

Aula 00 - Prof. André Castro

*ACFOR (Analista de Regulação - Área 2
- Ciências da Computação) Redes e
Segurança - 2024 (Pós-Edital)*

Autor:
André Castro

15 de Outubro de 2024

Índice

1) Apresentação do Curso - Prof. André Castro	3
2) Apresentação Flashcards	8
3) HTTP - Teoria	10
4) HTTP - Questões Comentadas - Cebraspe	27
5) HTTP - Questões Comentadas - FCC	37
6) HTTP - Questões Comentadas - FGV	44
7) HTTP - Questões Comentadas - Cesgranrio	46
8) HTTP - Lista de Questões - Cebraspe	47
9) HTTP - Lista de Questões - FCC	53
10) HTTP - Lista de Questões - FGV	58
11) HTTP - Lista de Questões - Cesgranrio	60



APRESENTAÇÃO

Olá, pessoal! Como estão? Espero que bem e animados para essa jornada.

Aqui é o **André Castro**, professor de Redes de Computadores e Segurança da Informação do Estratégia Concursos. Sou formado em **Engenharia de Redes de Comunicação pela Universidade de Brasília – UnB** e pós-graduado na área de Segurança e Administração de Redes também pela UnB.

Atualmente, após um ciclo de 14 anos no serviço público como servidor público, fiz uma transição de carreira para o setor privado. Hoje, estou exercendo a função de Estrategista de Governo e Especialista em Transformação Digital na Microsoft Brasil, em Brasília.

Na trajetória de Governo, exerci o último cargo de Analista em Tecnologia do Ministério da Economia ou atual Ministério da Gestão e Inovação, tendo exercido cargos de relevância à frente de unidades de tecnologia do Governo Federal. No último ciclo de Governo, estive como Assessor Especial de Tecnologia na AGU e antes disso, atuei como Subsecretário/CIO de Tecnologia da Informação do Ministério da Educação.

Fui **aprovado** ainda nos concursos de Analista Administrativo da Câmara dos Deputados, realizado em 2011 e **aprovado** no concurso de Analista para o Banco Central do Brasil em 2013. Exerci ainda atividades de instrução e apoio em alguns cursos na área de Redes e Segurança pela Escola Superior de Redes – ESR, da Rede Nacional de Pesquisa – RNP, além de outros projetos relacionados a concursos públicos, incluindo aulas presenciais.

Para você que se prepara para concursos públicos na área de tecnologia... Pois bem... preparei um material muito bacana e bem completo sobre os assuntos voltados para a nossa temática, que possuem algumas variações a depender do cargo e do concurso, e por isso buscamos trazer uma abordagem bem completa e eficiente para não deixar lacunas e não exceder conteúdos desnecessariamente.

A ideia é que você possa conhecer os tópicos mais importantes e ter uma abordagem diferenciada e com didática adequada para sua preparação. O meu foco é sempre buscar ser o mais preciso possível nos assuntos, otimizando e muito o seu tempo de preparação. Você perceberá isso ao longo do curso.

Abraço,

Prof. André Castro





@profandrecaastro



Instagram



YouTube



andrecastroprofessor@gmail.com



/professorandrecaastro

Também gostaria de convidá-lo a conhecer alguns projetos da equipe de TI:



Nosso podcast alternativo:

<https://anchor.fm/estrategia-tech>



Nosso grupo do Telegram:

https://t.me/estrategia_ti



Perfil no Instagram:

<http://instagram.com/estrategiaconcursosti>



INFORMAÇÕES GERAIS

É nítida a evolução conjunta das partes envolvidas em concursos públicos, uma vez que temos provas cada vez mais difíceis, com um nível maior de inteligência e preparação das questões, bem como o surgimento constante de novos conceitos e abordagens.

Além disso, o nível dos candidatos que têm concorrido às vagas de cargos públicos tem aumentado e tende a continuar aumentando, como se pode verificar pela simples análise das melhores notas obtidas em diversos concursos.

A **preparação para concursos** considerados de médio e alto nível **demandam tempo e dedicação prévia**.

Quando você tiver se preparando para o seu concurso, seja com edital ou não, tenho a intenção de possibilitar ao candidato a preparação, especificamente para o propósito a que propomos, bem como para os mais diversos editais na área de TI. A minha expectativa é que os nossos alunos estejam passos à frente dos demais candidatos nessa fase de preparação.

INFORMAÇÕES SOBRE O CURSO

Abordaremos nesse curso todos os tópicos apresentados em nosso cronograma. **Faremos juntos muitos exercícios para fixação do conteúdo ao final de cada aula**, sempre de forma objetiva, prática e complementar.

Entretanto, gostaria de lembrar da dificuldade de esgotar as possibilidades de cada assunto até o seu nível máximo de detalhe em cada aula por se tratar de assuntos demasiadamente extensos.

O ponto chave de cada assunto é entender o perfil da banca e o perfil do órgão para o qual a banca está prestando o serviço. Diante disso, buscarei estar alinhado a esses pontos para **direcioná-los** da melhor forma possível, realizando diversos exercícios, principalmente dos últimos concursos ou concursos equivalentes. Contem comigo para isso!

Ressalto ainda o meu compromisso de buscar cumprir o cronograma da melhor maneira possível. No entanto, ao longo do curso, posso identificar **alguns ajustes na ordem da apresentação dos conteúdos ou ainda a necessidade de adaptação a alguma alteração do Edital em caso de divulgação**, portanto, digo a vocês que o cronograma não é de todo rígido.

Desde já eu agradeço a confiança de cada um de vocês e tenham certeza que esse curso irá auxiliá-los bastante nessa jornada. Não deixem de me procurar no **fórum para esclarecimentos de dúvidas, por favor!**

Não deixem acumular lacunas em seu aprendizado pois a *"lei de Murphy"* se aplica aqui...!!! Vai ser exatamente essa lacuna que será cobrada na prova e você vai se arrepender depois de não ter perguntado. *Digo por experiência própria!*

Críticas, reclamações, sugestões, comentários ou identificação de erros de digitação **podem ser enviados para o nosso fórum**. Tentarei responder com a maior brevidade possível.



INFORMAÇÕES SOBRE AS AULAS

Apresento a vocês algumas metodologias adotadas em nossas aulas que aprendi ao estudar para concursos e que me ajudaram bastante, bem como no compartilhamento de experiências com outros professores:



1 - Parágrafos curtos e objetivos: Sempre que possível, os parágrafos serão reduzidos para facilitar a leitura e não a tornar cansativa, buscando sempre maior fluidez. O cronograma também segue esse princípio, deixando as aulas objetivas e eficazes em termos de organização e extensão do conteúdo. *De repente vocês terão tempo até para estudar as demais outras matérias...!!!*

2 - Entender o Básico (Princípios e Fundamentos): *Isso não é óbvio André?* Não, não é! Muitas das vezes nos preocupamos em aprender ou “decorar” os detalhes de determinada disciplina ou matéria, buscar tabelas e figuras para memorizar e esquecemos os princípios, o básico, aquilo que com certeza te ajudará a entender os detalhes. Portanto, estejam atentos a isso, por favor, ok?

3 - Linguagem Comum: Tentarei fazer com que a sua leitura se aproxime de **um diálogo ou uma aula expositiva e presencial**. O objetivo é não deixar a leitura cansativa para aqueles que talvez tenham dificuldades com leituras extensas, como eu. **Combinado?**

4 - Exercícios: Ler por si só já é bem cansativo. Imagina leituras bibliográficas, como o livro do Tanenbaum, Forouzan ou Kurose com mais de 600 páginas? Convenhamos, né? Na maioria das vezes não vale a pena, a não ser para dúvidas pontuais e consolidação de determinado conteúdo. Além disso, deixe esse trabalho comigo, a não ser que você tenha tempo sobrando. Invista seu tempo em uma boa leitura do material e **principalmente na resolução de exercícios!!!**

A essência dos exercícios muitas vezes se repete, portanto, se você já tiver feito muitos, mas muitos exercícios, é provável que você se depare com questões iguais ou semelhantes nas provas seguintes.

Utilizarei exercícios também para esclarecer ou mencionar algum ponto que tenha passado na parte teórica. Vamos nos esforçar para que você precise de apenas mais uma prova para sua aprovação, certo?

Focaremos nos exercícios da **Banca Examinadora do Concurso**. Porém, sempre que houver necessidade, seja para complementarmos o conteúdo ou por falta de exercícios da banca sobre determinada matéria, utilizaremos exercícios de outras bancas também.

5 - Artifícios Complementares: O conteúdo de redes possui a vantagem de ter muita figura ilustrativa, o que nos ajuda a entender o conteúdo. Então sempre buscarei trazer figuras, imagens, tabelas e diagramas para tornar a leitura mais saudável e clara. Geralmente, é mais fácil memorizar uma figura ilustrativa do que puramente o conteúdo escrito.



6 - Linhas Destacadas em vermelho: Utilizarei esse recurso de destaque em negrito e vermelho das palavras e frases que são mais importantes dentro de alguns parágrafos para uma posterior **leitura vertical** (Segunda leitura do material com o objetivo de revisão dos pontos destacados).

7 - Revisão em Exercícios: Pessoal, a tendência é que nos assuntos iniciais, façamos a leitura e façamos os exercícios com um bom índice de acerto, pois você ainda estará com a memória fresca. Porém, tal índice nem sempre se mantém após semanas da leitura daquele conteúdo.

Portanto, é muito importante que estejam sempre voltando e fazendo alguns exercícios avulsos para fixar o conhecimento, além do que, será a oportunidade para descobrir onde você está tendo mais dificuldade de memorização e aprendizado.

ATENÇÃO

As videoaulas estão sendo constantemente gravadas e, dessa forma, não há garantia de que teremos todo o conteúdo disponível em vídeo. Então seu curso pode ou não ter as gravações a depender do edital.

Mas tenham certeza de que tudo e mais um pouco estará em seus PDF's.

Ufa, chega de apresentações e informações, certo? Vamos ao que interessa! Procurem estar descansados e tranquilos com vistas a obter uma leitura suave do conteúdo para otimizarmos os resultados das nossas aulas.



ESTRATÉGIA FLASHCARDS

 Você tem dificuldade de estudar, memorizar e revisar os conteúdos que estuda em nossas aulas? Então nós temos a ferramenta perfeita para você!

Apresentamos o **Estratégia Cards**: app de flashcards que vai revolucionar sua forma de **estudar e revisar** conteúdos de provas de concurso público. Com nossa tecnologia inovadora e interface amigável, você dominará os tópicos mais complexos de maneira eficiente e divertida.

💡 Recursos do Estratégia Cards:

Curadoria de Flashcards	Flashcards criados e revisados por professores especializados em cada área, com qualidade e voltados para concursos públicos.
Flashcards Personalizados	Crie seus próprios flashcards, cobrindo os principais tópicos e matérias dos concursos públicos.
Repetição Espaçada	Técnica de aprendizagem que envolve revisar informações em intervalos crescentes para melhorar a retenção de longo prazo e combater o esquecimento.
Estatísticas Personalizadas	Visualize graficamente o percentual de acertos, erros ou dúvidas dos decks estudados.
Modo Offline	Estude em qualquer lugar, mesmo sem conexão à internet, fazendo o download dos decks.
Estudo por Áudio	<i>Está dirigindo ou fazendo esteira e quer continuar estudando?</i> Basta utilizar a opção “Escutar”.
Decks Favoritos	Você pode escolher decks específicos como favoritos e visualizá-los em uma aba separada do app.
Opções de Estudo	Você poderá estudar todos os cards de um deck; ou apenas os que você errou; ou apenas os que você não estudou ainda; entre outras opções.

E como eu consigo baixar?



É muito fácil! Basta pesquisar por “Estratégia Cards” na loja oficial do seu smartphone.

Se você tiver um Android, basta acessar a **Google Play**;



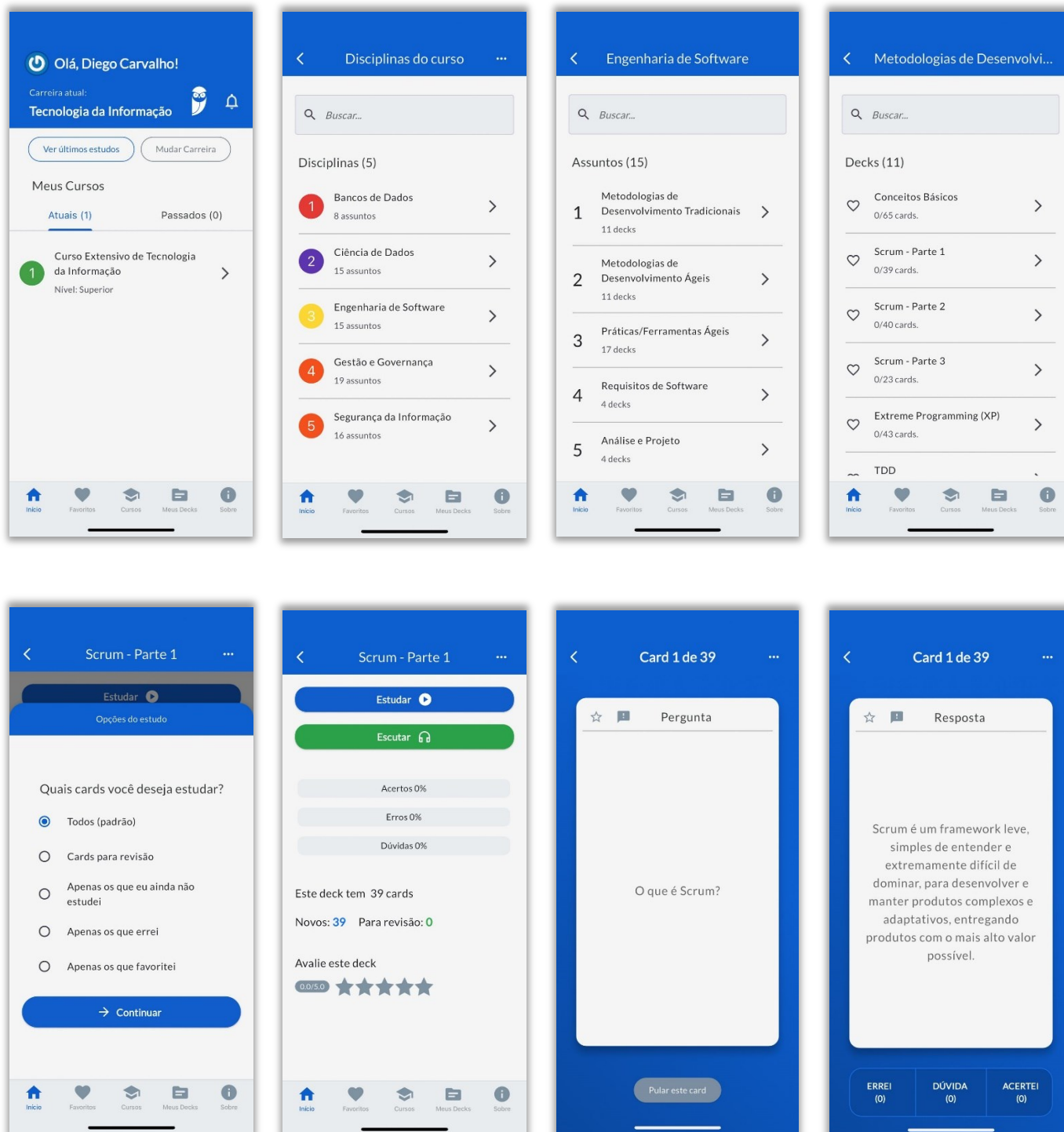
Se for tiver um iPhone, basta acessar a **App Store (iOS)**.



E para acessar?

Para acessar, basta ter uma conta no Estratégia Concursos. Em seguida, utilize suas credenciais de login e senha para acessar o aplicativo. Por fim, acesse a carreira de Tecnologia da Informação.

Como utilizar o app:



PROTOCOLOS E TECNOLOGIAS DA CAMADA DE APLICAÇÃO

Chegamos na etapa que será uma verdadeira sopa de letrinhas com diversos protocolos vinculados aos diversos tipos de serviços oferecidos via rede. As bancas cobram recorrentemente detalhes de cada tipo desses protocolos e por esse motivo, vamos esmiuçar um por um com vistas a termos um aprendizado completo sobre os assuntos.

Protocolo HTTP

O protocolo HTTP (Hypertext Transfer Protocol) foi criado sob a perspectiva de ser utilizado de uma arquitetura CLIENTE-SERVIDOR. É um protocolo chave para a comunicação de dados na Internet que permite a navegação WEB.

Algumas questões trazem a definição crua do HTTP:

Protocolo para a troca ou transferência de hipertexto utilizado em sistemas de hipermídia, distribuídos ou colaborativos.

Outra característica é a padronização de mensagens que os clientes enviam aos servidores e vice-versa.

Por ser baseado na arquitetura CLIENTE-SERVIDOR, utiliza o modelo de REQUISIÇÃO-RESPOSTA. Utiliza ainda o conceito de sessão a nível de aplicação. O seu procedimento básico ocorre nas seguintes etapas:



O cliente estabelece uma conexão TCP com o servidor, geralmente, na porta 80, sendo esta a porta padrão do protocolo;

O servidor responde à mensagem indicando o estado corrente da requisição, além da versão suportada e outras informações do servidor;

A partir de então, se não houver mensagem de erro, a conexão será estabelecida.

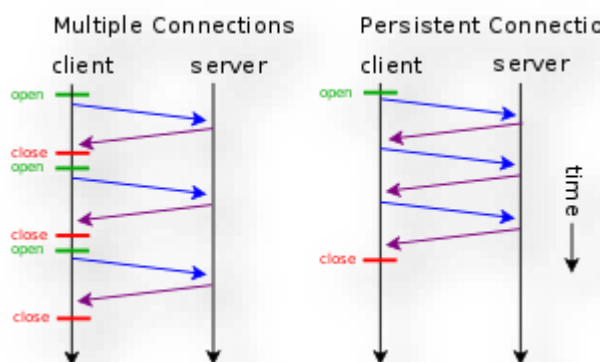




Utiliza codificação dos dados em textos ASCII, para que possam ser devidamente interpretados pelos servidores e clientes.

Para efeito de concurso, o HTTP possui 2 versões:

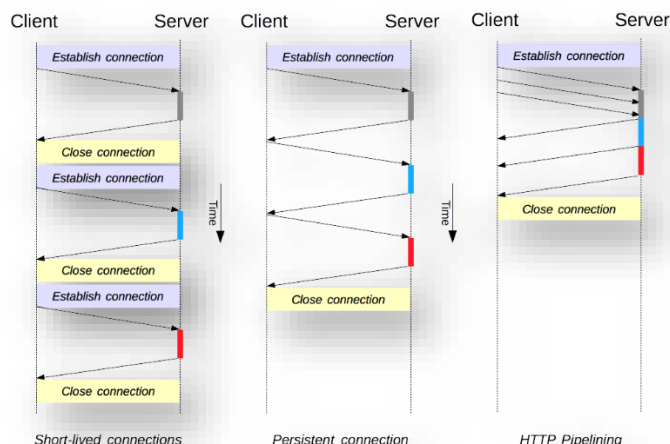
- **HTTPv1.0** – **Não realiza** conexões persistentes. Isto é, para cada troca de informação entre cliente e servidor, necessita-se estabelecer e encerrar uma nova conexão TCP;
- **HTTPv1.1** – **Realiza** conexões persistentes. Estabelece-se apenas uma requisição TCP para a troca de diversas mensagens entre o cliente e servidor. Além disso, pode-se enviar mais de uma requisição sem necessariamente aguardar a confirmação da requisição anterior.



Além disso, é importante destacar que o HTTP em sua versão persistente pode trabalhar ainda de forma sequencial ou paralelo. No primeiro caso, troca-se mensagens de requisição e resposta sempre par a par, ou seja, só se envia uma nova requisição depois do recebimento da referida resposta.

Já no modo paralelo (também conhecido como modo pipelining), pode-se apresentar várias requisições independentemente do recebimento das respostas. A figura abaixo representa todas as possibilidades.





Além disso, o protocolo **HTTP** é considerado um protocolo **sem estado (stateless)**, pois não armazena informações do usuário.

Um ponto importante a mencionar é que o servidor pode enviar informações ao usuário com vistas a manter a sessão entre eles aberta, além de poder recuperar certas informações futuramente. Esse recurso pode ser provido com o uso de COOKIES, que podem ser armazenados no browser do cliente.

Assim tem-se um ambiente statefull, porém, vale lembrar que isso é um recurso complementar. O HTTP nativamente é **stateless**.



(CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O protocolo HTTP, que não armazena informações sobre o estado do cliente, classifica-se como do tipo stateless.

Comentários:

Vimos que essa é uma característica nativa do protocolo HTTP.

Gabarito: C

Estrutura da Mensagem HTTP

Como vimos, existem dois tipos de mensagem HTTP: requisição e resposta. Vamos verificar a estrutura de cada uma delas:



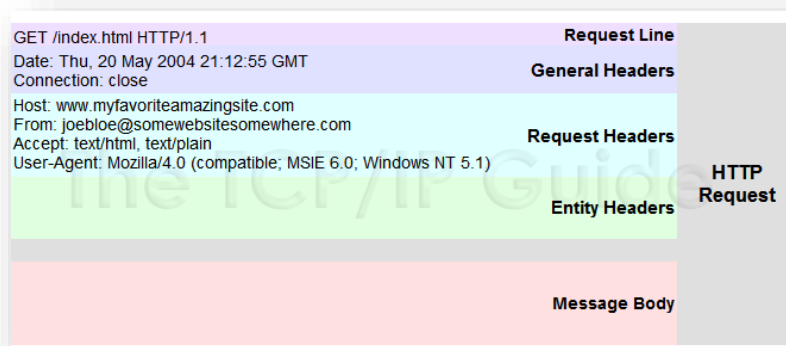


- **Requisição:** Pode ser dividida em 3 partes: **linha de requisição, cabeçalho e corpo da entidade;**

O método utilizado, o caminho do objeto e a versão do protocolo fazem parte da linha de requisição. Outras informações referentes ao nome da página, estado corrente da conexão, informações de navegador (User Agent) e línguas aceitas ficam por conta do cabeçalho.

Na requisição, o Corpo da Entidade é utilizado com o método POST uma vez que o cliente envia informações ao servidor para preenchimento do objeto de resposta.

A figura abaixo é um exemplo de composição da mensagem HTTP:



- **Resposta:** Pode ser dividida em 3 partes: **linha de estado, cabeçalho e corpo da entidade;**

A versão do protocolo e o estado da conexão são apresentados na linha de estado. Os demais campos são semelhantes às mensagens de Requisição. Abaixo temos o exemplo:



HTTP/1.1 200 OK	Status Line
Date: Thu, 20 May 2004 21:12:58 GMT	General Headers
Connection: close	
Server: Apache/1.3.27	Response Headers
Accept-Ranges: bytes	
Content-Type: text/html	Entity Headers
Content-Length: 170	
Last-Modified: Tue, 18 May 2004 10:14:49 GMT	
HTTP Response	
<html> <head> <title>Welcome to the Amazing Site!</title> </head> <body> <p>This site is under construction. Please come back later. Sorry!</p> </body> </html>	
	Message Body

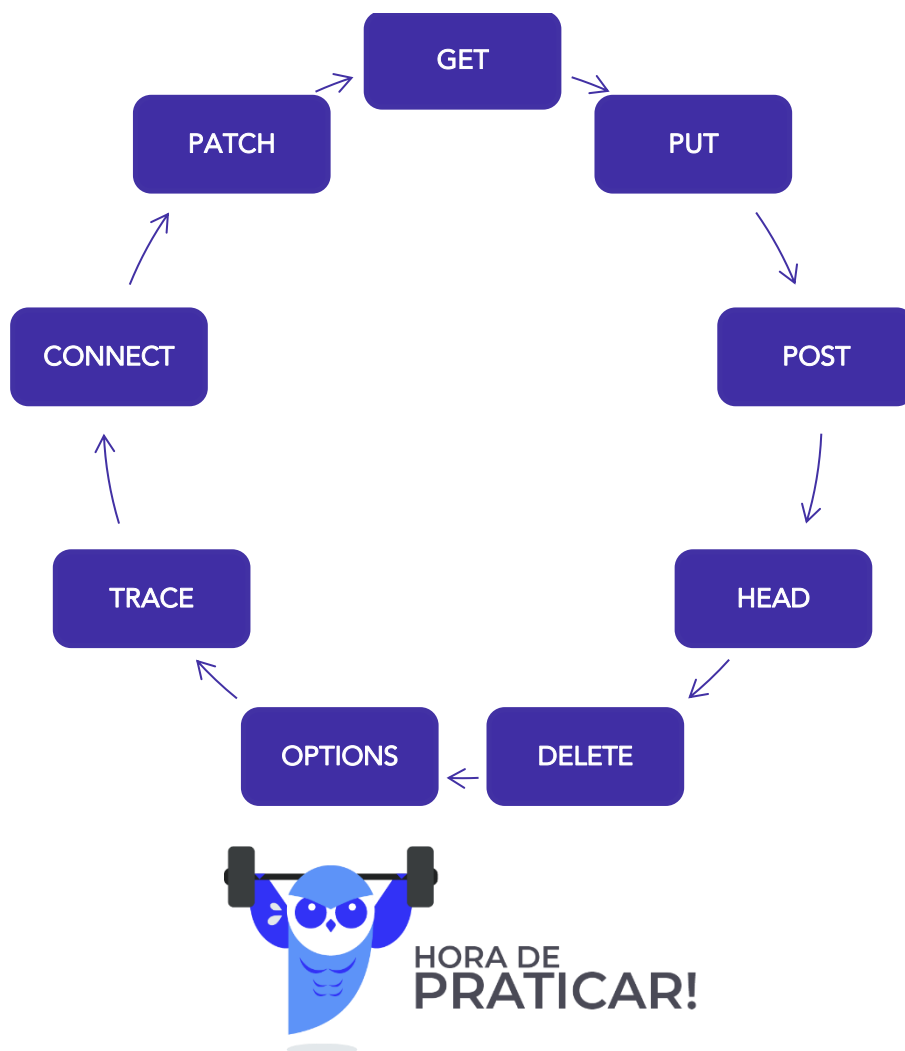
Métodos HTTP

Cada método é responsável por determinar o tipo de requisição feita e a forma como o dado será tratado. Atenção para o fato de que todos devem ser escritos em letras maiúsculas. O protocolo faz a devida diferenciação. Vamos conhecê-los:



- **GET** – Solicitação de leitura de determinado objeto. A requisição de páginas WEB pode ser feita através desse método;
- **PUT** – Solicitação de gravação de determinado objeto. Pode-se enviar páginas para um servidor remoto através desse método;
- **POST** – Método utilizado para anexar informações ou enviar arquivos de dados ou formulários como complemento de uma requisição de leitura. Dessa forma, a resposta dependerá da informação enviada. Basicamente trata a criação/atualização de um objeto ou recurso existente.
- **HEAD** – Mesma lógica do GET. Entretanto, solicita a leitura apenas do cabeçalho de um objeto ou página WEB. Tranquilo quando você vincula o nome do método com a estrutura do dado, certo? HEAD = CABEÇALHO. Com isso pode-se obter informações como a data da última modificação da página.
- **DELETE** – Remove o objeto ou página no servidor;
- **OPTIONS** – Realiza a consulta de determinadas opções;
- **TRACE** – Utilizado para teste com mensagens do tipo loopback;
- **CONNECT** – Utilizado para comunicação com servidores PROXY;
- **PATCH** – Utilizado para aplicar modificações parciais a um recurso;





(CESPE - TJ TRE MS/Apoio Especializado/Programação de Sistemas/2013) Com referência ao Hyper Text Transfer Protocol (HTTP) — protocolo de aplicação utilizado para o tratamento de pedidos e respostas entre cliente e servidor na Internet e com o qual, normalmente, são desenvolvidas as aplicações para a Web —, assinale a opção em que todas as expressões identificam métodos de requisição HTTP que devem ser implementados por um servidor HTTP 1.1 usado pelo cliente.

- A) SOAP, WS, WSDL, UDDI
- B) TCP, IP, NETBIOS, UDP, IPX
- C) NFS, SMB, IPP, SMTP, POP3, IMAP, XMPP, SIP
- D) SET, GET, CONSTRUCTOR, DESTRUCTOR
- E) GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS

Comentários:



A alternativa "E" descreve 7 dos 9 existentes. Faltam ainda os métodos CONNECT e PATCH. Os mais utilizados sem dúvida são os 3 primeiros.

Gabarito: E

Códigos de estado

Os códigos de estado são definidos em classes, conforme a seguir, com a descrição dos principais códigos:



- **1xx - Classe informacional** - Esta classe indica uma resposta provisória, que consiste de informações do estado da requisição e cabeçalhos opcionais.
- **2xx - Classe de Sucesso** - Indica que a requisição foi recebida, entendida, aceita e processada.
- **3xx - Classe de Redirecionamento** - Indica a necessidade de atuação por parte do cliente HTTP para completar a requisição. Pode ou não ser o caso de atuação direta do usuário.
- **4xx - Classe de Erro de Cliente** - Indica a possibilidade de que houve um erro na requisição por parte do cliente. Caso não seja uma requisição com método HEAD, o servidor enviará uma explicação da situação do erro e se esta é permanente ou temporária.

400 (BAD REQUEST) - A requisição não pode ser entendida pelo servidor devido erro de sintaxe.

401 (UNAUTHORIZED) - A requisição depende de autenticação por parte do usuário.

403 (FORBIDDEN) - O servidor entendeu a requisição, mas se recusa a atendê-la. Pode ser enviado a descrição do motivo da recusa.

404 (NOT FOUND) - O servidor não encontrou nenhum documento que coincida com a URI informada.

- **5xx - Classe de Erro de Servidor** - Indica que o servidor reconheceu um erro interno ou a incapacidade de atender a requisição.

500 (INTERNAL SERVER ERROR) - Erro inesperado que impediu o atendimento a requisição.

503 (SERVICE UNAVAILABLE) - Servidor está incapacitado de atender as requisições devido à sobrecarga ou manutenção. Indica uma condição temporária.



505 (VERSION NOT SUPPORTED) - O servidor não suporta ou não está habilitado a responder para a versão requisitada. O servidor indica o motivo do erro, além de informar as versões que são suportadas e permitidas.

Esses códigos são característicos das mensagens de resposta de um servidor WEB qualquer.



(CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) Ao receber uma requisição, o servidor procura pelo recurso requisitado e envia, ao cliente, uma resposta com um código, que pode iniciar-se por 1xx, que indica sucesso no recebimento da requisição; 2xx, que indica redirecionamento da requisição; 3xx, que informa erros acontecidos no cliente; e 4xx, que informa erros no servidor.

Comentários:

Pessoal, a ordem correta é:

- 1xx – Classe informacional
- 2xx – Classe de sucesso
- 3xx – Classe de redirecionamento
- 4xx – Erros no lado do cliente
- 5xx – Erros no lado do servidor

Gabarito: E

Conceito de CACHE WEB

O funcionamento do CACHE WEB reside na possibilidade de otimização do procedimento de Requisição e Resposta entre o cliente e o servidor. Esse CACHE WEB busca evitar que novas consultas que sejam idênticas a consultas anteriores consumam recursos do servidor de destino, além de diminuir o tempo de resposta.

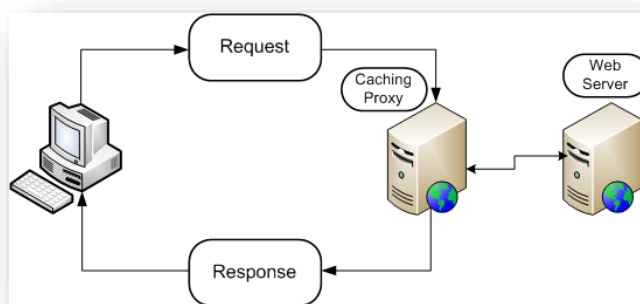
Sua implementação pode se dar:



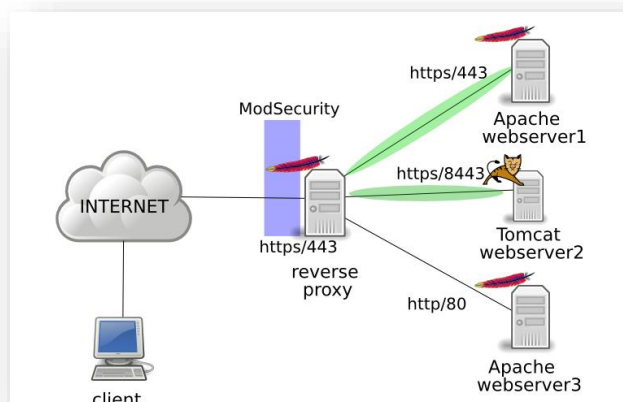


- **Servidor Proxy** – Pode-se adicionar um elemento intermediário entre o cliente e o servidor, de tal forma que as consultas necessariamente passem pelo nó intermediário antes de chegar ao destino. Esse nó, é chamado de Proxy e armazena as últimas informações requisitas pelos clientes aos servidores.

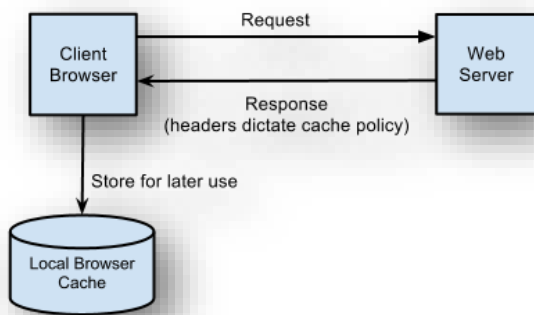
Dessa forma, caso haja uma nova requisição em que o proxy possua as informações necessárias para resposta, este não repassará a consulta ao servidor, atendendo a requisição imediatamente. É importante ressaltar que a presença do PROXY implica em duas conexões a serem estabelecidas: Cliente e PROXY; PROXY e Servidor.



- **Proxy reverso** – Esse conceito gera alguns benefícios na implementação de serviços HTTP no lado do servidor. Entre eles temos os recursos de proteção, balanceamento e distribuição de requisições e armazenamento em cache das informações estáticas. Dessa forma, quando há uma requisição a um objeto estático, o proxy reverso é capaz de responder diretamente à requisição. Já quando há uma requisição a objetos dinâmicos, este repassa a requisição aos servidores internos conforme a porta utilizada do serviço específico. A figura abaixo nos apresenta o modelo comentado:



- **Cache Local** – Os browsers possuem a capacidade de armazenar as informações recebidas do servidor de tal forma que uma nova requisição idêntica à anterior não enseje uma nova consulta ao servidor. Desse modo, a requisição será atendida diretamente pelo Browser.



Acrescento ainda a informação de que o protocolo HTTP pode ser utilizado de forma segura com a nomenclatura HTTPS, operando na porta 443/TCP.

A definição do tipo de criptografia a ser utilizado fica por conta dos protocolos SSL e TLS. Estes serão responsáveis por estabelecer uma camada de segurança para que o HTTP possa trafegar de forma segura.

Dessa forma, quando temos uma navegação em HTTPS, dizemos que os dados serão cifrados para uma **comunicação segura**, além da capacidade de se verificar a **autenticidade do servidor** através de recursos de certificados digitais. Acrescido a isso, temos também a possibilidade de autenticação do usuário de forma opcional. Essa é a diferença da versão de tunelamento: simples e mútua.



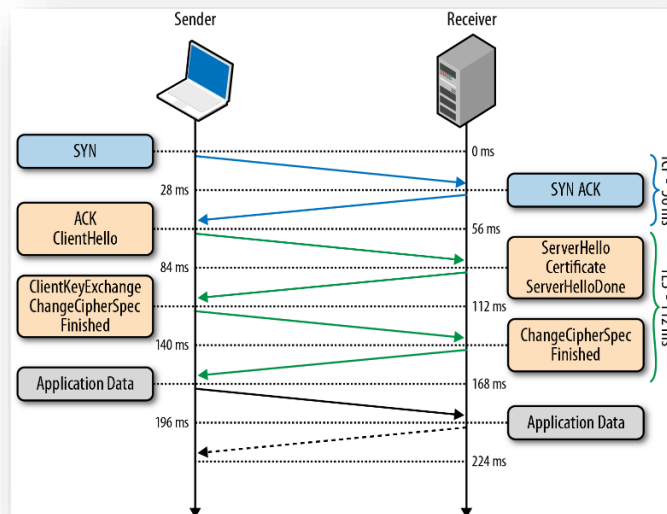
A primeira autentica apenas o servidor, enquanto a segunda, também autentica o cliente. Desse modo, deve haver uma intervenção no cliente para que se implemente a configuração e instalação de certificado digital para que este possa ser usado no processo de autenticação do cliente.

Esse ponto gerou uma polêmica com a banca CESPE ao afirmar que o HTTPS necessariamente tratará os aspectos de autenticação do servidor e cliente, quando na prática, isso não acontece.

Quando acessamos os serviços da GOOGLE por exemplo, não enviamos nosso certificado digital para a devida autenticação, utilizando, portanto, o modo simples do SSL/TLS.



A Imagem abaixo nos dá uma visão das fases envolvidas no processo de conexão, troca de chaves e, finalmente, troca dos dados:



As três primeiras mensagens são de estabelecimento da conexão TCP. Entretanto, a terceira mensagem indicada por "ACK/CLIENTHELLO" já congrega a última mensagem de ACK do TCP e a primeira do HTTPS (Hello). Em seguida, tem-se o reconhecimento e a definição dos algoritmos suportados com a devida troca de chaves, para, enfim, iniciar a troca de informação, de fato!



Algumas bancas em provas mais técnicas cobram as características de alguns campos dos cabeçalhos do protocolo HTTP. Dessa forma, recomendo a leitura do link: <http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html>



(CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) As estratégias usadas para diminuir o tráfego causado pelo grande número de acessos a páginas web podem ser do tipo cache web, que é implementado no cliente, no GET condicional ou na rede servidor Proxy Web.

Comentários:



Pessoal, vimos que o cache pode estar localizado tanto no cliente, em um browser por exemplo ou em um servidor Proxy. Complemento ainda o fato da existência da utilização do método GET de forma condicional. Na requisição GET, o cliente envia informações de data do objeto desejado em um cache web. Caso o objeto não tenha sido modificado a partir da data, extrai-se a informação do cache. Caso tenha havido mudança, o servidor envia o objeto atualizado.

Gabarito: C

HTTP 2.0

Aprofundando um pouco mais a nossa conversa a respeito do HTTP, gostaria de comentar com vocês diversas características do protocolo HTTP em sua versão 2.0. Algumas bancas já estão apresentando questões que exigem conhecimento da referida versão e como o nosso objetivo é sempre estar atualizado, nada mais certo do que abordarmos tal assunto.



O surgimento dessa versão veio com o objetivo de contemplar a nova forma de navegação web. Temos um cenário com sites mais elaborados com um grande volume de dados, regras e protocolos que visam garantir princípios de segurança, navegação em dispositivos móveis, muitos outros.

A empresa GOOGLE buscou largar na frente nessa jornada e apresentou um novo protocolo próprio conhecido como SPDY. Foi uma camada de complementação de serviços e recursos ao HTTP padrão. Essa camada torna diversos recursos obrigatórios, entre eles o fato de se compactar e criptografar os dados e os cabeçalhos HTTP. Outro recurso interessante que surge para otimizar a utilização da banda é a multiplexação no HTTP. Tal recurso possibilitar gerar diversas requisições ao mesmo tempo em uma mesma conexão.

Mas porque estamos falando desse protocolo Professor?



Devido aos excelentes resultados apresentados, ele tem servido como base para a elaboração da versão 2.0 do HTTP.



Desse modo, a versão 2.0 suporta todos os recursos básicos das versões anteriores, porém, com grande foco na eficiência da comunicação em termos de velocidade e racionamento de recursos.

A versão 2.0 incluiu outros tipos de quadros além dos padrões já conhecidos que são o HEADER e DATA, conforme versão anterior. Nesse contexto, surge quadros do tipo SETTINGS, WINDOW_UPDATE e PUSH_PROMISSE, com vistas a implementação de novos recursos no HTTPv2.0.

Surge ainda o conceito de STREAMS ou fluxos independentes e bidirecionais em uma mesma conexão. Desse modo, um problema de bloqueio ou congestionamento em algum desses fluxos não impacta os demais. Devido a essa característica, busca-se ainda implementar controles de fluxo e priorização de STREAMS.

Há de se mencionar que todas as conexões do HTTPv2.0 são persistentes. Desse modo, os clientes não devem ser capazes de abrir mais de uma conexão para o mesmo host/porta. Entretanto, pode-se estabelecer novas conexões em detrimento da anteriormente estabelecida para algumas finalidades, entre elas, a renegociação de chaves para uma conexão TLS ou conexões que estão com erros.

Vamos abordar então os diversos pontos que são mais relevantes a respeito da implementação do HTTPv2.0, inclusive em conjunto com protocolos auxiliares como o TLS.



- **Compressão Automática**

Nas implementações padrões das versões anteriores do HTTP, quando se almejava incremento do desempenho, utiliza-se a ferramenta GZIP no lado do servidor que era responsável pela compressão dos dados que serviam como respostas às requisições dos clientes.

Na versão 2.0, tal implementação é utilizada como padrão e de forma obrigatória. Além disso, utiliza-se um algoritmo conhecido como HPACK para compressão de todos os HEADERS, sejam aqueles destinados às requisições ou a respostas, diminuindo bastante o volume de dados trafegados nos HEADERS.

- **Criptografia e Segurança**

Para comunicações seguras, tem-se a utilização do HTTPS de forma obrigatória com vistas a tratar os diversos aspectos de segurança da informação. É importante mencionar que tal recurso implica



em uma difusão global de certificados digitais para que tenhamos ambientes mais robustos e seguros nas comunicações com HTTPS.

Desse modo, o SSL é um protocolo fundamental na implementação e transição do HTTPS para o HTTP2.0.

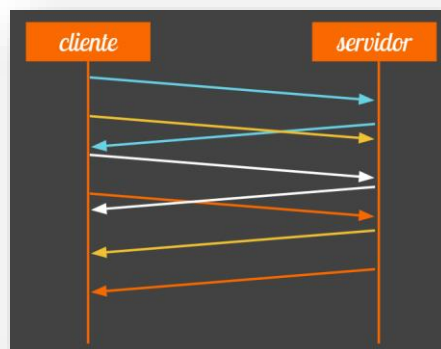
- **Paralelização de Fluxos com Multiplexing**

Como vimos anteriormente, o HTTP em suas versões anteriores utiliza o conceito de envio de recursos de forma sequencial. Assim, ao se abrir a conexão, envia-se um request e espera-se uma resposta para o referido request antes de enviar a nova requisição.

A evolução desse recurso, ainda implementado para as versões anteriores, era abrir diversas conexões e cada uma ter o seu próprio fluxo. Percebiam que aqui tínhamos uma paralelização de conexões, algo em torno de 4 a 8 conexões para um host comum.

O HTTP2.0 surge então com uma nova abordagem, a de paralelização de fluxos ou de requisições e respostas em uma mesma conexão, totalmente independentes entre si, assíncronos e bidirecionais.

Como já vimos e reforçamos, tal recurso é conhecido como MULTIPLEXING. A imagem abaixo nos traz essa representação em que não é necessário aguardar a resposta específica para uma requisição, antes de enviar uma nova requisição:



Diante do modelo proposto, o controle de fluxo em cada um desses streams é fundamental, devendo ser garantido esse aspecto. O HTTP2.0 utiliza o quadro WINDOW_UPDATE para tal funcionalidade. Ele pode ser aplicado tanto para controle de fluxo de cada stream como da conexão como um todo.





Outro recurso interessante que surge no HTTP2.0 é a otimização de tráfego com vistas a não enviar informações redundantes que já foram trafegadas. Ou seja, por padrão, o HTTP em sua versão anterior manda informações idênticas a cada requisição ou resposta, como é o caso do parâmetro "User-Agent" que informa características do Browser do cliente.

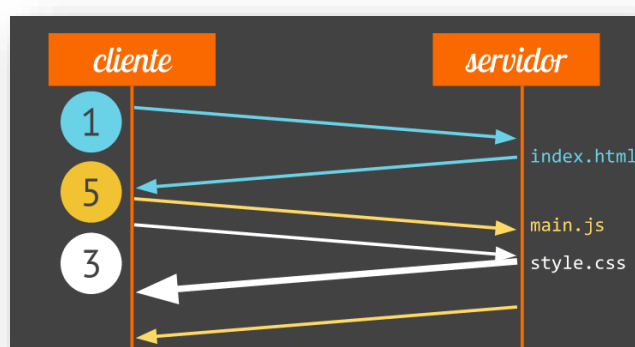
Na nova versão, envia-se apenas informações de cabeçalho que são diferentes das informações já enviadas, reduzindo, assim, o fluxo de dados desnecessários.

- **Priorização de Requests**

O HTTPv2.0 possui a capacidade de distinguir as respostas a serem enviadas e categorizá-las conforme a necessidade de montagem da página. Desse modo, pode-se enviar, por exemplo, de forma prioritária, o arquivo base da página "index.html" e posteriormente, complementá-la com as demais informações.

Assim, busca-se dar agilidade e trazer um caráter mais ágil na construção da página no lado do cliente.

A figura a seguir nos traz essa representação:



- **Server-Push**

A ideia desse recurso é identificar a necessidade do cliente de tal modo que ele não necessite fazer a requisição para cada recurso. Na figura acima, verificamos que para cada resposta, houve uma requisição. Ora, o servidor entende que sempre que há o pedido de envio da página index.html, necessariamente virá pedidos para as demais páginas. Desse modo, ele antecipa tal questão e já envia os recursos independentemente da requisição do cliente.



- **HTTP2.0 com TLS 1.2**

Para implementação do HTTP em sua versão 2.0, deve-se utilizar a extensão do TLS conhecida como Server Name Indication (SNI). Para as versões do TLS 1.3 ou superior, a implementação e suporte do SNI é suficiente.

Já a versão 1.2 apresenta uma série de requisitos que devem ser seguidos para que seja possível a sua implantação. Caso esses requisitos não sejam atendidos, pode-se ter problemas de diversos, principalmente no que concerne à troca de chaves e estabelecimento da sessão TLS na fase de negociação.

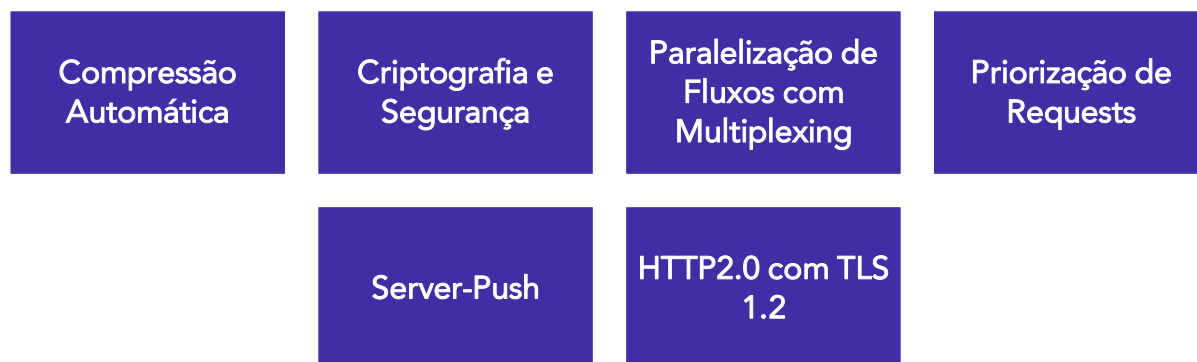
Nesses casos, utiliza-se mensagens do tipo INADEQUATE_SECURITY ou categoriza-se como erro de conexão.

Dessa forma, vamos checar quais são os requisitos que devem ser atendidos:



Desabilitar a COMPRESSÃO - A compressão pode gerar problemas de vazamento de dados ou exposição indevida. É importante lembrar que compressões genéricas são desnecessárias uma vez que o HTTPv2 apresenta recurso de compressão intrínseca criada e configurada para uma operação plena no HTTPv2 em termos de desempenho, seguranças e outros pontos.

Desabilitar a RENEGOCIAÇÃO - Por motivo da troca de chaves e certificados no estabelecimento da conexão, os terminais devem tratar a renegociação como um erro de conexão. A renegociação deve ser utilizada exclusivamente para fins de confidencialidade na troca de informações de credenciais no estabelecimento da conexão e não conectividade.





(CESPE – TJDFT/Analista Judiciário – Suporte em TI/2015) A técnica de compressão não é recomendada ao se utilizar a versão 2 do HTTP sobre o protocolo TLS 1.2.

Comentários:

Vimos que essa é uma das recomendações apresentadas a respeito do HTTP 2.0.

Gabarito: C



QUESTÕES COMENTADAS – HTTP - CESPE

1. CEBRASPE (CESPE) - AFM (Pref Fortaleza)/Pref Fortaleza/Ciência da Computação, Informática, Processamento de Dados/2023

HTTPs é a combinação do HTTP sobre a camada SSP (secure sockets layer), que é colocada entre a camada de aplicação e a camada de transporte, aceitando solicitações do navegador e enviando-as ao TCP (transmission control protocol) para transmissão ao servidor.

Comentários:

A intenção da banca era citar o HTTPS sobre a camada SSL. Porém, ela literalmente bagunçou as siglas. Originalmente a questão foi dada como CERTA, e posteriormente, anulada.

Caso as siglas estivessem corretas, temos, de fato, a descrição do HTTPS em conjunto com o SSL.

Gabarito: Anulada

2. CESPE / CEBRASPE - 2023 - MPE-RO - Analista de Suporte Computacional

A respeito de Internet e intranet, assinale a opção correta.

A) O dynamic HTML permite interatividade rápida, mas não permite modificação do conteúdo na página sem precisar recarregá-la.

B) Navegadores web permitem, nativamente, a leitura de vários tipos de arquivo; em alguns casos, por meio de plug-ins, permitem também a leitura de arquivos que não são suportados nativamente.

C) Os navegadores web se comunicam, geralmente, com servidores web usando o FTP.

D) A principal diferença entre páginas da Internet e da intranet é o protocolo de acesso aos dados.

E) A maioria dos navegadores web necessita de plug-ins para que o HTTPS seja suportado.

Comentários:

Vamos aos itens:

a) O dynamic traz, justamente como diferencial, a capacidade de modificação sem precisar recarregar. Sendo assim, o DHTML é um conjunto de ingredientes que proporcionam um maior controle sobre a apresentação do conteúdo de páginas da Web, além de possibilitar a inclusão de componentes multimídia, como animações, diretamente no código HTML, sem a necessidade de plug-ins ou de recarregar a página. **ERRADO**

b) Exato pessoal. Temos aí a descrição dos nossos recursos e usos da Internet diariamente. **CORRETO**



- c) Conforme vimos, o principal protocolo para navegação web é o HTTP, e não o FTP. **ERRADO**
- d) Não há diferença nos protocolos, mas sim, os tipos de acesso e restrições de segurança. **ERRADO**
- e) O HTTPS é um recurso nativo da arquitetura TCP/IP e, portanto, dos browsers. **ERRADO**

Gabarito: B

3. CESPE / CEBRASPE - 2022 - BNB - Analista de Sistemas - Desenvolvimento de Sistemas

Usuários que recebem um código de status HTTP 4XX podem refazer a solicitação mesmo sem alterar nada e ter sucesso na próxima resposta.

Alternativas

Comentários:

A questão estaria correta se fosse a categoria de erro HTTP 5XX, pois essa faz referência a um problema no lado do servidor. Logo, ele poderia manter a requisição, e o servidor, tendo sido corrigido, passaria a receber e processar a requisição. Agora um erro 4XX indica problema no lado do cliente. Logo, ele tem que verificar as formas da consulta e refazer a requisição com algum tipo de mudança.

Lembremos as categorias:

1xx – Informativo

2xx – Sucesso

3xx – Redirecionamento

4xx – Erro no cliente

5xx – Erro no servidor

Gabarito: Errado

4. Cebbraspe – Analista Judiciário – Tecnologia da Informação (TRT-AP/PA)/2022

O cabeçalho do protocolo HTTP que contém o DNS do servidor é o

- a) host.
- b) authorization.
- c) referer.



d) location.

e) server.

Comentários:

O HOST indica justamente o nome de DNS do servidor, com a possibilidade de indicação da porta.

Assim, é a sintaxe do parâmetro genérico:

Host: <host>:<port>

Agora com exemplo:

Host: developer.mozilla.org

b) O cabeçalho de requisição HTTP Authorization contém as credenciais para autenticar o agente de usuário com o servidor, geralmente o servidor responderá com um status 401 Unauthorized se não for possível fazer a autenticação, e com o cabeçalho WWW-Authenticate.

c) O cabeçalho de requisição HTTP Referer contém o endereço da página web anterior do qual a página atual requerida foi chamada. O Referer permite aos servidores identificar de onde as pessoas estão visitando-os e pode usar esses dados para análise, log e cacheamento otimizado, por exemplo.

d) O cabeçalho de resposta Location indica o URL para qual página deve-se ser redirecionada. Ele só tem significado quando é enviado junto a uma resposta de status 3xx (redirecionamento) ou 201 (criado).

e) O cabeçalho Server contém informação sobre o software usado pelo servidor de origem para manipular a solicitação.

Gabarito: **A**

5. (CESPE – STJ/Analista Judiciário – Suporte em TI/2015) Uma forma de se melhorar o desempenho do acesso a páginas web frequentemente visitadas é armazenar-se o conteúdo dessas páginas para que sejam rapidamente carregadas em solicitações futuras, estando, entre os possíveis processos para executar essa tarefa, o proxy, ao qual serão encaminhadas todas as requisições de acesso a páginas web.

Comentários:

De fato, um proxy poderá ser utilizado para este fim. Entretanto, é importante lembrarmos que a funcionalidade mencionada na questão é o recurso do cache. Através do cache, pode-se armazenar conteúdos estáticos das páginas web e disponibilizar tais recursos diretamente aos



hosts requisitantes sem necessariamente consultar o servidor. Isso possibilita um incremento de desempenho em tempo de resposta e alivia a carga de consultas ao servidor.

Gabarito: C

6. (CESPE - TJ TRE MS/Apoio Especializado/Programação de Sistemas/2013) O elemento em que uma das partes de uma informação é armazenada como cadeia de texto na máquina do usuário e cuja função principal é a de manter a persistência de sessões HTTP é denominado

- A) frame.
- B) Java Script.
- C) tag.
- D) cookie.
- E) XML.

Comentários:

Uma das funções do cookie é exatamente a apresentada na questão, além da possibilidade de ser armazenar informações específicas de cada host para agilizar consultas ou fornecer um serviço personalizado.

Gabarito: D

7. (CESPE - TJ TRE MS/Apoio Especializado/Programação de Sistemas/2013) Com referência ao Hyper Text Transfer Protocol (HTTP) — protocolo de aplicação utilizado para o tratamento de pedidos e respostas entre cliente e servidor na Internet e com o qual, normalmente, são desenvolvidas as aplicações para a Web —, assinale a opção em que todas as expressões identificam métodos de requisição HTTP que devem ser implementados por um servidor HTTP 1.1 usado pelo cliente.

- A) SOAP, WS, WSDL, UDDI
- B) TCP, IP, NETBIOS, UDP, IPX
- C) NFS, SMB, IPP, SMTP, POP3, IMAP, XMPP, SIP
- D) SET, GET, CONSTRUCTOR, DESTRUCTOR
- E) GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS

Comentários:

A alternativa “E” descreve 7 dos 9 existentes. Faltam ainda os métodos CONNECT e PATCH. Os mais utilizados sem dúvida são os 3 primeiros.

Gabarito: E



8. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O protocolo HTTP, que não armazena informações sobre o estado do cliente, classifica-se como do tipo stateless.

Comentários:

Vimos que essa é uma característica nativa do protocolo HTTP.

Gabarito: C

9. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) Um servidor HTTP consiste em um servidor de aplicações.

Comentários:

Um servidor HTTP é considerado um servidor WEB e não um servidor de aplicações completo com muito mais recursos. Dizemos que um servidor WEB integra um servidor um servidor de aplicações.

Gabarito: E

10. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) Ao receber uma requisição, o servidor procura pelo recurso requisitado e envia, ao cliente, uma resposta com um código, que pode iniciar-se por 1xx, que indica sucesso no recebimento da requisição; 2xx, que indica redirecionamento da requisição; 3xx, que informa erros acontecidos no cliente; e 4xx, que informa erros no servidor.

Comentários:

Pessoal, a ordem correta é:

1xx – Classe informacional

2xx – Classe de sucesso

3xx – Classe de redirecionamento

4xx – Erros no lado do cliente

5xx – Erros no lado do servidor

Gabarito: E

11. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) As estratégias usadas para diminuir o tráfego causado pelo grande número de acessos a páginas web podem ser do tipo cache web, que é implementado no cliente, no GET condicional ou na rede servidor Proxy Web.

Comentários:



Pessoal, vimos que o cache pode estar localizado tanto no cliente, em um browser por exemplo ou em um servidor Proxy. Complemento ainda o fato da existência da utilização do método GET de forma condicional. Na requisição GET, o cliente envia informações de data do objeto desejado em um cache web. Caso o objeto não tenha sido modificado a partir da data, extrai-se a informação do cache. Caso tenha havido mudança, o servidor envia o objeto atualizado.

Gabarito: C

- 12.(CESPE – MPU/Analista Judiciário – Suporte e Infraestrutura/2013) Os servidores proxy criam um cache com as solicitações de cada usuário, de forma a otimizar consultas futuras de um mesmo usuário, sendo esse cache de uso exclusivo de seu respectivo usuário.

Comentários:

Pessoal, vimos que o cache pode ser utilizado para armazenar informações de páginas para acesso geral de qualquer usuário desse servidor Proxy. Além disso, em relação às informações para customização do acesso, armazena-se informações em cache de cada usuário para uso de cada um no momento adequado.

Gabarito: E

- 13.(CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O código abaixo ilustra uma resposta de um servidor web.

```
GET /internet/index.html HTTP/1.0
User-agent: Mozilla /4.5 [en] (WinNT; I)
AcceptP: text/plain, text/html, image/gif, image/x-xbitmap,
image/jpeg, image/pjpeg, image/png, */*
Accept-Charset: isso-8859-1, *, utf-8
Accept-Encoding: gzip
Accept-Language: em
```

Comentários:

O lado que se utiliza dos métodos é o cliente e logo na primeira linha vemos o método GET, logo, o trecho é um tipo de requisição. As respostas são iniciadas com os códigos que vimos anteriormente.

Gabarito: E

- 14.(CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O protocolo HTTP utiliza, por padrão, a porta 80 para tráfego seguro de dados, sendo o pacote de sincronismo da conexão o responsável por indicar o tipo de cifra que será utilizado na sessão.

Comentários:



A porta 80 é utilizada pelo protocolo HTTP padrão. A implementação segura fica a cargo do protocolo HTTPS na porta TCP/443. A definição de critérios de criptografia ocorre no momento do estabelecimento da conexão.

Gabarito: E

15.(CESPE - TJ TRT17/Apoio Especializado/Tecnologia da Informação/2013) Como maneira de se evitar o desenvolvimento de novos protocolos de camada de aplicação, diversas aplicações usam o HTTP como forma de transferir dados fim a fim na camada de aplicação.

Comentários:

De fato. Por ser um protocolo amplamente consolidado, simples e eficiente, diversos protocolos acabam usando sua estrutura para reaproveitar o modelo na transferência de dados simples.

Gabarito: C

16.(CESPE - Tec MPU/Técnico Administrativo/Tecnologia da Informação e Comunicação/2013) O serviço HTTP é implementado sem estado, enquanto o HTTPS é sua versão stateful (com estado).

Comentários:

O HTTPS nada mais é do que uma implementação segura do protocolo HTTP. Os princípios do protocolo são mantidos os mesmos.

Gabarito: E

17.(CESPE - Ana MPU/Tecnologia da Informação e Comunicação/Suporte e Infraestrutura/2013) A primeira versão do serviço HTTP utiliza conexões não persistentes; a persistência foi acrescentada na versão subsequente desse serviço.

Comentários:

Exatamente como vimos não é pessoal. Somente a partir da versão 1.1 é que foi implementado o recurso de conexões persistentes.

Gabarito: C

18.(CESPE - TRT(DF e GO)/Técnico Judiciário - Tecnologia da Informação/2013) Os servidores de HTTP mais utilizados atualmente são Apache HTTP Server, Internet Information Server e Enterprise Server.

Comentários:

Pessoal, de fato os dois principais são o Apache (Sun Microsystems) e o Internet Information Server (IIS - Microsoft). O Enterprise Server, entendo que a banca tentou nos trazer um conceito mais geral de servidores corporativos, sendo essa uma verdade, com diversas possibilidades de



implementações. Trazendo então uma visão mais genérica, não vejo problema em considerarmos a questão como correta.

Gabarito: C

19.(CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) Se o endereço de página inicia com HTTPS, então os dados serão transmitidos por meio de uma conexão cifrada e a autenticidade do servidor e do cliente será verificada com o uso de certificados digitais.

Comentários:

Temos aqui a questão problemática de autenticação via HTTPS que mencionei. Percebam que o enunciado afirma que será realizado o método de autenticação mútua, o que não é bem verdade. É um recurso opcional que depende de configuração no lado do cliente. Desse modo, fiquemos com o aprendizado da forma de interpretação do CESPE para não errarmos esse mesmo ponto em provas futuras.

Gabarito: C (Gabarito do Professor: E)

20.(CESPE – TCU/Analista de Controle Externo – TI/2007) O protocolo HTTP, definido nas RFCs 1945 e 2616, não permite a utilização de conexões persistentes.

Comentários:

A versão 1.1 do HTTP suporta conexões persistentes.

Gabarito: E

21.(CESPE – TRT – 17ª Região (ES)/Técnico Judiciário – TI/2013) HTTPS usa certificados digitais, requer o uso de TLS e utiliza a porta 443 por padrão.

Comentários:

Questão bem tranquila, certo pessoal? Muito cuidado para não ficar buscando problemas onde não há. Atualmente, o SSL/TLS é considerado como sendo um mesmo protocolo apesar de suas pequenas diferenças e de não serem compatíveis entre si. Desse modo, não devemos encerrar com esse aspecto para essa questão, dizendo que seria possível a utilização de SSL ao invés do TLS.

Gabarito: C

22.(CESPE – TRE-GO/Técnico Judiciário/2015) Na busca de um produto em uma loja virtual por meio de um webservice, quando o produto é encontrado, o protocolo HTTP retorna um HTTP/1.1 404, o que facilita o tratamento do pedido no programa cliente.

Comentários:



Vimos na nossa lista de códigos que a família 4xx corresponde a erros do lado do cliente. Mais especificamente o 404, temos que o recurso não foi encontrado, retornando uma mensagem "not found", ou seja, tem-se um URI inválida.

Gabarito: E

23.(CESPE – TRE-GO/Técnico Judiciário – Programação de Sistemas/2015) Por meio do protocolo chave HTTP, é possível utilizar o método PUT para se criar um novo recurso de um webservice.

Comentários:

Vimos que o método PUT permite submeter um arquivo ou recurso no servidor a partir de um cliente. Pode-se enviar uma nova página sem maiores dificuldades.

Gabarito: C

24.(CESPE – TRE-GO/Técnico Judiciário – Programação de Sistemas/2015) Uma conexão entre um computador cliente a um computador considerado servidor, para visualizar uma página web, através do protocolo HTTP, é possível afirmar que será utilizado o protocolo de transporte TCP (transmission control protocol).

Comentários:

Pessoal, tenham cuidado para não confundir a obrigatoriedade de se usar o protocolo TCP como o fato do HTTP ser stateless. Lembremos que o primeiro está relacionado ao estabelecimento da conexão necessária para envio e recebimento dos dados, enquanto o segundo diz respeito ao armazenamento do estado da sessão, sendo que este último não é fornecido pelo HTTP.

Gabarito: C

25.(CESPE – TJDF/Analista Judiciário – Suporte em TI/2015) A técnica de compressão não é recomendada ao se utilizar a versão 2 do HTTP sobre o protocolo TLS 1.2.

Comentários:

Vimos que essa é uma das recomendações apresentadas a respeito do HTTP 2.0.

Gabarito: C

26.(CESPE – TJDF/Analista Judiciário – Suporte em TI/2015) Na implementação do HTTP versão 2 sobre o protocolo TLS 1.2, é mandatório desabilitar a renegociação da conexão.

Comentários:

Esse é um ponto necessário para o funcionamento do HTTP em conjunto com o TLS 1.2.

Gabarito: C



27.(CESPE – TJDFT/Analista Judiciário – Suporte em TI/2015) No HTTP, a técnica geral do controle de fluxo garante que não haja interferência entre as conexões independentes. Entretanto essa técnica foi abandonada na versão 2 do HTTP, que criou o conceito de WINDOW_UPDATE frame.

Comentários:

Muito pelo contrário. O WINDOW_UPDATE foi criado para tal funcionalidade.

Gabarito: E



QUESTÕES COMENTADAS – HTTP - FCC

1. (FCC – TRT – 15ª Região/Analista Judiciário – TI/2015) Um serviço da internet utiliza diferentes protocolos, por exemplo, protocolos relacionados com a função de roteamento, transmissão de dados e transferência de hipertexto para efetivar a comunicação. Os respectivos protocolos, do conjunto (suite) de protocolos TCP/IP, relacionados com as funções apresentadas, são:

- A) IP, TCP e HTTP.
- B) TCP, FTP e HTML.
- C) IP, FTP e HTML.
- D) ARP, FTP e HTTP.
- E) TCP, IP e HTTP.

Comentários:

Temos três aspectos para considerar.

1. Protocolo relacionado com roteamento nos leva a considerar a camada de rede e o principal protocolo para encaminhamento de pacotes entre redes, que é o IP.
2. Quando se fala de transmissão de dados, devemos remeter à capacidade de transportar a informação fim a fim. Isso nos leva à camada de transporte, logo, temos os protocolos TCP ou UDP como principais opções.
3. E por último, o protocolo de transferência de hipermídia, sendo essa a palavra chave para referenciarmos o protocolo HTTP.

Gabarito: A

2. (FCC – TRT – 16ª Região (MA) /Técnico Judiciário – TI/2014) Os diversos protocolos do conjunto (suite) TCP/IP são organizados em camadas de funcionalidade. Quando um usuário da internet realiza um acesso à página Web, ele está utilizando o protocolo da camada de Aplicação denominado

- A) W W W.
- B) IMAP.
- C) HTTP.
- D) TCP.
- E) IP.



Comentários:

Pessoal, vimos que as requisições WEB estão debaixo da operação e funcionamento do protocolo HTTP.

Gabarito: C

3. (FCC – TRT – 2ª Região (SP)/Técnico Judiciário – TI/2014) No modelo de referência de 4 camadas da suíte de protocolos TCP/IP, os protocolos Ethernet, HTTP e ICMP localizam-se, respectivamente, nas camadas

- A) Internet, Apresentação e Interface de rede
- B) Interface de rede, Aplicação e Internet.
- C) Transporte, Internet e Interface de rede.
- D) Transporte, Aplicação e Enlace de dados.
- E) Física, Transporte e Enlace de dados.

Comentários:

Mais uma questão que aborda o posicionamento dos diversos protocolos nas camadas da arquitetura TCP/IP. Bem tranquilo, certo? Vemos que a camada de Acesso à Rede está sendo referenciada como Interface de Rede. Vimos que o protocolo Ethernet está na camada 2 do modelo OSI, logo, faz parte da camada Interface de Rede. Já o HTTP atua na camada de aplicação, inclusive atuando na porta 80 conforme vimos. E por último o protocolo ICMP que atua de forma complementar ao IP na camada de rede.

Gabarito: B

4. (FCC – TRF – 4ª Região/Técnico Judiciário – TI/2014) Pedro, técnico em informática do TRF da 4ª Região, deve comprovar os seus conhecimentos sobre o modelo OSI identificando os protocolos às respectivas camadas do modelo. Assim, um correto relacionamento identificado por Pedro é:

- A) FTP - Camada de Transporte.
- B) HTTP - Camada de Transporte.
- C) ICMP - Camada de Aplicação.
- D) HTTP - Camada de Aplicação.
- E) SNMP - Camada de Rede.

Comentários:

Questão típica das provas de técnico judiciário em vincular os protocolos às camadas do modelo OSI. FTP, HTTP e SNMP são da camada de aplicação, enquanto o ICMP da camada de rede.



Gabarito: D

5. (FCC – TRF – 2ª Região/Analista Judiciário – Informática/2012) Sobre o protocolo HTTP, é correto afirmar:

- A) Usa o TCP e o UDP como seus protocolos de transporte e presta serviço por default na porta 80.
- B) Em uma mensagem de requisição HTTP, a linha de cabeçalho User-agent: especifica o agente de usuário, isto é, o browser que está fazendo a requisição ao servidor.
- C) Quando utiliza conexões persistentes, cada conexão TCP é encerrada após o servidor enviar o objeto resposta ao cliente que fez a requisição. Cada conexão TCP transporta exatamente uma mensagem de requisição e uma mensagem de resposta.
- D) A resposta do servidor a uma requisição HTTP é dividida em três seções. A primeira é denominada cabeçalho (header) e contém informações do servidor sobre o recurso solicitado. A segunda seção é denominada corpo (body) e contém o recurso propriamente dito. A terceira seção, denominada rodapé (footer), contém informações de status da requisição e o relatório de erros, quando houver.
- E) Os únicos métodos (comandos) de requisição do protocolo HTTP são GET e POST. O status de retorno de número 404 do método HTTP indica que o serviço está indisponível.

Comentários:

Vamos aos itens:

- A) Para efeito de prova, ficamos com a afirmação de que o HTTP utiliza somente o protocolo TCP na porta 80. **INCORRETO**
- B) Vimos que as informações referentes ao nome da página, estado corrente da conexão, informações do navegador (User Agent) e língua aceitas, entre outros, fazem parte da estrutura do cabeçalho HTTP. **CORRETO**
- C) Essa é uma característica das conexões não persistentes, ou seja, da versão 1.0. As conexões persistentes abrem uma única conexão para transporte de todos os dados da comunicação. **INCORRETO**
- D) A resposta à requisição é dividida em três partes: linha de estado, cabeçalho e corpo da entidade. **INCORRETO**
- E) Diversos são os métodos suportados pelo HTTP, não se restringindo ao GET e POST. **INCORRETO**

Gabarito: B

6. (FCC – TCE-SP/Auxiliar de Fiscalização Financeira/2012) Sobre o protocolo HTTP, é correto afirmar:

- A) Se um cliente solicita ao servidor o mesmo objeto duas vezes em um período de poucos segundos, o servidor responde dizendo que acabou de enviar o objeto ao cliente e não envia novamente o objeto.



B) É implementado em dois programas: um programa cliente e outro servidor. Os dois programas, implementados em sistemas finais diferentes, conversam um com o outro por meio da troca de mensagens HTTP. O HTTP não define a estrutura dessas mensagens, mas define o modo como cliente e servidor as trocam.

C) O HTTP usa o TCP como seu protocolo de transporte subjacente. O cliente HTTP primeiramente inicia uma conexão TCP com o servidor. Uma vez estabelecida a conexão, os processos do browser e do servidor acessam o TCP por meio de suas interfaces socket.

D) Os servidores web implementam apenas o lado cliente do HTTP e abrigam objetos web, cada um endereçado por um URL. O Apache e o IIS são servidores web populares.

E) O HTTP define como clientes web requisitam páginas web aos servidores, mas não define como eles as transferem aos clientes.

Comentários:

Vamos aos itens:

A) O protocolo HTTP é um protocolo sem estado. Ou seja, toda requisição recebida, ainda que do mesmo host a respeito do mesmo objeto, será interpretado como uma nova requisição. **INCORRETO**

B) O HTTP define muito bem a estrutura das mensagens de requisição e resposta. **INCORRETO**

C) Temos aí um exemplo de funcionamento do HTTP. **CORRETO**

D) Servidores WEB implementam o lado do servidor e não do cliente. O resto da questão está conforme esperado. **INCORRETO**

E) Conforme já conversamos, o HTTP possui uma estrutura completa de requisição e resposta. **INCORRETO**

Gabarito: C

7. (FCC – MPE-AM/Agente de Apoio – Manutenção e Suporte de Informática/2013) HTTPS (HyperText Transfer Protocol SecurE) é um protocolo que combina o uso do HTTP com o

A) SSL e o TLS, a fim de prover conexões seguras.

B) DES e AES, a fim de prover criptografia assimétrica.

C) RSA, a fim de prover certificação digital por meio de criptografia simétrica.

D) IDS e IPS, a fim de prover segurança contra invasores.

E) IMAP e POP, a fim de prover comunicação segura.

Comentários:



Conforme vimos, o HTTPS utiliza a porta 443 para uma implementação de uma camada de segurança abaixo do HTTP. Utiliza-se basicamente os protocolos SSL e TLS para o estabelecimento dessa camada de segurança.

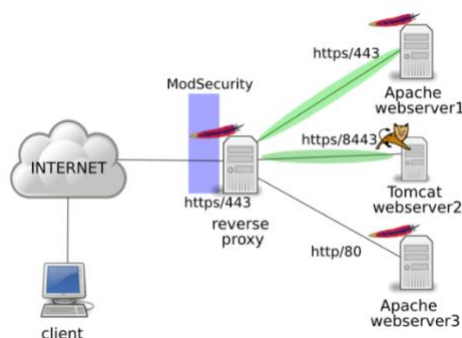
Gabarito: A

8. (FCC – TRF – 1ª Região/Analista Judiciário – Área de Apoio Especializado/2014) O recebe os pedidos HTTP na porta configurada e processa todos os pedidos da web que chegam, podendo distribuí-los. Os pedidos de objetos que podem ser armazenados no cache (informações estáticas que não mudam com frequência como páginas em HTML e imagens GIF) são processados pelo proxy. Os pedidos de objetos que não podem ser armazenados no cache (informações dinâmicas que mudam com frequência) são processados pelo servidor web de origem na porta configurada. Essa configuração pode ser feita para proteger um servidor intranet da Internet e reduzir a carga nos servidores web públicos mantidos na intranet, por exemplo, criando um front end para um servidor web. A lacuna é corretamente preenchida por

- A) cache HTTP.
- B) acelerador HTTPS.
- C) proxy estático-dinâmico.
- D) filtro de logs.
- E) proxy reverso.

Comentários:

Vimos que essas são as características do proxy reverso, conforme figura abaixo:



Gabarito: E

9. (FCC – TRT – 6ª Região (PE)/Analista Judiciário – TI/2012) Protocolos de rede podem ser classificados como "sem estados" (stateless) ou "com estado" (stateful). A este respeito é correto afirmar que

- A) protocolos sem estados exigem que tanto cliente como servidor mantenham um histórico da conexão.
- B) o uso de cookies é uma maneira de contornar o fato de que HTTP é um protocolo com estados.



- C) protocolos sem estados têm a desvantagem de não admitir encapsulamento criptográfico.
- D) o uso de cookies é uma maneira de contornar o fato de que HTTP é um protocolo sem estados.
- E) protocolos com estados exigem que cada mensagem trocada entre cliente e servidor contenha informação respectiva ao estado da transação.

Comentários:

Vimos que o HTTP é um protocolo sem estados. Vale lembrar que o conceito de persistência é diferente do fato de não armazenar estado. Nesse sentido, uma alternativa é a utilização de cookies no lado do cliente para que o servidor possa obter algumas informações e tentar retomar alguns aspectos ou características do usuário com vistas a "simular" uma condição com estados.

Gabarito: D

10. (FCC – TJ-AP/Analista Judiciário – TI/2014) O protocolo HTTPS (HyperText Transfer Protocol SecurE) é uma implementação elaborada a partir do protocolo HTTP, na qual se incorporou uma camada de segurança. O protocolo de segurança originalmente utilizado nessa camada é o

- A) POP₃ (Post Office Protocol).
- B) SMTP (Simple Mail Transfer Protocol).
- C) IMAP (Internet Message Access Protocol).
- D) SSL (Secure Sockets Layer).
- E) SSH (Secure Shell).

Comentários:

Conforme vimos, pode ser tanto SLL quanto TLS.

Gabarito: D

11. (FCC – Câmara Municipal de São Paulo – SP/Consultor Técnico Legislativo – Informática/2014) Quando há incompatibilidade entre as versões do protocolo HTTP instaladas no cliente e no servidor, é retornado um código de estado 5xx, com uma mensagem como "O servidor não é compatível com a versão do protocolo HTTP usada na solicitação".

Comentários:

Entrando mais no detalhe, o código específico é o de número 505. Lembrando que o grupo 5xx corresponde a erros ou negativa por parte do servidor.

Gabarito: C

12. (FCC – TRE-CE/Técnico Judiciário – Operação de Computador/2012) O protocolo HTTPS é uma implementação do protocolo HTTP utilizando um meio de comunicação seguro entre dois



computadores, como por exemplo TLS/SSL. Por padrão, a porta TCP utilizada para a comunicação HTTPS é a porta

- A) 80.
- B) 443.
- C) 993.
- D) 465.
- E) 512.

Comentários:

Mais uma questão bem tranquila, certo? A porta padrão do HTTP é 80 e a sua utilização de modo seguro se dá através da porta 443, ambos no protocolo TCP.

Gabarito: B

13. (FCC – AL-SP/Agente Técnico Legislativo Especializado – Segurança de Redes/2010) Protocolos de rede podem ser classificados como "sem estados" (stateless) ou "com estado" (stateful). Um exemplo de protocolo "sem estados" é o protocolo

- A) HTTP.
- B) FTP.
- C) SMTP.
- D) DHCP.
- E) NFS.

Comentários:

Pessoal, muito cuidado para não confundir o critério de ser com ou sem estados com o fato de ser persistente ou não (conexão). O HTTP, seja ele persistente ou não, sempre será sem estados ou stateless.

Gabarito: A



QUESTÕES COMENTADAS – HTTP - FGV

1. (FGV - Tec (DPE RS)/DPE RS/Apoio Especializado/Suporte de TI/2023)

Uma aplicação Web consiste em muitos componentes, entre eles navegadores e servidores. No contexto de transferência de informação e arquivos na Web, o protocolo de camada de aplicação que define o formato e a sequência das mensagens que são passadas entre o navegador e o servidor é o:

- a) RIP;
- b) ARP;
- c) DHCP;
- d) NAT;
- e) HTTP.

Comentários:

Questão introdutória sobre o HTTP. Sem muito o que acrescentar aqui, meus amigos.

Gabarito: E

2. FGV - 2021 - Banestes - Analista em Tecnologia da Informação - Suporte e Infraestrutura

O protocolo HTTP define um conjunto de métodos de requisição responsáveis por indicar a ação a ser executada para um dado recurso.

Um método HTTP é denominado idempotente se:

A as requisições em algum momento causam danos ou efeitos colaterais irreversíveis no servidor;

B as requisições com cabeçalhos e parâmetros diferentes causam uma mesma mudança no estado do recurso;

C toda requisição estabelecer um túnel para o servidor identificado pelo recurso de destino;

D o código de status for o mesmo entre requisições que aplicam modificações parciais em um recurso;

E uma requisição idêntica puder ser feita uma ou mais vezes em sequência com o mesmo efeito enquanto deixa o servidor no mesmo estado.



Comentários:

Na linha do que vimos, ao serem mantidos os parâmetros, não haverá alteração do estado do servidor.

Gabarito: E



QUESTÕES COMENTADAS – HTTP - CESGRANRIO

1. CESGRANRIO - 2024 - UNEMAT - Analista de Sistemas

Um desenvolvedor web está trabalhando em um projeto que envolve a transferência de dados do usuário através de um formulário on-line. Por questões de privacidade e segurança, ele precisa garantir que os dados submetidos pelos usuários não sejam expostos na URL do navegador.

Nesse contexto, o método de requisição definido no protocolo HTTP que deve ser utilizado durante a transferência é o

- A) GET
- B) HEAD
- C) POST
- D) QUERY
- E) SUBMIT

Comentários:

Vimos que os dois principais métodos do HTTP são justamente o GET e o POST. O primeiro traz os parâmetros diretamente na URL, tendo uma abertura e exposição da informação. Enquanto o POST, faz as chamadas diretamente ao servidor e backend sem a devida exposição.

Gabarito: C



LISTA DE QUESTÕES – HTTP - CESPE

1. CEBRASPE (CESPE) - AFM (Pref Fortaleza)/Pref Fortaleza/Ciência da Computação, Informática, Processamento de Dados/2023

HTTSPs é a combinação do HTTP sobre a camada SSP (secure sockets layer), que é colocada entre a camada de aplicação e a camada de transporte, aceitando solicitações do navegador e enviando-as ao TCP (transmission control protocol) para transmissão ao servidor.

2. CESPE / CEBRASPE - 2023 - MPE-RO - Analista de Suporte Computacional

A respeito de Internet e intranet, assinale a opção correta.

A) O dynamic HTML permite interatividade rápida, mas não permite modificação do conteúdo na página sem precisar recarregá-la.

B) Navegadores web permitem, nativamente, a leitura de vários tipos de arquivo; em alguns casos, por meio de plug-ins, permitem também a leitura de arquivos que não são suportados nativamente.

C) Os navegadores web se comunicam, geralmente, com servidores web usando o FTP.

D) A principal diferença entre páginas da Internet e da intranet é o protocolo de acesso aos dados.

E) A maioria dos navegadores web necessita de plug-ins para que o HTTPS seja suportado.

3. CESPE / CEBRASPE - 2022 - BNB - Analista de Sistemas - Desenvolvimento de Sistemas

Usuários que recebem um código de status HTTP 4XX podem refazer a solicitação mesmo sem alterar nada e ter sucesso na próxima resposta.

4. Cebbraspe – Analista Judiciário – Tecnologia da Informação (TRT-AP/PA)/2022

O cabeçalho do protocolo HTTP que contém o DNS do servidor é o

a) host.

b) authorization.

c) referer.



d) location.

e) server.

5. (CESPE – STJ/Analista Judiciário – Suporte em TI/2015) Uma forma de se melhorar o desempenho do acesso a páginas web frequentemente visitadas é armazenar-se o conteúdo dessas páginas para que sejam rapidamente carregadas em solicitações futuras, estando, entre os possíveis processos para executar essa tarefa, o proxy, ao qual serão encaminhadas todas as requisições de acesso a páginas web.

6. (CESPE - TJ TRE MS/Apoio Especializado/Programação de Sistemas/2013) O elemento em que uma das partes de uma informação é armazenada como cadeia de texto na máquina do usuário e cuja função principal é a de manter a persistência de sessões HTTP é denominado

A) frame.

B) Java Script.

C) tag.

D) cookie.

E) XML.

7. (CESPE - TJ TRE MS/Apoio Especializado/Programação de Sistemas/2013) Com referência ao Hyper Text Transfer Protocol (HTTP) — protocolo de aplicação utilizado para o tratamento de pedidos e respostas entre cliente e servidor na Internet e com o qual, normalmente, são desenvolvidas as aplicações para a Web —, assinale a opção em que todas as expressões identificam métodos de requisição HTTP que devem ser implementados por um servidor HTTP 1.1 usado pelo cliente.

A) SOAP, WS, WSDL, UDDI

B) TCP, IP, NETBIOS, UDP, IPX

C) NFS, SMB, IPP, SMTP, POP3, IMAP, XMPP, SIP

D) SET, GET, CONSTRUCTOR, DESTRUCTOR

E) GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS



8. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O protocolo HTTP, que não armazena informações sobre o estado do cliente, classifica-se como do tipo stateless.
9. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) Um servidor HTTP consiste em um servidor de aplicações.
10. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) Ao receber uma requisição, o servidor procura pelo recurso requisitado e envia, ao cliente, uma resposta com um código, que pode iniciar-se por 1xx, que indica sucesso no recebimento da requisição; 2xx, que indica redirecionamento da requisição; 3xx, que informa erros acontecidos no cliente; e 4xx, que informa erros no servidor.
11. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) As estratégias usadas para diminuir o tráfego causado pelo grande número de acessos a páginas web podem ser do tipo cache web, que é implementado no cliente, no GET condicional ou na rede servidor Proxy Web.
12. (CESPE – MPU/Analista Judiciário – Suporte e Infraestrutura/2013) Os servidores proxy criam um cache com as solicitações de cada usuário, de forma a otimizar consultas futuras de um mesmo usuário, sendo esse cache de uso exclusivo de seu respectivo usuário.
13. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O código abaixo ilustra uma resposta de um servidor web.
- ```
GET /internet/index.html HTTP/1.0
User-agent: Mozilla /4.5 [en] (WinNT; I)
AcceptP: text/plain, text/html, image/gif, image/x-xbitmap,
image/jpeg, image/pjpeg, image/png, */*
Accept-Charset: isso-8859-1, *, utf-8
Accept-Enconding: gzip
Accept-Language: em
```
14. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O protocolo HTTP utiliza, por padrão, a porta 80 para tráfego seguro de dados, sendo o pacote de sincronismo da conexão o responsável por indicar o tipo de cifra que será utilizado na sessão.



15. (CESPE - TJ TRT17/Apoio Especializado/Tecnologia da Informação/2013) Como maneira de se evitar o desenvolvimento de novos protocolos de camada de aplicação, diversas aplicações usam o HTTP como forma de transferir dados fim a fim na camada de aplicação.
16. (CESPE - Tec MPU/Técnico Administrativo/Tecnologia da Informação e Comunicação/2013) O serviço HTTP é implementado sem estado, enquanto o HTTPS é sua versão stateful (com estado).
17. (CESPE - Ana MPU/Tecnologia da Informação e Comunicação/Suporte e Infraestrutura/2013) A primeira versão do serviço HTTP utiliza conexões não persistentes; a persistência foi acrescentada na versão subsequente desse serviço.
18. (CESPE – TRT(DF e GO)/Técnico Judiciário – Tecnologia da Informação/2013) Os servidores de HTTP mais utilizados atualmente são Apache HTTP Server, Internet Information Server e Enterprise Server.
19. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) Se o endereço de página inicia com HTTPS, então os dados serão transmitidos por meio de uma conexão cifrada e a autenticidade do servidor e do cliente será verificada com o uso de certificados digitais.
20. (CESPE – TCU/Analista de Controle Externo – TI/2007) O protocolo HTTP, definido nas RFCs 1945 e 2616, não permite a utilização de conexões persistentes.
21. (CESPE – TRT – 17ª Região (ES)/Técnico Judiciário – TI/2013) HTTPS usa certificados digitais, requer o uso de TLS e utiliza a porta 443 por padrão.
22. (CESPE – TRE-GO/Técnico Judiciário/2015) Na busca de um produto em uma loja virtual por meio de um webservice, quando o produto é encontrado, o protocolo HTTP retorna um HTTP/1.1 404, o que facilita o tratamento do pedido no programa cliente.



23. (CESPE – TRE-GO/Técnico Judiciário – Programação de Sistemas/2015) Por meio do protocolo chave HTTP, é possível utilizar o método PUT para se criar um novo recurso de um webservice.
24. (CESPE – TRE-GO/Técnico Judiciário – Programação de Sistemas/2015) Uma conexão entre um computador cliente a um computador considerado servidor, para visualizar uma página web, através do protocolo HTTP, é possível afirmar que será utilizado o protocolo de transporte TCP (transmission control protocol).
25. (CESPE – TJDFT/Analista Judiciário – Suporte em TI/2015) A técnica de compressão não é recomendada ao se utilizar a versão 2 do HTTP sobre o protocolo TLS 1.2.
26. (CESPE – TJDFT/Analista Judiciário – Suporte em TI/2015) Na implementação do HTTP versão 2 sobre o protocolo TLS 1.2, é mandatório desabilitar a renegociação da conexão.
27. (CESPE – TJDFT/Analista Judiciário – Suporte em TI/2015) No HTTP, a técnica geral do controle de fluxo garante que não haja interferência entre as conexões independentes. Entretanto essa técnica foi abandonada na versão 2 do HTTP, que criou o conceito de WINDOW\_UPDATE frame.



## GABARITO

|    |    |    |    |    |    |
|----|----|----|----|----|----|
| 01 | 02 | 03 | 04 | 05 | 06 |
|    | B  | E  | A  | C  | D  |
| 07 | 08 | 09 | 10 | 11 | 12 |
| E  | C  | E  | E  | C  | E  |
| 13 | 14 | 15 | 16 | 17 | 18 |
| E  | E  | C  | E  | C  | C  |
| 19 | 20 | 21 | 22 | 23 | 24 |
| C* | E  | C  | E  | C  | C  |
| 25 | 26 | 27 |    |    |    |
| C  | C  | E  |    |    |    |

\* 19 - Gabarito do professor: E



## LISTA DE QUESTÕES – HTTP - FCC

1. (FCC – TRT – 15ª Região/Analista Judiciário – TI/2015) Um serviço da internet utiliza diferentes protocolos, por exemplo, protocolos relacionados com a função de roteamento, transmissão de dados e transferência de hipertexto para efetivar a comunicação. Os respectivos protocolos, do conjunto (suite) de protocolos TCP/IP, relacionados com as funções apresentadas, são:

- A) IP, TCP e HTTP.
- B) TCP, FTP e HTML.
- C) IP, FTP e HTML.
- D) ARP, FTP e HTTP.
- E) TCP, IP e HTTP.

2. (FCC – TRT – 16ª Região (MA) /Técnico Judiciário – TI/2014) Os diversos protocolos do conjunto (suite) TCP/IP são organizados em camadas de funcionalidade. Quando um usuário da internet realiza um acesso à página Web, ele está utilizando o protocolo da camada de Aplicação denominado

- A) W W W.
- B) IMAP.
- C) HTTP.
- D) TCP.
- E) IP.

3. (FCC – TRT – 2ª Região (SP)/Técnico Judiciário – TI/2014) No modelo de referência de 4 camadas da suíte de protocolos TCP/IP, os protocolos Ethernet, HTTP e ICMP localizam-se, respectivamente, nas camadas

- A) Internet, Apresentação e Interface de rede
- B) Interface de rede, Aplicação e Internet.
- C) Transporte, Internet e Interface de rede.



D) Transporte, Aplicação e Enlace de dados.

E) Física, Transporte e Enlace de dados.

4. (FCC – TRF – 4ª Região/Técnico Judiciário – TI/2014) Pedro, técnico em informática do TRF da 4ª Região, deve comprovar os seus conhecimentos sobre o modelo OSI identificando os protocolos às respectivas camadas do modelo. Assim, um correto relacionamento identificado por Pedro é:

A) FTP - Camada de Transporte.

B) HTTP - Camada de Transporte.

C) ICMP - Camada de Aplicação.

D) HTTP - Camada de Aplicação.

E) SNMP - Camada de Rede.

5. (FCC – TRF – 2ª Região/Analista Judiciário – Informática/2012) Sobre o protocolo HTTP, é correto afirmar:

A) Usa o TCP e o UDP como seus protocolos de transporte e presta serviço por default na porta 80.

B) Em uma mensagem de requisição HTTP, a linha de cabeçalho User-agent: especifica o agente de usuário, isto é, o browser que está fazendo a requisição ao servidor.

C) Quando utiliza conexões persistentes, cada conexão TCP é encerrada após o servidor enviar o objeto resposta ao cliente que fez a requisição. Cada conexão TCP transporta exatamente uma mensagem de requisição e uma mensagem de resposta.

D) A resposta do servidor a uma requisição HTTP é dividida em três seções. A primeira é denominada cabeçalho (header) e contém informações do servidor sobre o recurso solicitado. A segunda seção é denominada corpo (body) e contém o recurso propriamente dito. A terceira seção, denominada rodapé (footer), contém informações de status da requisição e o relatório de erros, quando houver.

E) Os únicos métodos (comandos) de requisição do protocolo HTTP são GET e POST. O status de retorno de número 404 do método HTTP indica que o serviço está indisponível.

6. (FCC – TCE-SP/Auxiliar de Fiscalização Financeira/2012) Sobre o protocolo HTTP, é correto afirmar:



- A) Se um cliente solicita ao servidor o mesmo objeto duas vezes em um período de poucos segundos, o servidor responde dizendo que acabou de enviar o objeto ao cliente e não envia novamente o objeto.
- B) É implementado em dois programas: um programa cliente e outro servidor. Os dois programas, implementados em sistemas finais diferentes, conversam um com o outro por meio da troca de mensagens HTTP. O HTTP não define a estrutura dessas mensagens, mas define o modo como cliente e servidor as trocam.
- C) O HTTP usa o TCP como seu protocolo de transporte subjacente. O cliente HTTP primeiramente inicia uma conexão TCP com o servidor. Uma vez estabelecida a conexão, os processos do browser e do servidor acessam o TCP por meio de suas interfaces socket.
- D) Os servidores web implementam apenas o lado cliente do HTTP e abrigam objetos web, cada um endereçado por um URL. O Apache e o IIS são servidores web populares.
- E) O HTTP define como clientes web requisitam páginas web aos servidores, mas não define como eles as transferem aos clientes.

7. (FCC – MPE-AM/Agente de Apoio – Manutenção e Suporte de Informática/2013) HTTPS (HyperText Transfer Protocol SecurE) é um protocolo que combina o uso do HTTP com o

- A) SSL e o TLS, a fim de prover conexões seguras.
- B) DES e AES, a fim de prover criptografia assimétrica.
- C) RSA, a fim de prover certificação digital por meio de criptografia simétrica.
- D) IDS e IPS, a fim de prover segurança contra invasores.
- E) IMAP e POP, a fim de prover comunicação segura.

8. (FCC – TRF – 1ª Região/Analista Judiciário – Área de Apoio Especializado/2014) O ..... recebe os pedidos HTTP na porta configurada e processa todos os pedidos da web que chegam, podendo distribuí-los. Os pedidos de objetos que podem ser armazenados no cache (informações estáticas que não mudam com frequência como páginas em HTML e imagens GIF) são processados pelo proxy. Os pedidos de objetos que não podem ser armazenados no cache (informações dinâmicas que mudam com frequência) são processados pelo servidor web de origem na porta configurada. Essa configuração pode ser feita para proteger um servidor intranet da Internet e reduzir a carga nos servidores web públicos mantidos na intranet, por exemplo, criando um front end para um servidor web. A lacuna é corretamente preenchida por

- A) cache HTTP.
- B) acelerador HTTPS.
- C) proxy estático-dinâmico.



D) filtro de logs.

E) proxy reverso.

9. (FCC – TRT – 6ª Região (PE)/Analista Judiciário – TI/2012) Protocolos de rede podem ser classificados como "sem estados" (stateless) ou "com estado" (stateful). A este respeito é correto afirmar que

A) protocolos sem estados exigem que tanto cliente como servidor mantenham um histórico da conexão.

B) o uso de cookies é uma maneira de contornar o fato de que HTTP é um protocolo com estados.

C) protocolos sem estados têm a desvantagem de não admitir encapsulamento criptográfico.

D) o uso de cookies é uma maneira de contornar o fato de que HTTP é um protocolo sem estados.

E) protocolos com estados exigem que cada mensagem trocada entre cliente e servidor contenha informação respectiva ao estado da transação.

10. (FCC – TJ-AP/Analista Judiciário – TI/2014) O protocolo HTTPS (HyperText Transfer Protocol SecurE) é uma implementação elaborada a partir do protocolo HTTP, na qual se incorporou uma camada de segurança. O protocolo de segurança originalmente utilizado nessa camada é o

A) POP3 (Post Office Protocol).

B) SMTP (Simple Mail Transfer Protocol).

C) IMAP (Internet Message Access Protocol).

D) SSL (Secure Sockets Layer).

E) SSH (Secure Shell).

11. (FCC – Câmara Municipal de São Paulo – SP/Consultor Técnico Legislativo – Informática/2014) Quando há incompatibilidade entre as versões do protocolo HTTP instaladas no cliente e no servidor, é retornado um código de estado 5xx, com uma mensagem como "O servidor não é compatível com a versão do protocolo HTTP usada na solicitação".



12. (FCC – TRE-CE/Técnico Judiciário – Operação de Computador/2012) O protocolo HTTPS é uma implementação do protocolo HTTP utilizando um meio de comunicação seguro entre dois computadores, como por exemplo TLS/SSL. Por padrão, a porta TCP utilizada para a comunicação HTTPS é a porta

- A) 80.
- B) 443.
- C) 993.
- D) 465.
- E) 512.

13. (FCC – AL-SP/Agente Técnico Legislativo Especializado – Segurança de Redes/2010) Protocolos de rede podem ser classificados como "sem estados" (stateless) ou "com estado" (stateful). Um exemplo de protocolo "sem estados" é o protocolo

- A) HTTP.
- B) FTP.
- C) SMTP.
- D) DHCP.
- E) NFS.

## GABARITO

|    |    |    |    |    |    |
|----|----|----|----|----|----|
| 01 | 02 | 03 | 04 | 05 | 06 |
| A  | C  | B  | D  | B  | C  |
| 07 | 08 | 09 | 10 | 11 | 12 |
| A  | E  | D  | D  | C  | B  |
| 13 | 14 | 15 | 16 | 17 | 18 |
| A  |    |    |    |    |    |



## LISTA DE QUESTÕES – HTTP - FGV

### 1. (FGV - Tec (DPE RS)/DPE RS/Apoio Especializado/Suporte de TI/2023)

Uma aplicação Web consiste em muitos componentes, entre eles navegadores e servidores. No contexto de transferência de informação e arquivos na Web, o protocolo de camada de aplicação que define o formato e a sequência das mensagens que são passadas entre o navegador e o servidor é o:

- a) RIP;
- b) ARP;
- c) DHCP;
- d) NAT;
- e) HTTP.

### 2. FGV - 2021 - Banestes - Analista em Tecnologia da Informação - Suporte e Infraestrutura

O protocolo HTTP define um conjunto de métodos de requisição responsáveis por indicar a ação a ser executada para um dado recurso.

Um método HTTP é denominado idempotente se:

- A) as requisições em algum momento causam danos ou efeitos colaterais irreversíveis no servidor;
- B) as requisições com cabeçalhos e parâmetros diferentes causam uma mesma mudança no estado do recurso;
- C) toda requisição estabelecer um túnel para o servidor identificado pelo recurso de destino;
- D) o código de status for o mesmo entre requisições que aplicam modificações parciais em um recurso;
- E) uma requisição idêntica puder ser feita uma ou mais vezes em sequência com o mesmo efeito enquanto deixa o servidor no mesmo estado.



## GABARITO

| 01 | 02 |
|----|----|
| E  | E  |



## LISTA DE QUESTÕES – HTTP - CESGRANRIO

### 1. CESGRANRIO - 2024 - UNEMAT - Analista de Sistemas

Um desenvolvedor web está trabalhando em um projeto que envolve a transferência de dados do usuário através de um formulário on-line. Por questões de privacidade e segurança, ele precisa garantir que os dados submetidos pelos usuários não sejam expostos na URL do navegador.

Nesse contexto, o método de requisição definido no protocolo HTTP que deve ser utilizado durante a transferência é o

- A) GET
- B) HEAD
- C) POST
- D) QUERY
- E) SUBMIT



## GABARITO

1. C



# 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.