre sistemas.

O FTP (File Transfer Protocol) é o protocolo responsável pela realização de transferências de arquivos entre um Cliente FTP e um Servidor FTP. Definições que já encontrei em prova:



- FTP é o protocolo de **transferência de arquivos** entre computadores;
- FTP é o protocolo para **transferência de arquivos** entre dois computadores conectados à Internet;
- FTP é o protocolo responsável pela **transferência de arquivos** remotos;
- FTP é o protocolo que permite a **cópia de arquivos** entre dois computadores;
- FTP é o protocolo responsável pelo **download/upload** de arquivos;
- FTP é o protocolo que permite fazer **upload de arquivos** para um servidor remoto.

Esse protocolo difere de outros por estabelecer duas conexões entre cliente e servidor: **uma para a transferência dos dados em si (Porta TCP 20) e a outra para a troca de informações de controle (Porta TCP 21)**. Essa divisão ocorre para tornar o protocolo mais eficiente, visto que as informações de controle utilizam uma conexão mais simples, enquanto a transferência de dados possui uma conexão mais complexa, permitindo o envio de múltiplos arquivos, etc.

Galera, por que nós utilizamos a internet? Basicamente para nos comunicar! E para haver comunicação, são necessárias duas partes: um emissor e um receptor. Quando você acessa um portal da web, quando você faz o download de um arquivo, quando você joga um jogo na internet, quando você acessa uma rede social ou quando você vê um vídeo no Youtube, **sempre haverá transferência (envio ou recebimento) de informações**.

Por falar nisso, há dois termos que eu tenho certeza que vocês estão bastante familiarizados porque já fazem parte do nosso vocabulário em português: Download e Upload! Nós já sabemos que a Internet funciona por meio de uma arquitetura ou modelo chamado Cliente/Servidor! **O que é isso, professor? Grosso modo, isso significa que ela é baseada em um conjunto de computadores que exercem a função de clientes ou servidores**. Relembrando...

Os computadores servidores são aqueles que fornecem um serviço e os computadores clientes são aqueles que consomem um serviço. Sabe aquele domingo à noite em que quer ver um filme maneiro? Você liga sua televisão, acessa a página web da Netflix, escolhe um filme e começa a assisti-lo! Nesse momento, sua televisão funciona como um cliente que está consumindo um serviço. *Esse serviço é disponibilizado por quem?* Pela Netflix!

A Netflix possui um bocado de computadores servidores que hospedam ou armazenam os filmes, então a sua televisão está consumindo um serviço de um servidor da Netflix. E quase tudo na internet é assim: você acessa o servidor do Estratégia para ver uma videoaula; você acessa o servidor do Spotify para ouvir uma música; você acessa o servidor do Google para acessar sua página e fazer alguma busca; e assim por diante. Dito isso, vamos ver o que é download e upload...

Ambos os termos são utilizados para referenciar a transmissão de dados de um dispositivo para outro através de um canal de comunicação previamente estabelecido. **O termo download está relacionado com a obtenção de conteúdo da Internet, em que um servidor hospeda dados que são acessados pelos clientes através de aplicativos específicos que se comunicam com o servidor por meio de protocolos preestabelecidos** (Ex: HTTP, FTP, etc).

De forma análoga, o termo upload faz referência a operação inversa à do download, isto é, refere-se ao envio de conteúdo à internet. **Do ponto de vista da participação do dispositivo que iniciou a transmissão de dados, a obtenção de dados de um dispositivo é chamada de download e a disponibilização de dados para um dispositivo é chamada de upload**. Tudo certo? Então, vamos prosseguir...





Eu já recebi essa dúvida no fórum dezenas de vezes, portanto vamos tentar deixar bastante claro para não haver margem para questionamentos! **O objetivo principal do FTP é transferir arquivos, no entanto nem toda transferência de arquivos ocorrerá por FTP.** *É possível transferir arquivos por e-mail? Sim, nesse caso estaremos utilizando SMTP/MIME. É possível transferir arquivos por uma página web? Sim, nesse caso estaremos utilizando HTTP/HTTPS.*

Quando você faz o download de uma aula ou vídeo em nosso site, você está utilizando o HTTP para transferência de arquivos do servidor web para a sua máquina local. **Em suma: HTTP é utilizado para transferência de hipertexto, mas pode ser utilizado alternativamente para transferência de arquivos; SMTP é utilizado para transferência de e-mails, mas pode ser utilizado alternativamente para transferência de arquivos; e existem dezenas de outros exemplos.**

Diversos outros protocolos possuem seus objetivos principais, mas alternativamente também permitem enviar arquivos - já o objetivo principal do FTP é a transferência de arquivos. A grande verdade é que o FTP tem sido cada vez menos utilizado - principalmente após a popularização do armazenamento em nuvem (Cloud Storage). Eu arrisco dizer que a maioria de vocês nunca usou esse protocolo em toda vida, apesar de fazer transferência de arquivos há anos na internet.

Há algum tempo, esse protocolo permanecia sendo utilizado para transferência de arquivos muito grandes. Hoje em dia, eu faço o upload do arquivo grande para nuvem e envio o link para quem eu quiser - sem precisar configurar um Cliente/Servidor FTP. Apesar de estar em desuso, ele continua sem bastante cobrado em prova. **Por essa razão, muito cuidado para não achar que toda transferência de arquivos ocorre por meio do FTP.**



Serviço VoIP

INCIDÊNCIA EM PROVA: MÉDIA

VOIP

VoIP (Voice over Internet Protocol) é uma tecnologia que permite a transmissão de voz e comunicações multimídia (como chamadas telefônicas, videotelefonia e sessões de conferência) através da Internet ou de outras redes baseadas em protocolos IP. Essencialmente, o VoIP transforma sinais de voz em dados digitais que podem ser enviados pela internet, como qualquer outro tipo de dado.

A tecnologia VoIP (Voz sobre IP) transformou a telefonia tradicional ao converter sinais de voz em dados digitais e transmiti-los pela internet, sem depender da comutação por circuitos das redes telefônicas convencionais (PSTN). Enquanto as redes PSTN estabelecem um caminho contínuo para as chamadas, o VoIP utiliza comutação por pacotes, tornando o uso da largura de banda mais eficiente e flexível para suportar diferentes serviços.

No VoIP, a voz é convertida em pacotes de dados IP, que contêm entre 10 e 30 milissegundos de áudio, e são enviados por meio de protocolos como o TCP ou UDP. Embora o TCP seja confiável e orientado à conexão, garantindo a entrega perfeita dos dados, o UDP é mais adequado para comunicações como chamadas de voz, onde pequenas perdas de pacotes são aceitáveis, pois a retransmissão de dados perdidos seria desnecessária.

O uso do UDP no VoIP se justifica em cenários de comunicação em tempo real, como ligações, onde breves interrupções não comprometem a qualidade geral da conversa. No entanto, apesar de o UDP ser um protocolo não confiável, o VoIP usa protocolos como SIP ou H.323 para estabelecer a conexão inicial e coordenar a chamada, o que torna o serviço orientado à conexão.

Logo, apesar de o VoIP usar o UDP, ele é considerado um serviço orientado à conexão, pois há mecanismos que garantem o estabelecimento da comunicação. O foco do VoIP está na simplicidade e na eficiência da transmissão, mesmo que ocorram pequenas perdas de dados, ao contrário de protocolos que exigem total integridade dos pacotes, como o TCP. Vejamos agora as principais vantagens desse serviço:

VANTAGENS DO VOIP

Permite fazer e receber ligações telefônicas tanto em uma rede local (LAN/Interna) quanto em uma rede pública (WAN/Externa).

Permite fazer e receber ligações para telefones fixos ou telefones celulares da telefonia convencional ou da telefonia digital por meio da utilização de um conjunto de dispositivos (adaptadores, gateways, etc).

Permite compartilhar o canal de comunicação de dados com outros serviços, podendo transmitir - além da voz - vídeos, imagens, entre outros.

Permite uma instalação extremamente escalável, podendo expandir com facilidade sem a necessidade de novas linhas dedicadas e aproveitando a infraestrutura de Redes IP⁸.

No entanto, a maior vantagem é a redução de custos de ligação. Na telefonia convencional, a cobrança se dá por tempo e pelo tipo de ligação, com valores diferentes, dependendo da distância (ligações locais,

⁸ Em geral, há duas alternativas: (1) substituir o telefone convencional por um telefone IP conectado por meio de um conector RJ-45; (2) ou utilizar um ATA (Adaptador de Terminal Analógico), que converte um sinal analógico em um sinal digital e vice-versa.



interurbanas e internacionais), operadora (mesma operadora ou concorrente), horários (chamadas diurnas ou noturnas) e dos dias (dia de semana ou final de semana). Já por meio do VoIP, é possível reduzir valores de ligações em até 70%.

DESVANTAGENS DO VOIP

Pode oscilar e perder a qualidade da ligação caso não esteja disponível uma conexão eficiente com a Internet.

Menos confiável que a telefonia convencional em relação a quedas de energia.

Podem ocorrer problemas de latência, atraso, interrupção e cortes na comunicação, além de perdas de dados.

Apresenta menor disponibilidade do canal de comunicação, uma vez que não possui um canal dedicado.



Glossário

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Segue abaixo uma tabela com um glossário de termos importantes relacionados a redes de computadores e internet e que podem vir em questões de prova:

TERMO	DESCRIÇÃO
PONTO-A-PONTO	Conexão direta entre dois dispositivos de rede.
PONTO-MULTIPONTO	Conexão de um ponto central com vários dispositivos.
SIMPLEX	Comunicação em um único sentido.
HALF-DUPLEX	Comunicação bidirecional, mas não simultânea.
FULL-DUPLEX	Comunicação bidirecional simultânea.
UNICAST	Envio de dados para um único destinatário.
MULTICAST	Envio de dados para múltiplos destinatários específicos.
BROADCAST	Envio de dados para todos os dispositivos de uma rede.
CLIENTE-SERVIDOR	Modelo de rede onde o cliente solicita e o servidor fornece serviços.
CABO COAXIAL	Cabo usado para transmitir sinais de dados e vídeo, comum em redes e TVs.
CABO DE PAR TRANÇADO	Cabo de rede com fios trançados, comum em redes Ethernet.
CABO DE FIBRA ÓPTICA	Cabo que transmite dados como pulsos de luz, usado para altas velocidades.
PLACA DE REDE	Hardware que conecta um computador à rede.
HUB	Dispositivo que conecta vários dispositivos em uma rede, transmitindo dados para todos.
BANDA LARGA	Conexão de internet de alta velocidade que permite múltiplos serviços simultâneos.
IP PÚBLICO	Endereço IP acessível globalmente na internet.
IP PRIVADO	Endereço IP usado dentro de redes locais, não acessível diretamente pela internet.
URL	Endereço de recurso na web (Uniform Resource Locator).
IP	Protocolo de endereçamento de dispositivos na internet (Internet Protocol).
DNS	Sistema que traduz nomes de domínio em endereços IP.
TCP	Protocolo que garante a entrega confiável de dados (Transmission Control Protocol).
HTTP	Protocolo para transferência de dados na web (Hypertext Transfer Protocol).
HTTPS	Versão segura do HTTP com criptografia.
FTP	Protocolo para transferência de arquivos na rede (File Transfer Protocol).



VOIP	Tecnologia para transmissão de voz pela internet (Voice over IP).
IMAP	Protocolo de e-mail que permite acesso a mensagens no servidor.
POP3	Protocolo de e-mail que baixa mensagens do servidor.
SMTP	Protocolo para envio de e-mails (Simple Mail Transfer Protocol).
VPN	Rede privada virtual que oferece segurança na comunicação.
FIREWALL	Sistema de segurança que monitora e controla o tráfego de rede.
PROXY	Servidor intermediário que lida com solicitações de rede.
ISP	Provedor de serviços de internet (Internet Service Provider).
WI-FI	Tecnologia sem fio para conectar dispositivos à internet.
PAN	Rede pessoal para conectar dispositivos próximos (Personal Area Network).
LAN	Rede local, geralmente limitada a uma área pequena (Local Area Network).
MAN	Rede que abrange uma cidade ou área metropolitana (Metropolitan Area Network).
WAN	Rede que cobre grandes distâncias, conectando LANs (Wide Area Network).
ROTEADOR	Dispositivo que direciona o tráfego entre redes diferentes.
SWITCH	Dispositivo que conecta dispositivos dentro de uma LAN, enviando dados apenas ao destinatário.
HUB	Dispositivo que transmite dados para todos os dispositivos conectados, sem distinção.
MODEM	Dispositivo que converte sinais digitais em analógicos para conexão à internet.
ETHERNET	Tecnologia padrão para redes locais com fio.
LARGURA DE BANDA	Quantidade de dados que pode ser transmitida em um período de tempo.
LATÊNCIA	Tempo que um pacote de dados leva para viajar de um ponto a outro.
BACKBONE	Rede principal que conecta partes de uma rede maior.
DATA CENTER	Instalação que armazena servidores e dados de rede.
COOKIE	Arquivo de dados armazenado no navegador para identificar usuários.
CACHE	Armazenamento temporário de dados para acesso rápido.
HTML	Linguagem de marcação usada para criar páginas web (Hypertext Markup Language).
PHISHING	Técnica de fraude para obter informações sensíveis.
MALWARE	Software malicioso destinado a danificar ou comprometer sistemas.



SPYWARE	Software que coleta informações sem o conhecimento do usuário.
WORM	Programa malicioso que se replica automaticamente e se espalha em uma rede.
TOPOLOGIA	Estrutura ou layout de uma rede de computadores.
LINK DEDICADO	Conexão de rede estabelecida exclusivamente entre dois dispositivos, garantindo uma via constante e exclusiva para a transmissão de dados.
LINK COMPARTILHADO	Conexão de rede na qual múltiplos dispositivos utilizam o mesmo canal ou meio de comunicação, compartilhando a largura de banda disponível.
BITCOIN	Primeira e mais conhecida criptomoeda, um tipo de moeda digital para controlar sua criação e gestão, sem a necessidade de uma autoridade central.
CRIPTOMOEDAS	Moedas digitais que usam criptografia para segurança.
METAVERSO	Espaço virtual interativo que mistura realidade virtual e aumentada com a internet.
NFT	Ativo digital único registrado em uma blockchain, usado para representar propriedade digital.
ARQUITETURA CLIENTE-SERVIDOR	Modelo onde o cliente solicita serviços ou recursos, e o servidor fornece esses recursos.
ARQUITETURA PONTO-A-PONTO	Modelo onde todos os nós podem atuar como clientes e servidores simultaneamente, compartilhando recursos sem um servidor central.
SPAM	Mensagens eletrônicas não solicitadas, geralmente enviadas em massa, frequentemente com conteúdo publicitário ou malicioso.
TELNET	Protocolo sem criptografia que permite acesso remoto a outro computador em uma rede, oferecendo um terminal de comando.
SSH	Protocolo que permite acesso remoto seguro a outro computador em uma rede, criptografando os dados para garantir a segurança.
ICMP	Protocolo utilizado para enviar mensagens de erro e diagnóstico na rede, como quando um pacote não pode ser entregue.



RESUMO

SERVIÇOS DA INTERNET	DESCRIÇÃO
WORLD WIDE WEB (WWW)	Trata-se do serviço de visualização de páginas web organizadas em sites em que milhares de pessoas possuem acesso instantâneo a uma vasta gama de informação online em hipermídia que podem ser acessadas via navegador – é o serviço mais utilizado na Internet. Em geral, esse serviço utiliza protocolos como HTTP e HTTPS.
CORREIO ELETRÔNICO	Trata-se do serviço de composição, envio e recebimento de mensagens eletrônicas entre partes de uma maneira análoga ao envio de cartas – é anterior à criação da Internet. Utiliza tipicamente um modo assíncrono de comunicação que permite a troca de mensagens dentro de uma organização. Em geral, esse serviço utiliza protocolos como POP3, IMAP e SMTP.
ACESSO REMOTO	Trata-se do serviço que permite aos usuários facilmente se conectarem com outros computadores, mesmo que eles estejam em localidades distantes no mundo. Esse acesso remoto pode ser feito de forma segura, com autenticação e criptografia de dados, se necessário. Em geral, esse serviço utiliza protocolos como SSH, RDP, VNC.
TRANSFERÊNCIA DE ARQUIVOS	Trata-se do serviço de tornar arquivos disponíveis para outros usuários por meio de downloads e uploads. Um arquivo de computador pode ser compartilhado ou transferido com diversas pessoas através da Internet, permitindo o acesso remoto aos usuários. Em geral, esse serviço utiliza protocolos como FTP e P2P.
WIKI	Wikis são plataformas colaborativas online que permitem que múltiplos usuários editem, criem e organizem conteúdo de forma conjunta. Qualquer pessoa pode modificar ou adicionar informações, facilitando a construção de conhecimento coletivo. Um exemplo famoso é a Wikipedia, onde o conteúdo é constantemente atualizado e expandido por sua comunidade de usuários.
FERRAMENTAS DE BUSCA	Ferramentas de busca são plataformas que permitem aos usuários pesquisar informações na web por meio de palavras-chave. Eles utilizam algoritmos para indexar e classificar páginas da internet, exibindo resultados relevantes em poucos segundos. Exemplos populares incluem Google, Bing e Yahoo, que ajudam a localizar websites, imagens, vídeos e outros conteúdos digitais.
REDES SOCIAIS	Redes sociais são plataformas digitais que conectam usuários, permitindo a criação e o compartilhamento de conteúdo como textos, imagens, vídeos e links. Elas facilitam a interação entre indivíduos e comunidades através de curtidas, comentários e mensagens. Exemplos incluem Facebook, Instagram e Twitter, que possibilitam a troca de informações em tempo real.
GRUPOS DE DISCUSSÃO	Grupos de Discussão são espaços virtuais onde pessoas com interesses comuns se reúnem para trocar informações, debater ideias e compartilhar experiências sobre um tema específico. Esses grupos podem ser organizados em fóruns online, listas de e-mails ou plataformas sociais, facilitando a comunicação e a colaboração entre os participantes em torno de tópicos variados.
COMPUTAÇÃO EM NUVEM	Computação em nuvem é a tecnologia que permite o armazenamento, processamento e gerenciamento de dados e aplicativos pela internet, em vez de servidores ou dispositivos locais. Os recursos de TI são fornecidos sob demanda, permitindo que empresas e usuários acessem dados remotamente, escalem operações e reduzam custos de infraestrutura física.
PORTAIS WEB	Portais Web são plataformas que centralizam e organizam uma vasta gama de informações e serviços em um único local online. Eles oferecem acesso a conteúdos diversos, como notícias, e-mails, fóruns, e-commerce e mais. Funcionam como uma porta de entrada para a navegação na web, facilitando o acesso a recursos variados em um só lugar.



TIPO	SIGLA	DESCRIÇÃO	DISTÂNCIA
PERSONAL AREA NETWORK	PAN	Rede de computadores pessoal (celular, tablet, notebook, etc).	De alguns centímetros a alguns poucos metros.
LOCAL AREA NETWORK	LAN	Rede de computadores de lares, escritórios, prédios, entre outros.	De algumas centenas de metros a alguns quilômetros.
METROPOLITAN AREA NETWORK	MAN	Rede de computadores entre uma matriz e filiais em uma cidade.	Cerca de algumas dezenas de quilômetros.
WIDE AREA NETWORK	WAN	Rede de computadores entre cidades, países ou até continentes.	De algumas dezenas a milhares de quilômetros.

COMPONENTES DA WEB	DESCRIÇÃO
HIPERTEXTO	A Web é baseada em documentos que contêm links (hiperlinks) para outros documentos relacionados. Isso permite que os usuários naveguem de uma página para outra, seguindo os links.
URL	Cada documento ou recurso na Web é identificado por um URL exclusivo, que é um endereço usado para acessar o recurso em um navegador.
NAVEGADORES DA WEB	São aplicativos que permitem aos usuários visualizar e interagir com documentos da Web. Exemplos populares de navegadores incluem o Google Chrome, Mozilla Firefox, Microsoft Edge e Safari.
PROTOCOLOS DE COMUNICAÇÃO	A Web utiliza protocolos de comunicação, como HTTP (Hypertext Transfer Protocol) e HTTPS (HTTP Secure), para transferir dados entre navegadores e servidores web.
SERVIDORES WEB	São computadores que hospedam documentos e recursos da Web. Eles respondem às solicitações dos navegadores e fornecem os conteúdos solicitados.
PÁGINAS DA WEB	São documentos criados usando linguagens de marcação, como HTML (Hypertext Markup Language). As páginas da web podem conter texto, imagens, links e outros elementos interativos.
MOTORES DE BUSCA	São ferramentas que ajudam os usuários a encontrar informações na Web, indexando e classificando páginas da web com base em palavras-chave.

CARACTERÍSTICAS	WEB 1.0	WEB 2.0	WEB 3.0
INTERATIVIDADE	Baixa	Alta	Muito Alta
CONTEÚDO	Estático e somente leitura	Dinâmico, com feedback do usuário	Inteligente, com semântica
USUÁRIOS	Consumidores passivos	Produtores de conteúdos	Participantes ativos
SOCIALIZAÇÃO	Ausente	Integração de redes sociais	Integração com IA e Internet das Coisas
EXPERIÊNCIA DO USUÁRIO	Limitada	Melhorada e personalizada	Altamente personalizada
TECNOLOGIA	HTML	AJAX, APIs e RSS	IA e Aprendizado de Máquina
EXEMPLOS	Sites estáticos de início da web	Redes sociais, blogs e wikis	Assistentes virtuais



PRINCIPAIS APLICAÇÕES	Sites informativos e institucionais	Redes sociais e colaboração online	Assistentes virtuais e Internet das Coisas
-----------------------	-------------------------------------	------------------------------------	--

SURFACE WEB	DESCRIÇÃO
ACESSIBILIDADE	Facilmente acessível por meio de mecanismos de busca e navegadores padrão.
CONTEÚDO PÚBLICO	Compreende sites, páginas e conteúdo que são acessíveis ao público em geral.
INDEXAÇÃO POR MECANISMOS DE BUSCA	Os motores de busca, como Google e Bing, indexam e exibem o conteúdo da Surface Web em resultados de pesquisa.
INFORMAÇÕES AMPLAMENTE VISÍVEIS	Notícias, blogs, lojas online, fóruns públicos e outros tipos de sites podem ser encontrados na Surface Web.
SEM RESTRIÇÕES SIGNIFICATIVAS	Os usuários podem navegar e acessar conteúdo sem a necessidade de credenciais ou permissões especiais.
EXEMPLOS	Páginas de notícias, blogs, lojas online e outros sites acessíveis ao público em geral.

DEEP WEB	DESCRIÇÃO
CONTEÚDO NÃO INDEXADO POR MOTORES DE BUSCA	O conteúdo da Deep Web não é indexado pelos mecanismos de busca tradicionais, o que o torna invisível nas pesquisas comuns.
REQUER AUTENTICAÇÃO	Muitos sites da Deep Web exigem credenciais ou autenticação para acessar, tornando o conteúdo acessível apenas a usuários autorizados.
INFORMAÇÕES CONFIDENCIAIS	Inclui informações privadas, como dados de empresas, registros médicos, sistemas de gerenciamento de bibliotecas e muito mais.
NÃO ACESSÍVEL POR LINKS COMUNS	Você não pode simplesmente clicar em um link para acessar o conteúdo da Deep Web; geralmente, precisa de informações de login ou URLs específicas.
VARIEDADE DE CONTEÚDO	A Deep Web abrange uma ampla gama de informações, desde bancos de dados privados a sistemas de gerenciamento de conteúdo corporativo.

DARK WEB	DESCRIÇÃO
ACESSÍVEL COM SOFTWARE ESPECÍFICO	A Dark Web é acessada por meio de redes criptografadas, como o Tor (The Onion Router), que requerem software especial para acesso.
CONTEÚDO ILEGAL E OSCURO	Inclui sites que hospedam atividades ilegais, como tráfico de drogas, armas, venda de informações roubadas e outros conteúdos obscuros.
ANONIMATO É VALORIZADO	Os usuários da Dark Web muitas vezes valorizam o anonimato, pois os serviços são frequentemente anônimos e transações são criptografadas.
RISCOS À SEGURANÇA	A Dark Web é um ambiente de alto risco, onde os usuários podem ser vítimas de fraudes e ataques cibernéticos.
NÍVEIS PROFUNDOS DE ANONIMATO	Diferentemente da Deep Web, a Dark Web oferece um nível mais profundo de anonimato e criptografia, tornando difícil rastrear usuários.

CARACTERÍSTICAS	SURFACE WEB	DEEP WEB	DARK WEB
ACESSIBILIDADE	Acessível por mecanismos de busca e navegadores comuns.	Requer credenciais específicas ou URLs exclusivas.	Acessível apenas por redes criptografadas, como o Tor.



CONTEÚDO COMUM	Contém informações e sites disponíveis publicamente.	Inclui conteúdo não indexado por mecanismos de busca, como bancos de dados privados.	Contém conteúdo obscuro e frequentemente ilegal.
ANONIMATO	Não oferece anonimato especial para usuários.	Pode exigir credenciais de login, mas não enfatiza o anonimato.	Valoriza altos níveis de anonimato e segurança.
CONTEÚDO COMERCIAL	Amplamente usado para negócios, educação, entretenimento e informações públicas.	Inclui recursos protegidos por senha, como e-mails, serviços bancários online e redes corporativas.	Muitas vezes associada a atividades ilegais e conteúdo obscuro.
EXEMPLOS	Sites de notícias, blogs, redes sociais, sites de compras online.	E-mails privados, intranets corporativas, bancos de dados de bibliotecas.	Sites de venda de drogas, mercados negros, fóruns de hackers.

INTERNET DAS COISAS

Trata-se de uma revolução tecnológica que se refere à conexão de dispositivos físicos e objetos do mundo real à internet. Esses dispositivos, também chamados de "coisas" na IoT, são integrados com sensores, software e outras tecnologias para coletar e trocar dados com outros dispositivos e sistemas pela internet.

COMPONENTES	DESCRIÇÃO
DISPOSITIVOS	São os elementos físicos que compõem a IoT, como sensores, atuadores e outros dispositivos conectados, como câmeras, medidores inteligentes, veículos e eletrodomésticos. Eles coletam dados do mundo real e podem executar ações com base nesses dados.
TECNOLOGIAS DE COMUNICAÇÃO	São os meios pelos quais os dispositivos IoT se comunicam entre si e com a nuvem. Isso pode incluir Wi-Fi, Bluetooth, 3G/4G/5G, Zigbee, LoRa, entre outros. As redes de comunicação são responsáveis pela transferência de dados dos dispositivos para a nuvem e vice-versa.
SENSORES E ATUADORES	Os sensores coletam informações do ambiente, como temperatura, umidade, localização, movimento e muito mais. Os atuadores são responsáveis por tomar ações, como ligar ou desligar um dispositivo. Eles são os olhos e as mãos da IoT.
NUVEM (CLOUD)	A nuvem é onde os dados coletados pelos dispositivos IoT são processados, armazenados e disponibilizados para acesso. Plataformas de nuvem fornecem recursos de computação, armazenamento e análise de dados em grande escala, tornando possível o processamento de grandes volumes de informações.

TECNOLOGIAS DE COMUNICAÇÃO	DESCRIÇÃO
WI-FI (802.11)	Trata-se de uma das tecnologias de comunicação sem fio mais amplamente utilizadas e oferece alta largura de banda. É adequado para dispositivos que têm acesso a redes locais de alta velocidade e energia suficiente.
BLUETOOTH (802.15)	Trata-se de uma tecnologia de comunicação sem fio de curto alcance, adequada para dispositivos pessoais, como fones de ouvido sem fio e dispositivos vestíveis. O Bluetooth Low Energy (BLE) é uma variante de baixo consumo de energia.
ZIGBEE	Trata-se de um padrão de comunicação sem fio de baixa potência projetado para redes de sensores e dispositivos IoT em ambientes domésticos e industriais.

VANTAGENS

DESVANTAGENS



Varejistas podem fornecer bônus de fidelidade para clientes preferenciais.	A dependência de compras online pode custar empregos.
As cidades podem avaliar as necessidades futuras de transporte.	Os varejistas podem saber tudo o que você está comprando.
Indivíduos podem reduzir os custos de energia e dos sistemas de aquecimento residenciais.	Os indivíduos podem receber mais e-mails de spam.
Fabricantes podem reduzir a inatividade prevendo as necessidades de manutenção dos equipamentos.	Uma falha da rede pode ser catastrófica.
Os governos podem monitorar o ambiente.	As empresas que criam dispositivos vestíveis têm muitas informações pessoais sobre os usuários.

TECNOLOGIAS DE ACESSO À INTERNET

Referem-se aos métodos e infraestruturas utilizados para conectar dispositivos, como computadores, smartphones e outros equipamentos, à Internet. Essas tecnologias permitem que os dispositivos acessem os serviços e recursos disponíveis na World Wide Web e em outros serviços online. Existem várias tecnologias de acesso à Internet (Ex: Dial-Up, ADSL, HFC, Fibra Óptica, PLC, Rádio, Satélite e Telefonia Móvel), e a escolha depende das necessidades e da disponibilidade em uma determinada região.

NÍVEIS	DESCRIÇÃO
ISP NÍVEL 1	São os provedores de acesso à internet de nível mais alto na hierarquia. Eles não precisam comprar acesso à internet de outros provedores, pois possuem uma rede global de alta capacidade e trocam tráfego diretamente uns com os outros. Exemplos de provedores de Nível 1 incluem AT&T, Verizon, NTT Communications e CenturyLink. Eles têm uma presença global e fornecem acesso à internet em escala internacional. Imagine ISPs de Nível 1 como rodovias federais, como a Rodovia Presidente Dutra (BR-116). Essas rodovias cruzam continentes e países sem precisar pagar pedágio a outras estradas menores. Os provedores de Nível 1 constroem e mantêm essas "rodovias da internet" e interconectam-se diretamente para permitir um tráfego rápido e eficiente.
ISP NÍVEL 2	Estes são provedores de acesso à internet que não possuem redes globais como os Nível 1, mas ainda têm uma rede significativa em uma área geográfica específica. Eles geralmente compram acesso à internet de Nível 1 ISPs e podem vender serviços a ISPs de nível inferior ou a empresas e consumidores diretos. Exemplos de provedores de Nível 2 incluem Cogent, Orange, Charter, Deutsche Telekom, entre outros. ISPs de Nível 2 podem ser comparados a rodovias estaduais. Eles atendem a áreas geográficas maiores, como estados ou regiões inteiras. Essas rodovias estaduais se conectam às autoestradas globais (Nível 1) e podem cobrar pedágio por permitir que o tráfego flua entre essas grandes autoestradas e áreas locais.
ISP NÍVEL 3	São provedores regionais ou locais que não possuem redes globais. Eles compram acesso à internet de provedores de Nível 1 ou 2 para fornecer conectividade a empresas e consumidores em áreas geográficas específicas. Esses ISPs podem se concentrar em uma única cidade, região ou país. Alguns provedores de Nível 3 podem ser ISPs de acesso final, que fornecem serviços diretamente a residências e empresas locais. ISPs de Nível 3 são como as estradas locais e ruas em cidades. Eles atendem áreas geográficas muito específicas, como uma cidade ou bairro. Essas estradas locais se conectam às rodovias regionais (Nível 2) ou diretamente às autoestradas globais (Nível 1) e permitem que o tráfego alcance destinos locais.

TECNOLOGIAS DE ACESSO	DESCRIÇÃO
-----------------------	-----------



DIAL-UP	Dial-Up é uma conexão à internet via linha telefônica convencional, onde a transmissão de dados é feita utilizando o tom de discagem. A velocidade é baixa, geralmente até 56 Kbps, e a linha telefônica fica ocupada durante o uso, sendo uma tecnologia obsoleta em comparação com as alternativas atuais.
ADSL	ADSL (Asymmetric Digital Subscriber Line) usa a linha telefônica comum para transmitir dados em alta velocidade, sem interromper as chamadas telefônicas. A velocidade de download é maior que a de upload, ideal para uso doméstico, com velocidades típicas de até 24 Mbps dependendo da qualidade da linha e da distância da central.
HFC	HFC (Hybrid Fiber-Coaxial) combina fibra óptica e cabos coaxiais para transmitir dados. A fibra é usada até uma certa distância, sendo complementada por cabos coaxiais até o usuário final. Comum em serviços de TV a cabo, permite velocidades de internet rápidas, dependendo da infraestrutura local.
FIBRA ÓPTICA	FTTH (Fiber to the Home) é uma tecnologia que utiliza fibra óptica diretamente até a residência do usuário, proporcionando conexões de alta velocidade, estáveis e com baixa latência. É uma das tecnologias mais avançadas para acesso à internet, suportando velocidades simétricas de upload e download.
PLC	PLC (Power Line Communication) usa a rede elétrica para transmitir dados de internet. É uma solução que permite a distribuição de sinal de internet por meio da infraestrutura de energia, sendo útil em áreas com baixa cobertura de outras tecnologias. A velocidade pode variar conforme a rede elétrica local.
RÁDIO	A tecnologia de rádio transmite sinal de internet sem fio por meio de torres de rádio, sendo uma opção para áreas rurais ou de difícil acesso. A velocidade e a estabilidade da conexão dependem da proximidade com a torre e das condições climáticas, sendo uma alternativa viável onde não há cabeamento.
SATÉLITE	Satélite permite o acesso à internet em áreas remotas, transmitindo dados via satélites em órbita. Apesar de ser uma solução para locais onde outras tecnologias não chegam, tem maior latência e menor velocidade em comparação a soluções terrestres, sendo influenciada por condições climáticas.
TELEFONIA MÓVEL	A Telefonia Móvel usa redes celulares 3G, 4G ou 5G para fornecer acesso à internet. A cobertura depende da infraestrutura de torres de telefonia, e a velocidade varia conforme a geração da rede. É amplamente utilizada devido à sua mobilidade, permitindo conexões em qualquer lugar com sinal disponível.

PROTOSCOLOS DE COMUNICAÇÃO

Protocolos são conjuntos de regras e convenções que especificam como os dispositivos em uma rede devem se comunicar. Eles definem os formatos dos dados, a sequência de mensagens, a detecção e correção de erros, o controle de acesso e muitos outros aspectos necessários para a comunicação eficaz entre computadores em uma rede. Esses protocolos desempenham um papel fundamental na garantia de que diferentes dispositivos de rede, com hardware e software diversos, possam se comunicar e trocar informações de maneira consistente.

MODELO OSI/ISO

O Modelo OSI (*Open Systems Interconnection / International Organization for Standardization*) é um modelo de referência utilizado para entender como os protocolos de rede funcionam e interagem. Ele divide as funções de comunicação em uma rede de computadores em sete camadas, cada uma com um propósito específico. Essas camadas são organizadas hierarquicamente e servem como um guia para o desenvolvimento e a compreensão de protocolos de comunicação em redes.

NÚMERO	CAMADA	DESCRIÇÃO	PROTOSCOLOS
7	APLICAÇÃO	Camada responsável por habilitar o usuário, seja ele humano ou software, a estabelecer a comunicação entre aplicações e a acessar a rede.	HTTP, SMTP, FTP, SSH, TELNET, SNMP, POP3, IMAP, DNS.



6	APRESENTAÇÃO	Camada responsável por definir o formato para troca de dados entre computadores, como se fosse um tradutor.	AFP, ICA, LPP, NCP, NDR, TOX, XDR, PAD.
5	SESSÃO	Camada responsável por permitir que duas ou mais aplicações em computadores diferentes possam abrir, usar e fechar uma conexão, chamada sessão.	NETBIOS.
4	TRANSPORTE	Camada responsável por organizar dados em segmentos e que eles cheguem ao destino livre de erros (sem perdas, sem duplicações e na ordem correta).	TCP, UDP, NETBEUI.
3	REDE	Camada responsável pelo endereçamento, roteamento e entrega de pacotes individuais de dados desde sua origem até o seu destino, provavelmente através de várias redes.	IP, ICMP, ARP RARP, NAT.
2	ENLACE	Camada responsável por organizar os dados em frames (ou quadros) e por estabelecer uma conexão nó-a-nó entre dois dispositivos físicos que compartilham o mesmo meio físico.	Ethernet, Token Ring, Bluetooth, Wi-Fi.
1	FÍSICA	Camada responsável por definir as especificações elétricas e físicas da conexão de dados.	USB, DSL.

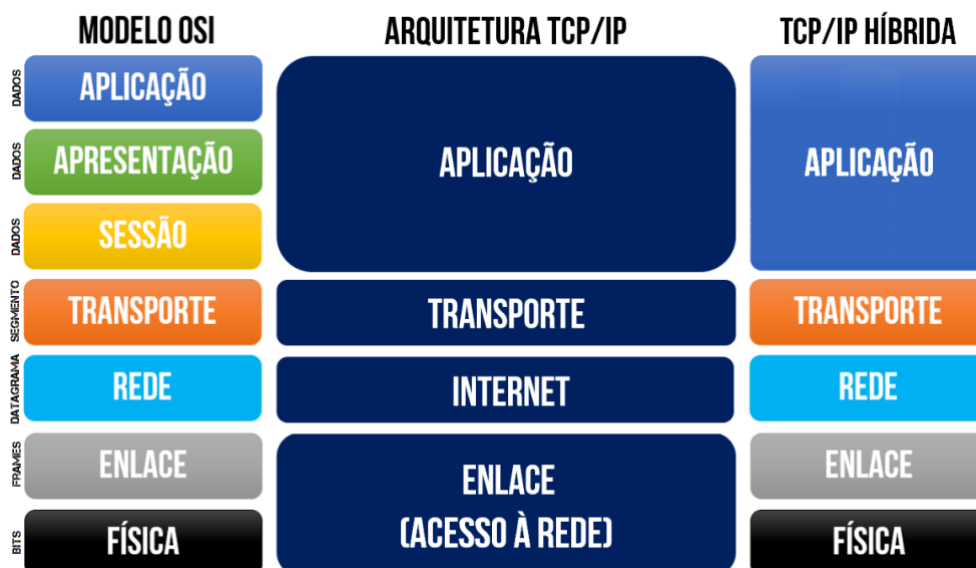
MNEMÔNICO DAS CAMADAS

F	E	R	T	S	A	A
FÍSICA	ENLACE	REDE	TRANSPORTE	SESSÃO	APRESENTAÇÃO	APLICAÇÃO
FLAMENGO	ENSACOU NA	REDE	TRÊS	SAPECADAS NO	ATLÉTICO E	AVAI

ARQUITETURA TCP/IP

A arquitetura TCP/IP (*Transmission Control Protocol / Internet Protocol*) é um conjunto de protocolos de comunicação que são amplamente utilizados na internet e em redes locais. Ela fornece um conjunto de regras e especificações que permitem que diferentes dispositivos se comuniquem em redes de computadores, independentemente do fabricante ou sistema operacional.





INTERNET PROTOCOL (IP)

O IP é a base da comunicação na Internet, sendo responsável por rotear pacotes de dados de origem para destino em uma rede. Cada dispositivo conectado à Internet recebe um endereço IP exclusivo, que é usado para identificar e encaminhar dados para o destinatário correto. Quando um dispositivo deseja enviar dados para outro, ele divide os dados em pacotes. Cada pacote contém informações sobre o remetente, destinatário, dados reais e outros metadados – esses pacotes são então enviados pela rede. O roteamento é o processo pelo qual os pacotes são direcionados do remetente para o destinatário através de vários dispositivos intermediários, como roteadores.

TRANSMISSION CONTROL PROTOCOL (TCP)

Protocolo da camada de transporte, considerado confiável e orientado à conexão. Ele utiliza portas para estabelecer conexões, utiliza controle de fluxo para evitar congestionamento na rede, permite a transferência de dados bidirecional e confirma o recebimento de pacotes, retransmitindo os que não são confirmados. Além disso, ele garante que os pacotes cheguem na ordem correta e utiliza a soma de verificação para detectar erros nos dados recebidos. O TCP é amplamente utilizado em aplicações que requerem entrega garantida de dados, como navegadores web e e-mail.

USER DATAGRAM PROTOCOL (UDP)

Protocolo da camada de transporte, considerado sem conexão e utiliza portas para comunicação de forma similar ao TCP. Ele não possui controle de fluxo e permite a transferência de dados rápida, mas sem garantias de entrega, ordem ou integridade. Esse protocolo é considerado não confiável porque não é capaz de confirmar o recebimento de pacotes e não retransmite os pacotes perdidos. Ele também não reordena pacotes e realiza apenas verificações básicas de erros nos dados recebidos (mas não os corrige). Por fim, ele não requer estabelecimento de conexão antes da transferência de dados, sendo ideal para aplicações que requerem transmissão rápida, como streaming de vídeo e jogos online.

TCP	UDP
É comparativamente mais lento que o UDP	É comparativamente mais rápido que o TCP
Entregas confiáveis	Entregas não confiáveis (melhor esforço)
Orientado à conexão	Não orientado à conexão
Dados perdidos são retransmitidos	Dados perdidos não são retransmitidos.
Tolera atrasos, mas não tolera perdas	Tolera perdas, mas não tolera atrasos
Bastante utilizada em e-mail, navegação, etc.	Bastante utilizada em VoIP, streaming, etc.



CLIENTE DE E-MAIL	Trata-se de uma aplicação instalada em uma máquina local que permite enviar/receber e-mails (Ex: Mozilla Thunderbird, Microsoft Outlook, etc);
SERVIDOR DE E-MAIL	Trata-se de uma máquina especializada que recebe e-mails de um cliente de e-mail ou de um webmail, e os envia para o servidor de e-mail de destino;
PROVEDOR DE E-MAIL	Trata-se de uma empresa ou serviço que hospeda e disponibiliza serviços de e-mail para outras empresas ou usuários finais (Ex: Gmail, Outlook, Yahoo, Uol, etc);
WEBMAIL	Trata-se de uma aplicação hospedada em um servidor remoto que permite enviar/receber e-mails (Ex: Outlook.com, Gmail.com, Yahoo.com, Uol.com, etc).

PROTOCOLOS DE E-MAIL	DESCRIÇÃO
SMTP	Protocolo utilizado basicamente para enviar e-mails. Ele transfere mensagens de e-mail de um cliente para um servidor ou entre servidores. Funciona bem para a entrega de mensagens, mas não para recuperá-las.
POP	Protocolo projetado para recuperar e-mails de um servidor. Quando você o utiliza, os e-mails são baixados para o seu dispositivo e geralmente são excluídos do servidor. Isso é útil para acessar e-mails offline, mas pode ser limitante se você usar vários dispositivos, pois as mensagens estão disponíveis apenas no dispositivo onde foram baixadas inicialmente.
IMAP	Também usado para recuperar e-mails de um servidor, mas - diferentemente do anterior - ele mantém as mensagens no servidor. Isso permite que você acesse seus e-mails de vários dispositivos, mantendo tudo sincronizado. As mudanças feitas em um dispositivo (como ler ou excluir uma mensagem) são refletidas em todos os outros dispositivos.

SMTP	POP3	IMAP
ENVIAR	RECEBER E COPIAR	RECEBER E ACESSAR

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

Protocolo da camada de aplicação responsável pelo envio de e-mails de um cliente para um servidor ou entre servidores de e-mail. Ele é bastante utilizado por clientes de e-mail e servidores de e-mail para a transmissão de mensagens de correio eletrônico, funcionando por meio de uma arquitetura cliente/servidor. Além disso, é interoperável com outros protocolos de e-mail (Ex: POP3 e IMAP) para uma funcionalidade de e-mail completa.

S	M	T	P
SUA	MENSAGEM	TÁ	PARTINDO

POST OFFICE PROTOCOL (POP)

Protocolo da camada de aplicação responsável por recuperar e-mails de um servidor de e-mail. Em regra, ele baixa os e-mails do servidor para o cliente local e os deleta do servidor, mas há outros modos de funcionamento. O POP3 suporta criptografia via SSL/TLS e autenticação através de usuário/senha, além de permitir a leitura de e-mails offline e controle limitado sobre as mensagens no servidor. Por outro lado, ele não sincroniza o estado da mensagem entre múltiplos dispositivos (lido/não lido, marcado/não marcado). Ele é menos flexível que IMAP, sendo ideal para usuários que acessam e-mail de um único dispositivo.



INTERNET MESSAGE ACCESS PROTOCOL (IMAP)

Protocolo da camada de aplicação responsável pelo acesso, gerenciamento e sincronização de e-mails armazenados em um servidor de e-mail. Ele permite ao usuário visualizar e manipular mensagens diretamente no servidor, além de sincronizar o estado das mensagens (lido/não lido, marcado/não marcado) entre múltiplos dispositivos. Ele suporta criptografia via SSL/TLS e autenticação através de usuário e senha. Esse protocolo é mais flexível que o POP3, sendo ideal para usuários que acessam e-mail de múltiplos dispositivos. As mensagens geralmente permanecem no servidor, permitindo acesso a partir de qualquer dispositivo.

POP3	IMAP
Post Office Protocol (Version 3)	Internet Message Access Protocol
Não recomendado para acesso em múltiplos dispositivos	Recomendado para acesso em múltiplos dispositivos
Não permite criar e organizar pastas no servidor	Permite criar e organizar pastas no servidor
Não permite verificar o cabeçalho antes de baixá-lo	Permite verificar o cabeçalho antes de baixá-lo
Modificações em um dispositivo não refletidas em outros	Modificações em um dispositivo refletidas em outros
Não permite baixar parcialmente um e-mail	Permite baixar parcialmente um e-mail
Por padrão, mensagens de e-mail são lidas offline	Por padrão, mensagens de e-mail são lidas online
Não permite múltiplas caixas postais	Permite múltiplas caixas postais
Porta 110	Porta 143

WEBMAIL

Um webmail é um serviço de e-mail que pode ser acessado e usado através de um navegador da web, em vez de um cliente de e-mail dedicado. Ele funciona como uma interface baseada na web para enviar, receber e gerenciar mensagens de e-mail (Ex: Gmail, Yahoo, Outlook, Hotmail, etc).

CARACTERÍSTICAS DE WEBMAIL	DESCRIÇÃO
ACESSIBILIDADE	Webmails podem ser acessados de qualquer dispositivo com uma conexão à internet e um navegador web, oferecendo grande conveniência e mobilidade.
NÃO QUERER INSTALAÇÃO DE SOFTWARE	Ao contrário dos clientes de e-mail que requerem instalação, como Microsoft Outlook ou Mozilla Thunderbird, o webmail opera inteiramente no navegador.
ARMAZENAMENTO NA NUVEM	As mensagens de e-mail são armazenadas no servidor do provedor de e-mail, não no dispositivo local. Isso facilita o acesso a e-mails de diferentes dispositivos.
INTERFACE DO USUÁRIO	Webmails geralmente têm interfaces de usuário ricas, semelhantes a aplicações desktop, com recursos como arrastar e soltar, pastas, e ferramentas de busca avançada.
SEGURANÇA E MANUTENÇÃO	A segurança e a atualização de software são gerenciadas pelo provedor do serviço, reduzindo a necessidade de manutenção por parte do usuário.
INTEGRAÇÃO COM OUTROS SERVIÇOS	Muitos webmails são integrados com outros serviços online, como calendários, gerenciamento de contatos, armazenamento em nuvem e aplicações de escritório.

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)



Protocolo da camada de aplicação responsável por atribuir automaticamente endereços IP e outras configurações de rede a dispositivos em uma rede. Ele funciona com um modelo cliente-servidor em que o Servidor DHCP atribui IPs dinamicamente aos clientes da rede e suporta alocação dinâmica, alocação automática e alocação estática de endereços IP. O DHCP simplifica o gerenciamento de endereços IP (especialmente em redes grandes), sendo amplamente utilizado em redes domésticas, corporativas e públicas para simplificar a configuração de rede.

DOMAIN NAME SYSTEM (DNS)

Protocolo da camada de aplicação responsável por traduzir (também chamado de resolver) nomes de domínio legíveis por humanos para Endereços IP. Ele funciona em um modelo de consulta e resposta, sendo estruturado de maneira hierárquica com vários níveis de Servidores DNS. Esse protocolo armazena as respostas recentes para reduzir o tempo de resposta e o tráfego na rede, incluindo extensões de segurança para proteger contra ataques. O DNS é essencial para a navegação na internet, permitindo o uso de URLs em vez de endereços IP numéricos.

D	N	S
DÁ	NOME AO	SITE

URL - SINTAXE ABSTRATA

PROTOCOLO://IP-OU-DOMÍNIO:PORTA/CAMINHO/RECURSO

COMPONENTES	DESCRIÇÃO
PROTOCOLO	Também chamado de esquema, trata-se do protocolo utilizado para acessar um recurso.
IP	Número de IP do Servidor (Host) que hospeda um recurso.
DOMÍNIO	Nome do Domínio do Servidor (Host) que hospeda um recurso.
PORTA	Ponto lógico que permite criar uma conexão em um processo.
CAMINHO	Estrutura de diretórios dentro do servidor que armazena um recurso.
RECURSO	Componente físico ou lógico disponível em um sistema computacional.

URL - SINTAXE COMPLETA

PROTOCOLO://NOME-DE-USUÁRIO@IP-OU-DOMÍNIO:PORTA/CAMINHO/RECURSO?QUERY#FRAGMENTO

COMPONENTES EXTRAS	DESCRIÇÃO
QUERY / QUERYSTRING	Utilizado para passar parâmetros adicionais para o servidor em formato chave-valor.
FRAGMENTO	Utilizado para navegar diretamente para uma seção específica de uma página da web.
NOME DE USUÁRIO	Utilizado em contextos em que é necessária a autenticação para acessar os recursos.

HYPERTEXT TRANSFER PROTOCOL (HTTP)



Protocolo da camada de aplicação utilizado para carregar páginas da web, enviar formulários, realizar transações online, obter recursos, entre outros. Trata-se de um protocolo baseado em um modelo de requisição-resposta entre um cliente (Navegador Web) e um servidor (Servidor Web): mensagens enviadas pelo cliente são chamadas de solicitações ou requisições (Requests) e as mensagens enviadas pelo servidor são chamadas de respostas (Responses).

HYPERTEXT TRANSFER PROTOCOL SECURE (HTTPS)

Protocolo da camada de aplicação utilizado para carregar páginas da web, enviar formulários, realizar transações online, obter recursos, entre outros, porém com uma camada adicional de segurança entre o cliente e o servidor. Possui recursos para criptografar a comunicação, protegendo a troca de dados contra interceptação e alteração. Esse protocolo requer certificados digitais para autenticar a identidade do servidor e garante que os dados transferidos sejam acessíveis apenas para o destinatário pretendido. Além disso, ele verifica se os dados enviados não foram alterados ou corrompidos durante a transferência e confirma a identidade do site para o usuário.

FILE TRANSFER PROTOCOL (FTP)

Protocolo da camada de aplicação baseado no modelo cliente/servidor utilizado para a transferência de arquivos entre sistemas. Ele pode transferir uma variedade de tipos de dados (incluindo arquivos binários e de texto), além de permitir upload e download de arquivos, além de suporte a comandos para manipulação de diretórios. Ademais, requer autenticação (nome de usuário e senha) para acesso, embora possa ter acesso anônimo. O FTP é amplamente utilizado para distribuição de arquivos, backup e transferência de dados entre sistemas.

VOIP

VoIP (Voice over Internet Protocol) é uma tecnologia que permite a transmissão de voz e comunicações multimídia (como chamadas telefônicas, videotelefonia e sessões de conferência) através da Internet ou de outras redes baseadas em protocolos IP. Essencialmente, o VoIP transforma sinais de voz em dados digitais que podem ser enviados pela internet, como qualquer outro tipo de dado.



QUESTÕES COMENTADAS – CESGRANRIO

1. (CESGRANRIO / CEFET-RJ - 2014) Os tipos de rede digital podem ser classificados em função dos seus alcances geográficos. A rede com alcance de até 500 metros, utilizada em escritórios ou andares de um edifício, é denominada rede local e é conhecida pela sigla:

- a) LAN
- b) RAN
- c) CAN
- d) MAN
- e) WAN

Comentários:

(a) Correto. LAN (Local Area Network) é o tipo de rede com alcance limitado, geralmente até 500 metros, usada em ambientes como escritórios, residências e andares de edifícios;

(b) Errado. RAN (Radio Access Network) é um conceito utilizado em redes móveis, não em redes locais cabeadas;

(c) Errado. CAN (Campus Area Network) conecta várias LANs dentro de uma área como um campus universitário ou parque industrial, com alcance maior que o citado;

(d) Errado. MAN (Metropolitan Area Network) cobre áreas urbanas inteiras, muito além do limite de 500 metros;

(e) Errado. WAN (Wide Area Network) conecta redes em áreas geográficas amplas, como cidades ou países.

Gabarito: Letra A

2. (CESGRANRIO / CMB - 2012) Os softwares navegadores são ferramentas de internet utilizadas para a interação dos usuários com a rede mundial. Para que essa interação seja possível, é necessário fazer uma conexão à internet por um dos diversos meios de acesso disponíveis aos usuários. O meio de acesso no qual o usuário utiliza um modem e uma linha de telefonia fixa para conectar-se com a internet é o:

- a) dial up
- b) ponte
- c) satélite
- d) wi-fi
- e) cabo coaxial

Comentários:

(a) Correto. O acesso via dial-up utiliza um modem conectado a uma linha de telefonia fixa, permitindo a conexão discada com a internet, com velocidades baixas (até 56 Kbps);

(b) Errado. Ponte (bridge) é um dispositivo de rede, não um meio de acesso à internet;



- (c) Errado. Satélite é outro meio de acesso, geralmente usado em áreas remotas, sem necessidade de linha telefônica fixa;
- (d) Errado. Wi-Fi é uma tecnologia de rede sem fio local, não um meio de acesso externo à internet;
- (e) Errado. Cabo coaxial é utilizado em serviços de internet a cabo, diferente da conexão via linha telefônica discada.

Gabarito: Letra A

3. (CESGRANRIO / EPE - 2009) Para encontrar o servidor de arquivos na rede, João perguntou ao seu suporte de rede qual era o endereço IP do servidor. Qual das opções abaixo representa um possível endereço IP para o servidor de arquivos?

- a) GG568934FH2
- b) 10.0.1.7
- c) axe@pax.com.br
- d) www.pax.com.br
- e) 02-34-98-89-78-00

Comentários:

- (a) Errado. GG568934FH2 não segue o formato de endereço IP, parece ser uma cadeia aleatória de caracteres;
- (b) Correto. 10.0.1.7 é um endereço IP válido no formato IPv4 (quatro números de 0 a 255 separados por pontos) e faz parte da faixa de endereços privados usados em redes locais;
- (c) Errado. *axe@pax.com.br* é um endereço de e-mail, não um endereço IP;
- (d) Errado. *www.pax.com.br* é um nome de domínio, que pode ser resolvido para um IP via DNS, mas não é um endereço IP propriamente dito;
- (e) Errado. 02-34-98-89-78-00 tem o formato de um endereço MAC (identificador de hardware), não de um IP.

Gabarito: Letra B

4. (CESGRANRIO / TJ-RO - 2008) Para que um computador possa se conectar a uma LAN (Local Area Network) é necessário que ele possua um(a):

- a) codificador.
- b) webcam.
- c) impressora.
- d) placa de rede.
- e) placa de som.

Comentários:

- (a) Errado. Codificador não é um componente necessário para conexão a redes locais;
- (b) Errado. Webcam é um dispositivo de captura de imagem, sem função na comunicação de rede;



- (c) Errado. Impressora é um periférico de saída, não necessária para conexão à rede;
- (d) Correto. A placa de rede é o componente essencial que permite a comunicação de um computador com outros dispositivos em uma LAN;
- (e) Errado. Placa de som é usada para reprodução de áudio, não tem relação com redes.

Gabarito: Letra D

5. (CESGRANRIO / PETROBRAS - 2011) No núcleo da Internet, o tráfego de informações entre os computadores, além de intenso, ocorre em grande velocidade, exigindo equipamentos de forte tecnologia. Esses equipamentos, em conjunto com outras tecnologias, constituem os:

- a) protocols
- b) backbones
- c) web softwares
- d) security softwares
- e) control cables

Comentários:

- (a) Errado. Protocols (protocolos) são regras que definem a comunicação entre dispositivos na rede, mas não se referem aos equipamentos que compõem a infraestrutura central da Internet;
- (b) Correto. Backbones são a espinha dorsal da Internet – redes de alta capacidade e velocidade, compostas por roteadores e links de comunicação que interligam grandes centros de dados e operadoras;
- (c) Errado. Web softwares são aplicações voltadas à navegação e uso da web, não à infraestrutura de tráfego da Internet;
- (d) Errado. Security softwares referem-se a programas de proteção, como antivírus e firewalls, sem relação com o núcleo físico da Internet;
- (e) Errado. Control cables não é um termo técnico apropriado no contexto de redes ou infraestrutura da Internet.

Gabarito: Letra B

6. (CESGRANRIO / BB - 2023) A configuração de rede de um computador pode ser realizada de forma estática ou dinâmica. Quando a forma estática é utilizada, o usuário deve configurar os parâmetros de rede manualmente, fornecendo, por exemplo, os endereços IP da estação de trabalho e do roteador padrão da rede local.

Por outro lado, quando se utiliza a forma dinâmica, o usuário deve configurar o computador para usar o protocolo de comunicação conhecido como:

- a) DNS
- b) VPN
- c) DHCP
- d) Wi-Fi



e) FTTH

Comentários:

- (a) Errado. O DNS é responsável pela tradução de nomes de domínio para endereços IP, mas não pela configuração dinâmica de rede;
- (b) Errado. VPN é uma tecnologia de rede para criar conexões seguras, sem função na atribuição dinâmica de IPs;
- (c) Correto. O DHCP (Dynamic Host Configuration Protocol) é o protocolo utilizado para configuração dinâmica de parâmetros de rede, como IP, máscara de sub-rede e gateway padrão;
- (d) Errado. Wi-Fi é um meio de acesso à rede sem fio, não um protocolo de configuração dinâmica de IPs;
- (e) Errado. FTTH refere-se a uma tecnologia de acesso à internet via fibra óptica, sem relação com configuração de IP.

Gabarito: Letra C

7. (CESGRANRIO / BB - 2023) A ferramenta de Webmail viabiliza o uso do serviço de correio eletrônico de empresas utilizando um navegador Web. Após a composição de uma nova mensagem de correio eletrônico, o usuário deve fazer a submissão do formulário para o servidor Web que, por sua vez, fará a submissão do conteúdo da mensagem para a fila do servidor de correio eletrônico. Os protocolos de comunicação utilizados nestas duas etapas são, respectivamente,

- a) HTTP e SMTP
- b) SMTP e HTTP
- c) POP3 e SMTP
- d) SMTP e POP3
- e) HTTP e POP3

Comentários:

- (a) Correto. A primeira etapa, onde o usuário envia o formulário pelo navegador, utiliza o protocolo HTTP (ou HTTPS). Na segunda etapa, o servidor web encaminha a mensagem para a fila de envio do servidor de e-mail usando o protocolo SMTP, responsável por transmitir e-mails entre servidores;
- (b) Errado. A ordem dos protocolos está invertida em relação ao processo descrito;
- (c) Errado. POP3 é um protocolo de recebimento de e-mails, não de envio;
- (d) Errado. SMTP é usado para envio, mas POP3 é usado para recebimento, não participando dessa sequência;
- (e) Errado. POP3 também não é usado nessa etapa de envio de mensagens.

Gabarito: Letra A

8. (CESGRANRIO / BB - 2021) O serviço de correio eletrônico é uma ferramenta essencial para o trabalho do dia a dia dos colaboradores de uma empresa. Para garantir a segurança da



comunicação do cliente de correio eletrônico com os servidores de correio eletrônico de entrada e de saída de mensagens, é importante configurar a utilização do padrão de segurança:

- a) TLS
- b) SMTP
- c) IMAP
- d) POP3
- e) HTTP

Comentários:

(a) Correto. TLS é um protocolo de segurança projetado para fornecer comunicação segura através de uma rede de computadores. Na comunicação de correio eletrônico, ele é usado para criptografar a conexão entre o cliente de e-mail e os servidores de correio, protegendo assim a troca de informações contra interceptação e outros ataques.

(b) Errado. SMTP é um protocolo para enviar e-mails, mas por si só não fornece segurança criptográfica;

(c) Errado. IMAP é um protocolo para acessar e-mails em um servidor, mas não é um padrão de segurança.

(d) Errado. POP3 é outro protocolo de e-mail, usado para baixar mensagens de e-mail de um servidor, mas não é um padrão de segurança.

(e) Errado. HTTP é um protocolo para transferência de documentos hipertexto, como páginas da web, mas não é um padrão de segurança específico para e-mails.

Gabarito: Letra A

9. (CESGRANRIO / CEF - 2021) O aplicativo de correio eletrônico pode ser configurado para enviar mensagens e acessar as caixas de mensagens que estão no servidor de correio. Um dos protocolos de comunicação mais utilizados para acessar as mensagens da caixa de entrada é o:

- a) SMTP.
- b) IMAP.
- c) SMB.
- d) SSH.
- e) RDP.

Comentários:

(a) Errado. O SMTP é utilizado para envio de mensagens, não para acessar a caixa de entrada;

(b) Correto. O IMAP é um dos protocolos mais utilizados para acessar e gerenciar mensagens diretamente no servidor de e-mail, mantendo-as sincronizadas entre diferentes dispositivos;

(c) Errado. O SMB é usado para compartilhamento de arquivos e impressoras em redes locais, não para acesso a e-mails;

(d) Errado. O SSH é um protocolo para acesso remoto seguro a terminais de servidores, não para correio eletrônico;

(e) Errado. O RDP é um protocolo de acesso remoto a desktops, sem relação com e-mails.



Gabarito: Letra B

10.(CESGRANRIO / BB - 2021) Apesar de os navegadores serem as ferramentas dominantes na internet, vários serviços possuem ferramentas próprias mais adequadas e, inclusive, mais otimizadas para protocolos específicos. Um desses protocolos foi desenvolvido para a transferência de arquivos, sendo usado a partir de programas como FileZilla. Esse protocolo é conhecido como:

- a) ftp.
- b) imap.
- c) pop3.
- d) ssh.
- e) elnet.

Comentários:

- (a) Correto. O protocolo FTP é específico para transferência de arquivos entre computadores na rede. Programas como o FileZilla são clientes FTP bastante utilizados para essa finalidade;
- (b) Errado. IMAP é um protocolo utilizado para acesso e gerenciamento de e-mails no servidor;
- (c) Errado. POP3 é também um protocolo de recebimento de e-mails, não de transferência de arquivos;
- (d) Errado. SSH é um protocolo usado para acesso remoto seguro a terminais, não para transferência de arquivos por FTP;
- (e) Errado. Provavelmente a intenção era mencionar o "Telnet", mas de qualquer forma, Telnet é para acesso remoto a terminais e não para transferência de arquivos.

Gabarito: Letra A

11.(CESGRANRIO / Banco do Brasil - 2021) Sabendo que o banco em que trabalha vai colocar centenas de ATMs em shoppings e postos de gasolina, um funcionário de TI propôs que cada ATM mandasse periodicamente um sinal de status, por meio do protocolo UDP. Esse protocolo do conjunto TCP/IP é considerado como parte da camada:

- a) de aplicações.
- b) de transporte.
- c) de rede.
- d) de enlace de dados.
- e) física.

Comentários:

- (a) Errado. A camada de aplicações é responsável pelas aplicações específicas e seus protocolos, mas o UDP não opera neste nível;
- (b) Correto. O UDP é parte da camada de transporte no modelo TCP/IP. Esta camada é responsável pela entrega de dados entre processos em diferentes hosts e inclui protocolos como o TCP e o UDP;



- (c) Errado. A camada de rede lida com o roteamento de pacotes, incluindo o protocolo IP, mas não o UDP;
- (d) Errado. A camada de enlace de dados é responsável pela transferência de dados entre entidades adjacentes na rede e controle de erros a nível físico, mas não inclui o UDP;
- (e) Errado. A camada física lida com a transmissão e recepção de dados brutos através de um meio físico e não trata de protocolos como o UDP.

Gabarito: Letra B

12.(CESGRANRIO / Banco do Brasil - 2021) Ao chegar para seu primeiro dia de emprego no banco, um novo gerente de TI percebeu que era demandado muito esforço no setor para controle do número IP de cada computador, o que causava, também, alguns erros por uso múltiplo do mesmo IP nas redes. Percebendo uma oportunidade de melhoria, o novo gerente decidiu que os computadores passariam a obter automaticamente um número IP, por meio do protocolo:

- a) HTTP.
- b) IMAP.
- c) DHCP.
- d) SMTP.
- e) DNS.

Comentários:

- (a) Correto. DHCP é usado para atribuir automaticamente endereços IP e outras informações de configuração de rede a dispositivos em uma rede. Isso evita a necessidade de configuração manual de endereços IP e os problemas associados a duplicação de IPs.
- (b) Errado. O Sistema de Nomes de Domínio (DNS) é utilizado para traduzir nomes de domínio em endereços IP, mas não para atribuir automaticamente endereços IP a dispositivos.
- (c) Errado. O Protocolo de Transferência de Hipertexto (HTTP) é usado para comunicação entre navegadores e servidores web, não para atribuição de endereços IP.
- (d) Errado. O Protocolo de Acesso a Mensagens da Internet (IMAP) é usado para acessar e-mails em um servidor de e-mail, não para a atribuição de endereços IP.
- (e) Errado. O Protocolo de Transferência de Correio Simples (SMTP) é usado para enviar e-mails, não para atribuir endereços IP.

Gabarito: Letra C

13.(CESGRANRIO / EPE - 2010) Determinado usuário comprou produtos em um site de vendas na Internet, por meio de um browser (Firefox, p.ex.).

Considerando-se que toda a navegação (seleção de produtos e compra) foi feita no endereço <http://www.siteexemplodevendas.com.br>, qual a falha de segurança desse procedimento de compra?

- a) Inexistência de FTP para transmissão de dados confidenciais.
- b) Seleção e compra de produtos no mesmo endereço WEB.



- c) Navegação por meio de um browser proprietário.
- d) Utilização de um navegador e não de um cliente de email.
- e) Utilização do HTTP, em detrimento ao HTTPS.

Comentários:

- (a) Errado. O FTP é um protocolo para transferência de arquivos, não usado para transações de comércio eletrônico;
- (b) Errado. Realizar seleção e compra no mesmo endereço web é uma prática comum e não representa, por si só, uma falha de segurança;
- (c) Errado. O uso de browsers proprietários, como o Firefox, não caracteriza uma falha de segurança por si só;
- (d) Errado. O cliente de e-mail não é o meio adequado para compras online, sendo o navegador a ferramenta correta;
- (e) Correto. A falha de segurança está no uso do protocolo HTTP, que não oferece criptografia na transmissão dos dados. O correto, em transações de compra online, é utilizar HTTPS, que garante a segurança das informações pessoais e financeiras.

Gabarito: Letra E

14.(CESGRANRIO / BASA - 2018) O protocolo que permite a navegação na internet segura através de criptografia de informações é o:

- a) HTTPS
- b) HTTP
- c) HTML
- d) XHTML
- e) XML

Comentários:

- (a) Correto. O HTTPS é uma extensão do HTTP utilizado para uma comunicação segura na Internet, pois adiciona uma camada de criptografia (SSL/TLS) para proteger os dados durante a transmissão;
- (b) Errado. O HTTP é o protocolo básico para transmissão de dados na Web, mas por si só não oferece criptografia;
- (c) Errado. HTML não é um protocolo, mas uma linguagem de marcação usada para criar e estruturar páginas na Web;
- (d) Errado. XHTML é uma linguagem de marcação semelhante ao HTML, mas mais rigorosa nas normas XML. Também não é um protocolo;
- (e) Errado. XML é uma linguagem de marcação utilizada para estruturar dados. Não é um protocolo e não está relacionado com a segurança de navegação na internet.

Gabarito: Letra A



15.(CESGRANRIO / LIQUIGÁS - 2018) A exploração da internet exige o uso de inúmeros protocolos, dentre os quais o protocolo FTP. Esse protocolo tem como objetivo:

- a) transferir arquivos entre cliente e servidor.
- b) confirmar a identidade de um servidor.
- c) prover serviço de datagrama não confiável.
- d) manipular caixas postais remotas como se fossem locais.
- e) gerenciar correio eletrônico.

Comentários:

- (a) Correto. O FTP é um protocolo da camada de aplicação usado para transferir arquivos entre um cliente e um servidor em uma rede TCP/IP;
- (b) Errado. A confirmação de identidade de um servidor é feita por protocolos como SSL/TLS (usado em HTTPS), não pelo FTP;
- (c) Errado. O serviço de datagrama não confiável é uma característica do protocolo UDP, não do FTP;
- (d) Errado. Manipular caixas postais remotas é função de protocolos como IMAP;
- (e) Errado. O gerenciamento de correio eletrônico é feito por protocolos como SMTP, IMAP e POP3.

Gabarito: Letra A

16.(CESGRANRIO / UNIRIO - 2016) Um usuário deseja acessar seus e-mails de vários dispositivos diferentes, sem baixar as mensagens para um dispositivo específico. Qual é o protocolo que permite que isso aconteça?

- a) HTTP
- b) SMTP
- c) POP
- d) IMAP
- e) FTP

Comentários:

- (a) Errado. O HTTP é utilizado para acesso a páginas web, não para gerenciamento direto de e-mails em servidores de correio;
- (b) Errado. O SMTP é usado exclusivamente para o envio de e-mails, não para o acesso à caixa de entrada;
- (c) Errado. O POP (geralmente POP3) baixa as mensagens para um dispositivo local e, por padrão, as remove do servidor, dificultando o acesso por múltiplos dispositivos;
- (d) Correto. O IMAP permite acessar e gerenciar os e-mails diretamente no servidor, mantendo as mensagens centralizadas e sincronizadas entre diferentes dispositivos;
- (e) Errado. O FTP é um protocolo para transferência de arquivos, sem relação com o acesso a e-mails.

Gabarito: Letra D



17.(CESGRANRIO / UNIRIO - 2016) Utilizando um computador da universidade, certo usuário deseja realizar uma transação bancária pela internet. Um procedimento para que esse usuário identifique, apenas visualmente, se o site acessado é um site seguro para este tipo de transação é verificar se:

- a) a URL começa com FTP.
- b) a URL começa com HTTP.
- c) a URL começa com HTTPS.
- d) a URL está com o nome correto da instituição.
- e) os campos digitáveis de agência e conta possuem o tamanho correto.

Comentários:

- (a) Errado. URLs que começam com FTP indicam um protocolo de transferência de arquivos, não de navegação segura para transações bancárias;
- (b) Errado. HTTP indica uma conexão sem criptografia, inadequada para operações financeiras;
- (c) Correto. A presença de "HTTPS" no início da URL indica que a conexão utiliza criptografia SSL/TLS, garantindo maior segurança na transmissão de dados sensíveis, como os de uma transação bancária;
- (d) Errado. O nome correto da instituição é importante, mas não garante a segurança da conexão sem o HTTPS;
- (e) Errado. O tamanho dos campos não assegura que o site seja seguro para transações.

▪ **Gabarito:** Letra C

18.(CESGRANRIO / PETROBRAS - 2015) O framework com designação universal abstrata para localizar um recurso na internet ou intranet é o:

- a) URL
- b) HTTP
- c) HTTPS
- d) TCP/IP
- e) Nome do arquivo

Comentários:

- (a) Correto. A URL é o padrão universal utilizado para identificar e localizar recursos na internet ou intranet, especificando o protocolo, o endereço do servidor e o caminho até o recurso;
- (b) Errado. HTTP é um protocolo de comunicação usado para acessar páginas web, mas não é um framework de localização de recursos;
- (c) Errado. HTTPS é a versão segura do HTTP, também um protocolo, e não um framework de localização;
- (d) Errado. TCP/IP é um conjunto de protocolos de comunicação de rede, não um padrão para localização de recursos;
- (e) Errado. O nome do arquivo é apenas parte de uma URL e não representa um framework completo de localização.



Gabarito: Letra A

19.(CESGRANRIO / BB - 2014) Um usuário entrou em um site da Internet e, ao digitar seu login e senha, recebeu a informação de que a partir daquele momento ele começaria a navegar em um site seguro. Ao lado da mensagem o seguinte ícone foi exibido:



Nessas condições, o protocolo exibido na barra de endereços do navegador desse usuário foi o:

- a) ftp
- b) http
- c) https
- d) ssl
- e) tcp/ip

Comentários:

- (a) Errado. O protocolo FTP é utilizado para transferência de arquivos, não para navegação segura;
- (b) Errado. HTTP indica navegação sem criptografia, ou seja, sem segurança garantida;
- (c) Correto. O ícone de cadeado indica que a conexão está usando HTTPS (Hypertext Transfer Protocol Secure), que implementa criptografia via SSL/TLS para garantir a segurança dos dados transmitidos;
- (d) Errado. SSL é a tecnologia de segurança utilizada por trás do HTTPS, mas não aparece diretamente na barra de endereços como protocolo;
- (e) Errado. TCP/IP é o conjunto de protocolos base de comunicação da Internet, mas não é um protocolo de aplicação exibido em URLs.

Gabarito: Letra C

20.(CESGRANRIO / LIQUIGÁS - 2014) Qual componente da Internet é responsável pela tradução de nomes de domínios para endereços IP e vice-versa?

- a) DNS
- b) TCP
- c) HTTP
- d) POP3
- e) HOST

Comentários:

- (a) Correto. O DNS é o componente da Internet responsável por traduzir nomes de domínio (Ex: www.exemplo.com) para endereços IP e vice-versa, permitindo que os usuários acessem serviços usando nomes amigáveis;



- (b) Errado. O TCP é um protocolo de transporte que garante a entrega confiável de dados, sem relação com tradução de nomes;
- (c) Errado. O HTTP é um protocolo da camada de aplicação usado para transferência de páginas web, não para resolução de nomes;
- (d) Errado. POP3 é um protocolo de recebimento de e-mails, sem função na tradução de domínios;
- (e) Errado. "HOST" é um termo genérico para designar um computador conectado à rede, não um sistema de resolução de nomes.

Gabarito: Letra A

21.(CESGRANRIO / BB - 2013) Uma transação financeira por meio de navegadores de internet deve usar, na mesma porta alocada ao protocolo HTTP, um protocolo mais seguro também conhecido como HTTP/TLS. A URL desse protocolo é diferenciada por começar com:

- a) t-http
- b) s-http
- c) https
- d) http-s
- e) httppt

Comentários:

Essa questão é fácil porque nenhuma das opções sequer existe, exceto a terceira – https é um protocolo de transferência de hipertexto combinado com o protocolo SSL/TLS para fornecer segurança de dados por meio de criptografia.

Gabarito: Letra C

22.(CESGRANRIO / CEF - 2012) Uma das funções de um cliente FTP instalado em uma estação de trabalho de uma intranet é:

- a) autenticar a senha do cliente junto ao controlador de domínio.
- b) criar um site web utilizando tecnologia Flash Player.
- c) transferir arquivos entre a estação de trabalho e um servidor.
- d) controlar os acessos da estação de trabalho à Internet.
- e) visualizar arquivos de imagem recebidos por e-mail.

Comentários:

- (a) Errado. A autenticação de senhas junto ao controlador de domínio é função de serviços como o Active Directory, não de um cliente FTP;
- (b) Errado. Criar sites em Flash Player é uma atividade de desenvolvimento web, não relacionada ao FTP;
- (c) Correto. A principal função de um cliente FTP é permitir a transferência de arquivos entre a estação de trabalho e um servidor, tanto para envio (upload) quanto para recebimento (download);
- (d) Errado. O controle de acesso à Internet é uma função típica de firewalls ou servidores proxy, não de clientes FTP;



(e) Errado. Visualizar arquivos de imagem recebidos por e-mail é tarefa de um cliente de e-mail, não de um cliente FTP.

Gabarito: Letra C

23.(CESGRANRIO / DECEA - 2012) Os computadores necessitam de um meio de comunicação para que possam acessar, através dos softwares navegadores, em modo on-line, o mundo de informações disponíveis na internet. Essa comunicação é feita por um conjunto de normas e procedimentos que constituem os protocolos de comunicação. Entre esses protocolos, incluem-se os seguintes:

- a) DNS e Cluster
- b) SAP e Telnet
- c) HTTP e HTML
- d) IMAP e SMTP
- e) HTTPS e Java

Comentários:

(a) Errado. DNS é um protocolo, mas "Cluster" não é um protocolo de comunicação de rede, e sim uma arquitetura de servidores;

(b) Errado. SAP é um software de gestão empresarial, não um protocolo de rede;

(c) Errado. HTTP é um protocolo, mas HTML é uma linguagem de marcação, não um protocolo de comunicação;

(d) Correto. IMAP e SMTP são ambos protocolos de comunicação de rede usados em serviços de e-mail: o IMAP para recebimento e gerenciamento de mensagens, e o SMTP para envio de e-mails;

(e) Errado. HTTPS é um protocolo, mas Java é uma linguagem de programação, não um protocolo de comunicação.

Gabarito: Letra D

24.(CESGRANRIO / BB - 2010) A Internet baseia-se no protocolo TCP/IP em que o endereço IP pode ser designado de maneira fixa ou variável. O responsável por designar endereços IP variáveis que possibilitam a navegação na Web é o servidor de:

- a) HTTP.
- b) HTML.
- c) DNS.
- d) DHCP.
- e) PHP.

Comentários:

(a) Errado. O HTTP é um protocolo utilizado para transferência de páginas web, não para atribuição de endereços IP;



- (b) Errado. HTML é uma linguagem de marcação usada para criar páginas web, sem relação com endereçamento IP;
- (c) Errado. O DNS traduz nomes de domínio para endereços IP, mas não atribui IPs aos dispositivos;
- (d) Correto. O DHCP (Dynamic Host Configuration Protocol) é o responsável por atribuir dinamicamente endereços IP aos dispositivos da rede, permitindo a navegação na web de forma automática;
- (e) Errado. PHP é uma linguagem de programação para desenvolvimento web, sem função no gerenciamento de endereços IP.

Gabarito: Letra D

25.(CESGRANRIO / IBGE - 2009) Em uma rede com TCP/IP, qual dos itens abaixo apresenta um protocolo utilizado para fazer upload e download de arquivos em máquinas remotas?

- a) SSL
- b) Telnet
- c) FTP
- d) NetBios
- e) DNS

Comentários:

- (a) Errado. SSL é um protocolo de segurança que oferece criptografia para outras aplicações, mas não é usado diretamente para upload ou download de arquivos;
- (b) Errado. Telnet é um protocolo de acesso remoto a terminais, não para transferência de arquivos;
- (c) Correto. O FTP (File Transfer Protocol) é o protocolo específico para transferência de arquivos entre máquinas remotas, permitindo upload e download em redes TCP/IP;
- (d) Errado. NetBIOS é um serviço usado em redes locais para comunicação entre aplicações, mas não para transferência de arquivos entre máquinas remotas;
- (e) Errado. O DNS é responsável pela resolução de nomes de domínio para IPs, sem relação com transferência de arquivos.

Gabarito: Letra C

26.(CESGRANRIO / LIQUIGÁS - 2018) Uma pessoa usou seu telefone celular para visitar um site Web no qual são encontrados vídeos científicos. Após informar seu endereço de e-mail e receber um link de confirmação, começou a procurar vídeos sobre cosmologia. Para sua surpresa, os vídeos a que assistiu estavam todos com legenda em português, embora ela não tivesse informado que estava acessando o site a partir do Brasil. Mais tarde, ao ler sobre o assunto na Internet, descobriu que o site científico soube de onde partiu o acesso tomando por base o:

- a) número do telefone celular a partir do qual o acesso foi feito.
- b) endereço de e-mail fornecido.
- c) endereço de IP usado na conexão com o site.
- d) o idioma do sistema operacional instalado no telefone celular.
- e) o idioma do navegador usado para acessar o site.



Comentários:

- (a) Errado. O número do telefone celular não é compartilhado com os sites acessados via navegador web;
- (b) Errado. O endereço de e-mail fornecido não indica a localização geográfica do usuário;
- (c) Correto. O endereço IP usado na conexão permite que o site identifique a localização geográfica aproximada do usuário, o que explica a exibição automática de conteúdo em português;
- (d) Errado. O idioma do sistema operacional pode influenciar interfaces locais, mas não é um dado diretamente acessível pelo site para definir a localização geográfica;
- (e) Errado. O idioma do navegador pode indicar preferência de idioma, mas não a localização geográfica exata.

Gabarito: Letra C

27.(CESGRANRIO / CEFET-RJ - 2014) Qual é o protocolo de internet para transferência segura, com uso de certificado digital, utilizado em sites de compras eletrônicas?

- a) IMAP
- b) HTTPS
- c) TOKEN RING
- d) POP3
- e) SNMP

Comentários:

- (a) Errado. IMAP é um protocolo para acesso e gerenciamento de e-mails, sem relação com segurança em sites de compras;
- (b) Correto. O HTTPS (Hypertext Transfer Protocol Secure) é o protocolo utilizado para transferência segura de dados em sites, incluindo comércio eletrônico, com uso de criptografia e certificados digitais;
- (c) Errado. TOKEN RING é uma tecnologia de topologia de rede antiga, sem relação com protocolos de segurança para web;
- (d) Errado. POP3 é um protocolo de recebimento de e-mails, não utilizado para sites de compras;
- (e) Errado. SNMP é um protocolo de gerenciamento de redes, sem relação com segurança em transações web.

Gabarito: Letra B

28.(CESGRANRIO / Banco do Brasil - 2014) Seja a seguinte URL, em que abcd.com.br é um host fictício:

ftp://abcd.com.br

O primeiro componente desse URL, ftp, indica que o usuário deseja:



- a) enviar um e-mail para outro usuário.
- b) enviar uma mensagem de texto, usando um terminal virtual.
- c) acessar arquivos de um grupo de discussão.
- d) acessar dados no formato de hipertexto.
- e) fazer download ou upload de arquivos.

Comentários:

- (a) Errado. O envio de e-mails utiliza protocolos como SMTP, IMAP ou POP3, não FTP;
- (b) Errado. O envio de mensagens de texto por terminal virtual é feito por protocolos como Telnet ou SSH;
- (c) Errado. Grupos de discussão na Internet utilizam protocolos como NNTP, não FTP;
- (d) Errado. O acesso a dados em formato de hipertexto é feito via HTTP ou HTTPS;
- (e) Correto. O prefixo "ftp://" indica o uso do protocolo FTP (File Transfer Protocol), que é utilizado para realizar download ou upload de arquivos entre cliente e servidor.

Gabarito: Letra E

29.(CESGRANRIO / BASA - 2015) Ao fazer compras pela Internet, uma das formas de preservar a segurança das suas informações de cartão de crédito ou conta corrente é fornecê-las sempre em um site no qual a URL comece por:

- a) ftp
- b) file
- c) hpml
- d) http
- e) https

Comentários:

- (a) Errado. O protocolo FTP é usado para transferência de arquivos, sem criptografia de dados sensíveis;
- (b) Errado. O esquema "file://" indica acesso a arquivos locais no próprio computador, não a sites da Internet;
- (c) Errado. "hpml" não é um protocolo válido nem reconhecido na web;
- (d) Errado. HTTP não oferece criptografia, tornando a transmissão de dados como informações bancárias insegura;
- (e) Correto. HTTPS (Hypertext Transfer Protocol Secure) garante que os dados enviados, como informações de cartão de crédito, sejam criptografados durante a transmissão, aumentando a segurança das transações online.

Gabarito: Letra E



30.(CESGRANRIO / Banco do Brasil - 2012) Na Internet, para evitar que o tráfego de dados entre os usuários e seus servidores seja visualizado por terceiros, alguns sites, como os de bancos e de comércio eletrônico, utilizam em suas conexões o protocolo:

- a) FTP
- b) X25
- c) BSC
- d) SMTP
- e) HTTPS

Comentários:

- (a) Errado. FTP é usado para transferência de arquivos e, na forma padrão, não oferece criptografia;
- (b) Errado. X.25 é um protocolo antigo de comunicação de redes de longa distância, em desuso para aplicações web modernas;
- (c) Errado. BSC (Binary Synchronous Communication) é um protocolo de comunicação legado, sem uso em web ou segurança de tráfego de dados;
- (d) Errado. SMTP é utilizado para envio de e-mails, sem relação com a navegação segura em sites;
- (e) Correto. O HTTPS (Hypertext Transfer Protocol Secure) é o protocolo padrão usado por bancos e sites de comércio eletrônico para garantir a criptografia e a segurança na transmissão de dados entre usuários e servidores.

Gabarito: Letra E

31.(CESGRANRIO / PETROBRAS - 2012) A vantagem de usar o protocolo IMAP em lugar do protocolo POP3 está no fato de o uso desse último obrigar o usuário a estar ligado à Internet para ler os e-mails a ele dirigidos.

PORQUE

Com o uso do protocolo IMAP, as mensagens são apagadas do servidor, automaticamente, logo após a abertura do e-mail.

Analisando-se as afirmações acima, conclui-se que:

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

Comentários:

O POP não obriga o usuário a estar ligado à internet – pelo contrário. A principal vantagem do IMAP é o gerenciamento de mensagens refletido no servidor, o que não ocorre no POP3. No IMAP, as mensagens



não são apagadas do servidor como é o caso do POP3 (que, por padrão, exclui as mensagens depois de baixadas).

Gabarito: Letra E

32.(CESGRANRIO / Caixa Econômica - 2012) O envio e o recebimento de um arquivo de textos ou de imagens na internet, entre um servidor e um cliente, constituem, em relação ao cliente, respectivamente, um:

- a) download e um upload
- b) downgrade e um upgrade
- c) downfile e um upfile
- d) upgrade e um downgrade
- e) upload e um download

Comentários:

- (a) Errado. Download é o recebimento de arquivos, enquanto upload é o envio, ou seja, a ordem está invertida;
- (b) Errado. Downgrade e upgrade referem-se a versões de software, não a operações de transferência de arquivos;
- (c) Errado. "Downfile" e "upfile" não são termos técnicos reconhecidos;
- (d) Errado. Upgrade e downgrade também são termos usados para indicar mudanças de versão de software, não envio ou recebimento de arquivos;
- (e) Correto. Enviar um arquivo para o servidor é um upload, e receber um arquivo do servidor é um download.

Gabarito: Letra E

33.(CESGRANRIO / PETROBRÁS - 2010) Os provedores de Internet disponibilizam a seus usuários um serviço de correio eletrônico para envio e recebimento de mensagens, que podem conter anexos como arquivos de fotos, documentos, programas de apresentação e muitos outros tipos de arquivos. Quando um usuário anexa um arquivo à mensagem que ele vai enviar, o destinatário da mensagem, para visualizar o conteúdo desse arquivo ao recebê-lo, precisará executar um procedimento denominado:

- a) download.
- b) sendmail.
- c) upload.
- d) file transfer.
- e) message transfer.

Comentários:

- (a) Correto. O destinatário precisa realizar o download do anexo, ou seja, transferir o arquivo do servidor de e-mail para o seu computador ou dispositivo local, para então visualizar o conteúdo;



- (b) Errado. Sendmail é um agente de transporte de e-mails, utilizado em servidores, não um procedimento executado pelo destinatário;
- (c) Errado. Upload é o envio de arquivos do computador local para um servidor, o oposto do que o destinatário faz ao receber um anexo;
- (d) Errado. "File transfer" é um termo genérico e não representa diretamente a ação realizada ao baixar um anexo de e-mail;
- (e) Errado. "Message transfer" refere-se ao envio de mensagens entre servidores de e-mail, não ao procedimento feito pelo destinatário para acessar um anexo.

Gabarito: Letra A

34.(CESGRANRIO / IBGE - 2009) Na Internet, fazer o upload de um arquivo consiste em:

- a) copiar um arquivo de um servidor.
- b) enviar um arquivo para um servidor.
- c) gravar um arquivo em um domínio.
- d) ler um texto em um host virtual.
- e) reduzir o tempo de acesso a um site.

Comentários:

Na internet, fazer o upload de um arquivo consiste basicamente em enviar um arquivo para um servidor. É a ação de enviar dados de um computador local para um computador ou servidor remoto, geralmente através da internet.

Gabarito: Letra B

35.(CESGRANRIO / TJ-GO - 2008) Em uma rede de computadores, a estrutura de dados unitária de transmissão constitui um:

- a) cronograma.
- b) datagrama.
- c) fluxograma.
- d) organograma.
- e) termograma.

Comentários:

- (a) Errado. Cronograma é uma ferramenta de planejamento de tempo, sem relação com redes de computadores;
- (b) Correto. Datagrama é a unidade de dados usada na transmissão de pacotes em redes baseadas no protocolo IP, representando um bloco de dados enviado de forma independente;
- (c) Errado. Fluxograma é uma representação gráfica de processos, não uma estrutura de transmissão de dados em redes;
- (d) Errado. Organograma representa a estrutura hierárquica de uma organização, sem relação com transmissão de dados;



(e) Errado. Termograma refere-se a registros de temperatura, não a dados em redes de computadores.

Gabarito: Letra B



LISTA DE QUESTÕES – CESGRANRIO

1. **(CESGRANRIO / CEFET-RJ - 2014)** Os tipos de rede digital podem ser classificados em função dos seus alcances geográficos. A rede com alcance de até 500 metros, utilizada em escritórios ou andares de um edifício, é denominada rede local e é conhecida pela sigla:

a) LAN
b) RAN
c) CAN
d) MAN
e) WAN
2. **(CESGRANRIO / CMB - 2012)** Os softwares navegadores são ferramentas de internet utilizadas para a interação dos usuários com a rede mundial. Para que essa interação seja possível, é necessário fazer uma conexão à internet por um dos diversos meios de acesso disponíveis aos usuários. O meio de acesso no qual o usuário utiliza um modem e uma linha de telefonia fixa para conectar-se com a internet é o:

a) dial up
b) ponte
c) satélite
d) wi-fi
e) cabo coaxial
3. **(CESGRANRIO / EPE - 2009)** Para encontrar o servidor de arquivos na rede, João perguntou ao seu suporte de rede qual era o endereço IP do servidor. Qual das opções abaixo representa um possível endereço IP para o servidor de arquivos?

a) GG568934FH2
b) 10.0.1.7
c) axe@pax.com.br
d) www.pax.com.br
e) 02-34-98-89-78-00
4. **(CESGRANRIO / TJ-RO - 2008)** Para que um computador possa se conectar a uma LAN (Local Area Network) é necessário que ele possua um(a):

a) codificador.
b) webcam.
c) impressora.
d) placa de rede.
e) placa de som.
5. **(CESGRANRIO / PETROBRAS - 2011)** No núcleo da Internet, o tráfego de informações entre os computadores, além de intenso, ocorre em grande velocidade, exigindo equipamentos de forte tecnologia. Esses equipamentos, em conjunto com outras tecnologias, constituem os:

a) protocols
b) backbones
c) web softwares



- d) security softwares
- e) control cables

6. (CESGRANRIO / BB - 2023) A configuração de rede de um computador pode ser realizada de forma estática ou dinâmica. Quando a forma estática é utilizada, o usuário deve configurar os parâmetros de rede manualmente, fornecendo, por exemplo, os endereços IP da estação de trabalho e do roteador padrão da rede local.

Por outro lado, quando se utiliza a forma dinâmica, o usuário deve configurar o computador para usar o protocolo de comunicação conhecido como:

- a) DNS
- b) VPN
- c) DHCP
- d) Wi-Fi
- e) FTTH

7. (CESGRANRIO / BB - 2023) A ferramenta de Webmail viabiliza o uso do serviço de correio eletrônico de empresas utilizando um navegador Web. Após a composição de uma nova mensagem de correio eletrônico, o usuário deve fazer a submissão do formulário para o servidor Web que, por sua vez, fará a submissão do conteúdo da mensagem para a fila do servidor de correio eletrônico. Os protocolos de comunicação utilizados nestas duas etapas são, respectivamente,

- a) HTTP e SMTP
- b) SMTP e HTTP
- c) POP3 e SMTP
- d) SMTP e POP3
- e) HTTP e POP3

8. (CESGRANRIO / BB - 2021) O serviço de correio eletrônico é uma ferramenta essencial para o trabalho do dia a dia dos colaboradores de uma empresa. Para garantir a segurança da comunicação do cliente de correio eletrônico com os servidores de correio eletrônico de entrada e de saída de mensagens, é importante configurar a utilização do padrão de segurança:

- a) TLS
- b) SMTP
- c) IMAP
- d) POP3
- e) HTTP

9. (CESGRANRIO / CEF - 2021) O aplicativo de correio eletrônico pode ser configurado para enviar mensagens e acessar as caixas de mensagens que estão no servidor de correio. Um dos protocolos de comunicação mais utilizados para acessar as mensagens da caixa de entrada é o:

- a) SMTP.
- b) IMAP.
- c) SMB.
- d) SSH.
- e) RDP.



10.(CESGRANRIO / BB - 2021) Apesar de os navegadores serem as ferramentas dominantes na internet, vários serviços possuem ferramentas próprias mais adequadas e, inclusive, mais otimizadas para protocolos específicos. Um desses protocolos foi desenvolvido para a transferência de arquivos, sendo usado a partir de programas como FileZilla. Esse protocolo é conhecido como:

- a) ftp.
- b) imap.
- c) pop3.
- d) ssh.
- e) elnet.

11.(CESGRANRIO / Banco do Brasil - 2021) Sabendo que o banco em que trabalha vai colocar centenas de ATMs em shoppings e postos de gasolina, um funcionário de TI propôs que cada ATM mandasse periodicamente um sinal de status, por meio do protocolo UDP. Esse protocolo do conjunto TCP/IP é considerado como parte da camada:

- a) de aplicações.
- b) de transporte.
- c) de rede.
- d) de enlace de dados.
- e) física.

12.(CESGRANRIO / Banco do Brasil - 2021) Ao chegar para seu primeiro dia de emprego no banco, um novo gerente de TI percebeu que era demandado muito esforço no setor para controle do número IP de cada computador, o que causava, também, alguns erros por uso múltiplo do mesmo IP nas redes. Percebendo uma oportunidade de melhoria, o novo gerente decidiu que os computadores passariam a obter automaticamente um número IP, por meio do protocolo:

- a) HTTP.
- b) IMAP.
- c) DHCP.
- d) SMTP.
- e) DNS.

13.CESGRANRIO / EPE - 2010) Determinado usuário comprou produtos em um site de vendas na Internet, por meio de um browser (Firefox, p.ex.).

Considerando-se que toda a navegação (seleção de produtos e compra) foi feita no endereço <http://www.siteexemplodevendas.com.br>, qual a falha de segurança desse procedimento de compra?

- a) Inexistência de FTP para transmissão de dados confidenciais.
- b) Seleção e compra de produtos no mesmo endereço WEB.
- c) Navegação por meio de um browser proprietário.
- d) Utilização de um navegador e não de um cliente de email.
- e) Utilização do HTTP, em detrimento ao HTTPS.

14.(CESGRANRIO / BASA - 2018) O protocolo que permite a navegação na internet segura através de criptografia de informações é o:

- a) HTTPS



- b) HTTP
- c) HTML
- d) XHTML
- e) XML

15.(CESGRANRIO / LIQUIGÁS - 2018) A exploração da internet exige o uso de inúmeros protocolos, dentre os quais o protocolo FTP. Esse protocolo tem como objetivo:

- a) transferir arquivos entre cliente e servidor.
- b) confirmar a identidade de um servidor.
- c) prover serviço de datagrama não confiável.
- d) manipular caixas postais remotas como se fossem locais.
- e) gerenciar correio eletrônico.

16.(CESGRANRIO / UNIRIO - 2016) Um usuário deseja acessar seus e-mails de vários dispositivos diferentes, sem baixar as mensagens para um dispositivo específico. Qual é o protocolo que permite que isso aconteça?

- a) HTTP
- b) SMTP
- c) POP
- d) IMAP
- e) FTP

17.(CESGRANRIO / UNIRIO - 2016) Utilizando um computador da universidade, certo usuário deseja realizar uma transação bancária pela internet. Um procedimento para que esse usuário identifique, apenas visualmente, se o site acessado é um site seguro para este tipo de transação é verificar se:

- a) a URL começa com FTP.
- b) a URL começa com HTTP.
- c) a URL começa com HTTPS.
- d) a URL está com o nome correto da instituição.
- e) os campos digitáveis de agência e conta possuem o tamanho correto.

18.(CESGRANRIO / PETROBRAS - 2015) O framework com designação universal abstrata para localizar um recurso na internet ou intranet é o:

- a) URL
- b) HTTP
- c) HTTPS
- d) TCP/IP
- e) Nome do arquivo

19.(CESGRANRIO / BB - 2014) Um usuário entrou em um site da Internet e, ao digitar seu login e senha, recebeu a informação de que a partir daquele momento ele começaria a navegar em um site seguro. Ao lado da mensagem o seguinte ícone foi exibido:



Nessas condições, o protocolo exibido na barra de endereços do navegador desse usuário foi o:

- a) ftp
- b) http
- c) https
- d) ssl
- e) tcp/ip

20.(CESGRANRIO / LIQUIGÁS - 2014) Qual componente da Internet é responsável pela tradução de nomes de domínios para endereços IP e vice-versa?

- a) DNS
- b) TCP
- c) HTTP
- d) POP3
- e) HOST

21.(CESGRANRIO / BB - 2013) Uma transação financeira por meio de navegadores de internet deve usar, na mesma porta alocada ao protocolo HTTP, um protocolo mais seguro também conhecido como HTTP/TLS. A URL desse protocolo é diferenciada por começar com:

- a) t-http
- b) s-http
- c) https
- d) http-s
- e) httppt

22.(CESGRANRIO / CEF - 2012) Uma das funções de um cliente FTP instalado em uma estação de trabalho de uma intranet é:

- a) autenticar a senha do cliente junto ao controlador de domínio.
- b) criar um site web utilizando tecnologia Flash Player.
- c) transferir arquivos entre a estação de trabalho e um servidor.
- d) controlar os acessos da estação de trabalho à Internet.
- e) visualizar arquivos de imagem recebidos por e-mail.

23.(CESGRANRIO / DECEA - 2012) Os computadores necessitam de um meio de comunicação para que possam acessar, através dos softwares navegadores, em modo on-line, o mundo de informações disponíveis na internet. Essa comunicação é feita por um conjunto de normas e procedimentos que constituem os protocolos de comunicação. Entre esses protocolos, incluem-se os seguintes:

- a) DNS e Cluster
- b) SAP e Telnet
- c) HTTP e HTML
- d) IMAP e SMTP
- e) HTTPS e Java

24.(CESGRANRIO / BB - 2010) A Internet baseia-se no protocolo TCP/IP em que o endereço IP pode ser designado de maneira fixa ou variável. O responsável por designar endereços IP variáveis que possibilitam a navegação na Web é o servidor de:



- a) HTTP.
- b) HTML.
- c) DNS.
- d) DHCP.
- e) PHP.

25.(CESGRANRIO / IBGE - 2009) Em uma rede com TCP/IP, qual dos itens abaixo apresenta um protocolo utilizado para fazer upload e download de arquivos em máquinas remotas?

- a) SSL
- b) Telnet
- c) FTP
- d) NetBios
- e) DNS

26.(CESGRANRIO / LIQUIGÁS - 2018) Uma pessoa usou seu telefone celular para visitar um site Web no qual são encontrados vídeos científicos. Após informar seu endereço de e-mail e receber um link de confirmação, começou a procurar vídeos sobre cosmologia. Para sua surpresa, os vídeos a que assistiu estavam todos com legenda em português, embora ela não tivesse informado que estava acessando o site a partir do Brasil. Mais tarde, ao ler sobre o assunto na Internet, descobriu que o site científico soube de onde partiu o acesso tomando por base o:

- a) número do telefone celular a partir do qual o acesso foi feito.
- b) endereço de e-mail fornecido.
- c) endereço de IP usado na conexão com o site.
- d) o idioma do sistema operacional instalado no telefone celular.
- e) o idioma do navegador usado para acessar o site.

27.(CESGRANRIO / CEFET-RJ - 2014) Qual é o protocolo de internet para transferência segura, com uso de certificado digital, utilizado em sites de compras eletrônicas?

- a) IMAP
- b) HTTPS
- c) TOKEN RING
- d) POP3
- e) SNMP

28.(CESGRANRIO / Banco do Brasil - 2014) Seja a seguinte URL, em que abcd.com.br é um host fictício:

ftp://abcd.com.br

O primeiro componente desse URL, ftp, indica que o usuário deseja:

- a) enviar um e-mail para outro usuário.
- b) enviar uma mensagem de texto, usando um terminal virtual.
- c) acessar arquivos de um grupo de discussão.
- d) acessar dados no formato de hipertexto.
- e) fazer download ou upload de arquivos.



29.(CESGRANRIO / BASA - 2015) Ao fazer compras pela Internet, uma das formas de preservar a segurança das suas informações de cartão de crédito ou conta corrente é fornecê-las sempre em um site no qual a URL comece por:

- a) ftp
- b) file
- c) hpml
- d) http
- e) https

30.(CESGRANRIO / Banco do Brasil - 2012) Na Internet, para evitar que o tráfego de dados entre os usuários e seus servidores seja visualizado por terceiros, alguns sites, como os de bancos e de comércio eletrônico, utilizam em suas conexões o protocolo:

- a) FTP
- b) X25
- c) BSC
- d) SMTP
- e) HTTPS

31.(CESGRANRIO / PETROBRAS - 2012) A vantagem de usar o protocolo IMAP em lugar do protocolo POP3 está no fato de o uso desse último obrigar o usuário a estar ligado à Internet para ler os e-mails a ele dirigidos.

PORQUE

Com o uso do protocolo IMAP, as mensagens são apagadas do servidor, automaticamente, logo após a abertura do e-mail.

Analisando-se as afirmações acima, conclui-se que:

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

32.(CESGRANRIO / Caixa Econômica - 2012) O envio e o recebimento de um arquivo de textos ou de imagens na internet, entre um servidor e um cliente, constituem, em relação ao cliente, respectivamente, um:

- a) download e um upload
- b) downgrade e um upgrade
- c) downfile e um upfile
- d) upgrade e um downgrade
- e) upload e um download

33.(CESGRANRIO / PETROBRÁS - 2010) Os provedores de Internet disponibilizam a seus usuários um serviço de correio eletrônico para envio e recebimento de mensagens, que podem conter anexos como arquivos de fotos, documentos, programas de apresentação e muitos outros tipos de arquivos. Quando um usuário anexa um arquivo à mensagem que ele vai enviar, o



destinatário da mensagem, para visualizar o conteúdo desse arquivo ao recebê-lo, precisará executar um procedimento denominado:

- a) download.
- b) sendmail.
- c) upload.
- d) file transfer.
- e) message transfer.

34.(CESGRANRIO / IBGE - 2009) Na Internet, fazer o upload de um arquivo consiste em:

- a) copiar um arquivo de um servidor.
- b) enviar um arquivo para um servidor.
- c) gravar um arquivo em um domínio.
- d) ler um texto em um host virtual.
- e) reduzir o tempo de acesso a um site.

35.(CESGRANRIO / TJ-GO - 2008) Em uma rede de computadores, a estrutura de dados unitária de transmissão constitui um:

- a) cronograma.
- b) datagrama.
- c) fluxograma.
- d) organograma.
- e) termograma.



GABARITO – CESGRANRIO

1. LETRA A
2. LETRA A
3. LETRA B
4. LETRA D
5. LETRA B
6. LETRA C
7. LETRA A
8. LETRA A
9. LETRA B
10. LETRA A
11. LETRA B
12. LETRA C
13. LETRA E
14. LETRA A
15. LETRA A
16. LETRA D
17. LETRA C
18. LETRA A
19. LETRA C
20. LETRA A
21. LETRA C
22. LETRA C
23. LETRA D
24. LETRA D
25. LETRA C
26. LETRA C
27. LETRA B
28. LETRA E
29. LETRA E
30. LETRA E
31. LETRA E
32. LETRA E
33. LETRA A
34. LETRA B
35. LETRA B



ESSA LEI TODO MUNDO CONHECE: PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.



1 Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.



2 Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).



3 Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).



4 Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).



5 Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).



6 Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).



7 Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.



8 O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.



Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.