Estratégia Concursos

Aula 01

Informática p/ Ministério do Trabalho (Auditor Fiscal do Trabalho - AFT) - 2021 - Pré-Edital

Autor:

Diego Carvalho, Equipe Informática e TI, Renato da Costa

30 de Julho de 2020

Sumário

APRESENTAÇÃO DA AULA

Fala, galera! O assunto da nossa aula de hoje é **Protocolos de Comunicação**! Pessoal, não há como se falar em redes de computadores como a internet sem falar sobre protocolos de comunicação. Para utilizar a Internet, você precisará dos protocolos IP, TCP ou UDP; para utilizar um navegador, você precisará dos protocolos HTTP, HTTPS e DNS; para enviar/receber e-mail, você precisará dos protocolos SMTP, POP3 ou IMAP; e assim por diante...

PROFESSOR DIEGO CARVALHO - WWW.INSTAGRAM.COM/PROFESSORDIEGOCARVALHO

Galera, todos os tópicos da aula possuem Faixas de Incidência, que indicam se o assunto cai muito ou pouco em prova. *Diego, se cai pouco para que colocar em aula?* Cair pouco não significa que não cairá justamente na sua prova! A ideia aqui é: se você está com pouco tempo e precisa ver somente aquilo que cai mais, você pode filtrar pelas incidências média, alta e altíssima; se você tem tempo sobrando e quer ver tudo, vejam também as incidências baixas e baixíssimas. *Fechado?*

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

INCIDÊNCIA EM PROVA: BAIXA

INCIDÊNCIA EM PROVA: MÉDIA

INCIDÊNCIA EM PROVA: ALTA

INCIDÊNCIA EM PROVA: ALTÍSSIMA

PROTOCOLOS DE COMUNICAÇÃO

1 – Conceitos Básicos

INCIDÊNCIA EM PROVA: BAIXA

Existe um renomado autor – chamado Andrew Tanenbaum – que afirma que "*um protocolo é um acordo entre as partes que se comunicam, estabelecendo como se dará a comunicação*". Outro grande autor – chamado Behrouz Forouzan – declara que um "*protocolo é um conjunto de regras que controlam a comunicação de dados*". **Já esse que vos escreve – chamado Diego Carvalho – gosta de pensar em protocolos simplesmente como um idioma.**

De forma similar, ocorre no mundo dos computadores. **Hoje em dia, existe um conjunto de protocolos padrão da internet chamado TCP/IP – ele é como o inglês das máquinas!** Não importa se é um notebook, um tablet ou um computador, também não importa se utiliza Linux ou Windows ou se possui arquitetura x86 ou x64. Se estiver conectado à Internet, ele estará necessariamente utilizando o TCP/IP – independentemente de seu hardware ou software.

Galera, um aluno certa vez me questionou: *professor, e se eu quiser utilizar outro protocolo na rede da minha casa, eu não posso?* Eu respondi que não havia problema algum e que ele poderia fazer isso quando quisesse! **No entanto, para que a sua rede se comunicasse com a internet, ela necessariamente deveria utilizar o TCP/IP**. *Entendido?* Vamos exemplificar esses conceitos futuramente com algumas questões :)

2 – Modelo OSI/ISO

INCIDÊNCIA EM PROVA: MÉDIA

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

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

Nós sabemos que a comunicação entre dois computadores é extremamente complexa, logo esse modelo sugere dividir essa complexidade em uma estrutura de sete camadas distintas, porém relacionadas entre si, cada uma das quais definindo uma parte do processo de transferência de informações através de uma rede. Compreender esses conceitos é importante para entender posteriormente a função de cada protocolo. *Vem comigo... é legal! Eu juro...*

Na tabela seguinte, nós veremos a função de cada uma dessas camadas. Entenda que esse assunto não é muito relevante para a prova em si, uma vez que raramente cai alguma questão. **No entanto, eu considero interessante que vocês passem rapidamente por cada um desses pontos para que vocês entendam ao fim como cada camada dessas possui uma responsabilidade no envio e recebimento de dados entre um remetente e um destinatário.** Além disso, é possível mapear alguns protocolos que veremos mais à frente para cada uma dessas camadas apresentadas na imagem ao lado. É isso... *Fechado?* Então vamos lá...

CAMADA	DESCRIÇÃO	PROTOCOLOS
APLICAÇÃO [CAMADA 7]	Essa camada habilita o usuário, seja ele humano ou software, a estabelecer a comunicação entre aplicações e a acessar a rede. Ela fornece interface com o usuário e suporte a serviços como e-mail, acesso e transferência de arquivos remotos, gerenciamento de bancos de dados compartilhados e outros tipos de serviços de informação distribuídos. Ela funciona como um portal em que os processos de aplicações possam acessar uma rede.	HTTP, SMTP, FTP, SSH, TELNET, IRC, SNMP, POP3, IMAP, DNS.
APRESENTAÇÃO [CAMADA 6]	Essa camada é responsável por definir o formato para troca de dados entre computadores, como se fosse um tradutor. *Como assim, professor?* Ela é responsável pela formatação e tradução de protocolos, pela criptografia, pela compressão de dados, pela conversão de caracteres e códigos, entre diversas tantas funcionalidades. Essa camada pega um texto que está em binário (010101101111) e converte para o alfabeto latino, por exemplo.	AFP, ICA, LPP, NCP, NDR, TOX, XDR, PAD.
SESSÃO [CAMADA 5]	Essa camada é responsável por permitir que duas ou mais aplicações em computadores diferentes possam abrir, usar e fechar uma conexão, chamada sessão. Ela gerencia a comunicação para que, caso haja alguma interrupção, ela possa ser reiniciada do ponto da última marcação recebida. Diz-se que essa camada controla o diálogo da rede – estabelecendo, mantendo e sincronizando a interação entre sistemas que se comunicam.	NETBIOS
TRANSPORTE [CAMADA 4]	Essa camada é responsável por organizar os dados em segmentos e que eles cheguem ao destino livre de erros (sem perdas, sem duplicações e na ordem correta), independentemente do tipo, topologia ou configuração de rede. Para tal, ela fornece uma comunicação fim-a-fim ou ponta-aponta confiável (isto é, o nó de origem se comunica apenas com o nó de destino, sem reconhecer nós intermediários).	TCP, UDP, NETBEUI.
REDE [CAMADA 3]	Essa camada é responsável pelo endereçamento, roteamento e entrega de pacotes individuais de dados desde sua origem até o seu destino, provavelmente através de várias redes. Embora a camada de enlace coordene a entrega do pacote entre	IP, ICMP, ARP RARP, NAT.

	dois sistemas na mesma rede, a camada de rede garante que cada pacote seja transmitido de seu ponto de origem até seu destino final.	
ENLACE [CAMADA 2]	Essa camada é responsável por organizar os dados em frames (ou quadros) e por estabelecer uma conexão nó a nó[1] entre dois dispositivos físicos que compartilham o mesmo meio físico. Ela transforma a camada física, de um meio de transmissão bruto, em um link confiável, fazendo que a camada física pareça livre de erros para a camada superior (camada de rede) e garantindo assim que os dados sejam recebidos corretamente.	ETHERNET, TOKEN RING, BLUETOOTH, WI-FI.
FÍSICA [CAMADA 1]	Essa camada define as especificações elétricas e físicas da conexão de dados. Por exemplo: ela pode dizer como os pinos de um conector estarão posicionados, quais as tensões de operação de um cabo elétrico, as especificações do cabo de fibra ótica, a frequência dos dispositivos sem fio, entre outros. essa camada é totalmente orientada a hardware, não reconhecendo softwares.	USB, DSL.

Cada camada chama os dados que ela processa por um nome diferente. Quando estamos na camada física, tratamos de **bits**; quando estamos na camada de enlace, tratamos de **frames ou quadros**; quando estamos na camada de rede, tratamos de **pacotes**; quando estamos na camada de transporte, tratamos de **segmentos**; e quando estamos nas outras camadas, tratamos de **dados**. Vejam só abaixo:

CAMADA	UNIDADE DE DADOS DO PROTOCOLO (DPU)
FÍSICA	BITS
ENLACE	FRAMES/QUADROS
REDE	PACOTES
TRANSPORTE	SEGMENTOS
SESSÃO	DADOS/MENSAGENS
APRESENTAÇÃO	
APLICAÇÃO	

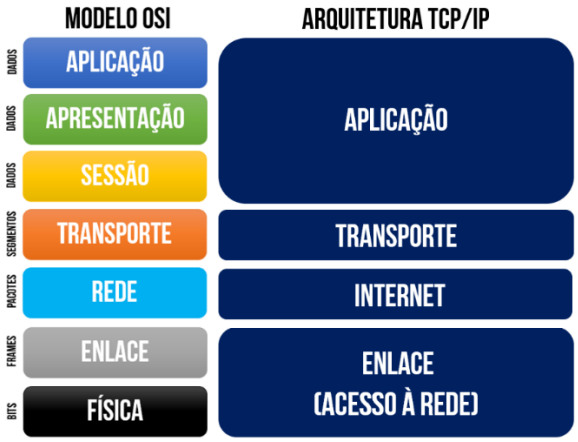
3 - Arquitetura TCP/IP

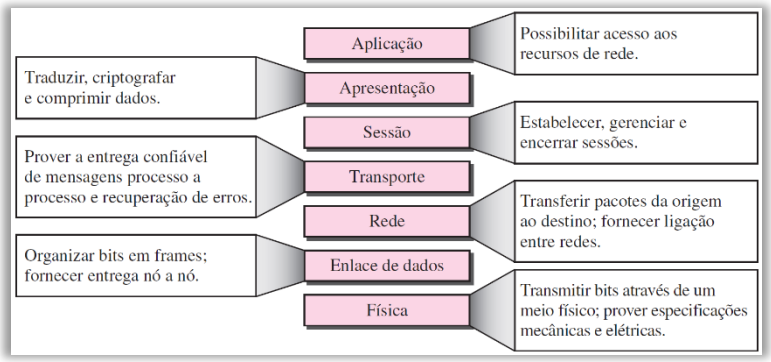
INCIDÊNCIA EM PROVA: ALTA

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

[1] Diferentemente da Camada de Transporte, a Camada de Enlace estabelece uma conexão ponto-a-ponto e, não, fim-a-fim. Em outras palavras, a Camada de Transporte estabelece uma conexão entre o emissor e o receptor; já a Camada de Enlace estabelece uma conexão entre cada nó intermediário no caminho entre emissor e receptor.

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





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

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

4 – Principais Protocolos

4.1 – IP (INTERNET PROTOCOL)

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Vamos explicar esse protocolo com várias analogias para que vocês consigam compreender. *O significa essa sigla?* Significa **Internet Protocol ou Protocolo de Internet**. *Vamos traduzir também Internet?* **Inter** significa *entre* e **net** significa *rede*, logo Internet significa *entre redes*. Agora vamos juntar tudo isso e dar um significado! IP é um protocolo – um conjunto de normas, padrões e convenções – para comunicação entre redes. Opa... já começou a ficar mais claro!

Pode-se afirmar que IP é o protocolo de distribuição de pacotes não confiável, de melhor esforço e sem conexão, que forma a base da internet. *O que significam esses conceitos?*

Galera, se nós fôssemos fazer uma analogia, o IP seria como o motorista dos Correios. **Ele é aquele cara que já dirigiu pelo Brasil inteiro e conhece as melhores rodovias e rotas para entregar os pacotes aos seus destinatários.** Esse cara é muito gente fina e vai tentar fazer o máximo possível para realizar a entrega, mas infelizmente ele não consegue garantir que ela ocorrerá.

Imaginem que futuramente ocorra uma outra greve dos caminhoneiros! Pode acontecer de o nosso motorista (IP) tentar passar por uma rota, mas ela estar bloqueada. Pode ser que ele tente outra rota, mas ela também pode estar bloqueada. Nesse caso, ele infelizmente pode atrasar a entrega dos pacotes! Pode acontecer pior que isso: imagine que o caminhão seja assaltado e ladrões levem todos os pacotes. Nesse caso, ele também não conseguirá entregar os pacotes!

Dessa forma, por mais que ele se esforce (e ele é esforçado), ele não é capaz de garantir que a entrega será realizada. Por conta disso, ele é um protocolo não confiável, mas é de melhor esforço (*best-effort*). *E por que ele é um protocolo sem conexão?* Esse eu vou explicar no próximo tópico, quando estivermos falando sobre o TCP! Vamos continuar... antigamente, para enviar uma informação a outra pessoa, eu utilizava o serviço de correspondências.

Eu pegava um pedaço de papel, escrevia diversas informações, colocava dentro de um envelope com endereço de origem e endereço de destino. Na internet, ocorre de maneira bastante similar: **as informações que eu desejo transmitir são encapsuladas dentro de um envelope chamado Pacote IP** que contém necessariamente um endereço IP de origem e um endereço IP de destino. Além disso, eu posso colocar outras informações acessórias no meu envelope (pacote IP)!

Eu posso carimbar esse envelope como confidencial; posso informar o tipo de conteúdo do envelope (arquivo, e-mail, áudio, etc). **Dessa forma, o pacote IP é formado por dados que eu queira enviar e por um cabeçalho contendo informações técnicas que facilitam a entrega**. Agora

uma pergunta: *eu posso enviar um processo com 50.000 páginas pelos Correios?* Posso! No entanto, os Correios não vão conseguir colocar 50.000 páginas dentro de um único envelope!

Os Correios impõem um tamanho limite para o pacote que ele é capaz de transportar, da mesma forma que existe um tamanho limite para o pacote IP. *E qual é o tamanho, Diego?* **Esse limite é de 64 Kb!** *Caraca, professor... por que tão pequeno?* Galera, quando a internet foi criada, isso era uma quantidade absurda de informação. Vejam essa imagem ao lado: isso é um HD de 1960 capaz de armazenar estrondosos 5 Mb de informação. *Incrível, não?* Claro que não é mais assim hoje em dia. Uma foto tirada pelo celular possui cerca de 6.4 Mb (= 6400 Kb). *E se eu quiser enviar essa foto para outra pessoa, caberá tudo em um pacote?* Jamais! **O IP terá que dividir a foto em pacotes de 64 Kb**. Como 6400 Kb dividido por 64 Kb é 100, teremos que dividir a foto em 100 pacotinhos e enviá-los um a um.

O endereço IP define de forma única e universal a conexão de um dispositivo (Ex: um computador ou um roteador). Eles são exclusivos no sentido de que cada endereço define uma única conexão com a Internet – dois dispositivos jamais podem ter o mesmo endereço ao mesmo tempo. Além disso, eles são universais no sentido de que o sistema de endereçamento tem de ser aceito por qualquer host que queira se conectar à Internet.

Esses são – portanto – os fundamentos básicos desse protocolo. Agora vamos falar um pouquinho sobre endereçamento e versões. Pessoal, nós dissemos várias vezes durante a aula que os computadores de uma rede possuem um endereço lógico chamado Endereço IP. **Da mesma forma que um carteiro precisa saber o CEP de uma casa, o protocolo IP precisa saber o endereço IP de uma máquina para entregar os dados destinados a ela.**

E como é esse endereço? Galera, há duas notações predominantes de endereço IP: **Octetos Binários ou Decimal Pontuada.** Antes de prosseguir, vamos falar um pouco sobre numeração...

ESCLARECENDO!

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

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

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

ENDEREÇO IP COM NOTAÇÃO DE OCTETOS BINÁRIOS			
10101010	01010101	11100111	10111101

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

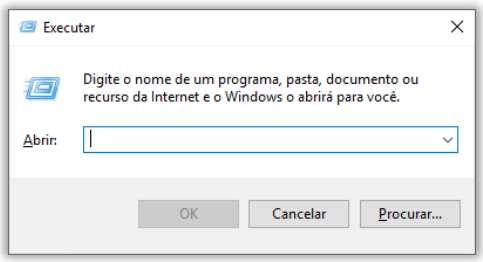
ENDEREÇO IP COM NOTAÇÃO DECIMAL PONTUADA						
170	.	85	.	231	.	189

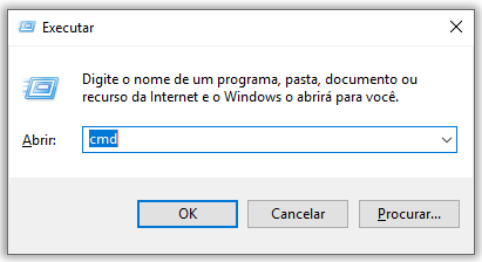
(PC/SP – 2017) Assinale a sequência numérica abaixo que pode representar o Endereço IP (Internet Protocol) válido de um microcomputador em uma rede:

a) 10.260.25.200
b) 10.35.29.129
c) 10.0.40.290
d) 10.0.290.129
e) 10.35.260.290

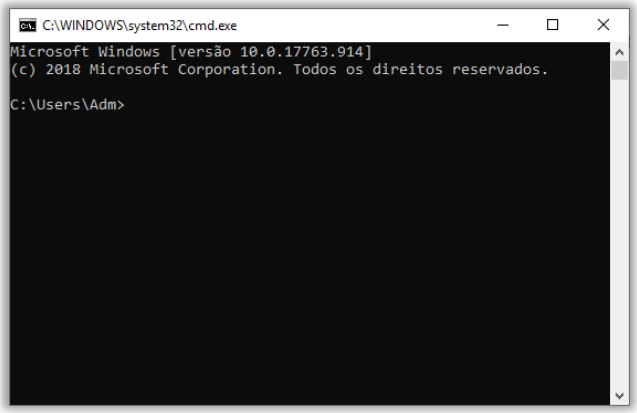
Comentários: conforme vimos em aula, ele varia de 0 a 255. O octeto binário 00000000 é 0 em decimal e o octeto binário 11111111 é 255 em decimal. (a) Errado, 260 > 255; (b) Correto; (c) 290 > 255; (d) 290 > 255; (e) 260 e 290 > 255 (Letra B).

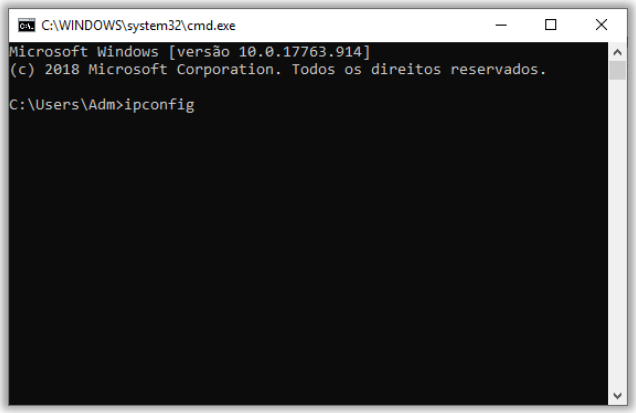
Professor, está tudo muito abstrato! Você pode dar um exemplo? Claro! Para tal, eu vou propor um exercício para vocês: eu quero que vocês pressionem simultaneamente as teclas Windows + R.



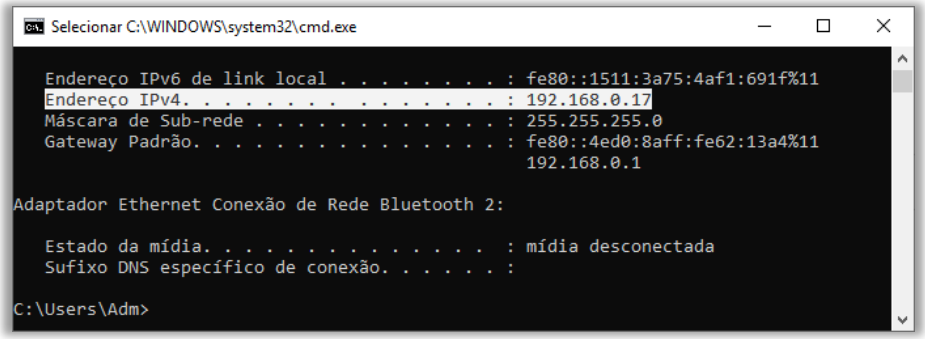


Quando vocês fizerem isso, aparecerá essa imagem da esquerda. Eu quero, então, que vocês escrevam o comando ***cmd*** conforme vemos na imagem da direita.





Notem que será exibida essa janela da esquerda. Em seguida, eu quero que vocês escrevam o comando ***ipconfig*** conforme vemos na janela da direita. No meu caso, foi exibido:



Eu destaquei em branco uma informação importante. *O que, professor?* Esse é o meu Endereço IPv4: **192.168.0.17**! Logo, se alguém quiser me encontrar, esse é o endereço lógico do meu computador na Internet. **Agora tem um porém... o meu endereço IP não é fixo**! *Como assim, Diego?* Pois é... cada vez que eu me conecto à internet, é atribuído um novo endereço IP a minha máquina. No meu caso, eu possuo um IP dinâmico! *Não entendi bulhufas...*

Na Internet, você pode ter dois tipos de endereço IP: **estático ou dinâmico**. O **primeiro**, também chamado de fixo, é um endereço que não muda – ele é bem pouco utilizado, sendo mais comuns em máquinas servidoras do que em máquinas clientes (Ex: IP do Estratégia Concursos). Já o **segundo** é um endereço que é modificado a cada conexão – ele é bem mais utilizado, principalmente em redes domésticas como em uma casa ou em um escritório.

Além disso, é importante entender que **esses endereços não são aleatórios** – existem diversas regras que devem ser obedecidas para cada endereço. Uma delas é o endereçamento com classes. *O que é isso, Diego?* Galera, nós já vimos quem um endereço IP (Versão 4) possui 32 bits e já sabemos que um bit só pode ter dois valores (0 ou 1). *Logo, existem quantos endereços possíveis?* 2^{32} ou 4.294.967.296 possibilidades.

Diante de tantos números, foram criadas diversas regras para realizar o endereçamento de um IP. Uma delas busca dividir o espaço de endereços possíveis em cinco classes: A, B, C, D e E. Logo,

todo e qualquer IP do universo pode ser classificado em uma dessas cinco classes. *E como eu faço para descobrir, professor?* É extremamente simples: basta analisar o primeiro número (na notação decimal pontuada). Eles seguem a seguinte tabela:

1º OCTETO	CLASSE	UTILIZAÇÃO
1 A 126	A	Inicialmente destinado a grandes organizações.
128 A 191	B	Inicialmente destinado a organizações de médio porte.
192 A 223	C	Inicialmente destinado a pequenas organizações.
224 A 239	D	Inicialmente destinado a reservado para *multicast*.
240 A 255	E	Inicialmente destinado a reservado para testes.

Como interpreta essa tabela? Muito fácil! Se o primeiro número de um endereço IP for de 1 a 126, ele será da Classe A – geralmente utilizado por grandes organizações; se for de 128 a 191, ele será da Classe B – geralmente utilizado por organizações de médio porte; se for e 192 a 223, ele será da Classe C – geralmente utilizado por pequenas organizações; se for de 224 a 239, será da Classe D – reservado para *multicast*; e se for de 240 a 254, será da Classe E – reservado para testes.

Galera, as falhas no método de endereçamento com classes combinada com o imenso crescimento da Internet levaram ao rápido esgotamento dos endereços disponíveis. Ficamos sem endereços de classe A e B, e um bloco de classe C é muito pequeno para a maioria das organizações de porte médio. Esse método está obsoleto atualmente, mas ainda cai em prova. Agora eu preciso fazer uma confissão...

Eu preciso confessar: o endereço IP mostrado algumas páginas atrás não é meu IP real! *Como assim, professor?* **Galera, todo dispositivo na internet necessita de um endereço IP único – não pode existir dois dispositivos com o mesmo IP**! No entanto, com o passar dos anos a quantidade de dispositivos conectados à internet subiu assustadoramente. Na minha casa, eu tenho um computador, minha esposa tem outro, nós temos um notebook e um tablet.

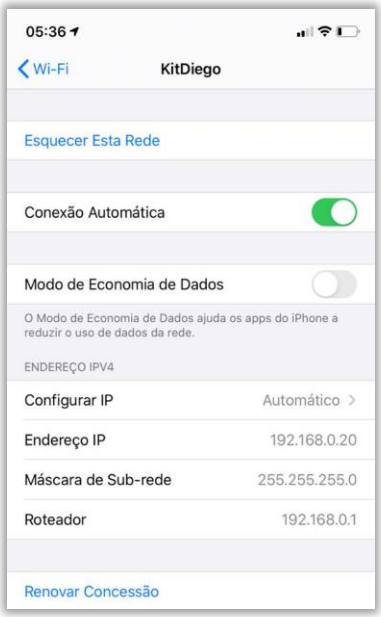
Além disso, temos o meu celular e o celular dela – todos com acesso à Internet! Por baixo, existe apenas na minha casa seis dispositivos conectados. Seguindo o que eu falei no parágrafo anterior, eu preciso de seis endereços únicos diferentes para os meus dispositivos. Agora imagine uma família com três filhos! Aliás, agora imagine uma empresa com mil funcionários. **Existem quatro bilhões de possibilidades de endereço IP, mas somente cerca de metade pode ser usada.**

Ora, como eu faço se existem dois bilhões de endereços úteis e nosso planeta tem uma população de sete bilhões de habitantes? E se considerarmos que cada habitante atualmente pode ter três, quatro ou até mais dispositivos conectados à internet? Pessoal, os engenheiros tiveram que quebrar a cabeça para conseguir uma solução para esse problema. *E como eles fizeram, Diego?* Cara, eles fizeram de uma maneira genial!

Uma coisa é a rede doméstica privada na sua casa/escritório e outra coisa é a rede mundial de computadores (Internet). Por conta disso, foram padronizadas faixas de endereços IP que

deveriam ser utilizados exclusivamente para redes privadas, isto é, eles não existem na internet – eles só existem como endereços internos. Na tabela a seguir, nós podemos ver quais são essas faixas de endereços:

ENDEREÇOS PARA REDES PRIVADAS
CLASSE A – 10.0.0.0 A 10.255.255.255 (2^{24} POSSIBILIDADES)
CLASSE B – 172.16.0.0 A 172.31.255.255 (2^{20} POSSIBILIDADES)
CLASSE C – 192.168.0.0 A 192.168.255.255 (2^{16} POSSIBILIDADES)

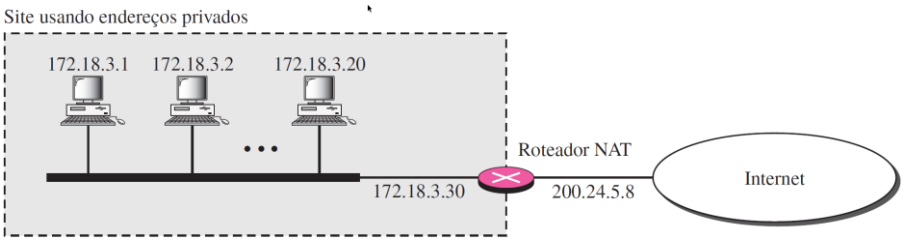


Professor, ainda não entendi por que você disse que mentiu? Pessoal, eu disse algumas páginas atrás que o meu IP era **192.168.0.17.** Façam-me um favor: **confiram agora na tabela anterior se esse endereço informado está presente em alguma dessas faixas**! Ora, está na Classe C! Logo, eu não menti exatamente para vocês – eu apenas informei qual era o meu endereço IP dentro da minha rede doméstica – esse endereço é chamado de IP Privado ou Local!

Para deixar mais claro ainda, eu olhei nas configurações de rede do meu celular para descobrir qual era o IP dele: **192.168.0.20**. **Como meu celular está conectado na minha wi-fi, ele faz parte da minha rede doméstica, logo esse também é um IP Privado ou Local.** Em outras palavras, eu possuo seis equipamentos na minha casa e cada um possui um endereço privado diferente. *Qual foi a grande sacada dos engenheiros?*

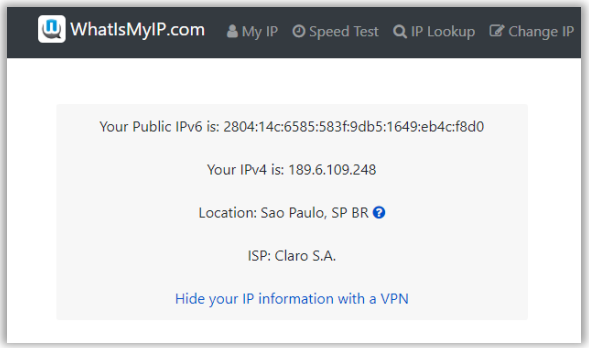
Foi um mecanismo chamado Network Address Translation (NAT). **Ele permite a um usuário ter internamente em sua rede doméstica uma grande quantidade de endereços e, externamente, possuir apenas um endereço** (ou um pequeno conjunto de endereços). Qualquer rede doméstica pode utilizar um endereço da nossa tabela sem a necessidade de pedir permissão para provedores de internet. *Capiche?*

Galera, olha que sacada... a internet chega em uma casa ou organização geralmente por meio de um modem ou um roteador que provavelmente implementa o NAT! *O roteador é um dispositivo conectado à internet?* Sim, então ele possui um IP! **Logo, sempre que um pacote sai da rede privada para a internet – passando por um roteador NAT – tem seu endereço de origem substituído pelo endereço do Roteador NAT.**



Dessa forma, se eu tiver 10 equipamentos conectados ao mesmo roteador na minha rede local, todos eles apresentarão um único endereço IP público e vários endereços privados. Vejam na imagem acima que temos três computadores com endereços IP privados diferentes. No entanto, sempre que qualquer pacote sai dessa rede a partir de qualquer equipamento e acessa a internet, ele sai com um único endereço público: **200.24.5.8**.

Professor, há uma maneira de descobrir meu IP público? Sim, basta acessar www.whatismyip.com. Vejam que esse site informa que meu IP público é: **191.176.124.141**.



Pessoal, o NAT é responsável manter uma tabela de endereços de origem e destino de modo que consiga mapear – quando um recurso vem da Internet para a rede privada – para qual máquina da rede privada as informações de fora devem ser enviadas. Em suma, ele traduz endereços privados (que existem apenas dentro de redes internas) para endereços públicos (que existem na internet e é utilizada por provedores e servidores de internet).

(TJ/SP – 2012) O uso de um endereço IP real para os computadores de uma rede local é dispendioso e torna os computadores mais vulneráveis aos ataques com o objetivo de quebra da segurança. Para minimizar esse problema, pode-se utilizar o esquema de IPs virtuais para os computadores de uma rede local. Para isso, é necessário o uso de um recurso de rede denominado:

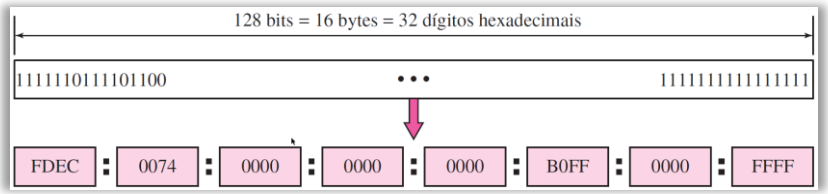
a) MIB. b) NAT. c) DNS. d) DHCP. e) LDAP.

Comentários: conforme vimos em aula, trata-se do NAT (Letra B).

Apesar de todas as soluções de curto prazo (Ex: DHCP, NAT, etc), **o esgotamento de endereços ainda é um problema de longo prazo para a Internet.** Esse e outros problemas no protocolo IP em si – como a falta de tratamento específico para transmissão de áudio e vídeo em tempo real e a criptografia/autenticação de dados para algumas aplicações – têm sido a motivação para o surgimento do IPv6 (IP Versão 6).

A nova versão possui 128 Bits, logo temos até 2^{128} possíveis endereços ou **340 undecilhões** de endereços ou 340.282.366.920.938.000.000.000.000.000. 000.000.000 de endereços!

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



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

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

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

Se existirem duas ocorrências de seções de zeros, apenas uma delas pode ser abreviada. A reexpansão do endereço abreviado é muito simples: devemos alinhar as partes não abreviadas e inserir zeros para obter o endereço original expandido. É interessante notar também que o IPv6 permite também o endereçamento local, isto é, endereços usados em redes privadas. Por fim, o IPv6 pode se comunicar com o IPv4. *Bacana?*

ENDEREÇO ORIGINAL
2001:0C00:0000:0000:5400:0000:0000:0009
ENDEREÇO ABREVIADO
2001:C00:0:0:5400:0:0:9
ENDEREÇO MAIS ABREVIADO

2001:C00::5400:0:0:9 ou 2001:C00:0:0:5400::9

NÃO PODE SER ABREVIADO

2001:C00::5400::9

(TJ/AC – 2012) O IPV6 é um endereçamento de IP que utiliza 32 bits.

_____

Comentários: IPv6 é um endereçamento de IP que utiliza 128 bits – em contraste com o IPv4, que utiliza 32 Bits (Errado).

4.2 – TCP (TRANSMISSION CONTROL PROTOCOL)

INCIDÊNCIA EM PROVA: ALTA

Seus lindos, nós vimos insistentemente que o protocolo IP é não confiável, porque ele não consegue garantir que as informações sejam entregues em perfeito estado, mas existe um cara que consegue garantir isso – ele se chama Transmission Control Protocol (TCP). *Vocês se lembram do exemplo do motorista do caminhão dos Correios?* Ele não garantia a entrega dos pacotes, porque ele poderia pegar um congestionamento na estrada, poderia ser assaltado, etc.

Agora suponha que o caminhão do nosso motorista infelizmente seja assaltado e os ladrões levem seu pacote embora. Ora, você não receberá seu pacote! Pergunto: *você entrará com um processo contra o motorista ou contra os Correios?* Imagino que a segunda opção, uma vez que eles são – como instituição – os responsáveis pela entrega e, não, o motorista. Voltando para nossa analogia, o motorista do caminhão é o IP e a Empresa de Correios e Telégrafos é o TCP!

O Protocolo de Controle de Transmissão (TCP) é um protocolo confiável, pois garante que os dados serão entregues íntegros, em tempo e em ordem. Logo, se eu quero garantir que meu pacote chegará ao seu destino final, eu devo usar tanto o IP (protocolo que vai levar o pacote por várias redes) quanto o TCP (que vai garantir a entrega do pacote). Para tal, encapsula-se o TCP dentro do pacote IP. Isso mesmo! O TCP vai dentro do IP controlando e monitorando tudo...

O IP é um protocolo muito bom, mas ele não estabelece um contato com o destino antes de enviar os pacotes; não é capaz de garantir a entrega dos dados; não é capaz de predizer quão congestionada está uma rede; e não é capaz controlar o fluxo de pacotes enviados para o destinatário. **Já o TCP é um protocolo orientado à conexão e confiável que faz o controle de congestionamento/fluxo e ainda permite a comunicação fim-a-fim**.

- **PROTOCOLO TCP É ORIENTADO A CONEXÕES:**

Porque comunica o destinatário que enviará pacotes antes de enviá-los de fato! *Como assim, Diego?* Imaginem que eu moro em uma casa pequena e quero me desfazer de algumas coisas para sobrar mais espaço em casa. Para tal, eu tenho a ideia de armazenar tudo em pacotes e deixá-los

na casa do meu pai – que é bem mais espaçosa. Antes de simplesmente enviar os pacotes para o meu pai, eu entro em contato:

- Oi, pai! Como você está?
- Tudo ótimo, filho! O que você manda?
- Eu queria te enviar 100 pacotes para armazenar na sua casa. Pode ser?
- Pode, sim! Sem problemas.
- Eu vou começar enviando dez pacotes agora. Ok?
- Ok! Estou pronto para receber os dez pacotes agora!
...

Vocês podem notar que, antes de enviar os pacotes efetivamente, eu bati um papo com meu pai e expliquei a situação de forma que ele ficasse preparado. Se eu falasse que iria enviar naquele momento dez pacotes e meu pai não recebesse nada, ele me avisaria que não havia recebido e eu poderia verificar o que aconteceu no meio do caminho. **Por meio desse mecanismo, é possível garantir que – ao final da conexão – todos os pacotes foram bem recebidos**.

Logo, quando um ponto A quer enviar e receber dados a um ponto B, os dois estabelecem uma conexão entre eles, depois os dados são efetivamente trocados em ambos os sentidos, e a conexão é encerrada. Nesse sentido, esse protocolo é diferente do UDP (que veremos no próximo tópico). **O UDP não é orientado à conexão, logo ele não estabelece nenhuma conversa inicial antes de enviar os pacotes de dados.**

- **PROTOCOLO TCP É CONFIÁVEL:**

Professor, como esse protocolo pode garantir a entrega confiável de pacotes de dados? Uma das maneiras é por meio do estabelecimento de uma conexão inicial, mas existem **diversas técnicas que ele pode implementar para recuperar pacotes perdidos, eliminar pacotes duplicados**, recuperar dados corrompidos e ele pode recuperar até mesmo a conexão em caso de problemas no sistema ou na rede.

- **PROTOCOLO TCP IMPLEMENTA CONTROLE DE CONGESTIONAMENTO:**

Galera, toda vez que meu pai recebe dez pacotes, ele me avisa que os recebeu. Se eu percebo que ele está demorando demais para receber os pacotes que eu estou enviando, eu posso concluir – por exemplo – que o tráfego está intenso e que o caminhão de entrega está em um congestionamento. Se eu percebo isso, eu posso reduzir a quantidade de pacotes enviados. **É basicamente dessa forma que esse protocolo faz um controle de congestionamento**.

- **PROTOCOLO TCP IMPLEMENTA CONTROLE DE FLUXO:**

Imaginem que meu pai me diga que hoje ele não conseguiu abrir muito espaço na casa dele para armazenar meus dez pacotes e me avise que – dessa vez – ele só tem espaço para armazenar apenas cinco pacotes. Eu posso reduzir meu fluxo e enviar apenas a quantidade que ele consegue absorver

de forma que ele não fique sobrecarregado. **É basicamente dessa forma que esse protocolo faz um controle de fluxo.**

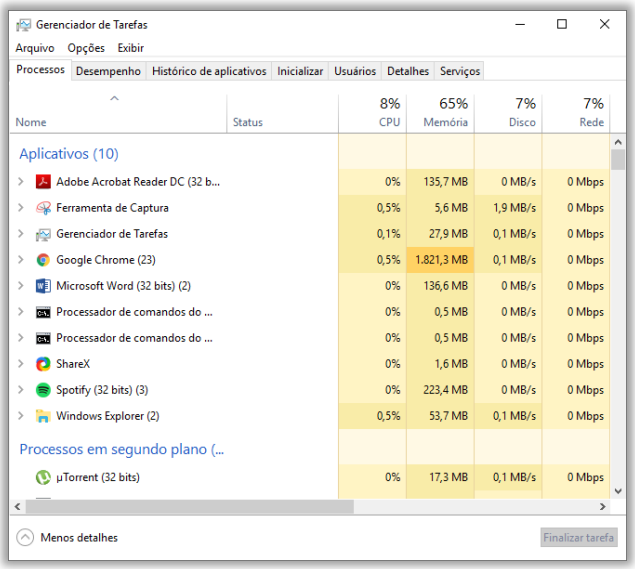
- **PROTOCOLO TCP PERMITE UMA CONEXÃO FIM-A-FIM:**

Imaginem que na rota terrestre entre duas capitais existam dezenas de cidades. Nós podemos dizer que entre esses dois pontos existem dezenas de caminhos diferentes. O protocolo TCP é capaz de criar uma conexão entre dois pontos – fim-a-fim – ignorando quaisquer nós intermediários que existam entre emissor e destinatário da informação. **O IP é um protocolo ponto-a-ponto e o TCP é um protocolo fim-a-fim**.

Vamos voltar agora para aquele exemplo lááááá de trás em que dividimos uma foto em cem pacotinhos. Quando a máquina de destino receber o primeiro dos cem pacotes, ela vai enviar uma confirmação para o emissor dizendo que tudo chegou corretamente. Quando o emissor receber a confirmação, ele enviará o segundo pacote, e assim por diante. Dessa forma, **ele garante que todos os pacotes chegaram íntegros, em tempo e na ordem correta**.

Ele monitora, acompanha, rastreia, controla e gerencia todo o transporte da informação. *Professor, e se acontecer algum problema e o pacote se perder no meio do caminho?* Pode acontecer! O TCP é responsável por requisitar o reenvio daquele pacote pela máquina de origem. Quando todos os cem pacotes chegarem, a máquina de destino os remonta de forma que o destinatário consiga abrir o conteúdo enviado.

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



Nesse sentido, podemos dizer que a sua casa possui um único endereço, mas ela possui diversos quartos, cada um com uma porta de modo que cada morador pode utilizar o serviço dos Correios. Agora acompanhem o Tio Diego: **imaginem que um pacote de dados viajou o planeta e por meio do seu endereço IP, ele finalmente chegou no seu computador**. Só que o seu computador possui dezenas de processos diferentes em execução. *E aí, qual deles é o dono do pacote? Processos, professor?* Sim, vejam só! Pressionem de forma simultânea as teclas CTRL+SHIFT+ESC! Esse atalho abrirá o Gerenciador de Tarefas. Observem que várias abas serão exibidas, sendo a primeira a aba de processos.

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

Pois é... na camada de enlace de dados, nós utilizamos o endereço MAC; na camada de rede, nós utilizamos o endereço IP; já na camada de transporte, nós utilizamos o número da porta para escolher um entre vários processos que estão em execução no destino. Então o pacote percorreu o mundo inteiro em rotas terrestres e submarinas, chegou no meu computador e agora ele precisa saber qual processo deve recebê-lo. Para tal, ele precisa do número da porta!

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

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

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

Notem que a página do Estratégia Concursos abrirá normalmente. Agora tentem com um número de porta diferente – por exemplo: ***http****://www.estrategiaconcursos.com.br****:21***.

Vejam que retornará um erro chamado **ERR_UNSAFE_PORT**. Esse erro é retornado quando você tenta acessar dados utilizando uma porta não recomendada pelo navegador. Em outras palavras, você está utilizando a porta errada! Agora para fechar a nossa analogia: **o endereço IP contém o endereço da sua casa, mas é a porta que determinará à qual quarto (processo) pertence o pacote**. *Bacana?* Então vamos ver uma listinha com as principais portas...

PROTOCOLO (CAMADA DE APLICAÇÃO)	PROTOCOLO (CAMADA DE TRANSPORTE)	NÚMERO DA PORTA
HTTP	TCP	80
HTTPS	TCP	443
POP3	TCP	110
SMTP	TCP	25/587[3]
IMAP4	TCP	143
FTP	TCP	20/21
TELNET	TCP	23
SSH	TCP	22
DNS	TCP/UDP	53
DHCP	UDP	67/68
IRC	TCP	194

EM VERMELHO, OS PROTOCOLOS CUJO NÚMERO DE PORTA MAIS CAEM EM PROVA!

(TJ/SP – 2012) Numa rede com o ISA Server 2006, os usuários necessitam acessar os protocolos POP3, HTTP, HTTPs e SMTP nas suas portas padrões. Assinale a alternativa que apresenta, correta e respectivamente, as portas correspondentes a esses protocolos.

a) 25, 80, 443,110
b) 110, 80, 443, 25
c) 110, 80, 25, 443
d) 443, 80, 25, 110
e) 443, 80, 110, 25

Comentários: conforme vimos em aula, trata-se das Portas 110, 80, 443 e 25 (Letra B).

4.3 – UDP (USER DATAGRAM PROTOCOL)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

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

[3] Via de regra, o padrão respaldado pela RFC do SMTP é Porta 25. Excepcionalmente, o Brasil adotou a porta 587 para evitar SPAM.

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

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

No entanto, não faz nenhum sentido tentar reenviar esses pacotes perdidos – como ocorre com o TCP. *Por que?* Porque nesses serviços *real-time* (tempo real), essas pequenas perdas são insignificantes. *Bacana?* **Então TCP e UDP possuem algumas vantagens e desvantagens em relação ao outro dependendo do contexto de utilização**. Por fim... eu quero fazer mais uma analogia para que vocês entendam melhor!

TCP é a aquele seu colega do trabalho que é bastante formal e sistemático e que – quando deseja ir na sua casa – liga antes para avisá-lo, verifica se você pode recebê-lo, verifica se você tem disponibilidade, marca uma data e chega na sua casa com pontualidade britânica. Já o UDP é aquele seu brother da época de faculdade que não avisa coisa nenhuma, bate na sua porta 22h de uma quarta-feira, diz que veio para assistir um jogo de futebol e peida no meio da sala.

4.4 – SMTP (SIMPLE MAIL TRANSFER PROTOCOL)

INCIDÊNCIA EM PROVA: ALTA

Protocolo da Camada de Aplicação, ele é o principal protocolo de envio de correio eletrônico (e-mail) através da rede. Esse protocolo é utilizado para enviar um e-mail de um cliente de correio eletrônico até um ou mais servidores de correio eletrônico. *Como assim, Diego?* Calma, nós vamos entender isso melhor, mas antes precisamos definir alguns termos importantes para todos os protocolos de correio eletrônico. Vejam só...

- **Cliente de E-Mail:** trata-se de uma aplicação geralmente instalada em uma máquina local que permite enviar/receber e-mails (Ex: Mozilla Thunderbird, Microsoft Outlook, etc);
- **Servidor de E-Mail:** trata-se do servidor remoto que recebe e-mails de um cliente de e-mail ou de um webmail e os envia para o servidor de e-mail de destino;
- **Provedor de E-Mail:** trata-se de uma empresa que hospeda e disponibiliza serviços de e-mail para outras empresas ou usuários finais (Ex: Gmail, Outlook, Yahoo, Uol, etc);
- **Webmail:** trata-se de uma aplicação geralmente hospedada em um servidor remoto que permite enviar/receber e-mails (Ex: Outlook.com, Gmail.com, Yahoo.com, Uol.com, etc).

Imaginemos um cenário em que uma menina chamada Maggie deseja enviar um e-mail para o seu amigo chamado Rob. Ela utiliza o Yahoo! como Provedor de E-Mail. Além disso, ela gosta de utilizar o Microsoft Outlook – instalado em seu computador – como seu Cliente de E-Mail. Para garantir que ele consiga se comunicar com o Servidor de E-Mail do Yahoo!, ela deve fazer uma série de configurações (Ex: Endereço do Servidor SMTP do Yahoo!).

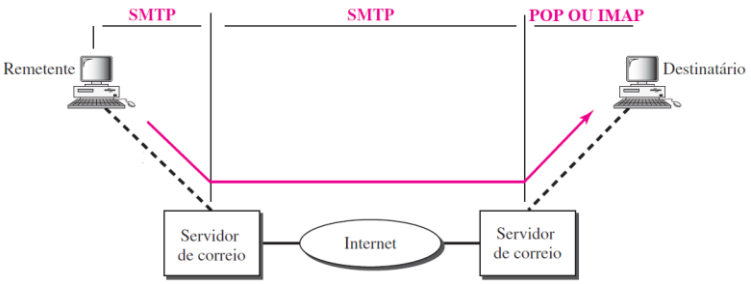
SMTP.EMAIL.YAHOO.COM

Bacana! Agora que ela configurou o endereço do Servidor de E-Mail (SMTP) do Yahoo!, ela pode enviar e-mails para quem ela quiser. Vamos supor que ela deseje enviar e-mails para o seu amigo Rob! No entanto, seu amigo utiliza outro provedor de e-mail – ele utiliza o Gmail. *Há algum problema?* **Não, não há problema algum!**

Nesse caso, quando ela clicar no botão de enviar e-mail, ocorrerão alguns passos. Primeiro, o Microsoft Outlook enviará a mensagem para o Servidor de E-Mail do Yahoo! Cadastrado anteriormente. Segundo, o Servidor SMTP dividirá o e-mail do destinatário – no caso, Rob – em duas partes: **rob** e **gmail.com**. Terceiro, ele ignorará a primeira parte, identificará o domínio na segunda parte (gmail.com) e procurará na Internet o Servidor SMTP do Gmail.

Quarto, quando ele encontrar o Servidor SMTP do Gmail, ele enviará a mensagem para esse servidor. Quinto, quando a mensagem chegar ao Servidor SMTP do Gmail, ele também quebrará o e-mail de Rob em duas partes, mas ignorará a segunda parte e identificará apenas a primeira (rob). **Se esse nome de usuário existir no servidor, ele armazenará a mensagem de Maggie na caixa de entrada de Rob**! *Ficou mais fácil de entender agora?*

Galera, eu preciso falar um pequeno detalhe para vocês. Isso caiu apenas uma vez em prova, mas foi uma polêmica absurda! Eu disse na primeira frase sobre esse protocolo que ele é o principal protocolo de envio de correio eletrônico através da rede. *Eu menti?* Não! **No entanto, notem que ele pode ser utilizado para receber e-mail em uma única situação**. Para entender melhor, vamos analisar a imagem a seguir:



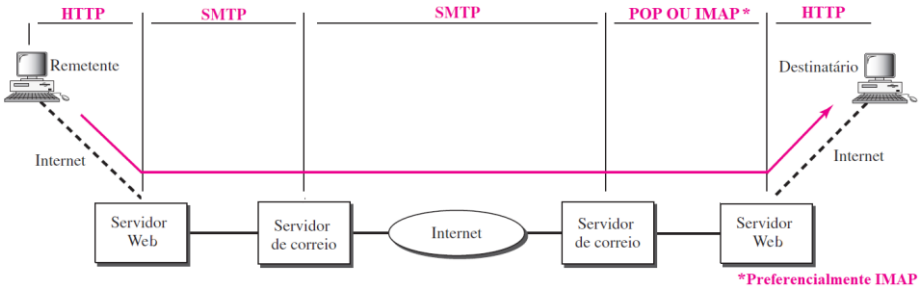
Percebam que o remetente utiliza o protocolo SMTP para enviar uma mensagem de correio eletrônico. **No entanto, notem que na comunicação entre o servidor de correio eletrônico do remetente e do destinatário também é utilizado o SMTP**. Logo, nesse caso específico de comunicação entre servidores, ele é utilizado tanto para recebimento quanto para envio de correio eletrônico. Não é o padrão, é apenas nesse caso! *Bacana?*

(Polícia Federal – 2018) SMTP é o protocolo utilizado para envio e recebimento de email e opera na camada de aplicação do modelo TCP/IP.

Comentários: conforme vimos em aula, ele realmente pode ser utilizado para envio e recebimento de e-mail (Correto).

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

Quando vocês acessam – por meio de um navegador – um serviço de e-mail, temos um... webmail! **É como se o cliente de e-mail apresentado no esquema anterior estivesse hospedado em um servidor web e você utilizasse um browser para acessá-lo.** Logo, a comunicação entre a máquina do remetente e o servidor web de origem se dá por meio do HTTP! Ao final, para recuperar o e-mail do servidor web para a máquina do destinatário também se utiliza o HTTP.



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

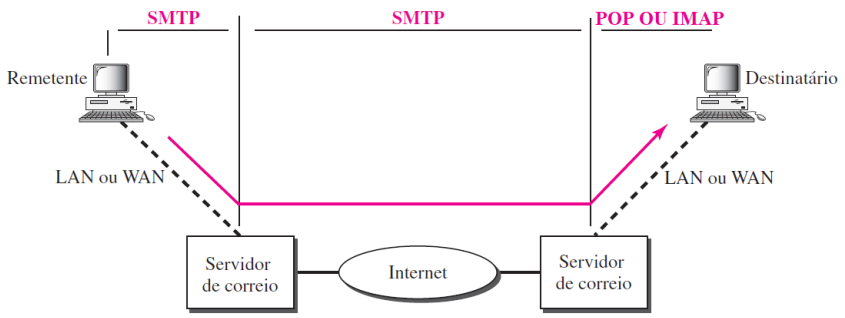
(CET – 2011) No serviço de emails por meio de browsers web, o protocolo HTTP é usado para acessar uma mensagem na caixa postal, e o protocolo SMTP, necessariamente, para enviar uma mensagem para a caixa postal.

Comentários: o serviço de e-mails por meio de browsers web é o webmail. A questão afirma que o HTTP é utilizado para acessar uma mensagem na caixa postal (isto é, no servidor de correio) – isso não é verdade! Vejam no esquema anterior que quem acessa a mensagem na caixa postal é o POP ou IMAP. O HTTP é utilizado apenas para transferir a mensagem do servidor web para o browser do destinatário (Errado).

4.5 – POP3 (POST OFFICE PROTOCOL, VERSÃO 3)

INCIDÊNCIA EM PROVA: ALTA

Protocolo da Camada de Aplicação, ele foi criado como uma forma simplificada para receber, baixar e deletar mensagens de um servidor de e-Mail. Vocês devem se lembrar que o SMTP é responsável por enviar o e-mail até o servidor de e-mail do destinatário. A partir daí, se ele estiver utilizando um cliente de e-mail, ele poderá utilizar o POP3 ou IMAP para recuperar do servidor de correio eletrônico os e-mails recebidos.



Esse protocolo trabalha em **dois modos distintos**! No Modo Delete, ele apaga as mensagens da caixa postal logo após a realização do download – era normalmente utilizado quando o usuário estava trabalhando em um computador fixo e tinha condições de salvar/organizar as mensagens recebidas após sua leitura ou resposta. No modo Keep, ele mantém uma cópia das mensagens na caixa postal mesmo após a realização do download.

Esse modo era normalmente utilizado quando o usuário acessava suas mensagens de outro computador que não fosse o seu principal – as mensagens eram lidas, mas mantidas no sistema para futura recuperação e organização. **Eu gostaria que vocês pensassem nesse protocolo como uma secretária eletrônica antiga – aquelas que utilizavam uma fita para gravar mensagens de voz**. *Todos sabem o que era uma secretária eletrônica?*

Para os mais novos: era um dispositivo para responder automaticamente chamadas telefônicas e gravar mensagens deixadas por pessoas que ligavam para um determinado número, quando a pessoa chamada não podia atender o telefone. Podia acontecer de várias pessoas deixarem mensagens de voz pela secretária. **Nesse caso, você poderia ouvir as mensagens e não as apagar ou você poderia ouvi-las e imediatamente após apagá-las (como no POP).**

Em geral, o protocolo utiliza – por padrão – o primeiro modo, isto é, apagam-se da caixa postal as mensagens logo após a realização do download. *Qual é o problema disso?* **Uma vez feito o download, as mensagens só ficam disponíveis para vê-las novamente na máquina em que foi feito o download.** Logo, após apagadas as mensagens, você não poderia vê-las por meio de um webmail, por exemplo.

Esse protocolo era indicado para as pessoas não conectadas permanentemente à Internet, para poderem consultar os e-mails recebidos de forma offline. **Lembrem-se que – até um tempo atrás**

– o acesso à Internet era algo bastante raro e muitas pessoas não podiam ficar sem acesso aos seus e-mails quando não estivessem conectadas à Internet. Nesse contexto, o POP era bastante indicado! *Bacana?*

> **(Prefeitura de Amontada – Adaptado – 2016)** O POP3 é responsável por receber e-mail do servidor do destinatário armazenando-a na máquina do destinatário.
>
> _____
>
> **Comentários:** conforme vimos em aula, ele é realmente utilizado para receber e-mail do servidor do destinatário e é armazenado na máquina do destinatário por padrão (Correto).

4.6 – IMAP (INTERNET MESSAGE ACCESS PROTOCOL)

INCIDÊNCIA EM PROVA: ALTA

O POP3 é ineficiente em diversas situações! Ele não permite ao usuário organizar mensagens ou criar pastas no servidor; não permite que o usuário verifique parte do conteúdo da mensagem antes de fazer o download; possui problemas quando configurado em mais de um computador; entre outros. **Já o IMAP permite que você acesse todos os seus correios eletrônicos a qualquer momento.** Além disso, ele traz diversas funções adicionais. Vejamos...

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

Ele permite armazenar seus e-mails nos servidores de e-mail do seu provedor de e-mail até que você os delete. Apesar de isso ser bem mais conveniente, alguns provedores de e-mail limitam a quantidade de e-mail que você pode armazenar em seus servidores e pode suspender temporariamente seus serviços se você exceder esse limite. *Alguém aí já chegou perto do limite gratuito de 15 Gb do Gmail?* Se sim, é esse o caso!

Vocês podem pensar no IMAP como uma secretária eletrônica online – possivelmente armazenada na nuvem. **Dessa forma, qualquer mensagem que ela receber fica armazenada na nuvem e pode ser acessada por meio de diferentes dispositivos ou softwares até que você as delete**. Não é necessária muita preocupação com segurança, visto que o IMAP possui uma versão mais segura chamada IMAPS (IMAP Secure).

Em geral, se você sempre utiliza seu e-mail em uma única localização ou por meio de um único dispositivo, ou até mesmo se você tem problemas com acesso à Internet – recomenda-se utilizar o POP. **Por outro lado, se você utiliza seu e-mail em diferentes localizações ou por meio de dispositivos diferentes, e se você não tem problemas com acesso à Internet – recomenda-se utilizar o IMAP**.

(TJ/RS – Adaptado – 2017) Qual protocolo de acesso ao correio eletrônico possui comandos que permitem a um usuário, através de sua ferramenta de correio eletrônico (agente de usuário), criar remotamente uma estrutura de pastas e subpastas em seu servidor de correio eletrônico para organizar suas mensagens?

a) IMAP b) HTTP c) POP3 d) SMTP e) SNMP

Comentários: conforme vimos em aula, trata-se do IMAP (Letra A).

4.7 – DNS (DOMAIN NAME SYSTEM)

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Galera, quantos números vocês sabem decorados? Eu, por exemplo, tenho uma péssima memória! Eu sei meu Nº de CPF, Nº de RG, Nº de Conta Bancária e Nº de Telefone. Fora isso, eu já começo a ter dificuldades de lembrar. Nós sabemos que os computadores na Internet são identificados utilizando endereços IP (Exemplo: 192.168.10.15). **Uma vez que é mais fácil decorar nomes que números, foi criado um sistema capaz de traduzir números em nomes e vice-versa**.

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

O servidor que armazena o Google tem o endereço lógico apresentado no parágrafo anterior. *Agora vocês já imaginaram se nós tivéssemos que decorar todos os endereços IP de todos os sites que nós acessamos diariamente?* Seria completamente inviável! Para resolver esse problema, surgiu o Domain Name System (DNS). **Trata-se de um protocolo da camada de aplicação responsável por atribuir endereços léxicos aos recursos da rede** – ele é como uma agenda de contatos da Internet!

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

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

Para fazer isso, ele consulta uma tabela parecida com uma agenda telefônica! *Quem aí é da época da lista telefônica?* Tô velho! Pessoal, se você possuísse o nome de uma pessoa, era possível descobrir seu número de telefone. Ocorria também o caso inverso: por meio de um número de telefone, era possível descobrir um nome. Bem, vejamos na tabela a seguir como tudo isso funciona no caso dos computadores:

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

Esse endereço que nós mostramos na tabela acima é um endereço de rede no qual se encontra um recurso informático – no caso, uma página web. No entanto, é possível buscar qualquer tipo de recurso (um computador, uma impressora, um arquivo, entre outros). Para tal, é preciso saber o nome desse recurso e esse nome nós chamamos de *Uniform Resource Locator* (URL). Uma URL é geralmente formada pela seguinte estrutura:

ESTRUTURA DE URL
PROTOCOLO-OU-ESQUEMA://IP-OU-DOMÍNIO:PORTA/CAMINHO

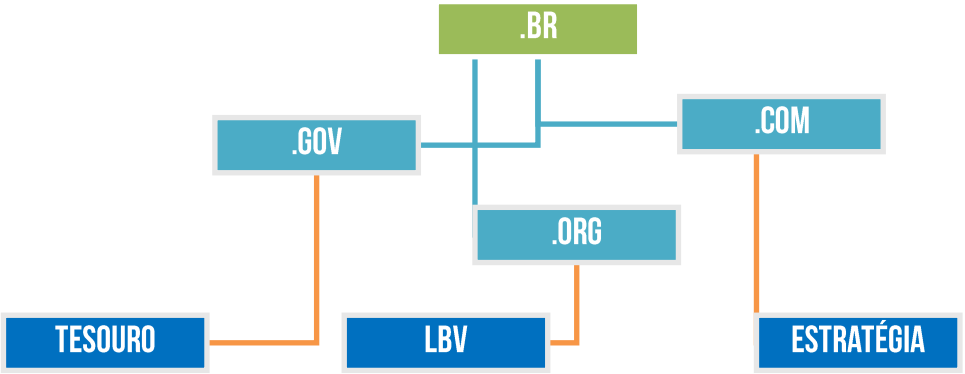
A URL – Localizador de Recursos Uniformes – oferece uma maneira uniforme e padronizada de localizar recursos na web. Claro que, na maioria das vezes, não é necessário utilizar toda essa estrutura apresentada acima para ter acesso aos recursos. Notem, por exemplo, que a porta e o caminho são atributos opcionais! Além disso, muitas vezes o protocolo ou esquema também é opcional. *O que temos, então?*

Protocolo: também chamado de esquema; **IP ou Domínio:** endereço lógico ou léxico da máquina hospedeira (host); **Porta:** ponto lógico em que se pode executar uma conexão; **Caminho:** especifica onde se encontra um determinado recurso. Na tabela abaixo, há diversos exemplos diferentes. Notem que alguns possuem porta, outros não; alguns possuem protocolo, outros possuem esquema, outros nenhum; alguns possuem caminho, outros não; e assim por diante.

DNS (DOMAIN NAME SYSTEM)
WWW.ESTRATEGIACONCURSOS.COM.BR
HTTP://WWW.ESTRATEGIACONCURSOS.COM.BR
HTTP://WWW.ESTRATEGIACONCURSOS.COM.BR:80
HTTP://WWW.ESTRATEGIACONCURSOS.COM.BR/PROFESSORES
FTP://ADMIN@DIEGOCARVALHO.COM.BR
MAILTO://CONTATO@DIEGOCARVALHO.COM.BR

Apesar de todas essas partes, **o nome do domínio é o principal membro da URL**! Por isso, dizemos que o DNS traduz, transforma, resolve um nome ou domínio em um endereço IP e um endereço IP

em um nome ou domínio. Percebam também na próxima imagem que **o DNS apresenta uma estrutura hierárquica e distribuída** em que seu espaço de nomes é dividido em vários servidores de domínio baseado em níveis.



Diego, o que é um espaço de nomes? Para evitar ambiguidades, os nomes atribuídos às máquinas devem ser cuidadosamente selecionados a partir de um espaço de nomes – que nada mais é que um conjunto organizado de possíveis nomes. Em outras palavras, **os nomes devem ser exclusivos, uma vez que os endereços IP também são**. Galera, caso vocês queiram registrar um domínio algum dia, vocês provavelmente terão que acessar o seguinte site:

WWW.REGISTRO.BR

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

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

(MPS – 2010) Um servidor DNS (Domain Name Service) permite identificar os endereços IP de usuários e servidores da Internet, por meio da associação de um conjunto de números com domínios.

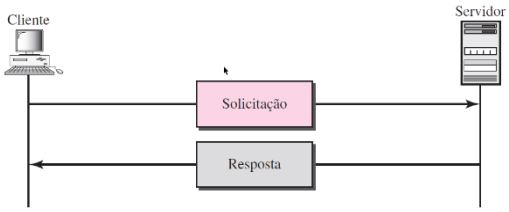
Comentários: ele permite identificar endereços lógicos (IP) de usuários e servidores da Internet, por meio da associação de um conjunto de números com domínios, isto é, é possível identificar um endereço IP por meio de um domínio e vice-versa (Correto).

4.8 – HTTP (HYPER TEXT TRANSFER PROTOCOL)

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Protocolo da Camada de Aplicação, **ele é utilizado por programas de navegação (*browsers*) para acessar dados na web**. Em português, seria traduzido como Protocolo de Transferência de

Hipertexto. *Por que, professor?* Porque ele é responsável pela transferência, formatação e apresentação de páginas web com conteúdo multimídia (textos, áudio, imagens, vídeos, entre outros) entre um servidor e um cliente na Internet.

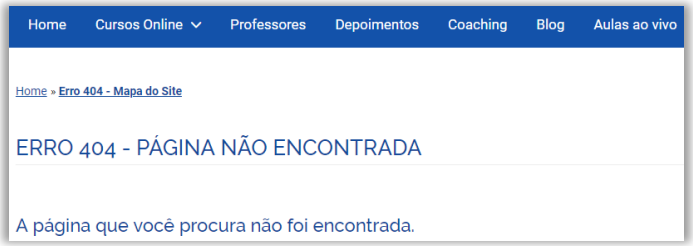


A imagem anterior ilustra uma transação típica entre um cliente e um servidor no HTTP. O cliente inicializa uma transação enviando uma mensagem de solicitação. O servidor responde enviando uma mensagem de resposta. *Como assim, Diego?* Galera, toda página web está armazenada em um servidor web. Logo, quando você acessa qualquer página pelo navegador, você está fazendo uma solicitação ao servidor para acessar aquela página.

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

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

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



Vocês viram que retornou um erro? Pois é, Erro 404! Esse erro é da categoria Erro do Cliente e significa que uma determinada página não foi encontrada. *Por que, professor?* Cara, essa página não foi encontrada basicamente porque ela não existe – eu acabei de inventar apenas para mostrar um

código de retorno! **Esse código sempre existirá para qualquer requisição, mas nem sempre será exibida para os usuários.**

Não confundam HTTP com HTML! HTML é uma linguagem para criação de páginas web. Basta lembrar da última letra: **HTTP** é Protocolo e **HTML** é Linguagem.

(IFTO – 2018) Os protocolos de comunicação, em redes de computadores, são o conjunto de regras que governam a interação entre sistemas de computadores distribuídos em rede. Os protocolos são usados para permitir a comunicação entre dois ou mais computadores. Os navegadores de internet utilizam um protocolo que é a base de comunicação de dados da world wide web, específico para a transferência e apresentação de páginas com conteúdo multimídia (informações de textos, áudio, imagens e vídeos). Assinale a opção correta que identifica o protocolo usado pelos browsers que permitem os usuários a navegar na internet.

a) File Transfer Protocol (FTP)
b) Internet Message Access Protocol (IMAP)
c) Simple Mail Transfer Protocol (SMTP)
d) Post Office Protocol (POP)
e) HyperText Transfer Protocol (HTTP)

Comentários: conforme vimos em aula, trata-se do HTTP (Letra E).

4.9 – HTTPS (HYPER TEXT TRANSFER PROTOCOL SECURE)

INCIDÊNCIA EM PROVA: ALTÍSSIMA

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

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

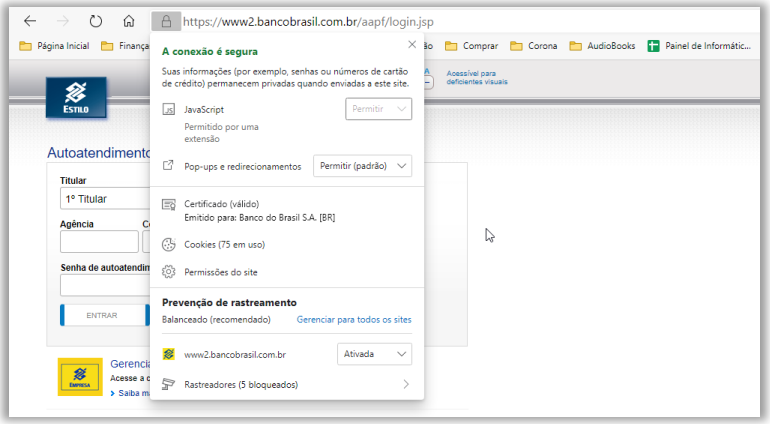
Imagine que você está em um Coffee Shop, tomando seu cafezinho com seu notebook e decide comprar um presente para sua mãe online em um site que utiliza apenas o HTTP e, não, HTTPS. Uma pessoa na mesa ao lado pode utilizar métodos maliciosos para interceptar sua transação e descobrir os dados do seu cartão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

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

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

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

Após recebê-lo, o navegador consulta diversas autoridades públicas e privadas para verificar se esse certificado é válido – é como se alguém enviasse uma assinatura e você fosse em vários cartórios para conferir se a assinatura é sua ou não. *Sabe quando você tenta acessar uma página e o navegador avisa que o certificado é inválido?* **Pois é, isso significa geralmente que o certificado não foi encontrado, expirou ou foi revogado.** Logo, tomem cuidado com esse tipo de mensagem!



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

(Banco da Amazônia – 2018) O protocolo que permite a navegação na internet segura através de criptografia de informações é o:

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

Comentários: conforme vimos em aula, trata-se do HTTPS (Letra A).

4.10 – FTP (FILE TRANSFER PROTOCOL)

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Protocolo da Camada de Aplicação, **ele é responsável pela realização de transferências de arquivos entre um Cliente FTP e um Servidor FTP**. Definições que já encontrei em prova:

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

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

Trata-se do protocolo-padrão para copiar arquivos de uma máquina para outra, possuindo três modos de transmissão diferentes: de fluxo contínuo, blocado e comprimido.

MODO DE TRANSMISSÃO	DESCRIÇÃO
FLUXO CONTÍNUO (STREAM)	O arquivo é enviado, por um fluxo contínuo de bytes, ao TCP. Quando chega nesse protocolo, ele separa os dados recebidos em porções com um tamanho apropriado para o transporte – trata-se do modo-padrão.
BLOCADO	Os dados são entregues do FTP para o TCP em blocos. Nesse caso, cada bloco é precedido por um cabeçalho de três bytes. O primeiro byte é chamado de descritor de blocos; os dois seguintes definem o tamanho do bloco em bytes.

COMPRIMIDO	No caso de arquivos muito grandes, os dados podem ser comprimidos, antes de serem enviados, usando um algoritmo.

(IFSP – 2012) Assinale a alternativa que informa o protocolo usado para transferência de arquivos entre computadores ligados na Internet.

a) IMAP b) FTP c) SMTP d) DHCP e) SNMP

Comentários: conforme vimos em aula, trata-se do FTP (Letra B).

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

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

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

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

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

De forma análoga, o termo upload faz referência a operação inversa à do download, isto é, refere-se ao envio de conteúdo à internet. Apesar de serem termos com sentidos opostos, do ponto de

vista técnico, a distinção de um processo de transmissão entre download ou upload pode ser associada simplesmente à uma questão de perspectiva, **pois sempre que um dispositivo faz um download, o dispositivo que disponibiliza o arquivo/informação faz um upload e vice-versa**.

No entanto, essa distinção é normalmente feita considerando a participação do dispositivo que iniciou a transmissão de dados, seja obtendo ou disponibilizando, isto é, **se está obtendo dados é um download; e se está disponibilizando dados é um upload**. Voltando agora à questão dos protocolos: FTP[4] (*File Transfer Protocol*) é um protocolo de transferência de arquivos entre computadores e HTTP (*HyperText Transfer Protocol*) é um protocolo de transferência de textos.

HTTP permite apenas a transferência de textos? Não! Quando você faz o download da nossa aula pelo navegador, você está transferindo arquivos por meio do Protocolo HTTP. *Bacana?*

(UFBA – 2018) FTP é o protocolo de transferência de arquivos entre computadores.

Comentários: conforme vimos em aula, a questão está impecável (Correto).

5 – Demais Protocolos

PROTOCOLO	PORTA	DESCRIÇÃO
ICMP	-	Protocolo da Camada de Internet/Rede que é utilizado para comunicar a ocorrência de situações anormais na transferência de um datagrama, gerando relatórios de erros à fonte original, etc.
ARP	-	Protocolo da Camada de Rede que é responsável por manter uma tabela de conversão de endereços lógicos (IP – Camada de Rede) em endereços físicos (MAC – Camada de Enlace).
DHCP	67/68	Protocolo da Camada de Aplicação que configura dinamicamente endereços de rede. Em uma rede, pode ser necessário que um mesmo Endereço IP possa ser utilizado em diferentes dispositivos em momentos distintos.
TELNET	23	Protocolo da Camada de Aplicação que permite conectar dois computadores de forma que um usuário consiga efetuar login em outro computador através da rede de forma remota.
SSH	22	Protocolo da Camada de Aplicação que é um protocolo de acesso remoto que utiliza autenticação de chave pública e oferece suporte à compressão de dados para a execução de aplicações com interfaces gráficas.
IRC	194	Protocolo da Camada de Aplicação que é utilizado basicamente para bate-papo e troca de arquivos, permitindo uma conversa em grupo ou privada.

[4] FTP tem sido cada vez menos utilizado após o surgimento de ferramentas de armazenamento em nuvem (Cloud Storage), que podem ser acessadas por meio de navegadores web por meio do Protocolo HTTP.

QUESTÕES COMENTADAS – BANCAS DIVERSAS

1. **(CONSULPLAN / Prefeitura de Patos de Minas – 2015)** Assinale a alternativa que se trata de um protocolo de internet de transferência de arquivo, bastante rápido e versátil utilizado.

   a) FTP.
   b) HTTP.
   c) HTM.
   d) HTML.

Comentários:

(a) Correto, esse é um protocolo de transferência de arquivos; (b) Errado, esse é um protocolo de transferência de hipertexto; (c) Errado, isso não é um protocolo; (d) Errado, isso não é um protocolo – trata-se de uma linguagem de marcação de hipertexto.

Gabarito: Letra A

---

2. **(ESAF / Ministério da Fazenda – 2013)** Para o funcionamento da Internet, há um sistema de gerenciamento de nomes hierárquico e distribuído, que resolve nomes de domínios em endereços de rede (IP), que é o:

   a) POP3
   b) DNS
   c) HTTP
   d) HTTPS
   e) SMTP

Comentários:

A questão trata do DNS! Ele busca transformar endereços numéricos em nomes de domínios amigáveis, mais compreensíveis para humanos e mais fáceis de memorizar. Ele apresenta uma estrutura hierárquica e distribuída, em que seu espaço de nomes é dividido em vários servidores de domínio baseado em níveis.

Gabarito: Letra B

---

3. **(ESAF / Ministério da Fazenda – 2013)** Um exemplo de protocolo de transporte utilizado na Internet é o protocolo:

   a) XTP
   b) TPP

c) UDP
d) TRP
e) HTTP

Comentários:

Os protocolos mais comuns da Camada de Transporte são: TCP (*Transmission Control Protocol*) e UDP (*User Datagram Protocol*).

Gabarito: Letra C

---

4. **(CONSULPLAN / Prefeitura de Cantagalo – 2013)** O Outlook Express é um aplicativo para gerenciamento de e-mail, porém, para enviar e receber, são necessárias algumas configurações, como as portas dos protocolos POP e SMTP. As portas dos protocolos POP e SMTP configuradas no Outlook Express são, respectivamente,

a) 25 e 115.
b) 110 e 587.
c) 466 e 25.
d) 587 e 965.
e) 993 e 587.

Comentários:

PROTOCOLO (CAMADA DE APLICAÇÃO)	PROTOCOLO (CAMADA DE TRANSPORTE)	NÚMERO DA PORTA
HTTP	TCP	80
HTTPS	TCP	443
POP3	TCP	110
SMTP	TCP	25/587[5]
IMAP3	TCP	220
IMAP4	TCP	143
FTP	TCP	20/21
TELNET	TCP	23
SSH	TCP	22
DNS	TCP/UDP	53
DHCP	UDP	67/68
IRC	TCP	194
SNMP	UDP	161/162

[5] Via de regra, o padrão respaldado pela RFC do SMTP é Porta 25. Excepcionalmente, o Brasil adotou a porta 587 para evitar SPAM.

Dessa forma, o SMTP utiliza a Porta 25 ou 587 (essa última, mais segura) e o POP3 utiliza a Porta 110.

Gabarito: Letra B

---

5. **(ESAF / Ministério da Fazenda – 2012)** O Correio Eletrônico é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação. O termo e-mail é aplicado aos sistemas que utilizam a Internet e são baseados no protocolo:

a) SNMP.
b) SMTP.
c) Web.
d) HTTP.
e) HTTPS.

Comentários:

A questão trata do SMTP (*Simple Mail Transfer Protocol*). Esse é o protocolo utilizado pelos clientes de e-mail para enviar correio eletrônico de um host a outro.

Gabarito: Letra B

---

6. **(ESAF / Ministério da Fazenda – 2012)** O componente mais proeminente da Internet é o Protocolo de Internet (IP), que provê sistemas de endereçamento na Internet e facilita o funcionamento da Internet nas redes. O IP versão 4 (IPv4) é a versão inicial usada na primeira geração da Internet atual e ainda está em uso dominante. Ele foi projetado para endereçar mais de 4,3 bilhões de computadores com acesso à Internet. No entanto, o crescimento explosivo da Internet levou à exaustão de endereços IPv4. Uma nova versão de protocolo foi desenvolvida, denominada:

a) IPv4 Plus.
b) IP New Generation.
c) IPV5.
d) IPv6.
e) IPv7.

Comentários:

O nome da nova versão do protocolo IP é IPv6 – nenhum dos outros nomes faz sentido!

Gabarito: Letra D

---

7. **(ESAF / Ministério da Fazenda – 2012)** Quando um visitante de um sítio Web se conecta a um servidor que está utilizando um protocolo específico de segurança, ele irá notar, na barra de endereços, que o protocolo de comunicação passa a ser https:// (no lugar do http:// padrão). Além disso, a maioria dos browsers (como o Internet Explorer por exemplo) mostram no browser o desenho de um cadeado. Quando este cadeado está sendo mostrado, o usuário passa a ter a tranquilidade de saber que as informações fornecidas àquele Website não poderão ser interceptadas no seu trajeto. Este protocolo específico de segurança é o:

a) WebSec
b) HTTP
c) HTML
d) SSL
e) TCP/IP

Comentários:

Quando um endereço começa com https:// significa que o protocolo que está sendo utilizado é o HTTPS (*HyperText Transfer Protocol Secure*) e, portanto, significa que o protocolo é seguro. HTTPS é o protocolo HTTP de forma segura, pois utiliza o protocolo TLS ou SSL para criptografia dos dados assim como certificados digitais para garantia de autenticidade.

Gabarito: Letra D

---

8. **(IBADE / IPERON – 2017)** Ao utilizar um software de correio eletrônico, um usuário precisou configurar o funcionamento do protocolo responsável pelo envio de e-mail através da rede. Nesse caso, ele acessou a configuração do protocolo:

a) WAP.
b) SMTP.
c) POP.
d) IMAP.
e) ARP.

Comentários:

(a) Errado. WAP (*Wireless Application Protocol*) é um protocolo para aplicações que utilizam comunicações de dados digitais sem fio;

(b) Correto. SMTP (*Simple Mail Transfer Protocol*) é um protocolo para envio de correio eletrônico pela Internet;

(c) Errado. POP (*Post Office Protocol*) é um protocolo utilizado no acesso remoto a uma caixa de correio eletrônico que permite o recebimento local de mensagens;

(d) Errado. IMAP (*Internet Message Access Protocol*) é um protocolo de gerenciamento de correio eletrônico que permite o recebimento de mensagens localmente ou remotamente;

(e) Errado. ARP (*Address Resolution Protocol*) é um protocolo de resolução de endereços lógicos (IP) para endereços físicos (MAC).

Gabarito: Letra B

---

9. **(IBADE / PREVES – 2017)** Um administrador de rede configurou as contas de e-mail dos usuários de uma empresa de modo a permitir que o status das mensagens recebidas seja igual tanto no servidor como no aplicativo de e-mail utilizado pelos usuários; que haja sincronia dessas mensagens, mantendo-se a conexão, para que as alterações e as novas mensagens recebidas no servidor sejam atualizadas quase que em tempo real no aplicativo de e-mail do usuário e que se mantivessem as duas cópias, tanto no servidor, quanto no aplicativo de e-mail. Para isso, esse administrador configurou o protocolo de recepção das mensagens de cada usuário como sendo o protocolo:

a) ARP
b) SMTP
c) FTP
d) IMAP
e) POP

Comentários:

(a) Errado. ARP (*Address Resolution Protocol*) é um protocolo de resolução de endereços lógicos (IP) para endereços físicos (MAC).

(b) Errado. SMTP (*Simple Mail Transfer Protocol*) é um protocolo para envio de correio eletrônico pela Internet;

(a) Errado. FTP (*File Transfer Protocol*) é um protocolo para transferência de arquivos (download/upload);

(d) Correto. IMAP (*Internet Message Access Protocol*) é um protocolo de gerenciamento de correio eletrônico que permite o recebimento de mensagens localmente ou remotamente;

(c) Errado. POP (*Post Office Protocol*) é um protocolo que permite o recebimento local de mensagens, mas não permite a sincronização de mensagens.

Gabarito: Letra D

---

10. (FUNRIO / Câmara Municipal de Nova Iguaçu – 2016) Dois tipos de protocolos que atendem de forma direta aos serviços de correio eletrônico na internet são os protocolos:

a) HTTP e NNTP.
b) SMTP e POP3.
c) RARP e ARP.
d) SSL e ICMP.

Comentários:

(a) Errado. HTTP é um protocolo de transferência de hipertexto que permite navegar em páginas na internet; NNTP é um protocolo que permite fazer o download de grandes quantidades de informações e que é bastante utilizado em grupos de notícia e discussão;

(b) Correto. SMTP é o protocolo utilizado por clientes de e-mail para o envio de mensagens de correio eletrônico; POP3 é um protocolo utilizado para receber mensagens e que permite o download de mensagens de correio eletrônico do provedor para o computador;

(c) Errado. RARP é um protocolo que possibilita que uma estação conheça um Endereço IP (Lógico) a partir de um Endereço MAC (Físico); ARP é o protocolo permite conhecer um Endereço MAC a partir de uma Endereço IP (Lógico).

(d) Errado. SSL é um protocolo utilizado em conjunto com outros (Ex: HTTP e FTP) para fornecer serviços de criptografia no tráfego de informações. ICMP é um protocolo utilizado para fornecer relatórios de erro de uma rede

Gabarito: Letra B

---

11. (FUNRIO / Câmara Municipal de Nova Iguaçu – 2016) O protocolo utilizado nos navegadores da internet para transmissão dos hipertextos é o:

a) BCP.
b) RARP.
c) HTTP.
d) SNMP.

Comentários:

O protocolo utilizado para transmissão de hipertexto é o HTTP – a sigla já dá a dica: HyperText Transfer Protocol.

Gabarito: Letra C

---

12. (FUNRIO / Câmara Municipal de Tanguá – 2016) As informações que trafegam durante uma navegação pela Internet podem ser facilmente capturadas. Uma forma de garantir seu sigilo é o uso de criptografia, encontrada em sites que usam o seguinte recurso:

a) https
b) firewall
c) antivírus
d) antispyware

Comentários:

O protocolo HTTP pode ser utilizado sobre uma camada de criptografia oferecida pelos protocolos TLS/SSL que fornece autenticidade –passando a se chamar HTTPS.

Gabarito: Letra A

---

13. (FUNRIO / CEITEC – 2012) Na internet o protocolo_____ permite a transferência de mensagens eletrônicas dos servidores de _____para caixa postais nos computadores dos usuários. As lacunas se completam adequadamente com as seguintes expressões:

a) Ftp/ Ftp.
b) Pop3 / Correio Eletrônico.
c) Ping / Web.
d) navegador / Proxy.
e) Gif / de arquivos.

Comentários:

Na internet, o protocolo POP3 permite a transferência de mensagens eletrônicas dos servidores de Correio Eletrônico para caixa postais nos computadores dos usuários.

Gabarito: Letra B

---

14. (FUNRIO / SEBRAE/PA – 2010) Sobre o modelo cliente/servidor utilizado pela Internet, qual afirmativa abaixo é a correta?

a) Um servidor SMTP é também conhecido como servidor de saída de e-mails.
b) Um servidor FTP é responsável pelo recebimento de e-mails.
c) Um cliente WWW realiza a função de mediar a comunicação da rede local com a Internet.
d) Um cliente Proxy fornece uma pasta para armazenamento de arquivos em servidores.
e) Um servidor POP serve para envio de arquivos para outros servidores.

Comentários:

(a) Correto, ele é também conhecido como Servidor de Saída; (b) Errado, um servidor FTP é responsável pelo envio e recebimento de arquivos; (c) Errado, essa é a função de um Proxy; (d) Errado, trata-se do Servidor FTP; (e) Errado, a questão trata do Servidor SMTP.

Gabarito: Letra A

---

15. (FUNRIO / DEPEN – 2009) Ao criar contas de e-mail para conexão numa ferramenta de correio eletrônico (como Microsoft Outlook Express ou Mozilla Thunderbird), deve-se escolher um protocolo para recebimento de mensagens. Qual das alternativas abaixo serve para essa finalidade?

a) FTP
b) POP
c) IP
d) SMTP
e) UDP

Comentários:

(a) Errado, esse é um protocolo de transferência de arquivos; (b) Correto, esse é um protocolo de recebimento de mensagens de correio eletrônico; (c) Errado, esse é um protocolo de roteamento de pacotes; (d) Errado, esse é um protocolo de envio de e-mails; (e) Errado, esse é um protocolo não confiável de transporte.

Gabarito: Letra B

---

16. (FUNRIO / DEPEN – 2009) Qual tipo de servidor utilizado para converter os nomes digitados na barra de endereços de um navegador para um endereço IP válido?

a) ISP
b) SMTP
c) Proxy
d) DHCP
e) DNS

Comentários:

O servidor utilizado para converter nomes digitados na barra de endereços de um navegador para um endereço IP válido é o Sistema de Nome de Domínio (DNS).

Gabarito: Letra E

---

17. (FUNRIO / MDIC – 2009) O protocolo HTTP (*Hiper Text Transfer Protocol*) tem a função básica de:

a) transferir arquivos.
b) exibir páginas em formato HTML.
c) traduzir URL em endereços IP.
d) evitar o acesso não autorizado aos recursos de uma rede.
e) criar páginas dinâmicas.

Comentários:

(a) Errado, essa é a função básica do FTP; (b) Correto, essa é a função básica do HTTP; (c) Errado, essa é a função básica do DNS: (d) Errado, essa é a função básica de um Firewall; (e) Errado, essa é a função básica de algumas linguagens de programação.

Gabarito: Letra B

---

18. (FUNRIO / Ministério da Justiça – 2009) O Protocolo da Internet responsável pelo recebimento de mensagens, copiando-as para o computador é o:

a) SMTP
b) http
c) Webmail
d) FTP
e) POP3

Comentários:

O protocolo responsável pelo recebimento de mensagens, copiando-as para o computador é o... POP3.

Gabarito: Letra E

---

19. (FUNRIO / Ministério da Justiça – 2009) O protocolo HTTPS é considerado seguro porque:

a) verifica com um AntiSpyware o endereço acessado.
b) escaneia os arquivos procurando por vírus antes de baixá-los.
c) só funciona dentro de uma Intranet.
d) utiliza criptografia.
e) impede o uso de Spoofing.

Comentários:

(a) Errado, ele não realiza essa atividade; (b) Errado, ele não realiza essa atividade; (c) Errado, ele funciona também na Internet; (d) Correto, ele realmente utiliza criptografia; (e) Errado, ele não impede uso de spoofing.

Gabarito: Letra D

---

20. (FUNRIO / SUFRAMA – 2008) No contexto da Internet, qual o significado da sigla DNS?

a) Provedor de serviços de internet através do qual um computador se conecta à internet.
b) Conjunto de protocolos que permitem a comunicação entre computadores.
c) Servidor de rede que controla o acesso dos demais computadores a uma rede.
d) Computador central que traduz nomes de domínios para endereços de protocolo na internet.
e) Sistema que permite localizar os computadores ligados a uma rede pelo seu nome.

Comentários:

(a) Errado, esse é o ISP; (b) Errado, esse é o TCP/IP; (c) Errado, isso seria uma pilha ou arquitetura de protocolos; (d) Correto. A sigla significa Serviço de Nome de Domínio, logo trata-se de um computador central capaz de traduzir nomes de domínios para endereços de protocolo na internet; (e) Errado, essa é a URL.

Gabarito: Letra D

LISTA DE QUESTÕES – BANCAS DIVERSAS

1. **(CONSULPLAN / Prefeitura de Patos de Minas – 2015)** Assinale a alternativa que se trata de um protocolo de internet de transferência de arquivo, bastante rápido e versátil utilizado.

   a) FTP.
   b) HTTP.
   c) HTM.
   d) HTML.

2. **(ESAF / Ministério da Fazenda – 2013)** Para o funcionamento da Internet, há um sistema de gerenciamento de nomes hierárquico e distribuído, que resolve nomes de domínios em endereços de rede (IP), que é o:

   a) POP3
   b) DNS
   c) HTTP
   d) HTTPS
   e) SMTP

3. **(ESAF / Ministério da Fazenda – 2013)** Um exemplo de protocolo de transporte utilizado na Internet é o protocolo:

   a) XTP
   b) TPP
   c) UDP
   d) TRP
   e) HTTP

4. **(CONSULPLAN / Prefeitura de Cantagalo – 2013)** O Outlook Express é um aplicativo para gerenciamento de e-mail, porém, para enviar e receber, são necessárias algumas configurações, como as portas dos protocolos POP e SMTP. As portas dos protocolos POP e SMTP configuradas no Outlook Express são, respectivamente,

   a) 25 e 115.
   b) 110 e 587.
   c) 466 e 25.
   d) 587 e 965.
   e) 993 e 587.

5. **(ESAF / Ministério da Fazenda – 2012)** O Correio Eletrônico é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação. O termo e-mail é aplicado aos sistemas que utilizam a Internet e são baseados no protocolo:

a) SNMP.
b) SMTP.
c) Web.
d) HTTP.
e) HTTPS.

6. **(ESAF / Ministério da Fazenda – 2012)** O componente mais proeminente da Internet é o Protocolo de Internet (IP), que provê sistemas de endereçamento na Internet e facilita o funcionamento da Internet nas redes. O IP versão 4 (IPv4) é a versão inicial usada na primeira geração da Internet atual e ainda está em uso dominante. Ele foi projetado para endereçar mais de 4,3 bilhões de computadores com acesso à Internet. No entanto, o crescimento explosivo da Internet levou à exaustão de endereços IPv4. Uma nova versão de protocolo foi desenvolvida, denominada:

a) IPv4 Plus.
b) IP New Generation.
c) IPV5.
d) IPv6.
e) IPv7.

7. **(ESAF / Ministério da Fazenda – 2012)** Quando um visitante de um sítio Web se conecta a um servidor que está utilizando um protocolo específico de segurança, ele irá notar, na barra de endereços, que o protocolo de comunicação passa a ser https:// (no lugar do http:// padrão). Além disso, a maioria dos browsers (como o Internet Explorer por exemplo) mostram no browser o desenho de um cadeado. Quando este cadeado está sendo mostrado, o usuário passa a ter a tranquilidade de saber que as informações fornecidas àquele Website não poderão ser interceptadas no seu trajeto. Este protocolo específico de segurança é o:

a) WebSec
b) HTTP
c) HTML
d) SSL
e) TCP/IP

8. **(IBADE / IPERON – 2017)** Ao utilizar um software de correio eletrônico, um usuário precisou configurar o funcionamento do protocolo responsável pelo envio de e-mail através da rede. Nesse caso, ele acessou a configuração do protocolo:

a) WAP.
b) SMTP.

c) POP.
d) IMAP.
e) ARP.

9. **(IBADE / PREVES – 2017)** Um administrador de rede configurou as contas de e-mail dos usuários de uma empresa de modo a permitir que o status das mensagens recebidas seja igual tanto no servidor como no aplicativo de e-mail utilizado pelos usuários; que haja sincronia dessas mensagens, mantendo-se a conexão, para que as alterações e as novas mensagens recebidas no servidor sejam atualizadas quase que em tempo real no aplicativo de e-mail do usuário e que se mantivessem as duas cópias, tanto no servidor, quanto no aplicativo de e-mail. Para isso, esse administrador configurou o protocolo de recepção das mensagens de cada usuário como sendo o protocolo:

a) ARP
b) SMTP
c) FTP
d) IMAP
e) POP

10. **(FUNRIO / Câmara Municipal de Nova Iguaçu – 2016)** Dois tipos de protocolos que atendem de forma direta aos serviços de correio eletrônico na internet são os protocolos:

a) HTTP e NNTP.
b) SMTP e POP3.
c) RARP e ARP.
d) SSL e ICMP.

11. **(FUNRIO / Câmara Municipal de Nova Iguaçu – 2016)** O protocolo utilizado nos navegadores da internet para transmissão dos hipertextos é o:

a) BCP.
b) RARP.
c) HTTP.
d) SNMP.

12. **(FUNRIO / Câmara Municipal de Tanguá – 2016)** As informações que trafegam durante uma navegação pela Internet podem ser facilmente capturadas. Uma forma de garantir seu sigilo é o uso de criptografia, encontrada em sites que usam o seguinte recurso:

a) https
b) firewall
c) antivírus
d) antispyware

13. **(FUNRIO / CEITEC – 2012)** Na internet o protocolo_____ permite a transferência de mensagens eletrônicas dos servidores de _____para caixa postais nos computadores dos usuários. As lacunas se completam adequadamente com as seguintes expressões:

a) Ftp/ Ftp.
b) Pop3 / Correio Eletrônico.
c) Ping / Web.
d) navegador / Proxy.
e) Gif / de arquivos.

14. **(FUNRIO / SEBRAE/PA – 2010)** Sobre o modelo cliente/servidor utilizado pela Internet, qual afirmativa abaixo é a correta?

a) Um servidor SMTP é também conhecido como servidor de saída de e-mails.
b) Um servidor FTP é responsável pelo recebimento de e-mails.
c) Um cliente WWW realiza a função de mediar a comunicação da rede local com a Internet.
d) Um cliente Proxy fornece uma pasta para armazenamento de arquivos em servidores.
e) Um servidor POP serve para envio de arquivos para outros servidores.

15. **(FUNRIO / DEPEN – 2009)** Ao criar contas de e-mail para conexão numa ferramenta de correio eletrônico (como Microsoft Outlook Express ou Mozilla Thunderbird), deve-se escolher um protocolo para recebimento de mensagens. Qual das alternativas abaixo serve para essa finalidade?

a) FTP
b) POP
c) IP
d) SMTP
e) UDP

16. **(FUNRIO / DEPEN – 2009)** Qual tipo de servidor utilizado para converter os nomes digitados na barra de endereços de um navegador para um endereço IP válido?

a) ISP
b) SMTP
c) Proxy
d) DHCP
e) DNS

17. **(FUNRIO / MDIC – 2009)** O protocolo HTTP (*Hiper Text Transfer Protocol*) tem a função básica de:

a) transferir arquivos.
b) exibir páginas em formato HTML.

c) traduzir URL em endereços IP.
d) evitar o acesso não autorizado aos recursos de uma rede.
e) criar páginas dinâmicas.

18. **(FUNRIO / Ministério da Justiça – 2009)** O Protocolo da Internet responsável pelo recebimento de mensagens, copiando-as para o computador é o:

a) SMTP
b) http
c) Webmail
d) FTP
e) POP3

19. **(FUNRIO / Ministério da Justiça – 2009)** O protocolo HTTPS é considerado seguro porque:

a) verifica com um AntiSpyware o endereço acessado.
b) escaneia os arquivos procurando por vírus antes de baixá-los.
c) só funciona dentro de uma Intranet.
d) utiliza criptografia.
e) impede o uso de Spoofing.

20. **(FUNRIO / SUFRAMA – 2008)** No contexto da Internet, qual o significado da sigla DNS?

a) Provedor de serviços de internet através do qual um computador se conecta à internet.
b) Conjunto de protocolos que permitem a comunicação entre computadores.
c) Servidor de rede que controla o acesso dos demais computadores a uma rede.
d) Computador central que traduz nomes de domínios para endereços de protocolo na internet.
e) Sistema que permite localizar os computadores ligados a uma rede pelo seu nome.

GABARITO – BANCAS DIVERSAS

1. LETRA A
2. LETRA B
3. LETRA C
4. LETRA B
5. LETRA B
6. LETRA D
7. LETRA D
8. LETRA B
9. LETRA D
10. LETRA B
11. LETRA C
12. LETRA A
13. LETRA B
14. LETRA A
15. LETRA B
16. LETRA E
17. LETRA B
18. LETRA E
19. LETRA D
20. LETRA D

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.