Eletrônico

MATERIAL PARA PRF

POLÍCIA RODOVIÁRIA FEDERAL

Aula 00

Noções de Informática p/ PRF - Policial - 2018 (Com videoaulas)

Professor: Victor Dalton

Estratégia CONCURSOS

"O SEGREDO DO SUCESSO É A CONSTÂNCIA NO OBJETIVO"

AULA 00: Redes e Fundamentos de Internet

SUMÁRIO

Olá a todos! E sejam bem-vindos ao projeto **Informática** para a **Polícia Rodoviária Federal**!

A nossa proposta de trabalho é apresentar **um curso teórico em PDF + videoaulas**, **que habilitará você a acertar as questões de concurso de Informática** para esse certame.

Nosso curso será focado na banca **CESPE** (banca examinadora do último concurso), e será reforçado com questões de outras bancas, para que sua preparação seja a mais robusta possível.

E por que estudar informática em PDFs + videoaulas?

Um dos bens mais preciosos que temos é o nosso **tempo**. E quem estuda para concursos sabe o quanto é difícil ter tempo para trabalho, família, lazer e estudos. No caso da informática, temos ainda um **agravante**: nossa matéria é uma verdadeira "colcha de retalhos", unindo conhecimentos esparsos, o que dificulta DEMAIS a vida de quem simplesmente resolve sair comprando livros e realiza pesquisa na Internet por conta própria para adquirir conhecimento. Fora a quantidade ENORME de **lixo** que temos na Web...

Nessas horas é interessante se perguntar.... Vale a pena o risco? Vale a pena o **TEMPO** desperdiçado até achar conteúdo que preste? Ou é melhor estudar material **direcionado**, **sob medida**, e com **exercícios comentados**?

Acho até que, se você precificar o tempo que você ganha em estudar conosco, vai ver que o nosso material tem um preço bem atraente.... ☺

> *"Tudo o que um sonho precisa para ser realizado é alguém que acredite que ele possa ser realizado."*
>
> *Roberto Shinyashiki*

Vem comigo?

Observação importante II: todo o conteúdo deste curso encontra-se completo em nossos textos escritos. As videoaulas visam reforçar o aprendizado, especialmente para aqueles que possuem maior facilidade de aprendizado com vídeos e/ou querem ter mais uma opção para o aprendizado.

Permitam-me que eu me apresente.

APRESENTAÇÃO

Eu sou Victor Dalton Teles Jesus Barbosa. Minha experiência em concursos começou aos 15 anos, quando consegui ingressar na Escola Preparatória de Cadetes do Exército, em 1999. Cursei a Academia Militar das Agulhas Negras, me tornando Bacharel em Ciências Militares, 1º Colocado em Comunicações, da turma de 2003.

Em 2005, prestei novamente concurso para o Instituto Militar de Engenharia, aprovando em 3º lugar. No final de 2009, me formei em Engenharia da Computação, sendo o 2º lugar da turma no Curso de Graduação. Decidi então mudar de ares.

Em 2010, prestei concursos para Analista do Banco Central (Área 1 – Tecnologia da Informação) e Analista de Planejamento e Orçamento (Especialização em TI), cujas bancas foram a **CESGRANRIO** e a **ESAF**, respectivamente. Fui aprovado em ambos os concursos e, após uma passagem pelo Ministério do Planejamento, optei pelo Banco Central do Brasil.

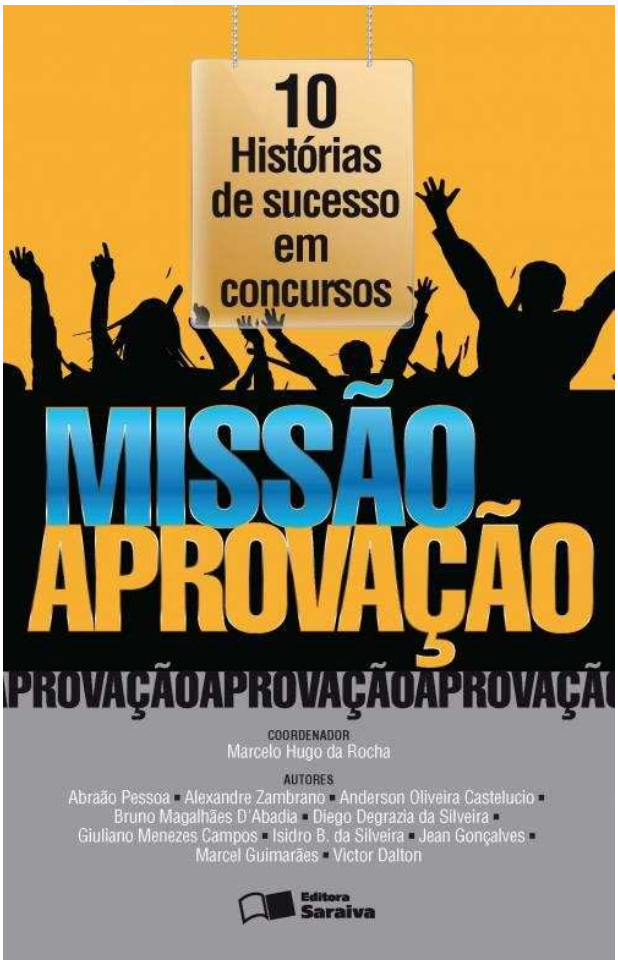
Em 2012, por sua vez, prestei concurso para o cargo de Analista Legislativo da Câmara dos Deputados, aplicado pela banca **CESPE**, e, desde o início de 2013, faço parte do Legislativo Federal brasileiro.

Além disso, possuo as certificações **ITIL Foundation**, emitida pela **EXIN**, e **Cobit Foundation**, emitida pela **ISACA**. Também sou especialista em Planejamento e Orçamento Governamental pela ENAP e em Direito Constitucional.

Aqui no Estratégia Concursos, já ministrei e ministro cursos para vários certames, como CGU, Receita Federal, ICMS/PR, ICMS/SP, ISS/SP, ICMS/RJ, ICMS/MS, ICMS/RS, ICMS/PE, ICMS/PI, ISS/Salvador, Banco Central, MPU, TCU, IBAMA, ANS, Ministério da Saúde, Polícia Federal, MPOG, PCDF, PRF, TCE-RS, AFT, ANCINE, TCDF, ANATEL, DATAPREV, Câmara dos Deputados, Caixa Econômica Federal, cursos para Tribunais, dentre outros. Além disso, também ministro aulas presenciais em diversos Estados, cujo feedback dos alunos tem me impulsionado a continuar cada vez mais a ministrar aulas.

Por fim, sou coautor do **Livro Missão Aprovação**, publicado pela Editora Saraiva, que conta 10 histórias de sucesso em concursos públicos. Quem sabe algumas dessas histórias não podem inspirar você em sua trajetória? Conheça a obra!

http://www.editorasaraiva.com.br/produto/direito/concursos/missao-aprovacao-10-historias-de-sucesso-em-concursos/



Pois bem, e como será o nosso curso?

CONTEÚDO PROGRAMÁTICO

Nosso curso trará as aulas na seguinte sequência:

Aula 00 3 Redes de computadores. 3.1 Conceitos básicos, ferramentas, aplicativos e procedimentos de Internet e intranet.

Aula 01 3.2 Programas de navegação (Microsoft Internet Explorer, Mozilla Firefox e Google Chrome).

Aula 02 3.3 Programas de correio eletrônico (Outlook Express e Mozilla Thunderbird).

Aula 03 3.4 Sítios de busca e pesquisa na Internet. 3.5 Grupos de discussão. 3.6 Redes sociais. 3.7 Computação na nuvem (cloud computing). 5.5 Armazenamento de dados na nuvem (cloud storage).

Aula 04 1 Noções de sistema operacional (ambiente Windows). 4 Conceitos de organização e de gerenciamento de informações, arquivos, pastas e programas.

Aula 05 2 Edição de planilhas (ambiente LibreOffice).

Aula 06 2 Edição de textos e apresentações (ambiente LibreOffice).

Aula 07 5 Segurança da informação. 5.1 Procedimentos de segurança. 5.2 Noções de vírus, worms e pragas virtuais. 5.3 Aplicativos para segurança (antivírus, firewall e anti-spyware). 5.4 Procedimentos de backup

Pois bem, sem mais delongas, iniciaremos o nosso curso falando sobre **Redes.** É um conteúdo basilar que, embora não caia tanto diretamente em prova, é subsídio para os assuntos vindouros.

Aos trabalhos!

1. REDE: CONCEITOS BÁSICOS

1.1 Definição, LAN, MAN e WAN

Uma **rede de computadores é conexão de dois ou mais computadores para permitir o compartilhamento de recursos e a troca de informações entre as máquinas**.

Em alguns casos, seria suficiente construir redes de computadores limitadas, que conectam somente algumas máquinas. Por exemplo, uma pequena empresa, com alguns computadores e uma impressora, poderia se construir uma pequena rede para permitir o compartilhamento da impressora entre os usuários. Ou, ainda, uma residência com um computador, impressora e um roteador local, na qual conectam-se um notebook e um *smartphone* também pode ser caracterizada como uma rede de computadores.

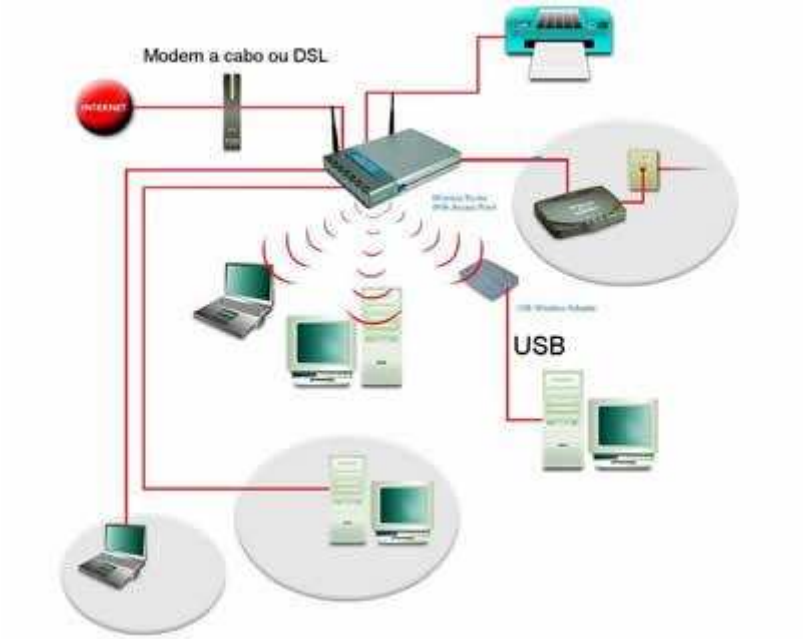


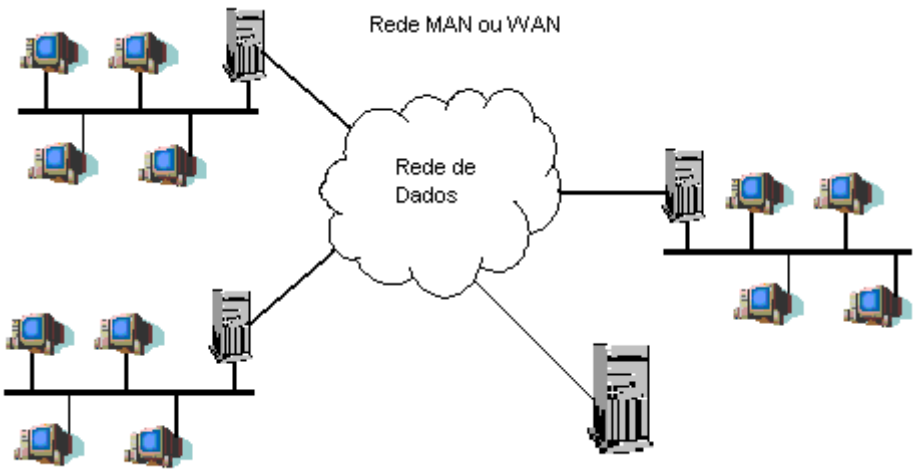
Ilustração de rede de computadores

Atualmente, com a importância cada vez maior de se dispor de acesso a informações e facilidades de comunicação, as redes de computadores estão projetadas para crescer indefinidamente, sendo a Internet um bom exemplo. No caso da pequena empresa, a pouco citado, além da possibilidade de compartilhamento de recursos, uma conexão com outras

redes e à Internet pode oferecer acesso a informações importantes, bem como possibilitar a esta empresa a prestação de serviços por este meio, como o *e-commerce*. Além de propiciar um meio de comunicação bastante ágil, facilitando o trabalho tanto da empresa como de seus clientes.

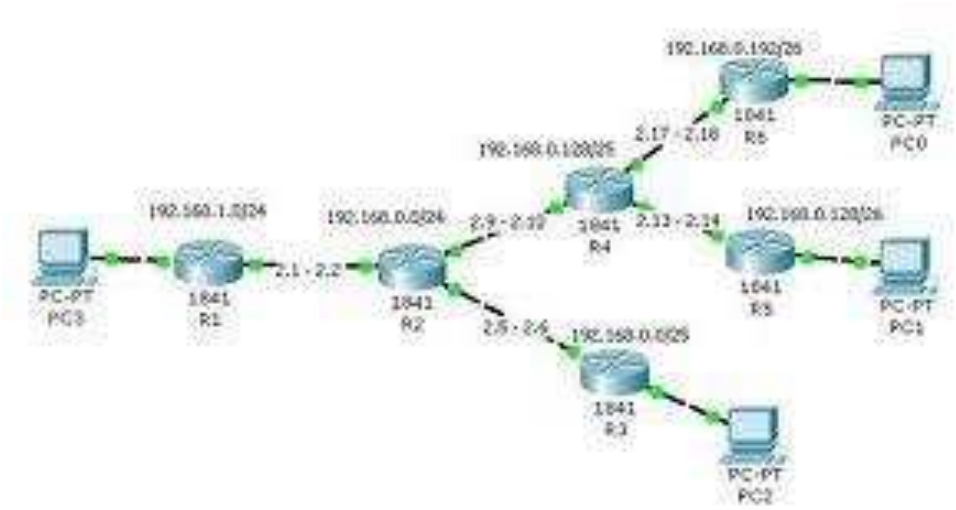
A conectividade dos computadores em rede pode ocorrer em diferentes escalas. A rede mais simples consiste em dois ou mais computadores conectados por um **meio físico**, tal como um par metálico ou um cabo coaxial. O meio físico que conecta dois computadores costuma ser chamado de **enlace de comunicação** e os computadores são chamados de **nós**. Um enlace de comunicação limitado a um par de nós é chamado de **enlace ponto-a-ponto**. Um enlace pode também envolver mais de dois nós, neste caso, podemos chamá-lo de **enlace multiponto**, como na figura acima. Um enlace multiponto, formando um barramento de múltiplo acesso, é um exemplo de enlace utilizado na tecnologia de **rede local** (**LAN** – *local area network*) do tipo Ethernet.

Se as redes de computadores fossem limitadas a situações onde todos os nós fossem diretamente conectados a um meio físico comum, o número de computadores que poderiam ser interligados seria também muito limitado. Na verdade, numa rede de maior abrangência geográfica, como as **redes metropolitanas** (**MAN** – *metropolitan area network)* ou **redes de alcance global** (**WAN** *wide área network*), nem todos os computadores precisam estar diretamente conectados.

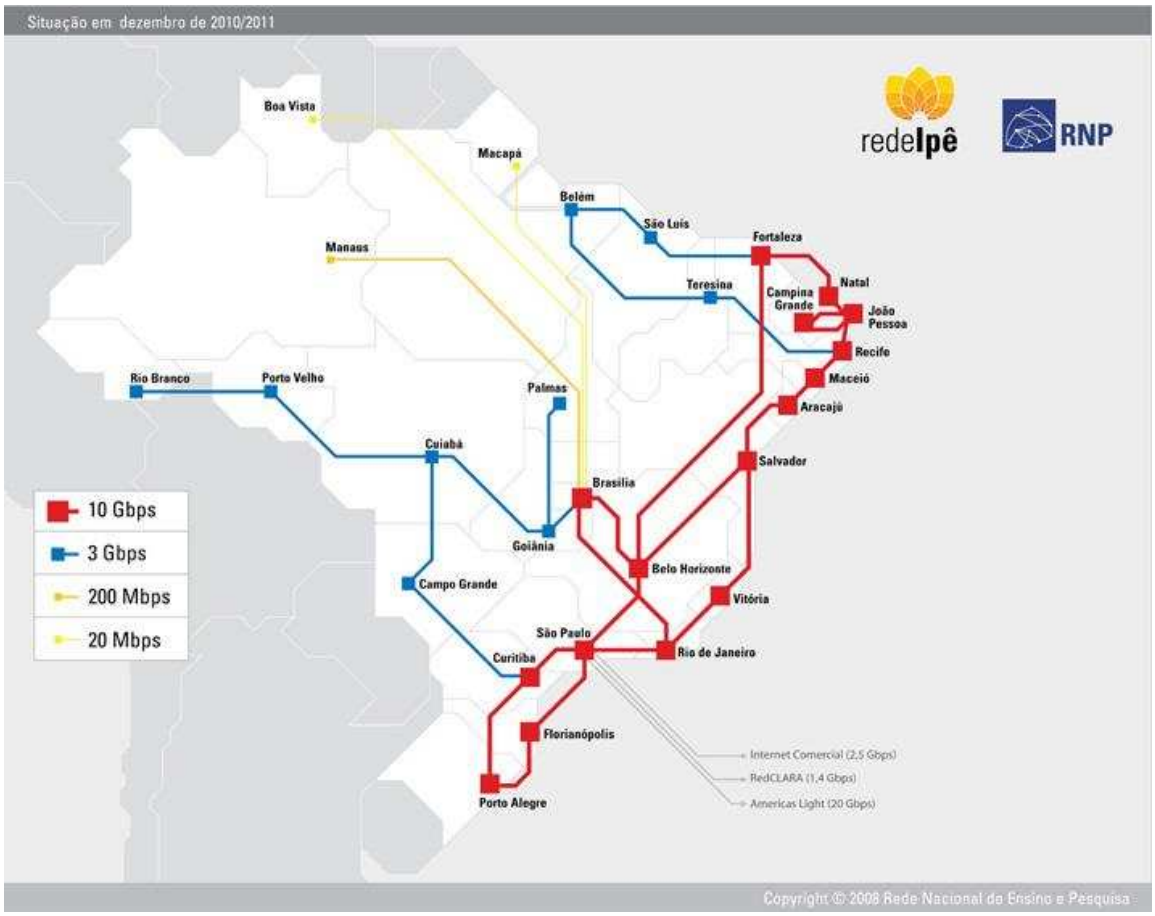


Uma conectividade indireta pode ser obtida usando uma **rede comutada**. Nesta rede comutada podemos diferenciar os **nós** da rede que estão na sua **periferia**, como computadores terminais conectados ao núcleo da rede via enlaces ponto-a-ponto ou multiponto, daqueles que

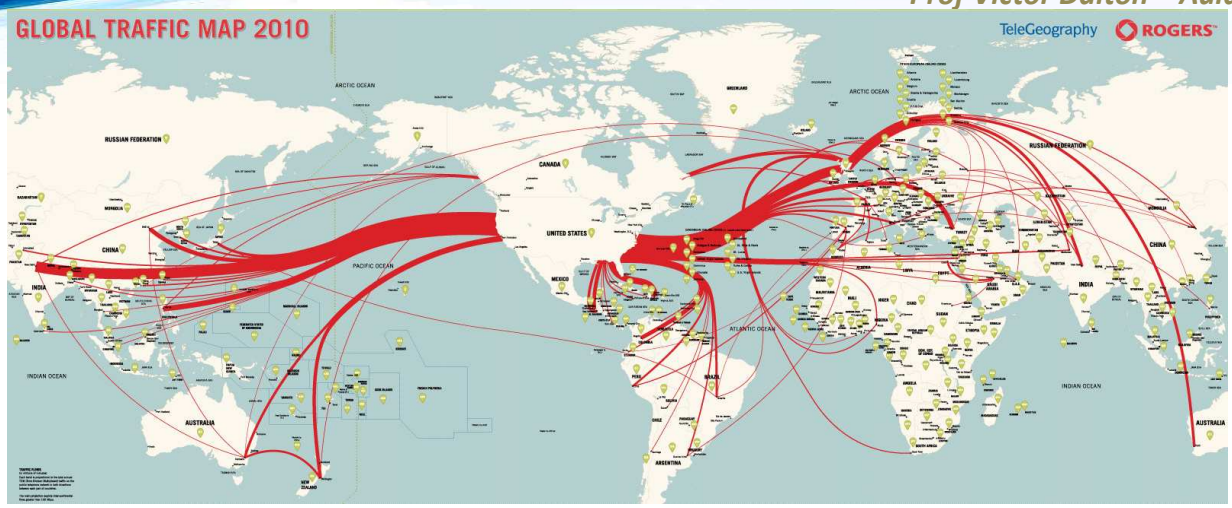
estão no **núcleo** da rede, formado por **comutadores** ou **roteadores**, como na figura abaixo.



Computadores interligados em rede por meio de comutadores ou roteadores. Pode-se estender esse modelo a nível mundial, formando a Internet.



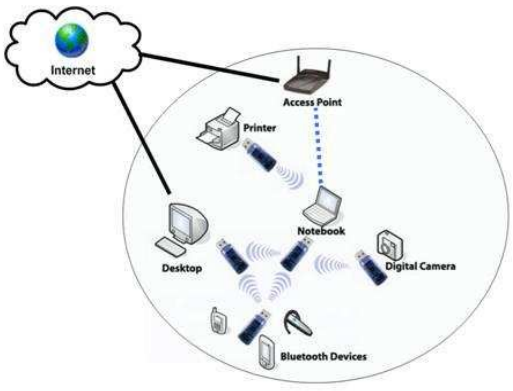
***Backbone* do Brasil em 2010. *Backbone* é a espinha dorsal que designa o esquema de ligações centrais de um sistema mais amplo, como o mostrado acima.**



Internet. Viu como é simples?

Existem inúmeros tipos de redes comutadas, as quais podemos dividir em redes de **comutação de circuitos** e redes de **comutação de pacotes.** Como exemplo, podemos citar o sistema telefônico e a Internet, respectivamente.

P.S.: Existe alguns conceitos mais modernos, como a **WLAN** (*Wireless LAN*, rede sem fio, que nem é tão moderno assim), e a **PAN** (*Personal Area Network,* esse sim, em franca expansão, com a utilização de tecnologias *wireless, bluetooh e NFC*, entre outros).

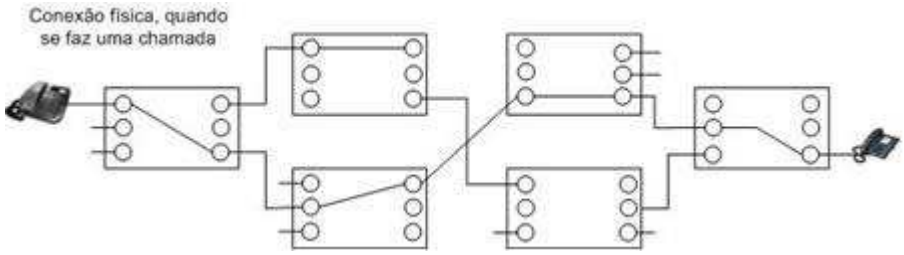


Exemplos de Personal Area Network

Existem dois paradigmas de comunicação de dados, no contexto de redes de computadores. A **comutação de circuitos** e a **comutação de pacotes**.

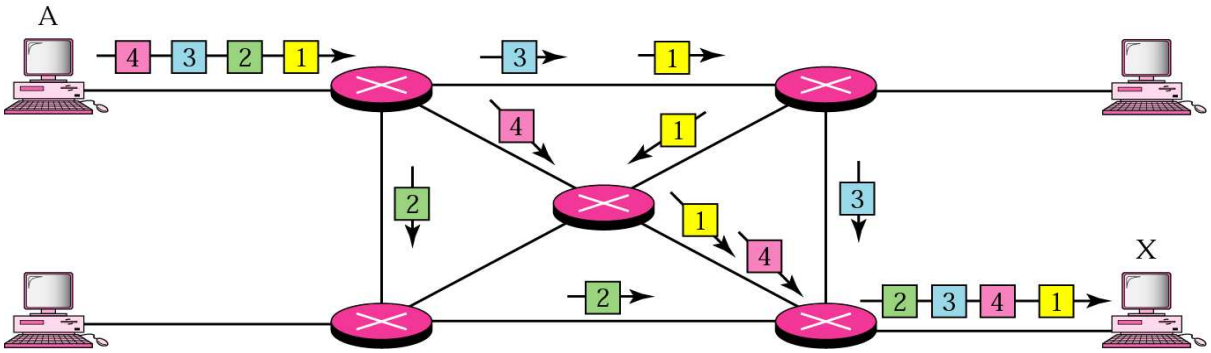
1.2 Comutação de circuitos x comutação de pacotes

A **comutação de circuitos** possui fundamento similar à telefonia fixa. Nela, todo o tráfego de informação entre dois dispositivos sempre passa pelo mesmo caminho. Tal caminho pode ser definido por um circuito físico, ou por compartilhamento de um meio, utilizando multiplexação.



Comutação de circuitos: ilustração

Na **comutação por pacotes**, por sua vez, os pacotes podem seguir vários caminhos diferentes para chegar ao destinatário, podendo, inclusive, chegarem fora de ordem, pois serão reordenados na máquina destino. É o paradigma que vigora na *Internet*.

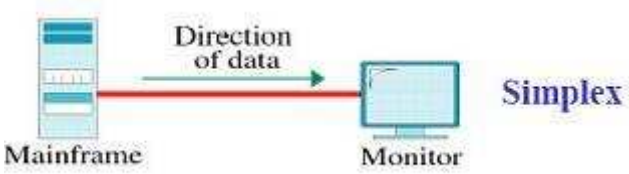


Comutação de pacotes: ilustração

1.3 Formas de utilização do meio físico

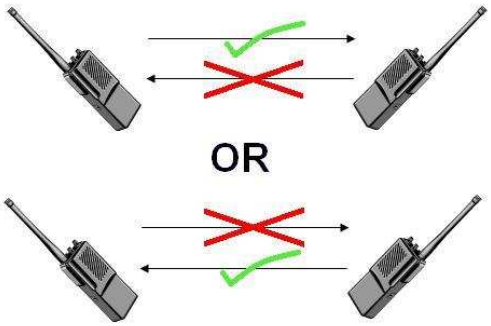
Quanto à forma de utilização do meio de transmissão, as conexões podem ser classificadas em **simplex**, **half-duplex** e **full-duplex**.

Uma conexão que permite o tráfego apenas em um sentido é chamada **simplex**. Uma rua de mão única é simplex. Outro exemplo de uma conexão **simplex** é uma fibra óptica com um laser em uma extremidade e um detector de luz na outra extremidade. Uma última analogia é a transmissão de TV de sinal aberto, na qual o receptor apenas recebe o sinal.



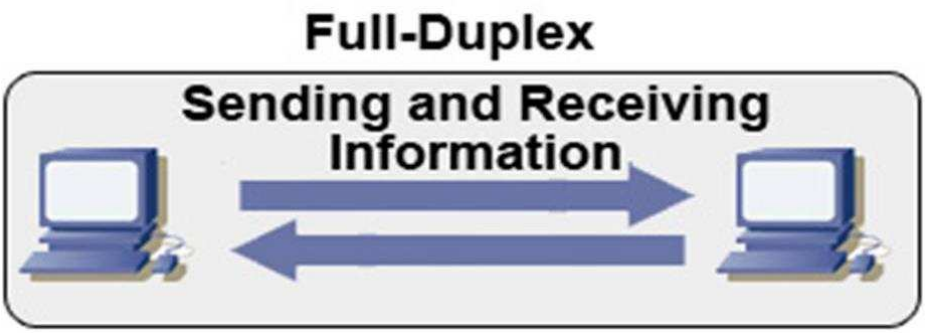
Conexão Simplex: ilustração

Uma conexão que permite o tráfego nos dois sentidos, mas apenas em um sentido de cada vez, é chamada half-duplex. Uma estrada de ferro única é **half-duplex**. Um par de walkie-talkies estabelece uma conexão half-duplex.



Conexão Half-Duplex: ilustração

Uma conexão que permite tráfego em ambos os sentidos simultaneamente é chamada **full-duplex**. Uma estrada de duas pistas é full-duplex. O padrão Ethernet permite a comunicação full-duplex.



Conexão Full-Duplex: ilustração

Aproveitando esta abordagem de direcionamento de fluxos, não custa enfatizar os conceitos de ***download*** e ***upload***.

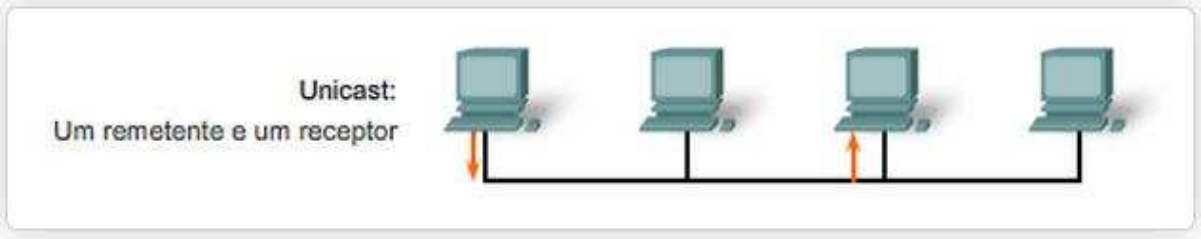
Download, um conceito muito comum do cotidiano online, diz respeito a quando trazemos conteúdo de outro local para o nosso computador. Baixar páginas web, programas, documentos e outros conteúdos, constitui ***download.***

Upload, por seu turno, é o procedimento inverso, ou seja, enviar conteúdo do nosso computador para a Internet ou outra maquina em uma rede. O procedimento mais comum de upload em nosso cotidiano provalmente é o envio de arquivos para armazenamento na nuvem.

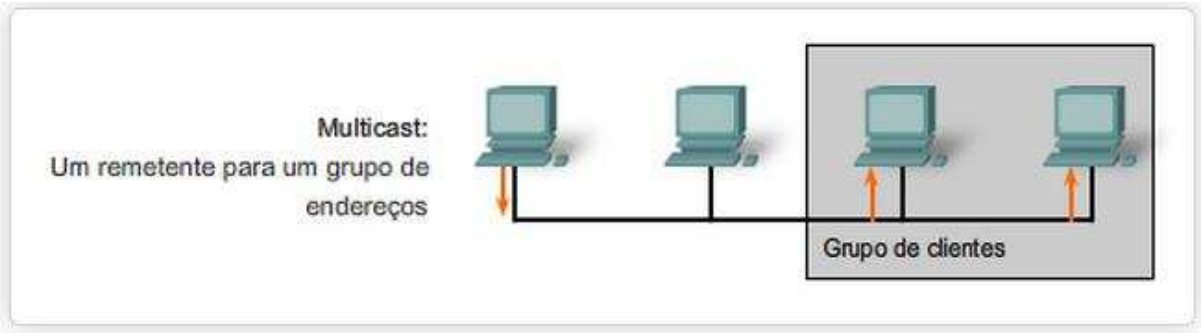
1.4 Unicast x Multicast x Broadcast

A classificação da comunicação em **unicast, multicast** ou **broadcast** diz respeito ao número de destinatários de uma transmissão.

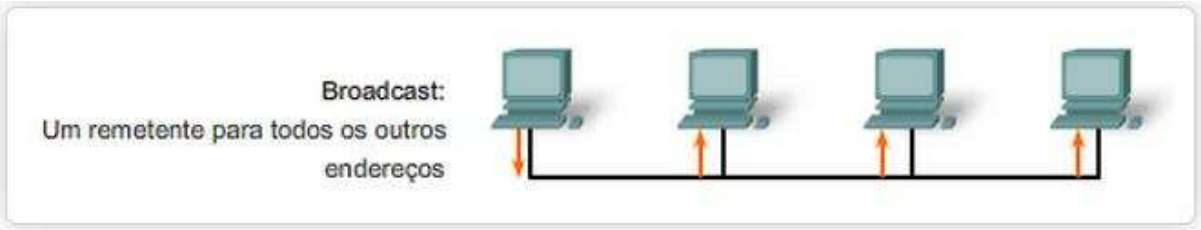
Unicast: Comunicação na qual um quadro é enviado de um host e endereçado a um destino específico. Na transmissão unicast, há apenas **um remetente e um receptor**. A transmissão unicast é a forma predominante de transmissão em redes locais e na Internet. Entre os exemplos de protocolos que usam transmissões unicast estão HTTP, SMTP, FTP e Telnet.



Multicast: Comunicação na qual um quadro é enviado para um **grupo específico de dispositivos ou clientes**. Os clientes da transmissão multicast devem ser membros de um grupo multicast lógico para receber as informações. Um exemplo de transmissão multicast é a transmissão de vídeo e de voz associada a uma reunião de negócios colaborativa, com base em rede.



Broadcast: Comunicação na qual um quadro é enviado de um endereço para **todos os outros endereços**. Nesse caso, há apenas um remetente, mas as informações são enviadas para todos os receptores conectados. A transmissão de broadcast é essencial durante o envio da mesma mensagem para todos os dispositivos na rede local. Um exemplo de transmissão de broadcast é a consulta de resolução de endereço que o protocolo de resolução de endereços (ARP, Address Resolution Protocol) envia para todos os computadores em uma rede local.



1.5 Comunicação síncrona e comunicação assíncrona

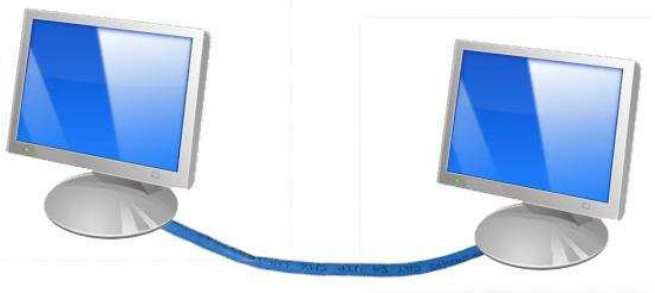
Em transmissão de dados, diz-se que a comunicação é **síncrona** quando o dispositivo emissor e o dispositivo receptor encontram-se num estado de sincronia (**estabelecimento de conexão**) antes de a comunicação iniciar e permanecem em sincronia durante a transmissão. Isto pode envolver o bloqueio das partes enquanto a transmissão ocorre. Por exemplo, um dispositivo pode enviar uma requisição a outro dispositivo, e somente continuar com suas tarefas após a resposta deste outro dispositivo. Uma boa analogia é a ligação telefônica, na qual os dois aparelhos precisam estar conectados para a ligação ocorrer.

Por outro lado, na comunicação **assíncrona**, não ocorre estabelecimento de conexão entre as partes, ficando a cargo de outros protocolos o ordenamento e eventual perda das mensagens. É como uma carta, enviada pelo correio, sem código de rastreamento. Quem envia não tem como saber se ela chegou ou não, e a leitura da mensagem só ocorre quando o destinatário abre a sua caixa de correio.

1.6 Topologias básicas de redes

Topologia de rede pode se relacionar ao modo que as redes de computadores se organizam fisicamente e/ou logicamente.

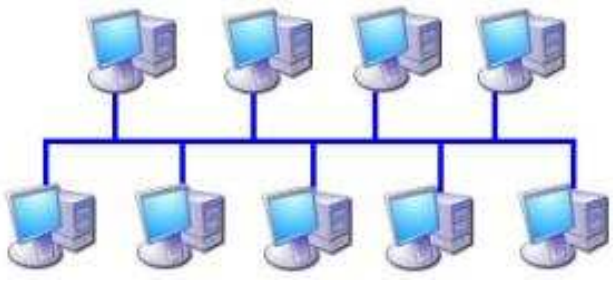
Ponto-a-ponto: União de dois computadores, através de um meio de transmissão qualquer. Quando feita com o famoso cabo azul (redes *Ethernet*), tal cabo é denominado de **cross-over.** Destaco que as placas de redes mais modernas já sabem diferenciar uma conexão ponto-a-ponto de uma conexão convencional (*autosensing*), não sendo mais necessário a utilização de um cabo próprio para tal.



Rede ponto-a-ponto.

Barramento: Todos os computadores são ligados em um mesmo barramento físico de dados. Apenas uma máquina pode "escrever" no barramento num dado momento. Todas as outras "escutam" e recolhem para si os dados destinados a elas. Quando um dispositivo transmitir um sinal, toda a rede fica ocupada (**broadcast**) e se outro computador tentar enviar outro sinal ao mesmo tempo, ocorre uma colisão e é preciso reiniciar a transmissão.

Talvez o protocolo mais conhecido para esse tipo de topologia seja o **CSMA/CD**(**Carrier Sense Multiple Access with Collision Detection**), onde cada estação que quiser acessar a linha de transmissão verifica sua ocupação, transmitindo caso esteja livre, ou esperando para transmitir, em caso de linha ocupada. Caso duas transmissões tentem transmitir ao mesmo tempo, ocorre a colisão, e a retransmissão obedece a um algoritmo de recuo exponencial, reduzindo a chance de novas colisões.



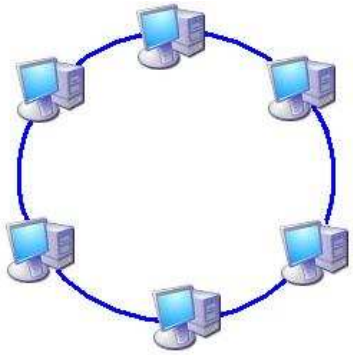
Topologia em barramento.

Como **vantagens**, a topologia barramento apresenta a facilidade de instalação, e a menor quantidade de cabeamento necessária (baixo custo). Por outro lado, o acréscimo de novos pontos à rede afeta diretamente a performance da mesma.

Anel: Na topologia em anel os dispositivos são conectados em série, formando um circuito fechado (anel). Os dados são transmitidos unidirecionalmente de nó em nó até atingir o seu destino. Uma mensagem

enviada por uma estação passa por outras estações, através das retransmissões, até ser retirada pela estação destino ou pela estação fonte. Os sinais sofrem menos distorção e atenuação no enlace entre as estações, pois há um repetidor em cada estação. Há um atraso de um ou mais bits em cada estação para processamento de dados. É possível usar anéis múltiplos para aumentar a confiabilidade e o desempenho.

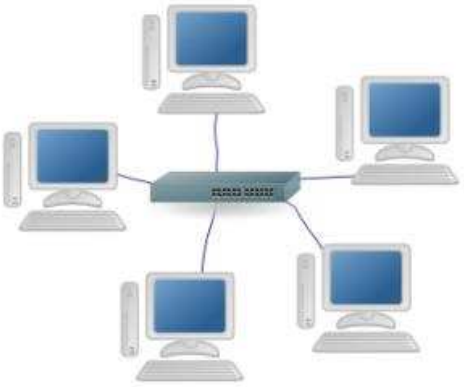
Um exemplo de protocolo relacionado a essa topologia é o Token Ring (**IEEE 802.5**), no qual apenas o detentor do Token pode transmitir dados na rede.



Topologia em anel.

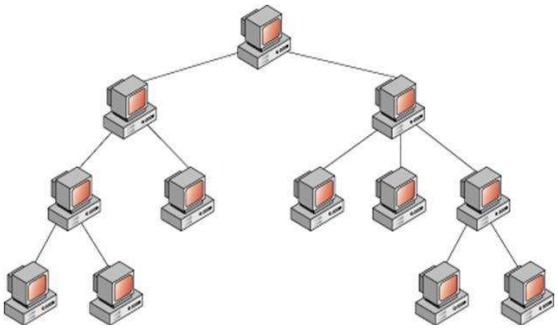
De uma certa forma, a rede em anel lida bem com o acréscimo de novos usuários na rede, sem impacto significativo na performance. Porém, a falha de um nó na rede, ou qualquer problema com o cabeamento, e toda a rede fica fora do ar.

Estrela(hub-and-spoke): A mais comum atualmente, a topologia em estrela utiliza cabos de par trançado e um concentrador como ponto central da rede. O concentrador se encarrega de retransmitir todos os dados para a estação de destino, mas com a vantagem de tornar mais fácil a localização dos problemas, já que se um dos cabos, uma das portas do concentrador ou uma das placas de rede estiver com problemas, apenas o nó ligado ao componente defeituoso ficará fora da rede. Por outro lado, o concentrador é o ponto vulnerável da rede.



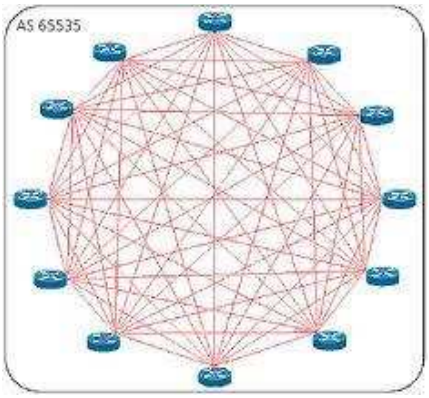
Topologia em estrela.

Árvore: A topologia em árvore é essencialmente uma série de barras interconectadas. Geralmente existe uma barra central onde outros ramos menores se conectam. Esta ligação é realizada através de derivadores e as conexões das estações realizadas do mesmo modo que no sistema de barra padrão.



Topologia em árvore.

Full Meshed: Todos os dispositivos replicam informações a todos. A rede é altamente confiável e altamente redundante.

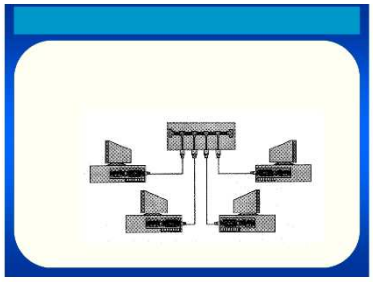


Topologia Full-Meshed.

COMPARAÇÃO ENTRE AS PRINCIPAIS TOPOLOGIAS DE REDE

TOPOLOGIA	VANTAGENS	DESVANTAGENS
PONTO A PONTO	Baixíssimo custo	Pequena e limitada
BARRAMENTO	Facilidade de instalação	Queda de qualidade com o acréscimo de novos usuários
ANEL	Performance equilibrada para todos os usuários	Baixa tolerância a falhas. A queda de um ponto paralisa toda a rede Dificuldade de localização do ponto de falha
ESTRELA	Fácil localização de problemas Facilidade de modificação da rede	O nó concentrador é um ponto vulnerável da rede Custos mais elevados que a topologia barramento
ÁRVORE	Facilidade de manutenção do sistema	Dependência do nó hierarquicamente superior
FULL MESHED	Altamente confiável	Altamente redundante (custos elevados)

PEGADINHA DO HUB! - O fato de um HUB concentrar todas as estações de uma rede e transmitir o pacote para todas elas permite caracterizar a existência simultânea de uma **topologia física** e uma **topologia lógica**. É neste ponto que quero chamar a sua atenção. Embora fisicamente o HUB mostre uma topologia **estrela**, na prática, o fluxo de dados ocorre como se a topologia fosse a de um **barramento**. O HUB é um "repetidor burro", e retransmite a todas as estações todos os dados que recebe. O roteador, esse sim operando em um nível mais elevado do modelo OSI, redireciona os dados recebidos apenas à estação de destino, funcionando logicamente também como uma topologia estrela.



HUB: aparência de estrela, funcionamento de barramento.

Se você não compreendeu essa ideia acerca do Modelo OSI, ou não sabe a diferença entre roteador e HUB, leia os próximos itens e volte nesta página, para retirar essa dúvida, tudo bem?

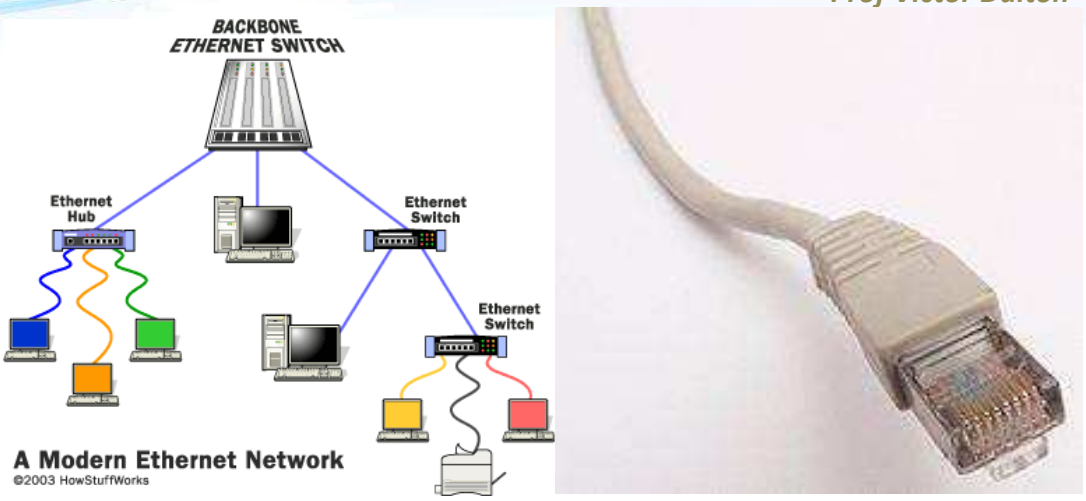
CAIU na prova!

(CESPE – TRE/GO – Técnico de Controle Externo – 2015) A topologia de uma rede refere-se ao leiaute físico e lógico e ao meio de conexão dos dispositivos na rede, ou seja, como estes estão conectados. Na topologia em anel, há um computador central chamado *token*, que é responsável por gerenciar a comunicação entre os nós.

Errado! Não existe nó central na rede em anel. O *token* é o "bastão" que circula entre as máquinas da rede, e quem possui o *token* em determinado momento é a máquina que pode enviar e receber dados.

1.7 *Ethernet* e Modelo OSI

Ethernet é uma tecnologia de interconexão para redes locais - Rede de Área Local (LAN) - baseada no envio de pacotes. Ela define cabeamento e sinais elétricos para a camada física, e formato de pacotes e protocolos para a camada de **controle de acesso ao meio** (Media Access Control - MAC) do modelo OSI. A Ethernet foi padronizada pelo IEEE como **802.3**.



A rede Ethernet e o famoso cabo Ethernet RJ-45 (quem nunca viu um cabo azul?)

Mas como uma máquina que roda Windows consegue trocar dados tanto com outra máquina Windows como com um servidor que roda Unix? Como um MSN em uma máquina rodando Windows troca mensagens com um Pidgin em uma máquina rodando Linux? Esta pergunta, que na verdade realça um aspecto de comunicabilidade que é válido para toda e qualquer informação trafegada na rede, é respondida pelos modelos de arquitetura de redes. Falemos primeiro do modelo OSI.

A Organização Internacional para a Normalização (do inglês: International Organization for Standardization - ISO), foi uma das primeiras organizações a definir formalmente uma arquitetura padrão com objetivo de facilitar o processo de interconectividade entre máquinas de diferentes fabricantes, assim em 1984 lançou o padrão chamado Interconexão de Sistemas Abertos (do inglês: Open Systems Interconnection - OSI) ou **Modelo OSI**.

O Modelo OSI permite comunicação entre máquinas heterogêneas e define diretivas genéricas para a construção de redes de computadores (seja de curta, média ou longa distância) independente da tecnologia utilizada.

Esta arquitetura é um modelo que divide as redes de computadores em 7 camadas, de forma a se obter camadas de abstração. Cada protocolo implementa uma funcionalidade assinalada a uma determinada camada.

A ISO costuma trabalhar em conjunto com outra organização, a União Internacional de Telecomunicações (do inglês: International Telecommunications Union - ITU), publicando uma série de especificações de protocolos baseados na arquitetura OSI. Estas séries são conhecidas

como 'X ponto', por causa do nome dos protocolos: X.25, X.500, etc. As camadas são:

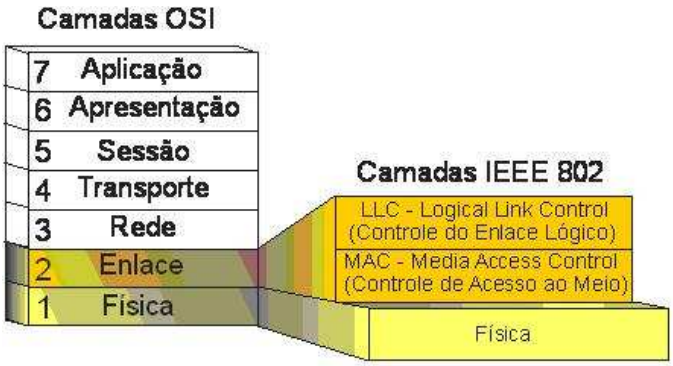
Modelo OSI.

Físico: A camada física trata da transmissão de **bits** brutos por um canal de comunicação. Nesse caso, as questões mais comuns são a voltagem a ser usada para representar um bit 1 e um bit 0, a quantidade de nanossegundos que um bit deve durar, o fato de a transmissão ser realizada ou não nos dois sentidos simultaneamente, a forma como a conexão inicial será estabelecida, etc.

Enlace: A principal tarefa da camada de enlace de dados é **transformar um canal de comunicação bruto em uma linha que pareça livre de erros de transmissão** não detectados para a camada de rede. Essa camada faz com que o transmissor divida os dados de entrada em quadros de dados (frames). Ainda, estabelece um protocolo de comunicação entre sistemas diretamente conectados, e estabelece controle de fluxo, por meio da medição do buffer do receptor no momento da transmissão, impedindo que uma quantidade excessiva de dados trave um receptor mais lento.

Cabe ainda destacar que a camada de **enlace de dados** subdivide-se em camada **MAC (Media Access Control – Controle de Acesso ao Meio)** e **LLC** (**Logical Link Control – Controle do Enlace Lógico**). Enquanto a camada MAC se preocupa com o endereçamento físico e com a conectividade ponto-a-ponto, a camada LLC "oculta" as diferenças entre os

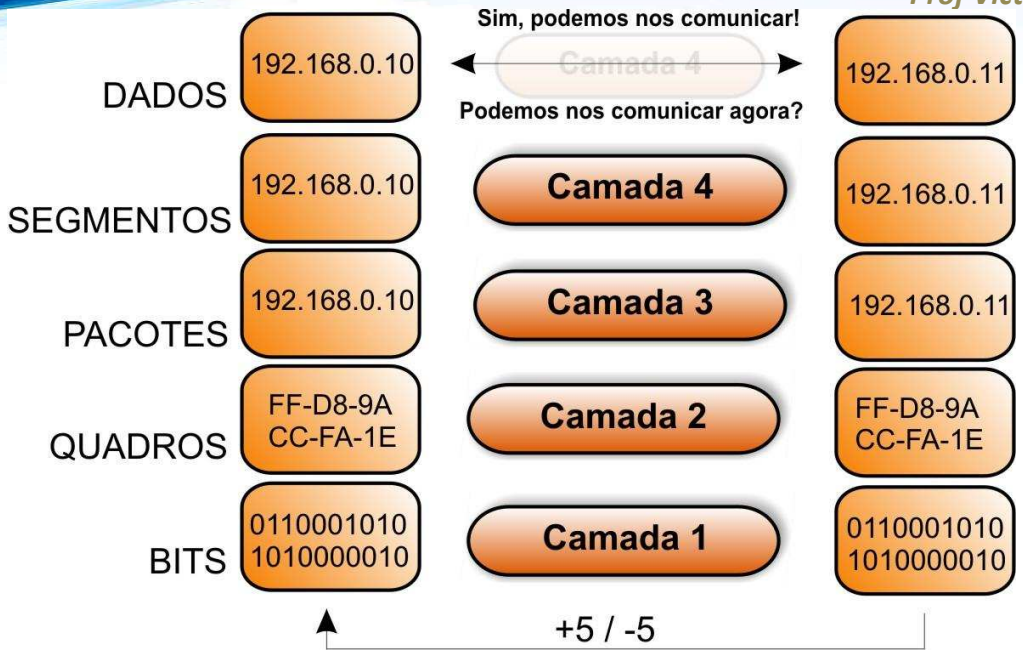
diversos tipos de redes 802, oferecendo à camada de rede um meio transparente (não importando se a conexão é via cabo azul, bluetooth, 3G, 4G ou WiFi, por exemplo).



Camadas MAC e LLC: ilustração

Rede: A camada de rede é responsável pelo **endereçamento dos pacotes de rede, também conhecidos por datagramas**, associando endereços lógicos (IP) em endereços físicos (MAC), de forma que os pacotes de rede consigam chegar corretamente ao destino. Essa camada também determina a rota que os pacotes irão seguir para atingir o destino, baseada em fatores como condições de tráfego da rede e prioridades. Falou-se em endereço IP, falou-se em camada de rede.

Transporte: A função básica da camada de transporte é **receber os dados da camada acima dela, dividi-los em unidades menores caso necessário (segmentos), repassar essas unidades à camada de rede e assegurar que todos os fragmentos chegarão corretamente à outra extremidade**. Na recepção, ela une os segmentos e encaminha à camada de Sessão. Realiza controle de fluxo, ordenação de pacotes e correção de erros, sendo considerada a primeira camada fim-a-fim.

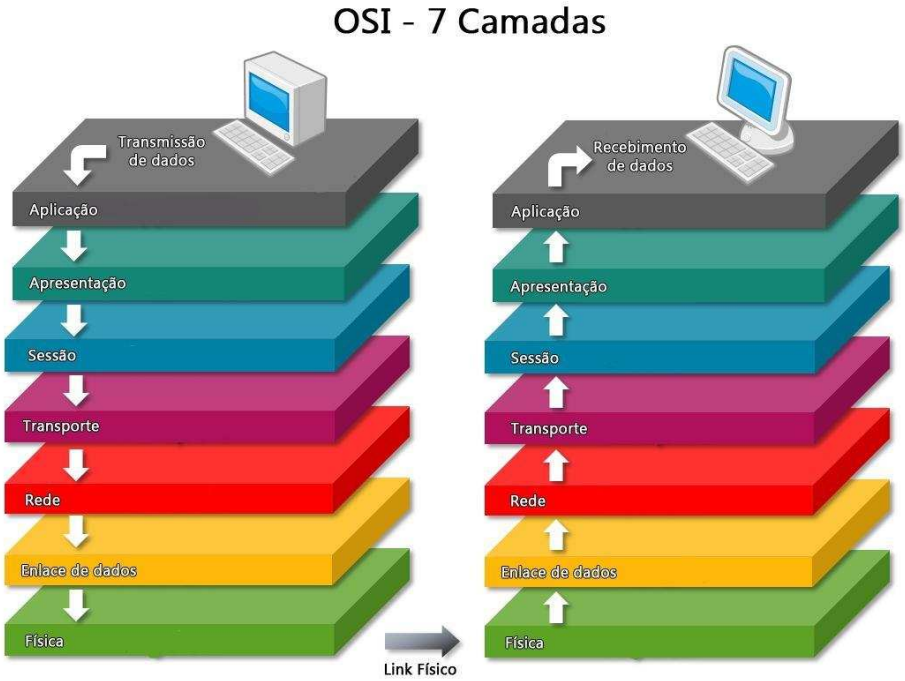


Sessão: A camada de sessão permite que os **usuários de diferentes máquinas estabeleçam sessões entre eles**. Uma sessão oferece diversos serviços, inclusive o controle de diálogo (mantendo o controle de quem deve transmitir em cada momento), o gerenciamento de token (impedindo que duas partes tentem executar a mesma tarefa crítica ao mesmo tempo) e a sincronização (realizando a verificação periódica de transmissões longas para permitir que elas continuem a partir do ponto em que estavam ao ocorrer uma falha). Ou seja, era por meio dela que o GetRight continuava seu download interrompido, na época que a internet era lenta (lembra?)

Apresentação: A camada de apresentação, ao invés de preocupar-se com a movimentação de bits, **preocupa-se com a sintaxe e a semântica das informações transmitidas**, para tornar possível a comunicação entre computadores com diferentes representações de dados. Dessa forma, seu computador usando MSN no Windows conversa com o seu colega que usa o Pidgin no Linux.

Aplicação: A camada de aplicação corresponde às aplicações (programas) no topo da camada OSI que serão utilizados para **promover uma interação entre a máquina destinatária e o usuário da aplicação**. Esta camada também disponibiliza os recursos (protocolo) para que tal comunicação aconteça. Por exemplo, ao solicitar a recepção de e-mail através do aplicativo de e-mail, este entrará em contato com a camada de Aplicação do protocolo de rede efetuando tal solicitação (POP3, IMAP). Tudo nesta camada é relacionado ao software. Alguns protocolos utilizados

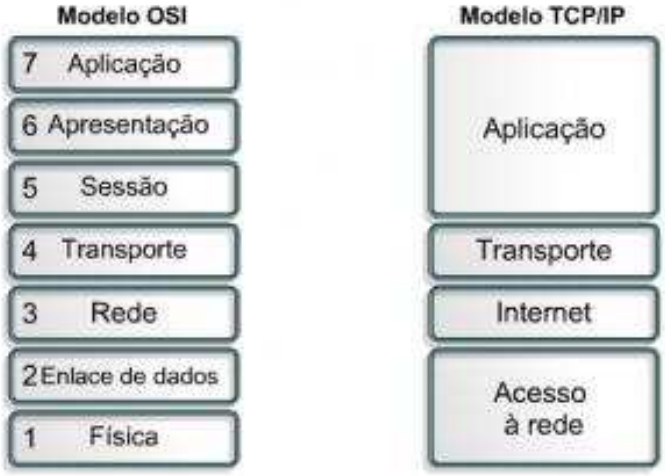
nesta camada são: HTTP, SMTP, FTP, SSH, Telnet, SIP, RDP, POP3, IMAP, enfim, os protocolos das camadas finais dos aplicativos.



Há quem use o famoso **FERTSAA** para decorar a sequência das camadas. Se servir para você, está valendo! ☺

1.8 Modelo OSI x Modelo TCP/IP

O modelo TCP/IP, por sua vez, possui pequenas diferenças em relação ao OSI:



Na camada **acesso à rede**, também conhecida como host/rede, o modelo TCP/IP não especifica nada. Apenas diz que o host deve se conectar ao meio físico utilizando um protocolo, a fim de que seja possível enviar pacotes IP. Este protocolo não é definido.

Quanto ao nível inter-rede (**internet**), seu objetivo é fazer com que pacotes enviados em um ponto da rede cheguem ao seu destino, independente de falhas em partes da rede. É possível que os pacotes cheguem ao destino em ordem diferente que partiram, obrigando as camadas superiores a reorganizar tudo.

O protocolo definido nessa camada para o modelo TCP/IP é o protocolo IP, e o roteamento é de grande importância aqui.

A camada de **transporte**, por sua vez, tem como objetivo permitir que os hosts de origem e destino conversem independente da distância, da mesma forma que o nível 4 do modelo OSI.

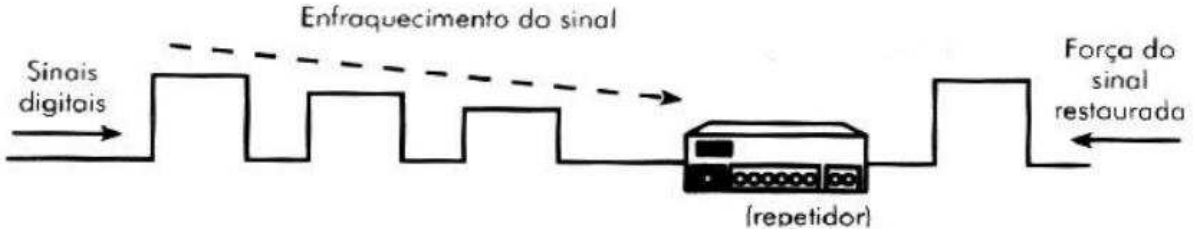
A camada de **aplicação**, por fim, contém os protocolos de alto nível, possuindo funções semelhantes às do nível de aplicação do modelo OSI.

Observação: alguns autores reconhecem a camada de **enlace** no modelo TCP/IP, criando uma espécie de "modelo híbrido". A única unaminidade entre os autores é a absorção das camadas de sessão e apresentação pela camada de aplicação.

1.9 Equipamentos de rede

Vejamos agora alguns equipamentos típicos de redes de computadores.

Repetidores – Como o nome diz, apenas repetem o sinal que recebem, servindo para leva-los a locais que o sinal não chegaria sem a utilização deste tipo de equipamento. Operam na camada 1 do modelo OSI. Não possui "inteligência", apenas oferecem o chamado "ganho" de sinal.

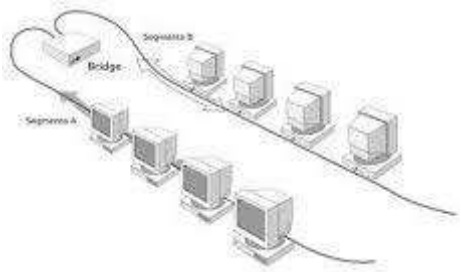


Ganho de sinal oferecido por repetidor: ilustração.

Hubs – antes dos roteadores domésticos, eram utilizados hubs. O hub é um repetidor local, sem amplificação do sinal (camada 1 do OSI). Funciona como um ponto concentrador de conexões.

Cabia às camadas superiores filtrar os dados recebidos para identificar a qual máquina conectada ao hub a informação pertencia. Típica utilização em redes do tipo "estrela".

Pontes – as *bridges* operam na camada 2 do modelo OSI. Basicamente, elas poderiam conectar duas ou mais LANs, e serem configuradas para deixar ou não o sinal passar ao "outro lado da ponte", analisando o endereço MAC de destino do quadro (frame).



Porém, hoje em dia, não faz sentido usar bridges para dividir a rede em segmentos por que os *switches* já desempenham essa função, essencialmente criando segmentos individuais para cada micro, o que praticamente elimina o problema das colisões, mas eles foram muito utilizados na época dos hubs burros.

Atualmente, o exemplo mais comum de bridge são os pontos de acesso wireless, que podem interligar os micros da rede cabeada aos micros conectados à rede wireless, criando uma única rede. Muitos pontos de

acesso incorporam também *switches* de 4 ou mais portas, ou até mesmo mini-roteadores, que permitem compartilhar a conexão entre os micros da rede local. Hoje em dia, dispositivos "tudo em um" são cada vez mais comuns, pois, com o avanço das técnicas de fabricação, tornou-se possível incluir cada vez mais circuitos em um único chip, fazendo com que um ponto de acesso "tudo em um" custe praticamente o mesmo que um ponto de acesso sem as funções extra.

Switches – também operante no nível 2 do modelo OSI, o *switch* também consegue ler o endereço MAC do frame. Entretanto, enquanto as pontes separam duas redes, o switch pode ser utilizado para redes estrela, direcionando ativamente o quadro para o endereço de destino(o que requer um buffer para evitar perda de informação). Diferentemente do HUB, não ocorrem colisões, uma vez que não ocorre disputa por meio de transmissão.

Switch

Roteador – opera no nível 3 do modelo OSI. É capaz de analisar o cabeçalho do pacote, e, segundo seus algoritmos, escolhe a rota mais adequada para encaminhá-lo.

Roteador. Quem nunca viu um desses?

CAIU na prova!

(CESPE - ANATEL – Analista – Tecnologia da Informação e Comunicação – 2014) Um repetidor regenera um sinal, interliga segmentos de uma LAN e não tem nenhum recurso de filtragem.

Correta. O repetidor opera no nível 1 do modelo OSI, apenas amplificando o sinal que recebe, sem nenhuma inteligência adicional.

1.10 Internet X Intranet X Extranet

A **Internet** conforme já dito anteriormente, é a rede mundial de computadores, composta por todos os computadores do mundo ligados em rede. Seu funcionamento é baseado na **Pilha de Protocolos TCP/IP**, cujos principais protocolos serão destacados mais adiante.

Protocolos Internet (TCP/IP)

Camada	Protocolo
5.Aplicação	HTTP, SMTP, FTP, SSH, Telnet, SIP, RDP, IRC, SNMP, NNTP, POP3, IMAP, BitTorrent, DNS, Ping ...
4.Transporte	TCP, UDP, RTP, SCTP, DCCP ...
3.Rede	IP (IPv4, IPv6) , ARP, RARP, ICMP, IPsec ...
2.Enlace	Ethernet, 802.11 WiFi, IEEE 802.1Q, 802.11g, HDLC, Token ring, FDDI, PPP,Switch ,Frame relay,
1.Física	Modem, RDIS, RS-232, EIA-422, RS-449, Bluetooth, USB, ...

Modelo híbrido entre o OSI e o TCP/IP. Representa, de maneira adequada, a pilha de protocolos do TCP/IP.

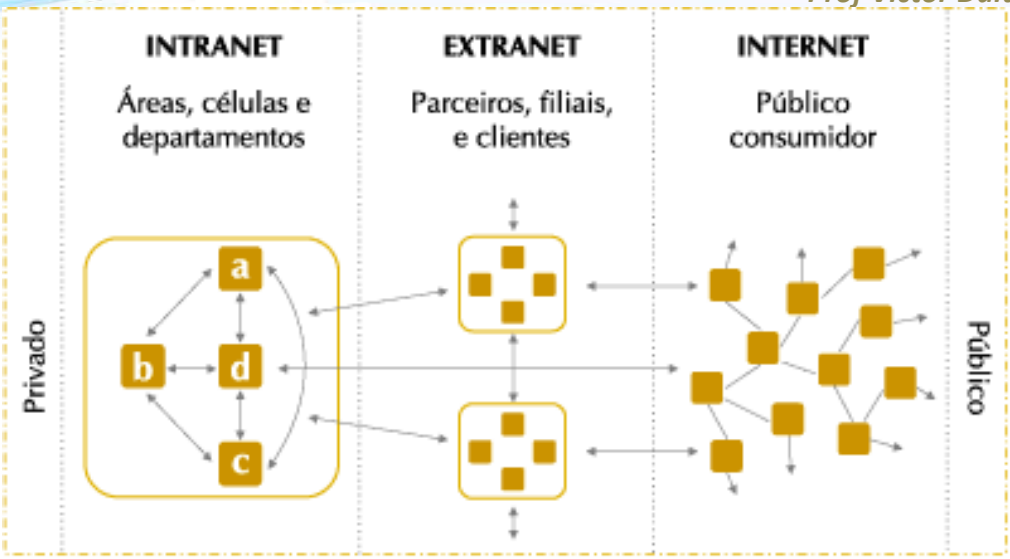
Para acessar a internet, é necessário um **provedor** de acesso à Internet, também conhecido como **ISP – Internet Service Provider.** Seja em uma organização, ou até mesmo para o acesso doméstico, é necessária a contratação de um provedor que irá interligar os dispositivos locais com os demais dispositivos pelo mundo. Nas residências, é comum a instalação de um **MODEM (Modulador-Demodulador)** que possibilita ao usuário o acesso à Internet, por meio de uma **banda de transmissão**, cuja velocidade é medida em **bits por segundo** (10Mbps, 30 Mbps...).

Ah: *cabe lembrar que as operadoras de telefonia celular, ao prover o acesso à Internet para os smartphones, realizam, efetivamente, o papel de ISPs aos seus clientes*.

Entretanto, é possível isolar um conjunto de computadores da Internet. É muito comum que empresas, universidades e órgãos públicos criem redes privadas, com as mesmas características da Internet, porém, isoladas da rede mundial, de modo que os serviços ofertados por esse conjunto de computadores fiquem restritos entre eles mesmos. São as chamadas **Intranets**. Se você já trabalhou em uma empresa ou órgão público com rede própria, sabe do que estou falando.

Contudo, essas mesmas instituições podem possibilitar o acesso às Intranets por computadores externos à Intranet, ou seja, via Internet. Às vezes, é conveniente ou necessário que usuários possam acessar determinados serviços da empresa remotamente, seja de casa, ou de um smartphone, ou em viagens de negócios. Ainda, para uma empresa, pode ser conveniente estender seus serviços internos a parceiros, fornecedores, filiais, ou clientes, com o objetivo de melhorar sua comunicação, mantendo-a restrita ao universo exterior.

Tal acesso é possibilitado pelo que chamados de **Extranet**. Via de regra, esse acesso é possibilitado mediante a utilização de login e senha, ou mesmo pela criação de um **Rede Privada Virtual**, pela qual o usuário recebe um endereço IP dentro da Intranet da empresa, mesmo estando fora dela.



Internet, Extranet e Intranet: ilustração

CAIU na prova!

(CESPE – SEDF – Técnico de Gestão Educacional – 2017) É correto conceituar intranet como uma rede de informações internas de uma organização, que tem como objetivo compartilhar dados e informações para os seus colaboradores, usuários devidamente autorizados a acessar essa rede.

Excelente descrição de Intranet. **Correto.**

1.11 Principais protocolos de rede

1.11.1 Protocolos da camada de Aplicação

HTTP: O **HyperText Transfer Protocol, ou Protocolo de Transferência de Hipertexto**, talvez seja o protocolo mais conhecido por todos. Afinal, o HTTP é o protocolo base para a comunicação na World Wide Web (www). É ele que transfere o conteúdo das páginas web para os navegadores (Browsers). Utiliza a porta **80**.

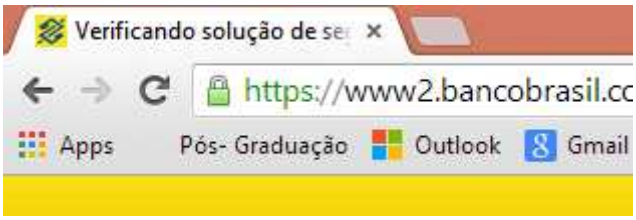
Aproveitando a abordagem dos navegadores, podemos destacar ainda o URL, **Uniform Resource Locator**, ou Localizador-Padrão de Recursos, que é o endereço de um recurso na web. Na prática, é o endereço que digitamos no navegador de Internet, no seguinte formato:

protocolo://domínio (ou máquina)/caminho/recurso

Por ser o mais utilizado na web, é comum que os endereços web iniciem com **http://**. Por convenção, a sequência **www** ainda é a mais utilizada no mundo para iniciar o endereço de uma máquina na Internet, embora já não seja mais obrigatória.

HTTPS: O **HyperText Transfer Protocol Secure** é a implementação do HTTP aliado a uma camada de segurança, criptografada, por meio da utilização do protocolo **SSL/TLS (Secure Sockets Layer/Transport Layer Security – Segurança da Camada de Transporte)**. O HTTPS, invariavelmente, é utilizado em endereços web que trafegam informações sensíveis, como senhas, dados bancários, dentre outros. Utiliza a porta **443**.

Os sites que utilizam https, além do nome do próprio protocolo, mostram um cadeado no seu navegador de Internet. Nos dias atuais, desconfie de *sites* que não utilizam https para o envio de senhas ou dados bancários.



Tela de login do site do Banco do Brasil. O cadeado verde aparece entes do endereço URL.

FTP: O **File Transfer Protocol**, ou Protocolo de Transferência de Arquivos, é um protocolo voltado exclusivamente para a transferência de dados pela web. Na época da internet discada, Quando as velocidades de acesso à web eram muito baixas, este protocolo era uma boa solução para transferência de arquivos em velocidades superiores ao protocolo HTTP, pois utiliza duas portas: a **20**, para a transferência propriamente dita dos arquivos, e a **21**, para controle da sessão. Nos dias atuais, embora ainda exista, perdeu importância, pois o HTTP tem atendido satisfatoriamente à atividade de transferir arquivos.

SMTP: O **Simple Mail Transfer Protocol**, ou Protocolo Simples de Transferência de Correio, é responsável apenas pelo **envio** de **email**. Utiliza a porta **25**, mas no Brasil está sendo substituída pela porta **587**, que impõe mecanismos de autenticação, para combater o envio de spam.

POP3: O **Post Office Protocol Version 3**, ou Protocolo de Agência de Correio, é utilizado para o **recebimento** de mensagens de **email**, transferindo a mensagem armazenada no servidor de email para a máquina do usuário. Utiliza a porta **110.** Foi o principal protocolo de email da era da internet discada, ainda é utilizado nos dias de hoje, mas tem perdido espaço para o protocolo seguinte.

IMAP: O **Internet Message Access Protocol**, ou Protocolo de Acesso à Mensagem da Internet, é o protocolo mais utilizado dentre os **webmails** modernos, que permitem que a mensagem seja lida sem transferi-la do servidor na qual se encontra. Dessa forma, você pode acessar o seu Gmail (por exemplo) da sua residência, do seu smartphone, ou de qualquer computador do mundo, e sua mensagem estará disponível para leitura.

1.11.2 Os Protocolos IP e DNS

IP: O Internet Protocol, pertencente à camada de **Rede (3)** do modelo OSI, é o protocolo responsável pelo endereçamento dos dados. O número de IP indica o endereço do destinatário do **pacote**.

O protocolo IP possui um esquema de endereçamento parecido com os números de telefone. Assim como qualquer telefone, no mundo todo, é único (considerando o DDD e o código de país), cada computador ligado na internet possui um número único, que é chamado de endereço IP ou número IP. Esse número serve para identificar o computador na internet. Se você precisar conversar com alguém pela internet, basta mandar mensagens endereçadas ao endereço IP do computador da pessoa.

Se você estiver em um computador com acesso à Internet, acesse http://meuip.datahouse.com.br/, e veja o seu endereço numérico no formato **nnn.nnn.nnn.nnn**. Este número identifica de maneira única o seu dispositivo **mundo**. Qualquer **pacote** (afinal, estamos na camada de Rede)

enviado pela Internet para este endereço chegará à sua máquina, caso esteja online.

No entanto, o protocolo IP em sua versão atual (a versão quatro, rotulada como IPv4) já é bastante antiga e tem muitos problemas. Os mais graves são falhas de segurança, que periodicamente são descobertas e não têm solução. A maioria dos ataques contra computadores hoje na internet só é possível devido a falhas no protocolo IP. A nova geração do protocolo IP, o **IPv6**, resolve grande parte dos problemas de segurança da internet hoje, herdados justamente do projeto antiquado do IPv4.

Mas o IPv4 tem um problema ainda mais premente do que sua inerente insegurança: já esgotou sua capacidade de expansão. Cada computador ligado à internet - seja um computador pessoal, uma estação de trabalho ou um servidor que hospeda um site - precisa de um endereço único que o identifique na rede. O IPv4 define, entre outras coisas importantes para a comunicação entre computadores, que o número IP tem uma extensão de 32 bits. **Cada grupo "nnn", conforme citado acima, pode assumir valores de 0 a 255, o que nos leva a 8 bits por grupo (2^8 = 256). 8 bits x 4 grupos = 32 bits**.

Com 32 bits, o IPv4 tem disponíveis em teoria cerca de quatro bilhões de endereços IP mas, na prática, o que está realmente disponível é menos da metade disso. Se contarmos que o planeta tem sete bilhões de habitantes e que cada dispositivo ligado na internet (o que inclui smartphones, PCs, notebooks e afins) precisa de um número só dele, é fácil perceber que a conta não fecha. Esse número, sendo finito, um dia acaba.

Em cima disso, os endereços IP são "travados" geograficamente. Dois endereços próximos estão necessariamente na mesma cidade ou região. Se considerarmos que cerca de três quartos dos endereços IP disponíveis para a internet estão localizados nos Estados Unidos (mesmo que nunca usados), sobram apenas pouco mais de um bilhão de endereços para o resto do mundo - aumentando ainda mais o problema de escassez.

A entrada de celulares e outros dispositivos móveis (que são baratos e extremamente populares) na internet contribuiu para que o número de endereços IP disponíveis seja ainda mais escasso.

O advento do **IPv6**, sexta versão do protocolo IP, resolverá todos esses problemas (assim se espera). Primeiro, porque dá fim a praticamente

todos os buracos de segurança conhecidos do IPv4, tornando as comunicações muitíssimo mais seguras. O IPv6 provavelmente será uma dor de cabeça sem tamanho para os hackers criminosos.

Em segundo lugar, o IPv6 define **128 bits** para endereçamento, e portanto conta com cerca de 3,4 × 10^38 endereços disponíveis (ou 340 seguido de 36 zeros). Para quem não quiser fazer a conta, basta saber que são muitos bilhões de quatrilhões de endereços disponíveis, garantindo que não vai faltar números IP para os humanos por milênios.

Um endereço IPv6 é representado por **8 blocos de 16 bits** cada um, separados pelo caracter dois pontos (:). Cada grupo de 16 bits, chamado de decahexateto ou duocteto, possui 4 símbolos hexadecimais que podem variar de 0000 a FFFF. Ou seja, são necessários **4bits (2^4 = 16)** para representar um número hexadecimal (cujos valores possíveis são 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F)

A escrita de cada endereço IPv6 é longa, o que dificulta a sua representação, com IPv6, o serviço de DNS que fornece um nome amigável a um computador será mais necessário do que nunca, simplesmente é impossível decorar os endereços v6 presentes numa infraestrutura de redes, como muitos profissionais de TI hoje o fazem com seus blocos IPv4.

Para facilitar sua representação, algumas regras de nomenclatura foram definidas:

1) **Zeros a esquerda em cada duocteto podem ser omitidos**

Assim, 2001:0DB8:00AD:000F:0000:0000:0000:0001 pode ser representado por:

2001:DB8:AD:F:0:0:0:1

2) **Blocos vazios contínuos podem ser representados pelos caracteres :: (quatro pontos) UMA ÚNICA VEZ dentro do endereço** (o que vem antes do primeiro dois pontos representa os primeiros bits e o que vem após o segundo dois pontos representa os ultimos bits do endereço).

Assim, 2001:0DB8:00AD:000F:0000:0000:0000:0001 pode ser representado por:

2001:DB8:AD:F::1

(CESPE – INSS – Técnico de Seguro Social – 2016) Na internet, os endereços IP (Internet Protocol) constituem recursos que podem ser utilizados para identificação de microcomputadores que acessam a rede.

Certo. O endereço IP pode ser utilizado para identificar computadores que acessam a rede.

(CESPE – TRE/GO – Técnico de Controle Externo – 2015) O endereço IPv6 tem 128 bits e é formado por dígitos hexadecimais (0-F) divididos em quatro grupos de 32 bits cada um.

Errado! Maldade da banca. O IPv6 realmente tem 128 bits, formado por dígitos hexadecimais, mas são divididos em **8 grupos** com quatro dígitos cada (16 bits por grupo).

DNS (***Domain Name System*** - Sistema de Nomes de Domínios)**:** o DNS é um sistema de gerenciamento de nomes hierárquico e distribuído operando segundo duas definições:

- Examinar e atualizar seu banco de dados.
- Resolver nomes de domínios em endereços de rede (IP).

O DNS funciona da seguinte maneira: para mapear um nome em um endereço IP, um programa aplicativo chama um procedimento de bilbioteca denominado RESOLVER e repassa a ele o nome como um parâmetro. O RESOLVER envia um pacote UDP a um servidor DNS local, que procura o nome e retorna o endereço IP ao RESOLVER. Em seguida, o resolvedor retorna o endereço IP ao programa aplicativo que fez a chamada. De posse do endereço IP, o programa pode então estabelecer uma conexão TCP com o destino ou enviar pacotes UDP até ele. **Em resumo: quando você digita www.estrategiaconcursos.com.br em seu navegador, o servidor**

DNS mais próximo de você descobre qual o endereço IP desse site (localização). Descoberto o endereço, o navegador então se comunica com esse endereço e baixa o conteúdo do site para você. No seu navegador aparece apenas o endereço "textual", mas, dentro da aplicação, é pelo endereço IP que o site é encontrado.

Normalmente, o servidor DNS utiliza a porta **53**. Apesar do relacionamento intrínseco com o protocolo IP, ele pertence à **camada de Aplicação** do modelo OSI. Ele foi posicionado intencionalmente próximo ao protocolo IP,

O servidor DNS secundário, por sua vez, é uma espécie de cópia de segurança do servidor DNS primário.

Sem o DNS, você teria que sair por aí decorando os endereços IP dos sites que gosta de visitar, e o pior, quando seus provedores modificassem seus IPs, teriam que dar um jeito de sair avisando pela Internet. Inviável, né? ☺

1.11.3 O Protocolo DHCP

O ***Dynamic Host Configuration Protocol***, ou Protocolo de Configuração Dinâmica de Cliente, é um protocolo que atribui dinamicamente endereços IP a máquinas de uma rede local.

Como ele faz isso?

Resumidamente, utilizando um modelo cliente-servidor, o DHCP faz o seguinte:

- Quando um cliente conecta-se a uma rede ele envia um pacote com um pedido de configurações DHCP.
- O servidor DHCP gerencia uma faixa fixa de IPs disponíveis juntamente com as informações e parâmetros necessários (gateway padrão, nome de domínio, DNS, etc).
- Quando este servidor recebe um pedido, ele entrega um destes endereços e configurações para o cliente.

Modos de Funcionamento

Ele pode operar de três formas: automática, dinâmica e manual.

Automática, no qual uma quantidade de endereços de IP (dentro de uma faixa) é definida para ser utilizada na rede. Neste caso, sempre que um dos computadores de uma rede solicitar a conexão com ela, um destes IPs será designado para a máquina em questão.

Na **dinâmica** o procedimento é bem parecido com o efetuado pela automática, porém a conexão do computador com determinado IP é limitada por um período de tempo pré-configurado que pode variar conforme desejado pelo administrador da rede.

No modo **manual** o DHCP aloca um endereço de IP conforme o valor de MAC (Medium Access Control) de cada placa de rede de forma que cada computador utilizará apenas este endereço de IP. Utiliza-se este recurso quando é necessário que uma máquina possua um endereço de IP fixo.

Não necessariamente um servidor precisa pertencer à rede para que o DHCP funcione. Roteadores domésticos e *Access Points* trabalham com DHCP, distribuindo os endereços IP dos dispositivos da sua casa. Se você possuir um roteador ou AP, experimente acessar as configurações dele, e veja se a atribuição de IPs que ele realiza não é via DHCP. ☺

1.11.4 Classes de Endereços IP

Um endereço IPv4 é formado por 32 bits, representados por quatro octetos na forma decimal (ex: 192.168.0.1). Uma parte desse endereço (bits mais significativos) indica-nos a rede e a outra parte (bits menos significativos) indica qual a máquina dentro da rede.

Com o objetivo de serem possíveis redes de diferentes dimensões, foram definidas cinco diferentes classes de endereços IP (Classes: A, B, C, D e E).

Originalmente, o espaço de endereçamento IP foi dividido estruturas de tamanho fixo designadas de "classes de endereço". As principais são a classe A, classe B e classe C. Com base nos primeiros bits (prefixo) de um endereço IP, conseguimos facilmente determinar a qual classe pertence determinado endereço IP.

Classe	Primeiro Octeto	Parte da rede (N) e parte para hosts (H)	Máscara	Nº Redes	Endereços por rede
A	1-127	N.H.H.H	255.0.0.0	**126** (2^7-2)	**16,777,214** (2^{24}-2)
B	128-191	N.N.H.H	255.255.0.0	**16,382** (2^{14}-2)	**65,534** (2^{16}-2)
C	192-223	N.N.N.H	255.255.255.0	**2,097,150** (2^{21}-2)	**254** (2^8-2)
D	224-239	Multicast	NA	NA	NA
E	240-255	experimental	NA	NA	NA

Analisando as três principais classes (A, B e C) podemos verificar o seguinte:

A **classe A** possui um conjunto de endereços que vão desde o **1.0.0.0 até 127.0.0.0**, onde o primeiro octeto (primeiros 8 bits **N.H.H.H**) de um endereço IP identifica a rede e os restantes 3 octetos (24 bits) irão identificar um determinado host nessa rede.

- Exemplo de um endereço Classe A – **120.2.1.0**

A **classe B** possui um conjunto de endereços que vão desde o **128.0.0.0 até 191.255.0.0**, onde os dois primeiros octetos (16 bits **N.N.H.H**) de um endereço IP identificam a rede e os restantes 2 octetos (16 bits) irão identificar um determinado host nessa rede.

- Exemplo de um endereço Classe B – **152.13.4.0**

A **classe C** possui um conjunto de endereços que vão desde o **192.0.0.0 até 223.255.255.0**, onde os três primeiros octetos (24 bits **N.N.N.H**) de um endereço IP identificam a rede e o restante octeto (8 bits) irão identificar um determinado host nessa rede.

- Exemplo de um endereço Classe C – **192.168.10.0**

1.11.5 O Protocolo NAT

Network Address Translation, ou NAT, é uma técnica que consiste em reescrever os endereços IP de origem de um pacote que passam por um roteador ou firewall de maneira que um computador de uma rede

interna tenha acesso externo à rede, com um endereço IP distinto do endereço utilizado dentro da rede (normalmente, o endereço IP do *gateway* é o endereço de todas as máquinas internas à rede).

Quem utiliza uma rede doméstica com roteador, ou utiliza uma máquina no trabalho com acesso à *web*, já deve ter notado que o endereço IP dá máquina da rede é diferente do endereço IP aos "olhos" da Internet, o que pode ser facilmente verificado em http://www.whatismyip.com/.

O NAT já foi uma primeira tentativa de reação face à previsão da exaustão do espaço de endereçamento IP, e rapidamente adaptada para redes privadas também por questões econômicas. Afinal, a contratação de serviços de Internet empresarial também pode ser cobrada por números de endereços IP que a empresa demanda.

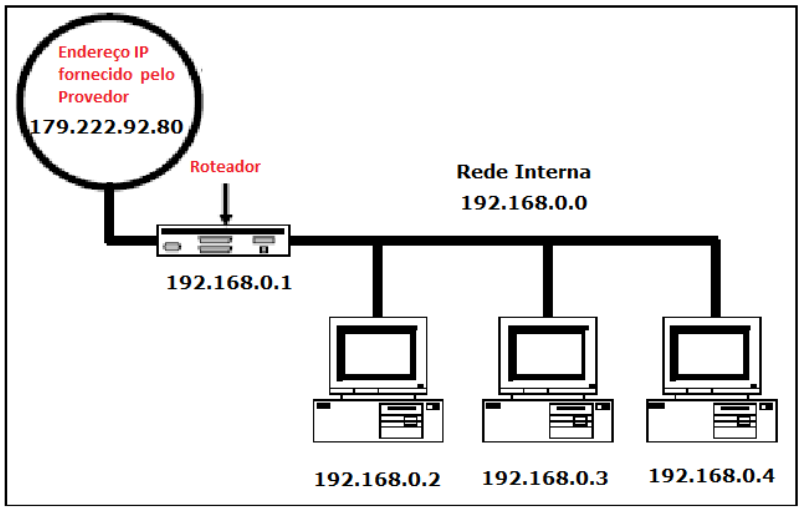
Para o NAT, três intervalos de endereços foram reservados. A saber:

10.0.0.0 a 10.255.255.255/8 – 16.777.216 hosts (classe A)

172.16.0.0 a 172.31.255.255/12 – 1.048.576 hosts (classe B)

192.168.0.0 a 192.168.255.255/16 – 65.536 hosts (classe C)

O último grupo de endereços é o mais comum em redes domésticas. Se você possui um roteador em sua casa, provavelmente já viu algum endereço parecido com 192.168.0.2 como endereço IP de sua máquina, 192.168.0.1 como endereço IP do seu roteador, e 192.168.0.3 sendo o endereço IP do seu notebook. Mas, se o único endereço IP que seu provedor de Internet lhe forneceu foi o 179.222.92.80 (por exemplo), e todos os seus aparelhos desfrutam da Internet simultaneamente, como é que o roteador faz as trocas de endereços IPs na ida e vinda dos dados?



Sempre que um pacote de saída entra no roteador, o endereço de origem 192.x.y.z é substituído pelo endereço IP verdadeiro da casa, fornecido pelo provedor de Internet (ISP – Internet Service Provider). Além disso, o campo Source port (Porta de Origem) do TCP é substituído por um índice para a tabela de conversão de 65.536 entradas da caixa NAT. Essa entrada de tabela contém a porta de origem e o endereço IP original.

Quando um pacote chega à caixa NAT vindo do ISP, o campo Source port do cabeçalho de TCP é extraído e usado como índice para a tabela de mapeamento da caixa NAT (desempenhado pelo roteador). A partir da entrada localizada, o endereço IP interno e o campo Source port do TCP original são extraídos e inseridos no pacote. O pacote é então repassado ao dispositivo de endereço 192.x.y.z.

1.11.6 O Protocolo ICMP

A operação da Internet é monitorada rigorosamente pelos roteadores. Quando ocorre algo inesperado, os eventos são reportados pelo **ICMP** (**Internet Control Message Protocol**), que também é usado para testar a Internet. Existe aproximadamente uma dezena de tipos de mensagens ICMP definidos. Os mais importantes estão listados abaixo. Cada tipo de mensagem ICMP é encapsulado em um pacote IP. Ou seja, este protocolo também pertence à camada de rede.

Tipo de mensagem	Descrição
Destination unreachable	Não foi possível entregar o pacote
Time exceeded	O campo Time to live chegou a 0
Parameter problem	Campo de cabeçalho inválido
Echo	Pergunta a uma máquina se ela está ativa
Echo reply	Sim, estou ativa
Timestamp request	Igual a Echo, mas com timbre de hora
Timestamp reply	Igual a Echo reply, mas com o timbre de hora

A mensagem DESTINATION UNREACHABLE é usada quando a sub-rede ou um roteador não consegue localizar o destino.

A mensagem TIME EXCEEDED é enviada quando um pacote é descartado porque seu contador chegou a zero. Esse evento é um sintoma de que os pacotes estão entrando em loop, de que há congestionamento ou de que estão sendo definidos valores muito baixos para o timer.

A mensagem PARAMETER PROBLEM indica que um valor inválido foi detectado em um campo de cabeçalho. Esse problema indica a existência de um bug no software IP do host transmissor ou, possivelmente, no software de um roteador pelo qual o pacote transitou.

A mensagem REDIRECT é usada quando um roteador percebe que o pacote pode ter sido roteado incorretamente. Ela é usada pelo roteador para informar ao host transmissor o provável erro.

As mensagens ECHO e ECHO REPLY são usadas para verificar se um determinado destino está ativo e acessível. Ao receber a mensagem ECHO, o destino deve enviar de volta uma mensagem ECHO REPLY. As mensagens TIMESTAMP REQUEST e TIMESTAMP REPLY são semelhantes, exceto pelo fato de o tempo de chegada da mensagem e o tempo de saída da resposta serem registrados na mensagem de resposta. Esse recurso é usado para medir o desempenho da rede.

1.11.7 O Protocolo Telnet

O **TELNET** é, ao mesmo tempo, um protocolo da camada de aplicação e um programa que permite a um usuário estabelecer uma sessão remota em um servidor. O protocolo oferece suporte somente a terminais alfanuméricos, ou seja, ele não oferece suporte a mouses e outros dispositivos apontadores nem oferece suporte a interfaces gráficas do

usuário. Em vez disso, todos os comandos devem ser digitados na linha de comando.

O protocolo Telnet **oferece muito pouca segurança**. Em uma sessão Telnet que não usa autenticação NTLM, todos os dados, incluindo senhas, são transmitidos entre o cliente e o servidor em texto sem formatação. Por causa dessa limitação e das recomendações gerais relacionadas ao acesso de usuários não confiáveis a servidores de segurança crítica, não se recomenda executar o servidor Telnet em computadores que armazenam dados confidenciais.

1.11.8 O Protocolo SSH

Como resposta ao TELNET, surgiu o **Secure Shell – SSH.** O SSH possui as mesmas funcionalidades do TELNET, com a vantagem da criptografia na conexão entre o cliente e o servidor.

É comum estabelecer **redes privadas virtuais** (VPNs) com SSH. Mas VPN é um assunto mais aprofundado em Segurança da Informação.

(CESPE – DPU – Agente Administrativo – 2016) Os protocolos de comunicação SSH e TELNET garantem comunicação segura, uma vez que os dados são criptografados antes de serem enviados.

Apenas SSH possui criptografia. Portanto, a questão realmente está **Errada**.

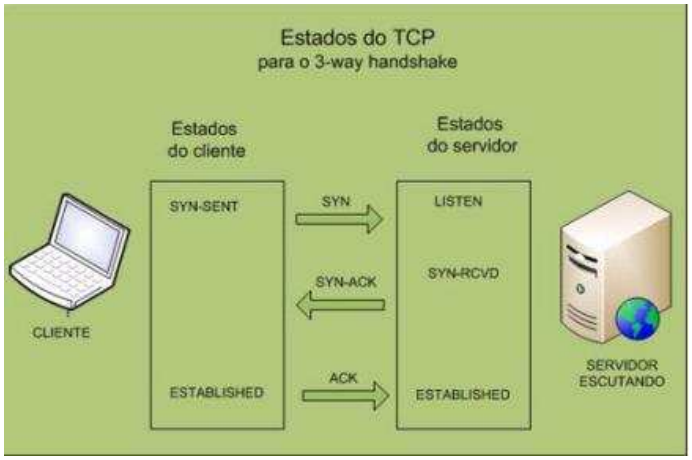
1.12 Os Protocolos TCP e UDP (camada de transporte)

O protocolo padrão da camada de rede é o IP (Internet Protocol). Ele não garante uma série de coisas que são desejáveis na transmissão de dados. Segundo o IP, pacotes podem ser entregues fora de ordem, podem ser perdidos ou duplicados. Tais situações devem, portanto, ser tratadas na camada de transporte.

Nesse conexto, entra em ação o **TCP.** O **Transmission Control Protocol**, ou Protocolo de Controle de Transmissão, é um **protocolo orientado à conexão**, localizado na camada de **Transporte (4)** do modelo OSI. Sua principal tarefa é assegurar que mensagens de qualquer tamanho possam trafegar pela Internet, uma vez que ele é responsável por quebrar as mensagens em **segmentos**, para que possam trafegar pela rede. Por realizar **controle de fluxo**, ele se responsabiliza por retransmitir os segmentos que tenham extraviado na rede, para garantir que o destinatário receba todos os pacotes da mensagem original.

O TCP **garante a entrega ordenada de segmentos**, efetua retransmissão de segmentos quando necessário, implementa controle de congestionamento e possui semântica fim-a-fim, ou seja, ACKs enviados à origem pelo destinatário garantem que o ele recebeu o segmento. O TCP passa ao IP diversos parâmetros, como a precedência dos segmentos, o nível de atraso, a vazão, a confiabilidade e a segurança.

Nesse protocolo há o estabelecimento de conexão entre pares de portas, utilizando o chamado **three way handshake**.



Legenda:

ACK = *Acknowledgement* (Reconhecimento)
SYN = *Synchronize* (Sincronizar)

Basicamente, ao iniciar uma conexão a aplicação (**Parte 1**) envia um SYN com número de sequência = x (SEQ=x) à parte com a qual deseja se comunicar (**Parte 2**).

A outra parte, então, "aproveita" a comunicação para enviar também estabelecer a sua comunicação, enviando também um número de sequência = y (SEQ=y), e envia um ACK informando o número da próxima mensagem a ser aguardada (ACK=x+1).

Por fim, a **Parte 1** confirma o recebimento da **Parte 2** com ACK = y+1, e já pode iniciar o envio dos dados.

Por sua vez, o **UDP**, **User Datagram Protocol**, ou Protocolo de Datagramas de Usuário, também da camada de **Transporte** (**4**), é um protocolo **que não é orientado a conexões**, e que **não realiza controle de fluxo**. Desta forma, ele não se "preocupa" em garantir que as mensagens sejam entregues ao destinatário final. É muito utilizado em *streaming* de áudio e vídeo, uma vez que a perda de determinados **segmentos** pelo "caminho" não impede que a mensagem seja compreendida pelo destinatário.

Por fim, destaco que o UDP também é utilizado pelo **DNS**. A vantagem é que os servidores DNS não precisam estabelecer nenhuma conexão com os solicitantes de endereços. Ele recebe o pacote UDP com a requisição e o responde. Em caso de extravio do pacote (o que é raro), basta o solicitante pedir novamente.

EXERCÍCIOS COMENTADOS CESPE

1. (CESPE – SEDF – Técnico de Gestão Educacional – 2017) É correto conceituar intranet como uma rede de informações internas de uma organização, que tem como objetivo compartilhar dados e informações para os seus colaboradores, usuários devidamente autorizados a acessar essa rede.

Excelente descrição de Intranet. **Certa**.

2. (CESPE – SEDF – Técnico de Gestão Educacional – 2017) Embora exista uma série de ferramentas disponíveis na Internet para diversas finalidades, ainda não é possível extrair apenas o áudio de um vídeo armazenado na Internet, como, por exemplo, no Youtube. (http://www.youtube.com**)**

Não soa estranho que, em pleno 2017, ano desta questão, não exista uma ferramenta que não consiga extrair um áudio de um vídeo na Internet? Pois é, ferramentas como essa existem aos montes. Item **errado**.

3. (CESPE – SEDF – Técnico de Gestão Educacional – 2017) Embora os gerenciadores de downloads permitam que usuários baixem arquivos de forma rápida e confiável, essas ferramentas ainda não possuem recursos para que arquivos maiores que 100MB sejam baixados.

Não faz sentido um gerenciador de download conseguir baixar um arquivo de 99MB, mas "faltar recursos" para baixar um arquivo de 101MB. Item **errado**.

4. (CESPE – FUB – Nível Médio – 2016) Para conectar-se a uma rede wireless, um computador do tipo notebook deve estar conectado a algum tipo de receptor para o recebimento do sinal, como, por exemplo, um receptor integrado.

Ora, para um dispositivo conectar-se a uma rede sem fio, é necessário ter um equipamento *wireless*. No caso dos notebooks, eles costumam vir com um receptor integrado. **Certa**.

5. (CESPE – INSS – Técnico de Seguro Social – 2016) Na internet, os endereços IP (Internet Protocol) constituem recursos que podem ser utilizados para identificação de microcomputadores que acessam a rede.

O endereço IP pode ser utilizado para identificar computadores que acessam a rede. Na internet, cada dispositivo possui um endereço IP que o identifica na rede. **Certa**.

6. (CESPE – INSS – Analista – 2016) A área administrativa do INSS informou a todos os servidores públicos lotados nesse órgão que o acesso a determinado sistema de consulta de dados cadastrais seria disponibilizado por meio da Internet, em substituição ao acesso realizado somente por meio da intranet do órgão. Nessa situação, não haverá similaridade entre os sistemas de consulta, porque sistemas voltados para intranet, diferentemente dos voltados para Internet, não são compatíveis com o ambiente web.

A Intranet é um conjunto de serviços ANÁLOGO à Internet. OS sistemas de consulta, a princípio, podem ser idênticos. **Errada**.

7. (CESPE – DPU – Agente Administrativo – 2016) Os protocolos de comunicação SSH e TELNET garantem comunicação segura, uma vez que os dados são criptografados antes de serem enviados.

Apenas SSH possui criptografia. Portanto, a questão realmente está **Errada**.

8. (CESPE – DPU – Agente Administrativo – 2016) O principal protocolo que garante o funcionamento da Internet é o FTP, responsável por permitir a transferência de hipertexto e a navegação na Web.

O protocolo seria o **HTTP**. Questão visivelmente **errada**.

9. (CESPE – DPU – Analista – 2016) O TCP/IP, conjunto de protocolos criados no início do desenvolvimento da internet, foi substituído por protocolos modernos como o Wifi, que permitem a transmissão de dados por meio de redes sem fio.

Se os protocolos do TCP/IP tivessem sido substituídos, provavelmente não existiriam mais conexões com fio. O que, naturalmente, torna a questão **errada.**

10. (CESPE – TCU – Técnico de Controle Externo – 2015) Mesmo que seja uma rede privada de determinado órgão ou empresa destinada a compartilhar informações confidenciais, uma intranet poderá ser acessada por um computador remoto localizado na rede mundial de computadores, a Internet.

Por meio da Extranet é possível disponibilizar a intranet a computadores remotos localizados na Internet. **Correto.**

11. (CESPE – TRE/GO – Técnico de Controle Externo – 2015) A topologia de uma rede refere-se ao leiaute físico e lógico e ao meio de conexão dos dispositivos na rede, ou seja, como estes estão conectados. Na topologia em anel, há um computador central chamado *token*, que é responsável por gerenciar a comunicação entre os nós.

Não existe nó central na rede em anel. O *token* é o "bastão" que circula entre as máquinas da rede, e quem possui o *token* em determinado momento é a máquina que pode enviar e receber dados. **Errado!**

12. (CESPE – TRE/GO – Técnico de Controle Externo – 2015) O endereço IPv6 tem 128 bits e é formado por dígitos hexadecimais (0-F) divididos em quatro grupos de 32 bits cada um.

Maldade da banca. O IPv6 realmente tem 128 bits, formado por dígitos hexadecimais, mas são divididos em **8 grupos** com quatro dígitos cada (16 bits por grupo). **Errado!**

13. (CESPE – STJ – Técnico Judiciário – 2015) A topologia física de uma rede representa a forma como os computadores estão nela interligados, levando em consideração os tipos de computadores envolvidos. Quanto a essa topologia, as redes são classificadas em homogêneas e heterogêneas.

Topologias físicas de rede são: anel, estrela, barramento, ponto-a-ponto... não existem topologias homogêneas e heterogêneas. **Errado!**

14. (CESPE – FUB – Conhecimentos Básicos – 2015) O cabo coaxial, meio físico de comunicação, é resistente à água e a outras

substâncias corrosivas, apresenta largura de banda muito maior que um par trançado, realiza conexões entre pontos a quilômetros de distância e é imune a ruídos elétricos.

Saber informações sobre o cabo coaxial pode ser um exagero, mas existem tantos erros na sentença que basta encontrar um para acertar a questão.

O cabo coaxial:

1 – Não é resistente a substancias corrosivas;

2 – Não apresenta largura de banda muito maior do que o par trançado (alguns cabos de rede podem alcançar 10Gbps);

3 – Não pode ser lançado por quilômetros, variando entre 100 e 500 metros (no máximo);

4 – Não é imune a ruídos elétricos (apenas a fibra ótica é imune).

Resposta: **Errado!**

15. (CESPE – TJDFT – Analista Judiciário – 2015) Uma virtual private network é um tipo de rede privada dedicada exclusivamente para o tráfego de dados seguros e que precisa estar segregada dos backbones públicos da Internet. Em outras palavras, ela dispensa a infraestrutura das redes comuns.

Uma rede privada virtual é uma rede privativa "tunelada" dentro da própria internet. Ou seja, essa rede não está segregada da internet. Pelo contrário, utiliza a mesma estrutura das redes comuns. Porém, seu acesso é **exclusivo** aos integrantes da VPN. **Errado.**

16. (CESPE – TJDFT – Técnico Judiciário – 2015) Deep Web é o conjunto de conteúdos da Internet não acessível diretamente por sítios de busca, o que inclui, por exemplo, documentos

hospedados em sítios que exigem login e senha. A origem e a proposta original da Deep Web são legítimas, afinal nem todo material deve ser acessado por qualquer usuário. O problema é que, longe da vigilância pública, essa enorme área secreta foi tomada pelo desregramento, e está repleta de atividades ilegais.

Essa definição foi copiada do Mundo Estranho (**confira aqui**), e está correta. Daí a importância de manter nossa "cultura geral" de informática em dia. **Correto.**

17. (CESPE - ANTAQ – Analista – Infraestrutura de TI – 2014) O padrão Fast Ethernet permitiu um aumento na velocidade de transmissão de dados nas redes locais para até 1.000 Mbps.

Fast Ethernet vai até 100Mbps. O padrão de 1000Mbps é o *Gigabit Ethernet*. **Errada!**

18. (CESPE - ANATEL – Analista – Suporte e Infraestrutura de TI – 2014) Na estrutura hierárquica de funcionamento do serviço DNS, ao receber uma requisição para resolução de nome, o servidor local de nomes DNS verifica se o nome está no cache DNS local ou se consta do seu banco de dados. Se o encontrar, retorna o endereço IP correspondente ao solicitante; caso contrário, o servidor DNS local repassa a consulta a um servidor DNS de nível mais alto.

E assim sucede até que um servidor DNS seja capaz de responder a requisição, ou então o domínio será identificado como inválido. **Correta.**

19. (CESPE - ANATEL – Analista – Tecnologia da Informação e Comunicação – 2014) Um repetidor regenera um sinal, interliga segmentos de uma LAN e não tem nenhum recurso de filtragem.

O repetidor opera no nível 1 do modelo OSI, apenas amplificando o sinal que recebe, sem nenhuma inteligência adicional. **Correta.**

20. (CESPE – TELEBRÁS – Especialista em Gestão de Telecomunicações – Analista Superior/Subatividade Comercial - 2013) TCP/IP (Transmission Control Protocol/Internet Protocol) é o conjunto de protocolos projetados para controlar a transmissão e a recepção de dados entre diferentes redes, independentemente dos tipos de máquinas e de sistemas operacionais utilizados.

A pilha de protocolos TCP/IP permite que computadores com Mac, Windows ou Linux, ou smartphones se comuniquem via rede de forma transparente. Ainda, não importando se estão em uma rede com ou sem fio, ou via 3G... **Correto.**

21. (CESPE – TJDFT – Técnico Judiciário Área Administrativa - 2013) Uma URL contém o nome do protocolo utilizado para transmitir a informação ou arquivo e informações de localização da máquina onde esteja armazenada uma página web.

É o **http, https**, ou **ftp**, que antecede o endereço web. **Certo.**

22. (CESPE – Polícia Federal – Perito - 2013) Considere que um usuário necessite utilizar diferentes dispositivos computacionais, permanentemente conectados à Internet, que utilizem diferentes clientes de email, como o Outlook Express e Mozilla Thunderbird. Nessa situação, o usuário deverá optar pelo uso do protocolo IMAP (Internet Message Access Protocol), em detrimento do POP3 (post office protocol), pois isso permitirá a ele manter o conjunto de emails no servidor remoto ou, alternativamente, fazer o download das mensagens para o computador em uso.

O IMAP permite ambas as opções (download ou manter no servidor remoto), bem como o acesso por diferentes clientes de email. O POP3 não oferece a alternativa de manter as mensagens no servidor remoto. **Correto.**

23. (CESPE – MPE/PI – Técnico Ministerial – Informática - 2011) A execução de programas em outros computadores da rede Internet, interagindo com os mesmos programas a partir de um computador pessoal é realizada através do serviço FTP.

O **File Transfer Protocol** é um protocolo orientado à transferência de arquivos. A execução de aplicações web ocorre via HTTP. **Errada!**

24. (CESPE – MPE/PI – Técnico Ministerial – Informática - 2011) WWW (world wide web) é um sistema de documentos de hipertexto ligados entre si e que são acessíveis através da Internet. Cada página WWW possui um endereço único, denominado http.

O endereço único que a questão se refere é o **IP**, ou **Internet Protocol**. O **HTTP**, ou **HyperText Transfer Protocol**, é o protocolo que interliga a Internet, permitindo a visualização de páginas pelos navegadores web. **Errada!**

25. (CESPE – MPE/PI – Técnico Ministerial – Informática - 2011) A Internet provê dois serviços a suas aplicações distribuídas: um serviço confiável, orientado para conexão, e um serviço não confiável, não orientado para conexão. Este último não oferece garantia alguma de entrega final dos dados no destino.

Esses serviços são o **TCP** e o **UDP**. O **Transmission Control Protocol** é o serviço orientado à conexão. É através dele, por exemplo, que uma página da internet ou um arquivo são "baixados" em um computador. O **User Datagram Protocol**, por sua vez, é não confiável. Ele é utilizado, principalmente, por aplicações que fazem streaming de áudio e vídeo. É por

isso que, ao utilizar um Skype, por exemplo, ocorrem falhas no áudio ou no vídeo. As falhas são dados que foram perdidos na transmissão dos dados. **Correta.**

26. (CESPE – MPE/PI – Técnico Ministerial – Informática - 2011) A intranet é uma rede de computadores que utiliza praticamente as mesmas tecnologias que são utilizadas na Internet, a principal diferença entre elas está no fato de que a intranet não permite utilizar todos os serviços de rede comuns na Internet, como o http e o FTP.

A diferença da internet pra intranet é que a **intranet** é restrita apenas a um determinado grupo de computadores, como, por exemplo, os computadores de uma empresa. A internet, por sua vez, é pública. **Errada!**

27. (CESPE – CNPQ – Cargo 1 - 2011) A intranet utiliza os protocolos da Internet, mas no âmbito interno de empresas, para que os empregados possam acessar remotamente dados e informações corporativas a partir de suas residências. O protocolo específico para transferência de arquivos na Internet, que deve ser configurado de forma diferenciado quando utilizado na intranet, é o IN-FTP (file transfer protocol-intranet).

Dentro da empresa, as máquinas podem acessar a intranet livremente. Quando em sua residência, para acessar a intranet da empresa, duas soluções podem ser adotadas. Ou cria-se uma **extranet**, que, na prática, significa oferecer um sistema de autenticação (login e senha) para que o usuário acesse a intranet, ou cria-se uma **VPN** (rede privada virtual), que é um aparato um pouco mais complexo. Na VPN, a máquina remota utiliza sistemas criptográficos para trafegar dados pela internet, e recebe um endereço IP dentro da intranet da empresa, utilizando a intranet como se estivesse "dentro da empresa". **Errado!**

28. (CESPE – CNPQ – Cargo 1 - 2011) Para acessar a Internet, utiliza-se o protocolo TCP/IP em conjunto com o

protocolo POP3, que possibilita a transferência de arquivos, autenticação de usuários e o gerenciamento de arquivos e diretórios.

A combinação correta é a do **TCP/IP** com o **HTTP**. **POP3** é um protocolo para recebimento de email pela internet. Diga-se de passagem, está caindo em desuso e sendo substituído pelo **IMAP (Internet Message Access Protocol)**, que é o protocolo adotado pelos e-mails web, como o Gmail. **Errado!**

29. (CESPE – EBC – Cargo 4 - 2011) Os usuários registrados em uma extranet podem acessar os aplicativos internos dessa rede por meio da utilização de smartphones, via browser.

Sendo disponibilizada a extranet, o usuário registrado precisará apenas fazer seu login. Portanto, poderá fazê-lo de qualquer computador ou dispositivo móvel, como um smartphone. **Correto.**

30. (CESPE – SEGER/ES – Todos os cargos - 2010) Caso o endereço que o usuário esteja acessando se inicie por ftp://, o navegador Internet Explorer usará o protocolo de transferência de arquivos ftp.

Correto.

31. (CESPE – Câmara dos Deputados 2012 – Analista Legislativo: Técnica Legislativa - 2012) A camada de enlace de uma rede de computadores consiste, tecnicamente, no meio físico por onde os dados trafegam. Esse meio pode ser constituído de fios de cobre ou fibra óptica.

O modelo OSI possui 7 camadas:

Modelo OSI.

O meio pelo qual os dados trafegam é a **camada física**. **Errado!**

32. (CESPE – Câmara dos Deputados 2012 – Analista Legislativo: Técnica Legislativa - 2012) Uma rede local (LAN — local area network) é caracterizada por abranger uma área geográfica, em teoria, ilimitada. O alcance físico dessa rede permite que os dados trafeguem com taxas acima de 100 Mbps.

Questão para lhe confundir. A velocidade dos dados em uma rede, seja lá qual for o seu tamanho, não possui relação com o alcance físico dessa rede, mas sim com as tecnologias empregadas. Tanto que é possível desfrutar da Internet com velocidades elevadas, como 100Mbps, por meio de provedores de Internet com fibra ótica. **Errado!**

33. (CESPE – Câmara dos Deputados 2012 – Analista Legislativo: Técnica Legislativa - 2012) O TCP/IP, pilha de protocolos na qual a Internet funciona, é dividido em camadas específicas, cada uma com características próprias. Por meio do TCP/IP, é possível, em conjunto com as aplicações, navegar na Internet e enviar correio eletrônico.

O TCP/IP possui uma pilha de protocolos que viabiliza a utilização da Internet como a conhecemos.

Protocolos Internet (TCP/IP)

Camada	Protocolo
5.Aplicação	HTTP, SMTP, FTP, SSH, Telnet, SIP, RDP, IRC, SNMP, NNTP, POP3, IMAP, BitTorrent, DNS, Ping ...
4.Transporte	TCP, UDP, RTP, SCTP, DCCP ...
3.Rede	IP (IPv4, IPv6) , ARP, RARP, ICMP, IPsec ...
2.Enlace	Ethernet, 802.11 WiFi, IEEE 802.1Q, 802.11g, HDLC, Token ring, FDDI, PPP,Switch ,Frame relay,
1.Física	Modem, RDIS, RS-232, EIA-422, RS-449, Bluetooth, USB, ...

Modelo híbrido entre o OSI e o TCP/IP. Representa, de maneira adequada, a pilha de protocolos do TCP/IP.

Correto.

34. (CESPE – ANAC – Técnico em Regulação áreas 1,3 e 4 - 2012) URL (uniform resource locator) é um repositório de informações interligadas por diversos pontos espalhados ao redor do Mundo.

Uniform Resource Locator é o endereço de um recurso, ou, simplesmente, endereço web. Por exemplo, o endereço (ou a URL) do site do Estratégia é www.estrategiaconcursos.com.br. Não é um repositório.
Errado!

35. (CESPE – Hemobrás – Técnico de Informática - 2008) Na camada de transporte do TCP/IP, estão os protocolos TCP e UDP, sendo que o UDP é orientado a conexão e tem controle de fluxo.

O TCP é orientado a conexões e tem controle de fluxo. **Errado!**

CONSIDERAÇÕES FINAIS

E encerramos a parte de redes!

Embora seja um assunto demasiadamente técnico, considero de entendimento fundamental, para dar sedimentação ao usuário de computador atual, que vive conectado na Internet.

Espero revê-lo, como um aluno (a) efetivo (a).

Rumo à **PRF**!

Victor Dalton

LISTA DE EXERCÍCIOS CESPE

1. (CESPE – SEDF – Técnico de Gestão Educacional – 2017) É correto conceituar intranet como uma rede de informações internas de uma organização, que tem como objetivo compartilhar dados e informações para os seus colaboradores, usuários devidamente autorizados a acessar essa rede.

2. (CESPE – SEDF – Técnico de Gestão Educacional – 2017) Embora exista uma série de ferramentas disponíveis na Internet para diversas finalidades, ainda não é possível extrair apenas o áudio de um vídeo armazenado na Internet, como, por exemplo, no Youtube. (http://www.youtube.com**)**

3. (CESPE – SEDF – Técnico de Gestão Educacional – 2017) Embora os gerenciadores de downloads permitam que usuários baixem arquivos de forma rápida e confiável, essas ferramentas ainda não possuem recursos para que arquivos maiores que 100MB sejam baixados.

4. (CESPE – FUB – Nível Médio – 2016) Para conectar-se a uma rede wireless, um computador do tipo notebook deve estar conectado a algum tipo de receptor para o recebimento do sinal, como, por exemplo, um receptor integrado.

5. (CESPE – INSS – Técnico do Seguro Social – 2016) Na internet, os endereços IP (Internet Protocol) constituem recursos que podem ser utilizados para identificação de microcomputadores que acessam a rede.

6. (CESPE – INSS – Analista – 2016) A área administrativa do INSS informou a todos os servidores públicos lotados nesse órgão que o acesso a determinado sistema de consulta de dados cadastrais seria disponibilizado por meio da Internet, em substituição ao acesso realizado somente por meio da intranet do órgão. Nessa situação, não haverá similaridade entre os sistemas de consulta, porque sistemas voltados para intranet, diferentemente dos voltados para Internet, não são compatíveis com o ambiente web.

7. (CESPE – DPU – Agente Administrativo – 2016) Os protocolos de comunicação SSH e TELNET garantem comunicação segura, uma vez que os dados são criptografados antes de serem enviados.

8. (CESPE – DPU – Agente Administrativo – 2016) O principal protocolo que garante o funcionamento da Internet é o FTP, responsável por permitir a transferência de hipertexto e a navegação na Web.

9. (CESPE – DPU – Analista – 2016) O TCP/IP, conjunto de protocolos criados no início do desenvolvimento da internet, foi substituído por protocolos modernos como o Wifi, que permitem a transmissão de dados por meio de redes sem fio.

10. (CESPE – TCU – Técnico de Controle Externo – 2015) Mesmo que seja uma rede privada de determinado órgão ou empresa destinada a compartilhar informações confidenciais, uma intranet poderá ser acessada por um computador remoto localizado na rede mundial de computadores, a Internet.

11. (CESPE – TRE/GO – Técnico de Controle Externo – 2015) A topologia de uma rede refere-se ao leiaute físico e lógico e ao meio de conexão dos dispositivos na rede, ou seja, como estes

estão conectados. Na topologia em anel, há um computador central chamado *token*, que é responsável por gerenciar a comunicação entre os nós.

12. (CESPE – TRE/GO – Técnico de Controle Externo – 2015) O endereço IPv6 tem 128 bits e é formado por dígitos hexadecimais (0-F) divididos em quatro grupos de 32 bits cada um.

13. (CESPE – STJ – Técnico Judiciário – 2015) A topologia física de uma rede representa a forma como os computadores estão nela interligados, levando em consideração os tipos de computadores envolvidos. Quanto a essa topologia, as redes são classificadas em homogêneas e heterogêneas.

14. (CESPE – FUB – Conhecimentos Básicos – 2015) O cabo coaxial, meio físico de comunicação, é resistente à água e a outras substâncias corrosivas, apresenta largura de banda muito maior que um par trançado, realiza conexões entre pontos a quilômetros de distância e é imune a ruídos elétricos.

15. (CESPE – TJDFT – Analista Judiciário – 2015) Uma virtual private network é um tipo de rede privada dedicada exclusivamente para o tráfego de dados seguros e que precisa estar segregada dos backbones públicos da Internet. Em outras palavras, ela dispensa a infraestrutura das redes comuns.

16. (CESPE – TJDFT – Técnico Judiciário – 2015) Deep Web é o conjunto de conteúdos da Internet não acessível diretamente por sítios de busca, o que inclui, por exemplo, documentos hospedados em sítios que exigem login e senha. A origem e a proposta original da Deep Web são legítimas, afinal nem todo material deve ser acessado por qualquer usuário. O problema é que, longe da vigilância pública, essa enorme área secreta foi tomada pelo desregramento, e está repleta de atividades ilegais.

17. (CESPE - ANTAQ – Analista – Infraestrutura de TI – 2014) O padrão Fast Ethernet permitiu um aumento na velocidade de transmissão de dados nas redes locais para até 1.000 Mbps.

18. (CESPE - ANATEL – Analista – Suporte e Infraestrutura de TI – 2014) Na estrutura hierárquica de funcionamento do serviço DNS, ao receber uma requisição para resolução de nome, o servidor local de nomes DNS verifica se o nome está no cache DNS local ou se consta do seu banco de dados. Se o encontrar, retorna o endereço IP correspondente ao solicitante; caso contrário, o servidor DNS local repassa a consulta a um servidor DNS de nível mais alto.

19. (CESPE - ANATEL – Analista – Tecnologia da Informação e Comunicação – 2014) Um repetidor regenera um sinal, interliga segmentos de uma LAN e não tem nenhum recurso de filtragem.

20. (CESPE – TELEBRÁS – Especialista em Gestão de Telecomunicações – Analista Superior/Subatividade Comercial - 2013) TCP/IP (Transmission Control Protocol/Internet Protocol) é o conjunto de protocolos projetados para controlar a transmissão e a recepção de dados entre diferentes redes, independentemente dos tipos de máquinas e de sistemas operacionais utilizados.

21. (CESPE – TJDFT – Técnico Judiciário Área Administrativa - 2013) Uma URL contém o nome do protocolo utilizado para transmitir a informação ou arquivo e informações de localização da máquina onde esteja armazenada uma página web.

22. (CESPE – Polícia Federal – Perito - 2013) Considere que um usuário necessite utilizar diferentes dispositivos computacionais, permanentemente conectados à Internet, que utilizem diferentes clientes de email, como o Outlook Express e Mozilla Thunderbird. Nessa situação, o usuário deverá optar pelo uso do protocolo IMAP (Internet Message Access Protocol), em detrimento do POP3 (post office protocol), pois isso permitirá a ele manter o conjunto de emails no servidor remoto ou, alternativamente, fazer o download das mensagens para o computador em uso.

23. (CESPE – MPE/PI – Técnico Ministerial – Informática - 2011) A execução de programas em outros computadores da rede Internet, interagindo com os mesmos programas a partir de um computador pessoal é realizada através do serviço FTP.

24. (CESPE – MPE/PI – Técnico Ministerial – Informática - 2011) WWW (world wide web) é um sistema de documentos de hipertexto ligados entre si e que são acessíveis através da Internet. Cada página WWW possui um endereço único, denominado http.

25. (CESPE – MPE/PI – Técnico Ministerial – Informática - 2011) A Internet provê dois serviços a suas aplicações distribuídas: um serviço confiável, orientado para conexão, e um serviço não confiável, não orientado para conexão. Este último não oferece garantia alguma de entrega final dos dados no destino.

26. (CESPE – MPE/PI – Técnico Ministerial – Informática - 2011) A intranet é uma rede de computadores que utiliza praticamente as mesmas tecnologias que são utilizadas na Internet, a principal diferença entre elas está no fato de que a intranet não permite utilizar todos os serviços de rede comuns na Internet, como o http e o FTP.

27. (CESPE – CNPQ – Cargo 1 - 2011) A intranet utiliza os protocolos da Internet, mas no âmbito interno de empresas, para que os empregados possam acessar remotamente dados e informações corporativas a partir de suas residências. O protocolo específico para transferência de arquivos na Internet, que deve ser configurado de forma diferenciado quando utilizado na intranet, é o IN-FTP (file transfer protocol-intranet).

28. (CESPE – CNPQ – Cargo 1 - 2011) Para acessar a Internet, utiliza-se o protocolo TCP/IP em conjunto com o protocolo POP3, que possibilita a transferência de arquivos, autenticação de usuários e o gerenciamento de arquivos e diretórios.

29. (CESPE – EBC – Cargo 4 - 2011) Os usuários registrados em uma extranet podem acessar os aplicativos internos dessa rede por meio da utilização de smartphones, via browser.

30. (CESPE – SEGER/ES – Todos os cargos - 2010) Caso o endereço que o usuário esteja acessando se inicie por ftp://, o navegador Internet Explorer usará o protocolo de transferência de arquivos ftp.

31. (CESPE – Câmara dos Deputados 2012 – Analista Legislativo: Técnica Legislativa - 2012) A camada de enlace de uma rede de computadores consiste, tecnicamente, no meio físico por onde os dados trafegam. Esse meio pode ser constituído de fios de cobre ou fibra óptica.

32. (CESPE – Câmara dos Deputados 2012 – Analista Legislativo: Técnica Legislativa - 2012) Uma rede local (LAN — local area network) é caracterizada por abranger uma área geográfica, em teoria, ilimitada. O alcance físico dessa rede permite que os dados trafeguem com taxas acima de 100 Mbps.

33. (CESPE – Câmara dos Deputados 2012 – Analista Legislativo: Técnica Legislativa - 2012) O TCP/IP, pilha de protocolos na qual a Internet funciona, é dividido em camadas específicas, cada uma com características próprias. Por meio do TCP/IP, é possível, em conjunto com as aplicações, navegar na Internet e enviar correio eletrônico.

34. (CESPE – ANAC – Técnico em Regulação áreas 1,3 e 4 - 2012) URL (uniform resource locator) é um repositório de informações interligadas por diversos pontos espalhados ao redor do Mundo.

35. (CESPE – Hemobrás – Técnico de Informática - 2008) Na camada de transporte do TCP/IP, estão os protocolos TCP e UDP, sendo que o UDP é orientado a conexão e tem controle de fluxo.

GABARITO

1	C
2	E
3	E
4	C
5	C
6	E
7	E
8	E
9	E
10	C
11	E
12	E

13	E
14	E
15	E
16	C
17	E
18	C
19	C
20	C
21	C
22	C
23	E
24	E

25	C
26	E
27	E
28	E
29	C
30	C
31	E
32	E
33	C
34	E
35	E

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.