Estratégia Concursos

# Aula 00

*Senado Federal (Analista Legislativo - Informática - Análise de Sistemas) Redes e Segurança*

Autor:
**André Castro**

22 de Outubro de 2024

# Índice

# 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:

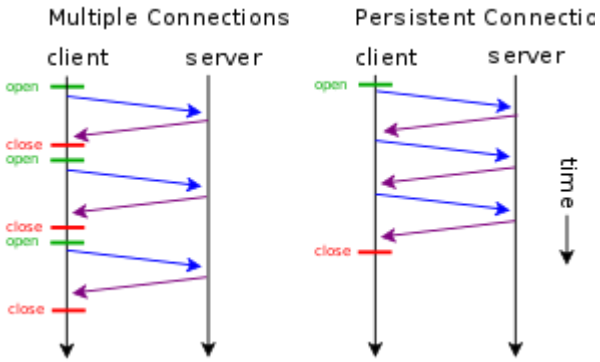
- O cliente estabelece uma conexão TCP com o servidor, geralmente, na porta 80, sendo esta a porta padrão do protocolo;
- O servidor responde à mensagem indicando o estado corrente da requisição, além da versão suportada e outras informações do servidor;
- A partir de então, se não houver mensagem de 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:

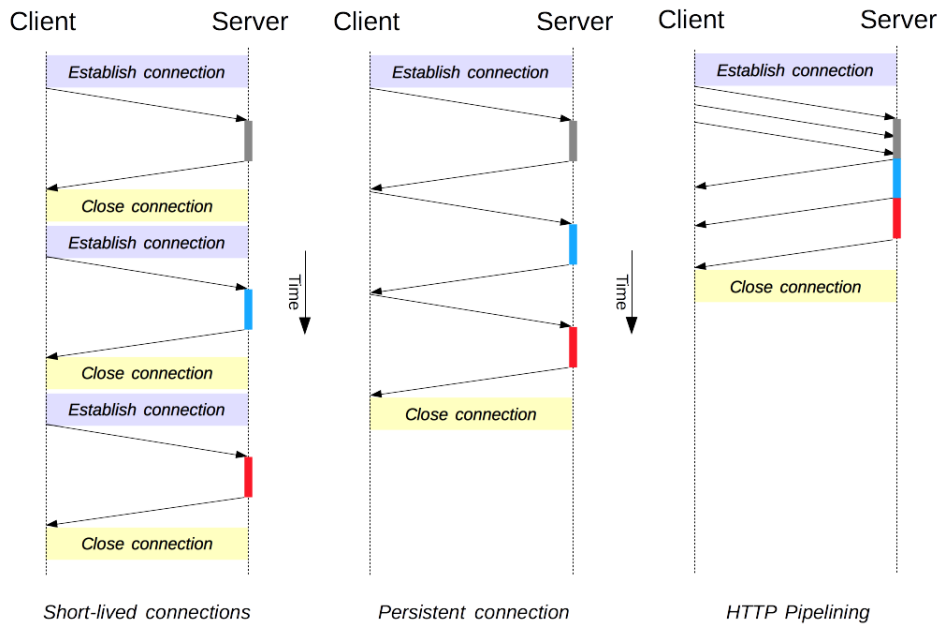
- **HTTPv1.0** – Não realiza conexões persistentes. Isto é, para cada troca de informação entre cliente e servidor, necessita-se estabelecer e encerrar uma nova conexão TCP;

- **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 paralela. 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.

## ESTRUTURA DA MENSAGEM HTTP

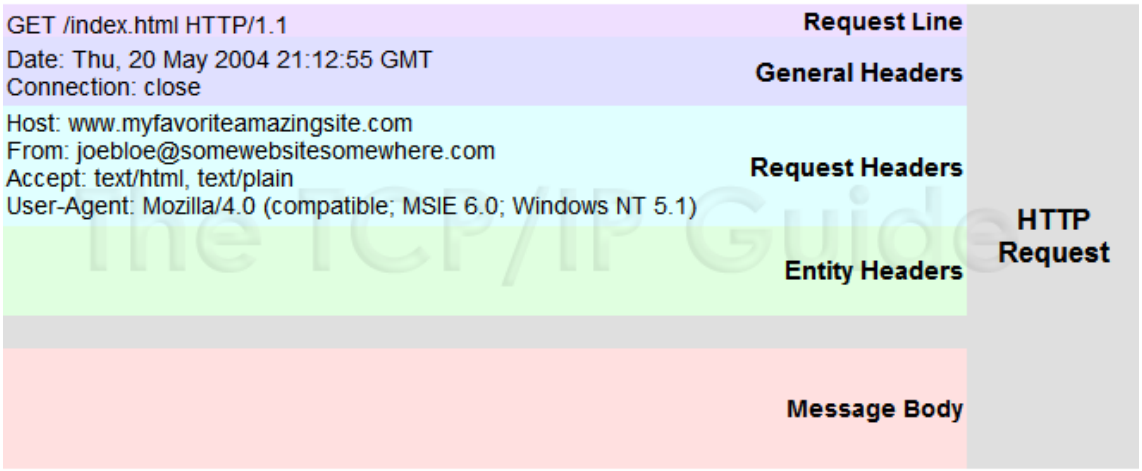
Como vimos, existem dois tipos de mensagem HTTP: requisição e resposta. Vamos verificar a estrutura de cada uma delas:

- ***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.

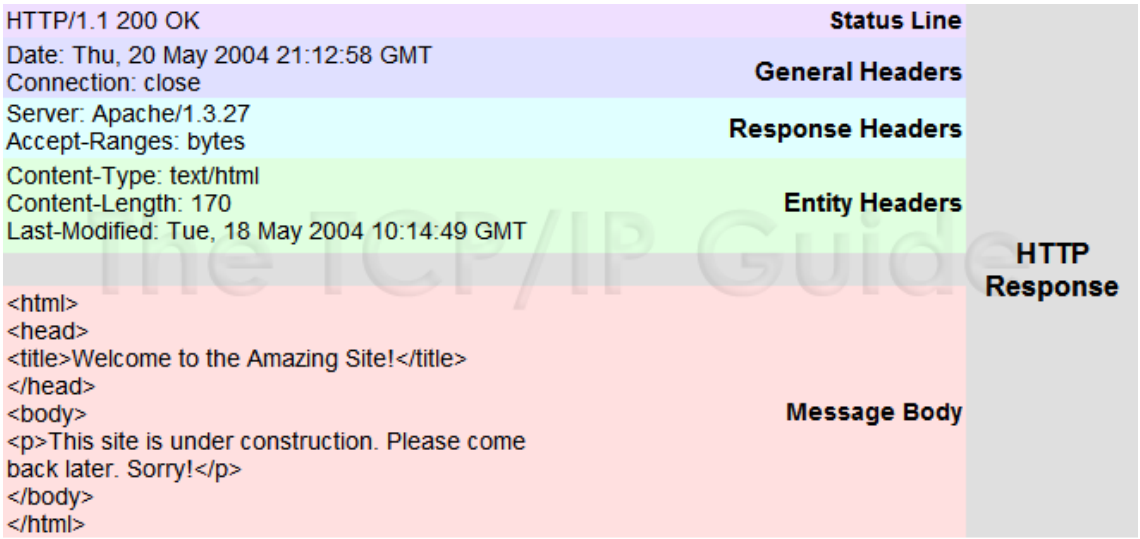
  Na requisição, o Corpo da Entidade é utilizado com o método POST uma vez que o cliente envia informações ao servidor para preenchimento do objeto de resposta.

  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:




## 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;

## 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.

## CONCEITO DE CACHE WEB

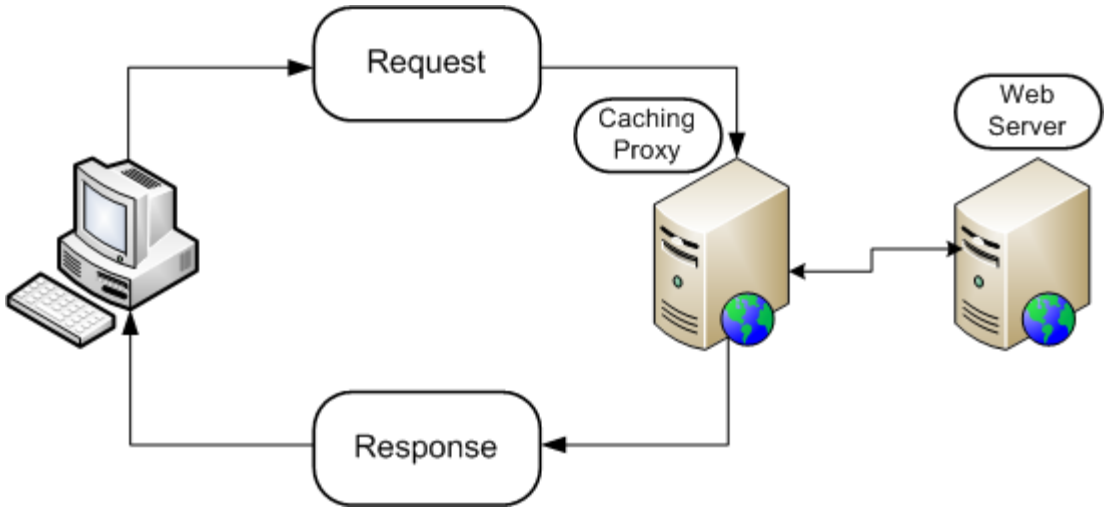
O funcionamento do CACHE WEB reside na possibilidade de otimização do procedimento de Requisição e Resposta entre o cliente e o servidor. Esse CACHE WEB busca evitar que novas consultas que sejam idênticas a consultas anteriores consumam recursos do servidor de destino, além de diminuir o tempo de resposta.

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

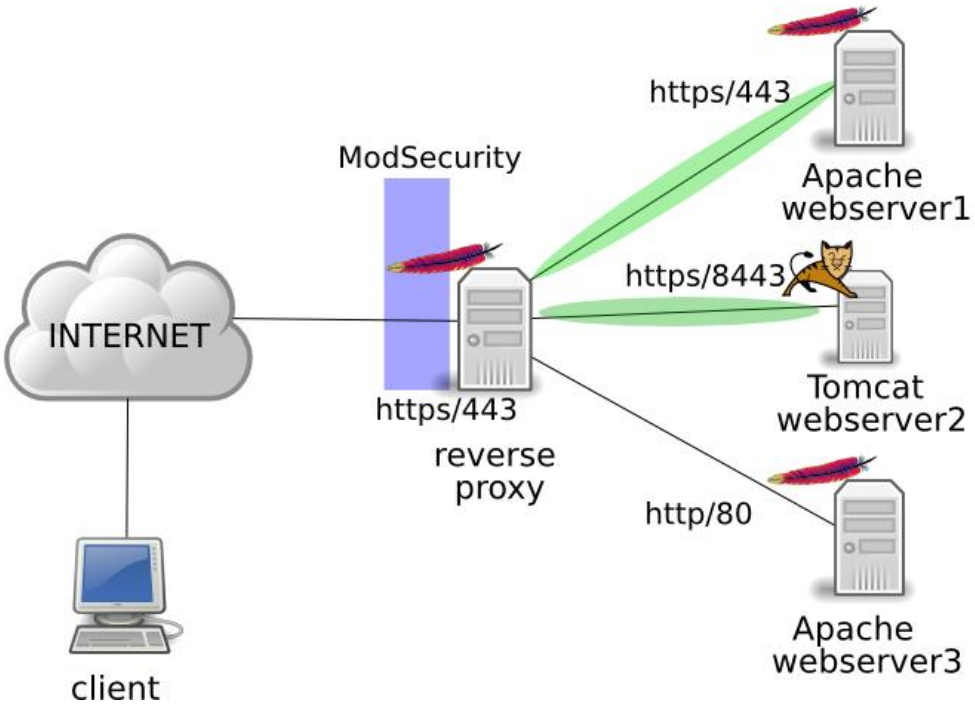
ao destino. Esse nó, é chamado de Proxy e armazena as últimas informações requisitas pelos clientes aos servidores.

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.

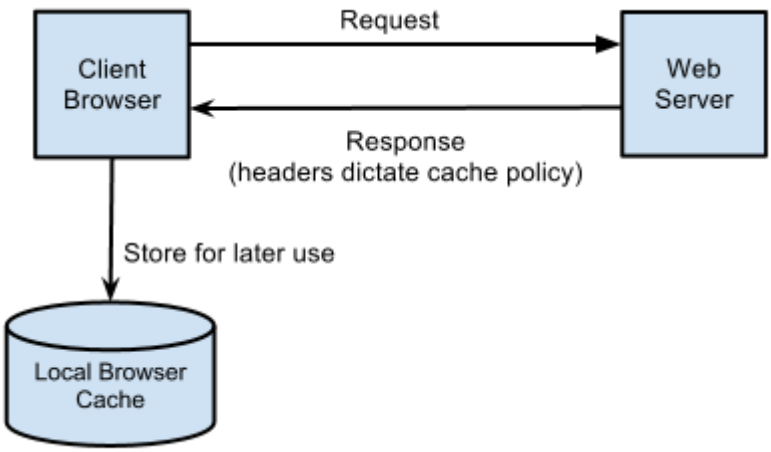



- **Proxy reverso** – Esse conceito gera alguns benefícios na implementação de serviços HTTP no lado do servidor. Entre eles temos os recursos de proteção, balanceamento e distribuição de requisições e armazenamento em cache das informações estáticas. Dessa forma, quando há uma requisição a um objeto 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.

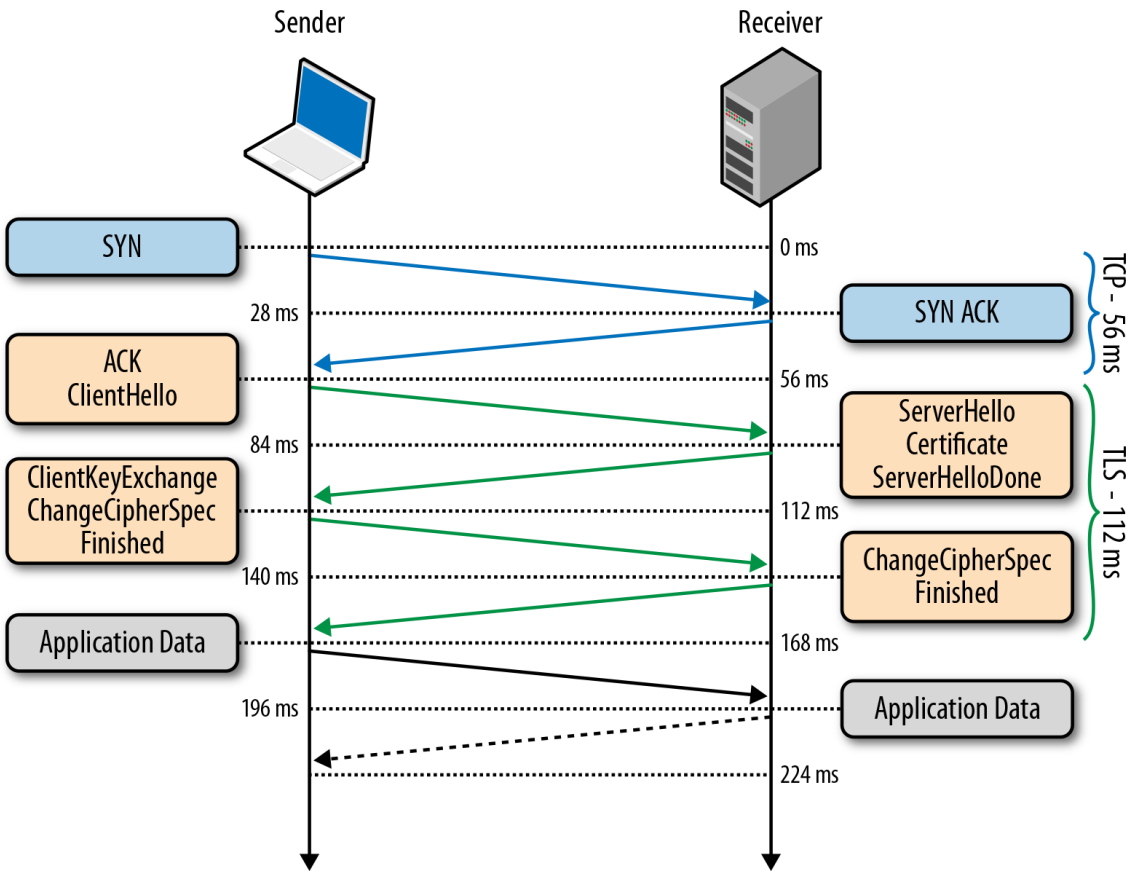
Dessa forma, quando temos uma navegação em HTTPS, dizemos que os dados serão cifrados para uma comunicação segura, além da capacidade de se verificar a autenticidade do servidor através de recursos de certificados digitais. Acrescido a isso, temos também a possibilidade de autenticação do usuário de 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

---

## 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 André? 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.

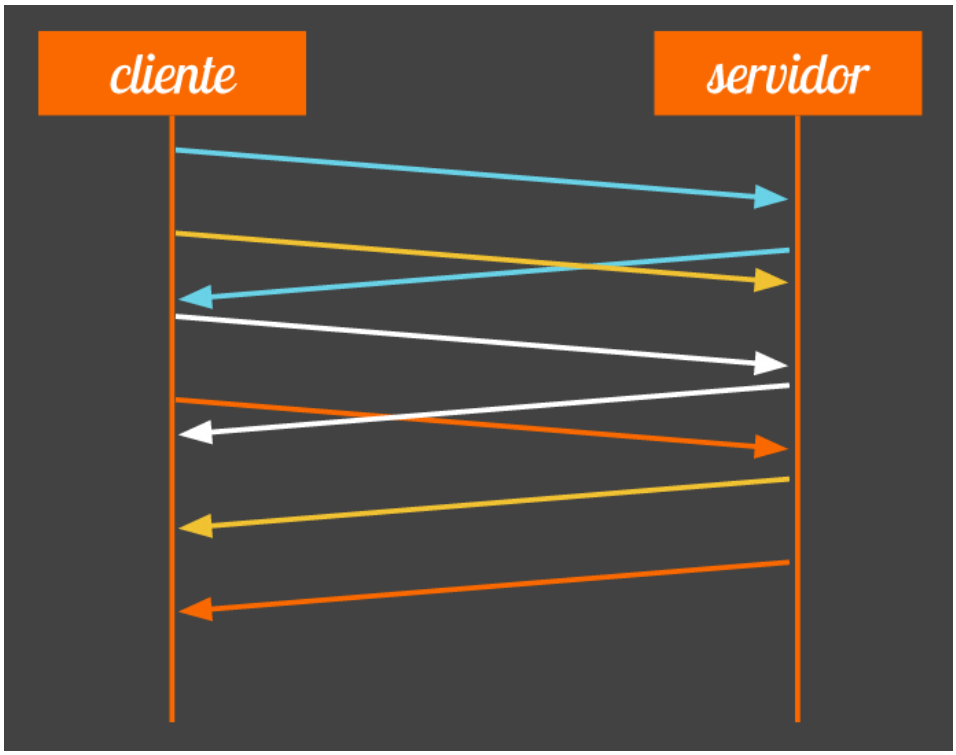
- **Paralelização de Fluxos com Multiplexing**

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. Percebam 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.

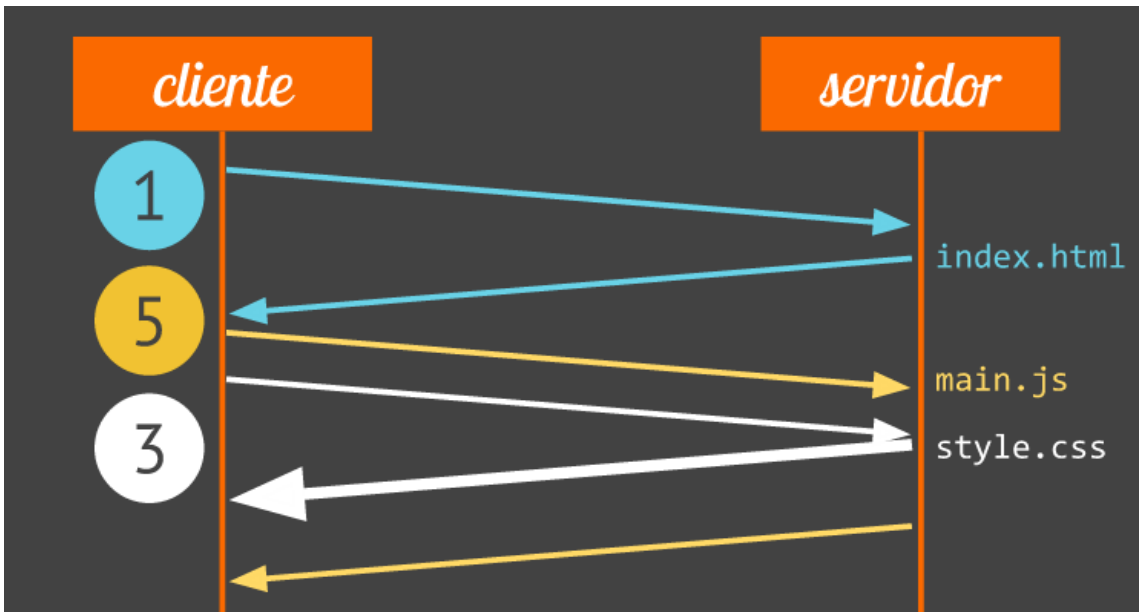
Na nova versão, envia-se apenas informações de cabeçalho que são diferentes das informações já enviadas, reduzindo, assim, o fluxo de dados desnecessários.

- **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.

# EXERCÍCIOS COMENTADOS

## HTTP

### 1. 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 possibilidade um incremento de desempenho em tempo de resposta e alivia a carga de consultas ao servidor.

**Gabarito: C**

---

### 2. 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**

### 3. 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**

---

### 4. 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**

---

### 5. 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**

---

**6. 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**

---

**7. 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**

---

### 8. 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**

---

### 9. 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-agente:      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
```

**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**

---

### 10. 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 carga do protocolo HTTPS na porta TCP/443. A definição de critérios de criptografia ocorre no momento do estabelecimento da conexão.

**Gabarito: E**

---

### 11. 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 sem um protocolo amplamente consolidado, simples e eficiente, diversos protocolos acabam usando sua estrutura para reaproveitar o modelo na transferência de dados simples.

**Gabarito: C**

---

### 12. 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**

---

### 13. 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**

---

**14.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 coorporativos, 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**

---

**15.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 intepretação do CESPE para não errarmos esse mesmo ponto em provas futuras.

**Gabarito: C (Gabarito do Professor: E)**

---

**16.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**

---

### 17.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 encrencar com esse aspecto para essa questão, dizendo que seria possível a utilização de SSL ao invés do TLS.

**Gabarito: C**

---

### 18.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**

---

### 19.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**

---

### 20.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**

---

### 21.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**

---

### 22.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.*

**Comentários:**

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

**Gabarito: C**

---

### 23.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**

---

## PROTOCOLOS DE CORREIO ELETRÔNICO (SMTP,IMAP E POP3)

### 24.CESPE – TCE-PR/Analista de Controle – Área TI/2016

*O padrão que viabiliza a transmissão de dados não ASCII por email por meio da utilização de SMTP é denominado*
*A Mail Transfer Protocol.*
*B Multiporpose Internet Mail Extension.*
*C Post Office Protocol.*
*D Internet Message Access Protocol.*
*E Hypertext Transfer Protocol.*

**Comentários:**

Temos aí o MIME, certo pessoal? Questão bem tranquila passível de ser resolvida por eliminação. O MIME surgiu exatamente no contexto em que o padrão de codificação ASCII não era mais suficiente para representação de anexos de binários e conteúdos multimídia. O MIME passa então a suportar padrões de textos como HTML e XML, imagens do tipo GIF e JPEG, áudio e vídeo.

**Gabarito: B**

---

### 25.CESPE – TCE-SC/AFCE – Área TI/2016

*Após o servidor local SMTP aceitar uma mensagem para subsequente envio, é necessário determinar o endereço do servidor de email do destinatário. Essa etapa é realizada mediante consulta DNS a um servidor de nomes capaz de prover a informação, no qual serão verificados os registros especiais MX (mail Exchange).*

**Comentários:**

Temos a descrição do princípio exercido pelo protocolo DNS, que é a tradução de nomes para endereços IP. Além disso, temos uma especificidade do seu funcionamento no que tange ao tipo de consulta realizada. O DNS é capaz de realizar diversos tipos de serviços, as quais são definidas a partir das referências a seguir, em um caráter não exaustivo:

- A – Address IPv4 – Quando um cliente usa esse tipo de registro, o objetivo é descobrir o endereço IPv4 que responde por determinado nome de domínio;

- AAAA – Address IPv6 - Quando um cliente usa esse tipo de registro, o objetivo é descobrir o endereço IPv6 que responde por determinado nome de domínio;

- CNAME (Canonical Name) - Faz o mapeamento de um alias (apelido) ou um DNS alternativo.

- PTR – Pointer – Realiza o caminho inverso. A partir de um endereço IPv4, deseja-se obter o respectivo nome de domínio;

- NS – Nameserver – Especifica o nome do servidor DNS responsável por determinado domínio;

- MX – Mail Exchange – Fornece o nome do servidor de e-mail de maior prioridade que responde por determinado domínio de e-mail. Após a obtenção desse nome, é

preciso ainda realizar uma consulta do tipo address para se determinar o endereço IP;

Essas identificações serão fornecidas no campo TYPE da estrutura de resposta DNS. Portanto, percebemos que o MX, de fato, diz respeito à tradução do nome do servidor de e-mail para o respectivo endereço IP.

**Gabarito: C**

---

**26.CESPE - STF/Apoio Especializado/Suporte em Tecnologia da Informação/2013**

*Caso o emissor da mensagem não envie nenhum comando ao servidor SMTP, servidores de correio eletrônico modernos com suporte ao SMTP implementarão técnicas de timeout.*

**Comentários:**

Pessoal, vimos que o protocolo SMTP encerra a sessão com o comando QUIT. Entretanto, possui um tempo default de 5 minutos. Caso não haja troca de mensagens nesse intervalo, automaticamente o servidor derruba a conexão.

**Gabarito: C**

---

**27.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012**

*O SMTP (simple mail transfer protocol) é um protocolo de correio eletrônico para recebimento de e-mail pelos usuários.*

**Comentários:**

Não né pessoal? O SMTP é para envio. Os protocolos para recebimento são o IMAP e o POP3.

**Gabarito: E**

---

**28.CESPE – Banco da Amazônia/Técnico Científico/2012**

*O protocolo SMTP, ao utilizar a porta 25 para enviar e receber mensagens, é capaz de criptografar o cabeçalho da mensagem transmitida.*

## Comentários:

O SMTP nativamente e por si só não implementa recursos de criptografia. Vale observar que o protocolo SMTP foi referenciado na porta 25 para enviar e receber mensagens. Na prática, o cliente abre uma conexão TCP na porta 25 do servidor. Sob a perspectiva do cliente então, a porta 25 será utilizada para envio, sob a perspectiva do servidor, a porta 25 será utilizada para recebimento. Não vejo motivo para esse trecho, portanto, estar errado.

**Gabarito: E**

---

### 29.CESPE – Câmara dos Deputados/Analista – Engenharia Eletrônica/2012

*O SMTP consiste em um protocolo muito utilizado pelos servidores de transporte de email modernos, apesar de possuir tecnologia bastante arcaica, surgida antes mesmo do protocolo HTTP.*

## Comentários:

*De fato, o SMTP é bem antigo, vindo antes mesmo do HTTP, conforme vimos. Isso não limita seu uso em servidores atuais e modernos, por ele ser simples e eficaz frente ao seu propósito.*

**Gabarito: C**

---

### 30.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012

*O protocolo SMTP é um protocolo cliente-servidor, uma vez que os servidores de correio eletrônico funcionam ora como clientes, ao enviarem emails, ora como servidores, ao receberem emails.*

## Comentários:

Vimos que essa é uma das formas de atuação dos MTA's. Possui uma função de relay na rede ao repassar essas informações. Atenção para o detalhe muito bem pontuado pela banca. Ao enviar, atua como cliente, ao receber, atua como servidor. Se tivesse escrito de forma inversa estaria errado.

**Gabarito: C**

---

**31.CESPE - STF/Apoio Especializado/Suporte em Tecnologia da Informação/2013**

*Ainda que uma mensagem de email com SMTP possua diversos destinatários, o comando RCPT é realizado no servidor de destino somente uma vez.*

**Comentários:**

Pessoal, vimos que o comando RCPT aceita somente uma entrada de email por vez. Portanto, para múltiplos destinatários, deve-se enviar diversos comandos RCPT com os endereços dos destinatários.

**Gabarito: E**

---

**32.CESPE - STF/Apoio Especializado/Suporte em Tecnologia da Informação/2013**

*O uso de Open Relay para configurar servidores de email ligados à Internet é considerado má prática administrativa. Normalmente, esse tipo de servidor é passível de ser inscrito em listas negras na Internet.*

**Comentários:**

Vimos que o conceito de open relay são aqueles MTA's mal configurados ou sem implementação de recursos de segurança. Dessa forma, tendem a repassar conteúdo indesejado e malicioso e acabam por diversas vezes figurando nas blacklists (listas negras) na Internet.

**Gabarito: C**

---

**33.CESPE - ANTT/Tecnologia da Informação/Infraestrutura de TI/2013**

*Quando um serviço de correio eletrônico disponibiliza o IMAP (Internet message access protocol) para o usuário final, este utiliza um software cliente de email para manipular e manter suas mensagens no servidor de correio eletrônico.*

**Comentários:**

Vimos que a principal característica dos servidores IMAP é justamente a capacidade de se acessar e gerenciar os e-mails diretamente no servidor de e-mails, sem a necessidade de realizar o download das mensagens. Detalhe para o software cliente que pode ser um software específico ou o próprio browser com acesso web.

**Gabarito: C**

---

**34.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012**

*Os protocolos OSPF e LDAP são utilizados para ler, editar, responder e criar novos e-mails.*

**Comentários:**

Bem tranquilo, não é pessoal? OSPF é um protocolo de roteamento e o LDAP é um protocolo de acesso a serviços de diretórios em redes TCP/IP. Protocolos para tais recursos são o SMTP, IMAP e POP.

**Gabarito: E**

---

**35.CESPE – Banco da Amazônia/Técnico Científico – Suporte Técnico/2012**

*O recurso de greylist recusa, de forma temporária, o recebimento de uma mensagem e aguarda sua retransmissão, levando em consideração que servidores de e-mail legítimos possuem políticas de retransmissão em caso de erros.*

**Comentários:**

Vimos que o método greylist é um híbrido, entre o whitelist e blacklist que implementa justamente o funcionamento descrito no enunciado.

**Gabarito: C**

---

**36.CESPE – Banco da Amazônia/Técnico Científico – Suporte Técnico/2012**

*O bloqueio de conteúdo pelo servidor SMTP pode recusar a mensagem enviando um código de erro, acrescido da mensagem Message Content Rejected ou desviando-a para uma área chamada de quarentena.*

**Comentários:**

Pessoal, vimos que essas duas são possibilidades de atuação de um MTA frente a um possível email malicioso ou considerado SPAM.

**Gabarito: C**

---

### 37.CESPE – Banco da Amazônia/Técnico Científico – Suporte Técnico/2012

*Ao detectar que uma mensagem de e-mail é um spam, as ferramentas de antispam são capazes de modificar o assunto da mensagem, para alertar o usuário de que se trata de spam, e depois entregá-la na conta de e-mail do usuário.*

**Comentários:**

Mais uma vez, temos a descrição de uma possibilidade de atuação do servidor de email, agora frente a um possível SPAM, transferindo a responsabilidade para o usuário considerar ou não a ponderação do servidor de email.

**Gabarito: C**

---

### 38.CESPE – TRE/RS / Técnico Judiciário – Área 7/2015 (ADAPTADA)

*Para a transferência efetiva de mensagens de email, o SMTP deve estar disponível nos servidores de correio do remetente e do destinatário, sem a possibilidade de implementação de outros protocolos.*

**Comentários:**

A característica do SMTP é seu funcionamento assíncrono ou também conhecido como store-and-forward. Ou seja, caso um servidor receba determinada mensagem, ele por guardar essa mensagem pelo tempo necessário até que o servidor que deva recebê-la esteja online, não necessitando que seja feito de forma simultânea.

**Gabarito: E**

---

### 39.CESPE – TRE/RS / Técnico Judiciário/2015 (ADAPTADA)

*O POP é um protocolo para envio de email.*

**Comentários:**

O SMTP é um protocolo de envio, enquanto o POP3 e IMAP são para recebimento.

**Gabarito: E**

### 40.CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015

*PGP (Pretty Good Privacy) é um pacote que fornece recursos de compactação, privacidade e assinaturas digitais, além de poder criptografar mensagens de correio eletrônico.*

**Comentários:**

O PGP É um pacote que é implementado na camada de aplicação que utiliza recursos de funções HASH, como o SHA-1 e criptografia simétrica e assimétrica. Somando-se todos esses recursos, é possível buscar os princípios de confidencialidade, integridade e autenticidade através da assinatura digital e criptografia dos dados com chaves de sessão. Suporta o recurso de múltiplas assinaturas, compressão de forma segura, fragmentação de mensagens. Há de se mencionar que esses recursos não necessariamente são utilizados em conjunto, podendo ser aplicados de forma independentes, ou seja, posso querer não implementar o recurso de compressão e manter todos os demais.

**Gabarito: C**

---

### 41.CESPE – TRE-PE/Área 1 – Operação de Computadores/2016 (ADAPTADA)

*Os protocolos IP, SNMP, SMTP e ARP fazem parte da camada de rede (Internet) do modelo TCP/IP.*

**Comentários:**

Somente os protocolos IP e ARP fazem parte da camada de rede. O SNMP e SMTP fazem parte da camada de aplicação.

**Gabarito: E**

# EXERCÍCIOS COMENTADOS COMPLEMENTARES

## HTTP

### 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.*

**Comentário:**

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.*

**Comentário:**

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.*

**Comentário:**

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.*

**Comentário:**

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.*

**Comentário:**

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.*

**Comentário:**

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.*

**Comentário:**

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**

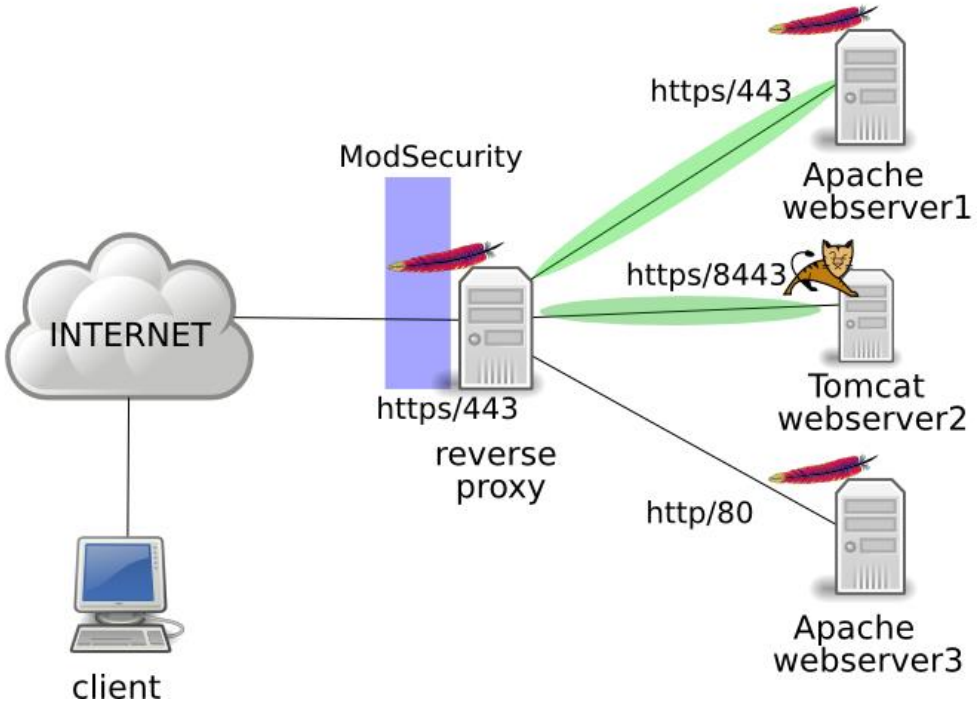
*O ..... recebe os pedidos HTTP na porta configurada e processa todos os pedidos da web que chegam, podendo distribuí-los. Os pedidos de objetos que podem ser armazenados no cache (informações estáticas que não mudam com frequência como páginas em HTML e imagens GIF) são processados pelo proxy. Os pedidos 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.*

## Comentário:

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.*

## Comentário:

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).*

**Comentário:**

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".*

**Comentário:**

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.*

**Comentário:**

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.*

**Comentário:**

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**

---

# LISTA DE EXERCÍCIOS

## HTTP

**1. 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.*

---

**2. 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.*

---

**3. 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*

---

**4. 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.*

---

**5. CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013**

*Um servidor HTTP consiste em um servidor de aplicações.*

---

**6. 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.*

---

**7. 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.*

---

**8. 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.*

---

**9. 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-agente:      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
```

---

**10.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.*

---

**11.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.*

---

**12. 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).*

---

**13. 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.*

---

**14. 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.*

---

**15. 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.*

---

**16. CESPE – TCU/Analista de Controle Externo – TI/2007**

*O protocolo HTTP, definido nas RFCs 1945 e 2616, não permite a utilização de conexões persistentes.*

---

**17. 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.*

---

**18. 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.*

---

**19.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.*

---

**20.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).*

---

**21.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.*

---

**22.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.*

---

**23.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

## GABARITO – QUESTÕES CESPE

| | |
|---|---|
| 1 | C |
| 2 | D |
| 3 | E |
| 4 | C |
| 5 | E |
| 6 | E |
| 7 | C |
| 8 | E |
| 9 | E |
| 10 | E |
| 11 | C |
| 12 | E |
| 13 | C |
| 14 | C |
| 15 | C |
| 16 | E |
| 17 | C |
| 18 | E |
| 19 | C |
| 20 | C |
| 21 | C |
| 22 | C |
| 23 | E |

# LISTA DE EXERCÍCIOS COMPLEMENTARES

## HTTP

**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

## GABARITO – QUESTÕES FCC

| | |
|---|---|
| 1 | A |
| 2 | C |
| 3 | B |
| 4 | D |
| 5 | B |
| 6 | C |
| 7 | A |
| 8 | E |
| 9 | D |
| 10 | D |
| 11 | C |
| 12 | B |
| 13 | A |

# Protocolo DNS (Domain Name System)

Um dos protocolos mais importantes em termos de prova vem sendo cobrado constantemente. Como sabemos, o protocolo DNS (Domain Name System) atua na camada de aplicação e por esse motivo, necessita de uma porta para funcionar. Atua na porta 53, tanto em UDP (consultas simples) quanto em TCP (respostas acima de 512 bytes e transferências de zonas). Veremos com mais detalhes à frente. Importante apenas para registrar que a essência do funcionamento do DNS para seus clientes e interação com os servidores é por meio da UDP/53.

A sua principal função é traduzir nomes de domínio em endereços IP em uma estrutura hierárquica global. Sob a ótica do usuário final, é muito mais fácil aprender endereços com mnemônicos e nomes completos do que sequências de endereços IP.


Ao acessarmos quaisquer endereços na Internet, utilizamos nomes de domínio, como por exemplo, www.gmail.com. Entretanto, para que os computadores sejam capazes de trocar informações, o endereço IP do servidor que responde ao endereço gmail.com deverá ser conhecido e é nesse momento em que o DNS atua.

O cliente deverá então consultar algum servidor DNS na rede para fazer a tradução desse endereço e, após descoberto o endereço IP, a informação será enviada. Vale ressaltar que o procedimento inverso é chamado de Reverse DNS. Veremos com mais detalhes a seguir.

O conjunto de pacotes e softwares DNS padrões de sistemas UNIX é o BIND (Berkeley Internet Name Domain). É o servidor mais utilizado na INTERNET. Atualmente se encontra em sua versão 9 com suporte a requisitos de segurança e IPv6.

Podemos trazer algumas características associadas ao BIND:

1. Flexibilidade: O BIND é altamente flexível e suporta vários tipos de configurações de servidor DNS, incluindo servidores primários, secundários e escravos.

2. Escalabilidade: O BIND é escalável e pode lidar com grandes quantidades de tráfego de consultas ao DNS. Ele também permite a adição de novos registros DNS sem interrupção do serviço.

3. Segurança: O BIND inclui suporte para DNSSEC (Domain Name System Security Extensions), o que o torna mais seguro contra ataques como cache poisoning e redirecionamento de DNS.

4. Configuração simples: O BIND é fácil de configurar e tem uma ampla documentação disponível para ajudar os administradores a configurar o software de acordo com suas necessidades.

5. Larga Adoção: O BIND é amplamente utilizado na Internet e é suportado por vários sistemas operacionais, incluindo Unix, Linux, macOS e Windows.

---

FGV - 2018 - MPE-AL - Analista do Ministério Público - Administrador de Rede

A rede da empresa Kanguroo Tec apresenta problemas com a conexão de uma estação de trabalho aos servidores DNS. Foi identificado que o problema encontrava-se na camada de transporte. Para resolver o problema deve ser verificado se o protocolo de transporte utilizado está correto e se a porta do servidor DNS está aceitando conexões.

O protocolo de transporte e a porta padrão utilizada pelo DNS, são, respectivamente,

A UDP e 50.

B TCP e 25.

C UDP e 443.

D TCP e 22.

E UDP e 53.

Comentários:

Conforme vimos, em que pese haja outras possibilidades de uso com o TCP, mas a essência é na porta UDP/53.

Gabarito: E

FGV - 2021 - Câmara de Aracaju - SE - Técnico de Tecnologia da Informação

Um técnico incumbido da instalação de software nos computadores de uma empresa pediu ao responsável pelos serviços da empresa o endereço do servidor de e-mail corporativo, e lhe foi informado o endereço mail.empresa.com.br. O técnico concluiu a instalação do software e verificou rapidamente que o servidor de e-mail estava localizado no endereço IP 192.168.16.30. A localização do servidor (internet ou intranet) e o recurso utilizado para descobrir o endereço IP a partir daquele informado pelo responsável pelos serviços foram, respectivamente:

A Intranet; ARP;

B Internet; IPX;

C Intranet; DNS;

D Internet; VPN;

E Internet; NAT.

Comentários:

A primeira parte da questão nos traz uma cobrança tradicional do assunto de IP. Lembrando que as faixas privadas contemplam as redes internas ou intranets para uso.

Bom, mas o que nos interessa é a segunda parte da questão, onde se busca descobrir o endereço IP a partir do recurso informado pelo responsável. O que vale destacar nessa questão, é que não há restrição do tipo de recurso. Pois há vários modos de se solicitar o endereço IP. Veremos ainda ao longo dessa aula tais tipos.

Gabarito: C

FGV - 2022 - MPE-GO - Assistente Programador

Uma equipe de suporte de redes foi chamada para resolver um problema de conectividade de um computador que se comunica normalmente com os demais dispositivos da rede, mas falha em navegar na Internet. A equipe verificou, porém, que quando se digita o endereço IP dos sites, a navegação ocorre normalmente. A experiente equipe de suporte de redes concluiu que houve uma desconfiguração no endereço do servidor

A User Datagram Protocol.

B Transmission Control Protocol.

C Windows Internet Name Service.

D Domain Name System.

E Dynamic Host Configuration Protocol.

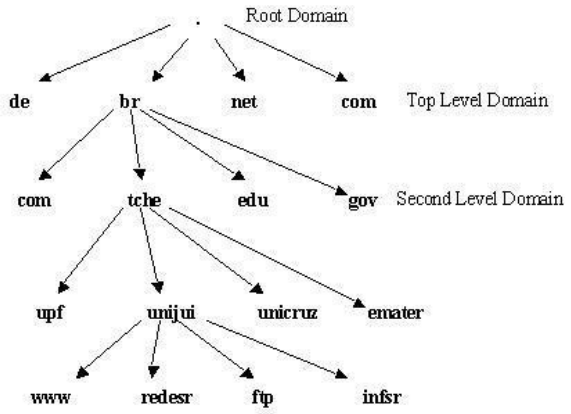
Comentários:

Temos nesse enunciado a descrição clássica de um problema associado ao protocolo DNS. Se o usuário em questão conseguiu acessar e navegar pelo endereço IP, indica-se que não há problema de conectividade, mas sim, de tradução do nome para acesso e recuperação do endereço IP para navegação.

Gabarito: D

## Estrutura e Funcionamento

O DNS, como vimos, possui uma estrutura hierárquica com banco de dados distribuído. A seguir temos um exemplo dessa organização. Reparem que a raiz é identificada a partir da simbologia ".".




Cada nó é conhecido como DOMÍNIO DNS. E naturalmente, pode-se criar subdomínios, desmembrando cada vez mais. A composição de um nome de domínio completo começa a partir do nó mais descentralizado, rumo ao nó de maior raiz. Poderíamos, de acordo com a árvore anterior, ter um nome como: ftp.unijui.tche.br. O nome completo até raiz é conhecido como nome de domínio totalmente qualificado ou fully qualified domain Name (FQDN).

Esse FQDN deve ser único na rede. Portanto, pode-se ter subdomínios iguais desde que pertencentes a domínios superiores distintos, fazendo com que ao considerar o FQDN, este será único.

A estrutura em árvore apresentada é definida pela RFC como DOMAIN NAME SPACE.


A administração desses subdomínios fica por conta de cada responsável e a este cabe a possibilidade de desmembramento. Um exemplo ainda na figura anterior seria a administração do subdomínio UNIJUI criar seus subdomínios internos. Essa estrutura permite uma maior organização, gerência e administração desses ambientes.

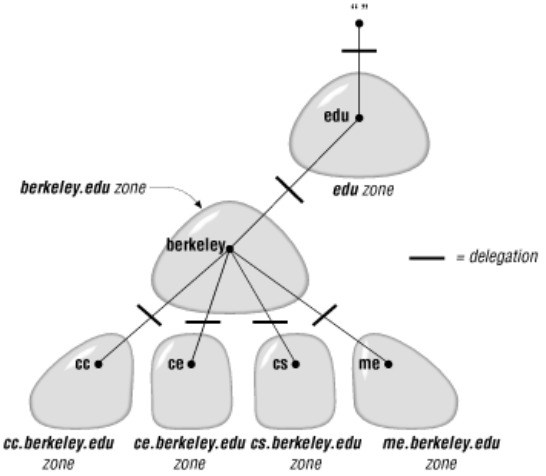
Cada nome na árvore pode ser definido em até 63 caracteres.

Os principais domínios que fazem parte da primeira no espaço de domínios são:

- COM – Organização comercial
- EDU – Organização educacional
- GOV – Organização governamental
- MIL – Organização militar
- NET – Organização da Rede
- ORG – Organização não comercial
- INT – Organização internacional

Dessa forma, podemos definir o conceito de ZONA que nada mais é do que a delegação de autoridade para gerência e controle dos nomes em uma hierarquia inferior a partir de um nó de hierarquia superior.

A imagem a seguir nos traz essa representação:




Esses servidores que detêm a autoridade de forma delegada de suas zonas acabam trocando informações entre si e com seus nós hierarquicamente superiores. Esse procedimento é conhecido como transferência de zonas, a qual ocorre na porta 53/TCP.

Nessa relação, estabelece-se ainda o papel de mestre, que é aquele que detém as informações, e o escravo, aquele que requisita as atualizações de suas zonas. Cabe, portanto, definirmos os

três tipos de mensagens do protocolo DNS: Consultas e Respostas que acontecem do cliente para o servidor, e as atualizações, que acontecem entre servidores.

Nesse contexto, existem duas formas de implementação de transferência de zonas:

- AXFR – Implica em transferência completa ou integral da zona. Nesse sentido, o servidor DNS mestre envia todas as informações conhecidas para que o servidor DNS escravo possua uma base completamente replicada. Gera um custo de banda e processamento muito grande quando comparado ao outro método.
- IXFR – Também conhecido como transferência incremental. Nesse sentido, busca-se atualizar apenas aquelas informações desatualizadas entre os servidores mestre e escravo. Assim, gera-se um menor custo de processamento e de consumo de banda.

Existe ainda o conceito de zona reversa, que são zonas criadas para tratar as consultas que pretendem resolver endereços IP em nomes DNS, isto é, ao contrário da maioria das consultas DNS.

Além disso, temos a zona raiz ou ROOT HINT, que é composta por servidores que estão no topo da hierarquia de resolução de nomes, chamados de raiz, da Internet. Possuem endereços amplamente conhecidos e divulgados a serem cadastrados nos demais servidores de DNS da Internet. Caso os demais servidores não sejam capazes de resolver os nomes requisitados, buscam informações de outros servidores a partir das Zonas Raízes.

Avançando um pouco sobre o DNS, que trazer a vocês os conceitos de servidores primários e secundários.

Conforme Forouzan, trago o excerto abaixo:

> *"O DNS define dois tipos de servidores: primários e secundários.* ***Servidor primário é aquele servidor que controla e armazena o arquivo sobre a zona que detém autoridade.*** *É responsável pela criação, manutenção e atualização do arquivo de zonas.* ***Armazena o arquivo de zonas em um disco local****. Servidor secundário é o que transfere as informações completas sobre uma zona de outro servidor (primário ou secundário) e armazena o arquivo em seu disco local.* ***O servidor secundário não cria nem atualiza os arquivos de zona. Se for necessária a atualização, ela deve ser feita pelo servidor primário, que transmite uma versão atualizada para o secundário.***
>
> *Tanto os servidores primários como os secundários têm autoridade sobre as zonas que atendem. A ideia não é colocar o servidor secundário em um nível de autoridade inferior, mas sim, o de criar redundância para os dados de modo que, se um servidor falhar, o outro poderá continuar a*

*atender às solicitações dos clientes. Note também que um servidor pode ser primário para determinada zona e secundário para outra. Consequentemente, quando nos referimos a um servidor como um servidor primário ou secundário, devemos ser cautelosos a qual zona nos referimos.*

FGV - 2018 - MPE-AL - Analista do Ministério Público - Administrador de Rede

O Bind é um software Open Source que implementa o serviço de DNS.

Considerando a implementação de um DNS autoritativo, com Bind a partir da versão 9 (estável e superiores), assinale a afirmativa correta.

A O servidor DNS, que opera como primário para algumas zonas, não pode operar como secundário para outras zonas.

B O servidor DNS secundário é o local onde é mantida a cópia principal de uma zona.

C O servidor DNS não pode operar como recursivo para um grupo de clientes locais.

D O servidor DNS primário precisa ter dois ou mais servidores secundários para realizar a tradução reversa.

E O servidor DNS secundário recebe o conteúdo de uma zona de outro servidor, por meio de um processo de sincronização.

Comentários:

Em que pese a questão traga os conceitos associado ao BIND em seu enunciado, mas temos que as características básicas são do próprio DNS.

Vamos aos itens:

a) É possível ele atuar como primário e secundário, normalmente, a depender das zonas. INCORRETO

b) O erro está em dizer que o DNS secundário armazena a cópia principal da zona, em vez de ser a réplica. INCORRETO

c) Não há qualquer restrição quanto à sua configuração dos modos recursivo ou interativo. Veremos esse conceito mais à frente. INCORRETO

d) Não há essa vinculação. Como fora destacado inclusive pelo Forouzan, trata-se de um recurso de redundância, e organização das zonas. INCORRETO

e) Exatamente pessoal. Esse é o termo mais adequado para o processo. CORRETO

Gabarito: E

## Tipos de Consulta

Antes de definirmos os tipos de consulta, definiremos o papel do "*resolver*, que nada mais do que a aplicação responsável por efetuar tradução do nome, de fato! Essa aplicação pode estar separada ou em conjunto com o cliente.


Em termos das possíveis respostas às consultas, definiremos as 4 principais:

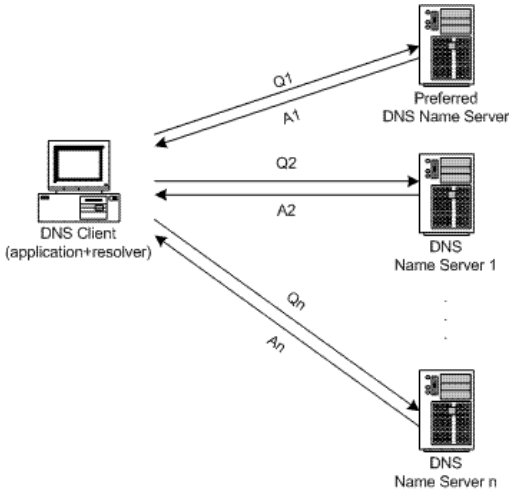
| | |
|---|---|
| Autoritária (authoritative) | É uma característica da resposta positiva com o diferencial de que a resposta foi obtida diretamente de um servidor responsável por uma zona, ou seja, é um servidor autoritário. Esses servidores fazer parte de uma zona primária. |
| Positiva | Resposta com a informação requisitada na consulta proveniente de qualquer nameserver. Os servidores que emitem respostas positivas fazer parte de zonas secundárias. |
| Referencial | Condição em que o servidor requisitado não possua uma resposta positiva e dessa forma, informa-se novos servidores que podem contribuir na resolução de nomes em questão. |
| Negativa | Ocorre sempre quando a consulta chega a um servidor autoritário sobre determinado domínio e este não possui a resposta. Pode-se apontar o motivo de registro inexistente ou o tipo utilizado não condiz com o nome do registro. |

O protocolo DNS possui dois grandes métodos de consulta: Recursivo e Iterativo.

- Iterativo – O cliente que deseja resolver determinado nome encaminha sua requisição ao elemento *resolver*. O *resolver* então começa a atuar para resolver (agora do verbo em português) o nome requisitado. Caso o servidor DNS possua a resposta, seja como autoridade, seja em cache, haverá uma resposta direta. O cache armazena as informações mais recentes obtidas de consultas recentes.

Caso desconheça o nome de registro, o servidor encaminhará ao "*resolver*" a sua melhor resposta como referência para uma nova requisição. Caso este novo servidor não possua a resposta, será informado novamente a melhor resposta de referência possível para uma nova consulta a outro servidor.

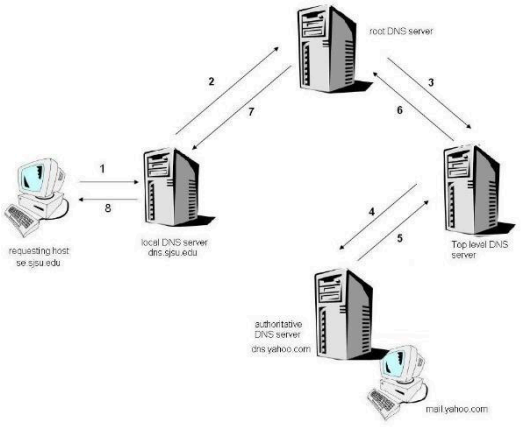
Esse procedimento continua até que o "*resolver*" seja capaz de traduzir o nome de registro em questão. A figura abaixo representa esse modelo:




- Recursiva – Método mais utilizado na Internet. Sob a ótica do cliente e "*resolver*", esses realizam apenas uma consulta. Caso o servidor preferencial não saiba responder à consulta, ele se responsabilizará em repassar a consulta a outros servidores DNS, ou seja, ele passa a funcionar como cliente até a obtenção de uma resposta.

Novos servidores também podem repassar as suas consultas adiante até que seja obtida a resposta em algum servidor DNS na Internet e assim, as respostas são dadas até que chegue ao "*resolver*". Vale ressaltar que a resolução de nomes nesse modelo acontece da direita para esquerda a partir dos Root Hints da Internet.

Existem 13 Root Hints que nada mais são do que servidores autoritários sobre o "root domain".




Trazendo uma analogia básica para os dois modelos isolados, para facilitar o entendimento, vamos criar o cenário que você precisa enviar um email para o reitor de uma universidade.

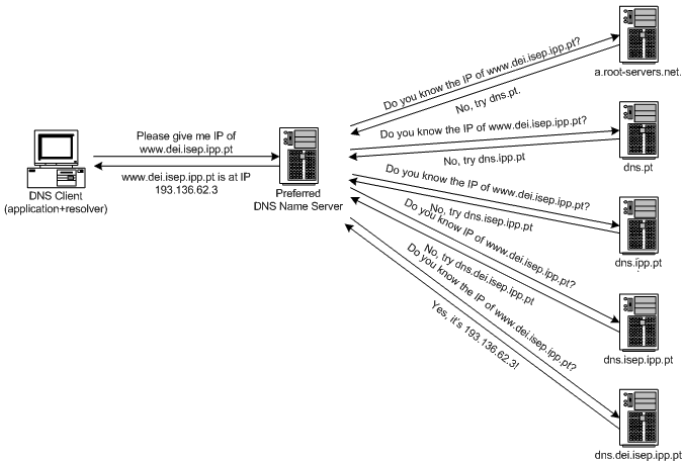
Assim, o seu ponto de contato seria o seu orientador. Nesse cenário, você vai fazer a seguinte pergunta para o orientador...

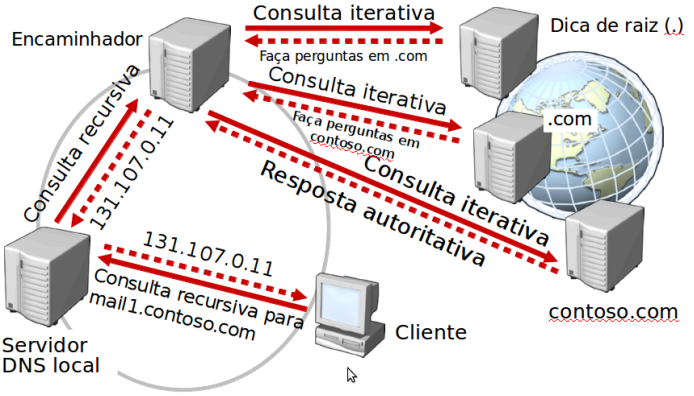
"Preciso enviar um email para o reitor. Sabe o email dele?"

Assim, o seu orientador poderá atuar de duas formas.

1. Modo Iterativo – "Eu não sei. Mas a melhor informação que eu tenho é que a Secretária do departamento saiba". Assim, você irá agora perguntar para a Secretária e ela te informará o email.
2. Modo Recursivo – "Eu não sei. Aguarde um instante". Em seguida, o orientador ligará para a Secretária e pegará o email do reitor. Finalmente ele retorna a informação. "Segue o email do reitor".

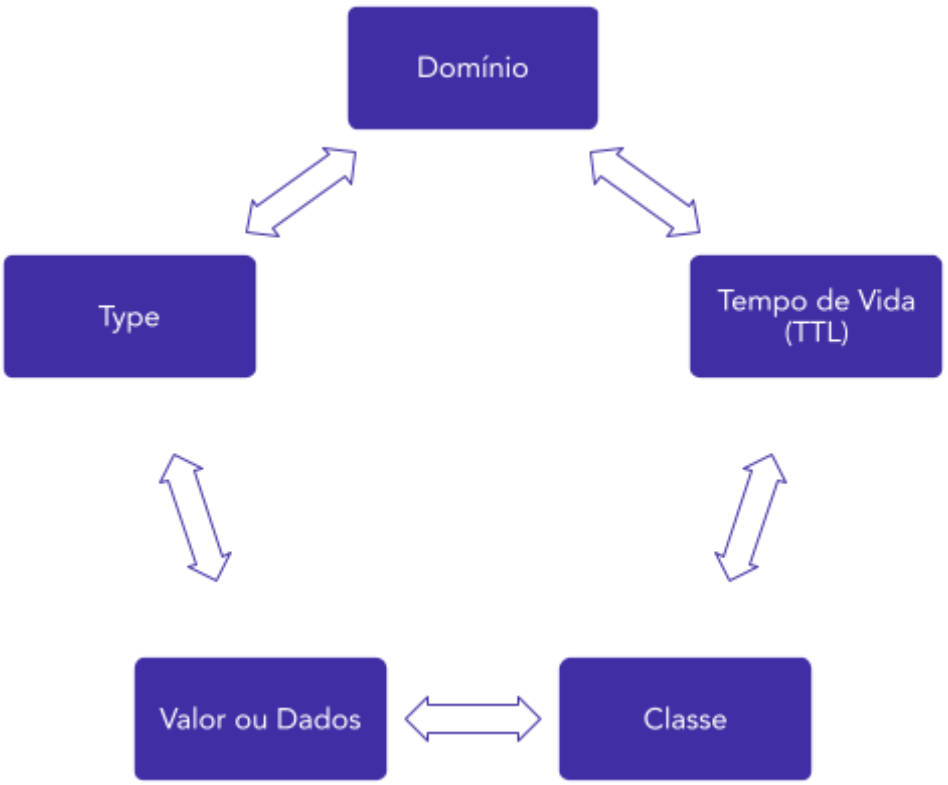
A seguir, temos duas possíveis representações de modelos híbridos, que utilizam parte inicial no modelo RECURSIVO e a parte final de tratamento entre os servidores de modo ITERATIVO:




## Campos DNS

As respostas às requisições DNS possuem diversos campos, os quais listo abaixo:




Domínio - É o nome de domínio usado na pesquisa. Possui o mesmo padrão e formato utilizado na requisição.

Tempo de Vida (TTL) - Em alguns tipos de registro, este campo é opcional. Ele determinará por quanto tempo o registro ficará armazenado no cache dos servidores, após uma consulta realizada. Quando este tempo é zerado o registro é descartado. Quando há uma nova consulta, há a restauração do valor ou atualização para um novo valor fornecido. Pode ser usado com tempos variados conforme quão estável é a informação oferecida.

Classe - Contém um texto indicativo da classe do registro. É um campo obrigatório. Como a maioria absoluta de requisições são provenientes da INTERNET, este campo na sua maioria das vezes estará com a informação IN. O Windows Server 2000 só aceita este tipo de classe.

Valor ou Dados - Contém a informação propriamente dita formatada de acordo com o tipo. Pode-se utilizar formatação ASCII.

Type - Possui um texto que indica o tipo de registro e consequentemente o tipo de serviço DNS oferecido.

A estrutura do cabeçalho de requisição e resposta seguem o mesmo padrão, com um tamanho de 12 bytes. Os dois últimos bytes são utilizados para definir a quantidade de informações adicionais.

## Serviços DNS

Apesar de na maioria das vezes o DNS ser usado conforme apresentado no início dessa sessão, ele também possui outros tipos de serviços de tradução de nomes em recursos específicos na rede. Os principais tipos de recursos são apresentados abaixo com a sua respectiva representação:


- A – Address IPv4 – Quando um cliente usa esse tipo de registro, o objetivo é descobrir o endereço IPv4 que responde por determinado nome de domínio;
- AAAA – Address IPv6 - Quando um cliente usa esse tipo de registro, o objetivo é descobrir o endereço IPv6 que responde por determinado nome de domínio;
- CNAME (Canonical Name) - Faz o mapeamento de um alias (apelido) ou um DNS alternativo.
- ALIAS - Funciona como um CNAME, mas pode ser usado na raiz do domínio. Comuns em serviços de DNS gerenciado.
- DNAME (Delegation Name) - Aponta um domínio e todos os seus subdomínios para outro domínio.
- PTR – Pointer – Realiza o caminho inverso. A partir de um endereço IPv4, deseja-se obter o respectivo nome de domínio;
- NS – Nameserver – Especifica o nome do servidor DNS responsável por determinado domínio;
- MX – Mail Exchange – Fornece o nome do servidor de e-mail de maior prioridade que responde por determinado domínio de e-mail. Após a obtenção desse nome, é preciso ainda realizar uma consulta do tipo *address* para se determinar o endereço IP;
- SRV – Service – Permite definir serviços disponíveis em um domínio. Especifica informações sobre serviços disponíveis no domínio, como servidores SIP ou LDAP.

- SOA (Start of Authority): Contém informações sobre o domínio, como o servidor de nomes autoritativo, o administrador, e parâmetros de controle de cache.

- CAA (Certification Authority Authorization): Especifica quais autoridades de certificação podem emitir certificados para um domínio.

- CERT (Certificate): Armazena certificados para o domínio, normalmente usados em operações de segurança.

- SPF (Sender Policy Framework): Define quais servidores de e-mail estão autorizados a enviar e-mails em nome do domínio.

- TXT (Text): Armazena texto arbitrário, frequentemente usado para verificação de domínio e informações SPF.

Essas identificações serão fornecidas no campo TYPE da estrutura de resposta DNS.

Algumas questões têm cobrado também as características dos registros dos servidores autoritativos, ou seja, o primeiro registro para determinado nome em uma zona DNS e seu responsável. Esse registro é conhecido como SOA (Start Authority), sendo, portanto, a melhor fonte de informações para o referido nome de domínio.

Nesse registro, tem-se as seguintes informações:


Host de Origem - Endereço do host em que o arquivo foi criado.

Email de Contato – Endereço de e-mail da pessoa ou organização responsável pelo arquivo de zona.

Número de Série – Número de revisão do arquivo de zona. É incrementado toda vez que o arquivo de zona é alterado. Tal funcionalidade é importante para que as alterações possam ser distribuídas aos servidores secundários, utilizando como parâmetro de verificação se a informação está atualizada ou não por parte dos outros servidores.

Intervalo de Atualização – Tempo em segundos que o servidor secundário deve esperar até realizar nova consulta ao registro SOA no servidor primário. Geralmente o valor padrão é igual a 3600.

Intervalo entre Tentativas – Tempo de espera por parte do servidor secundário em caso de falha na transferência de zona. Normalmente o tempo de tentativa é menor do que o tempo de atualização, sendo como padrão igual a 600.

TTL mínimo – O valor do tempo de vida mínimo se aplica a todos os registros de recursos no arquivo de zona. Esse valor é fornecido em respostas de consulta para informar a outros servidores quanto tempo eles devem manter os dados no cache. O valor padrão é 3600.

A imagem a seguir nos traz uma representação desses campos em um servidor Windows:


Como todo bom serviço de rede, existem alguns comandos que são utilizados para resolução de problemas (troubleshooting) ou verificação de configuração. Entre eles, podemos citar o próprio *ipconfig* e o *nslookup* de ambientes Windows.

O *nslookup* é utilizado para obter informações no todo ou em parte de um servidor DNS. Após a inserção do comando, pode-se complementar com diversos outros comandos e recursos e busca de informações específicas.

HORA DE PRATICAR!

FGV - 2022 - TJ-DFT - Analista Judiciário - Suporte em Tecnologia da Informação

Andréa administra o DNS (Domain Name System) do órgão onde trabalha e precisa gerenciar vários registros de domínio para um endereço único de domínio.

De forma a permitir esse tipo de apontamento, Andréa configurou um registro CNAME, apontando-o para o:

A nome real do hospedeiro;

B endereço IP do hospedeiro;

C endereço IP do servidor DNS autoritativo daquele registro;

D nome do cliente DNS utilizado na consulta;

E nome do servidor DNS autoritativo daquele registro.

Comentários:

O CNAME criado é utilizado para criar um alias ou um nome alternativo. Agora, obviamente, a sua referência e apontamento precisa indicar para o nome real do hospedeiro, para manter esse relacionamento.

Gabarito: A

(CESPE - ANATEL/Engenharia/2014) O DNS (domain name system) é uma base de dados distribuída, armazenada em uma hierarquia de servidores, responsável pela tradução de identificadores mnemônicos de hosts, como, por exemplo, cespe.unb.br, para endereços IP, já que estes são necessários para os roteadores encaminharem corretamente os pacotes.

Comentários:

Questão certinha, não é pessoal? Os roteadores e dispositivos precisam conhecer endereços IP para envio e roteamento dos pacotes. Dessa forma, o DNS traduz os nomes de registro em endereços IP.

Gabarito: C

## DNSSEC (Domain Name System Security Extensions)

Vimos diversos aspectos do DNS. Um ponto muito importante é sempre o fator segurança. E nesse contexto foi criada a extensão DNSSEC.

Trata-se de uma tecnologia de segurança para o sistema de nomes de domínio (DNS) que ajuda a proteger contra ataques de envenenamento de cache DNS. O ataque de envenenamento de cache DNS é uma técnica usada por hackers para alterar as informações armazenadas em um servidor DNS. Isso pode levar a respostas falsas que direcionam os usuários para sites maliciosos ou roubam informações pessoais. Percebam o nível de exposição e vulnerabilidade que os usuários ficam, pois, mesmo inserindo uma URL correta no browser, pode haver o desvio pelo processo de resolução de DNS.

O DNSSEC adiciona uma camada de autenticação e integridade aos registros DNS, permitindo que os usuários confiem nas respostas que recebem quando fazem uma consulta DNS.

Os principais recursos do DNSSEC incluem:

1. Assinatura Digital de recursos: O DNSSEC adiciona uma camada de segurança ao assinar digitalmente as informações DNS, garantindo que os dados não foram alterados ou manipulados. Cada registro DNS é assinado digitalmente com uma chave privada e a assinatura é verificada com a chave pública correspondente antes de ser usada. São os princípios garantidos pela assinatura digital. Todo processo de assinatura digital é baseado em Infraestrutura de Chaves públicas e privadas, onde o DNSSEC usa chaves públicas e privadas para assinar e verificar as assinaturas digitais. As chaves são geradas por uma autoridade de registro (RA) e distribuídas aos servidores DNS.

2. Verificação de recursos: Quando um cliente faz uma solicitação DNS, o DNSSEC verifica a assinatura digital para garantir que a resposta seja autêntica e não tenha sido adulterada.

3. Cadeia de confiança: O DNSSEC usa uma cadeia de confiança, semelhante ao SSL, que permite verificar a autenticidade da assinatura digital em uma resposta DNS. Também conhecido como Validação de Origem, garantindo que ele tenha sido gerado por uma fonte confiável.

4. Melhor resolução de nomes: O DNSSEC também ajuda a melhorar a resolução de nomes, pois impede que os usuários sejam direcionados para sites falsos ou maliciosos que possam roubar informações pessoais ou instalar malware em seus computadores.

5. Assinatura de zona: O DNSSEC permite que os administradores de DNS assinem digitalmente zonas inteiras em vez de registros individuais, tornando o processo de gerenciamento de segurança mais eficiente. Também referenciado por Respostas Autoritativas, em que o DNSSEC usa respostas autoritativas para garantir que uma consulta ao DNS retorna uma resposta confiável. As respostas autoritativas são retornadas pelo servidor DNS autoritativo para o domínio em questão.

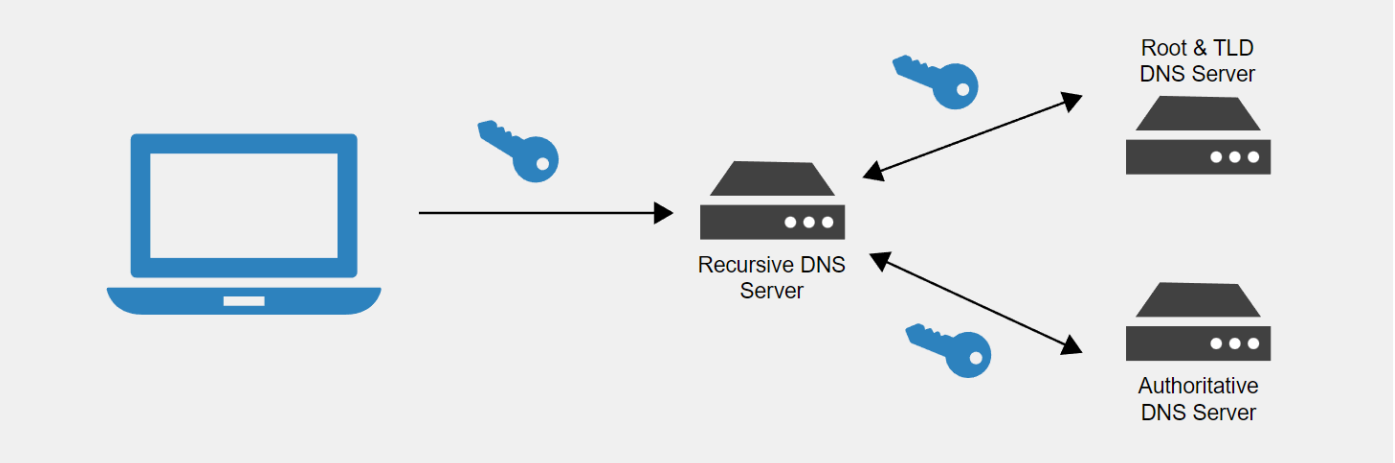
Em resumo, o DNSSEC ajuda a proteger contra ataques de envenenamento de cache DNS, garantindo que os usuários recebam respostas autênticas e protegendo suas informações pessoais e dispositivos contra malwares e outras ameaças.

O DNSSEC utiliza várias mensagens para garantir a autenticidade e integridade das informações DNS. Alguns dos principais tipos de mensagens do DNSSEC incluem:

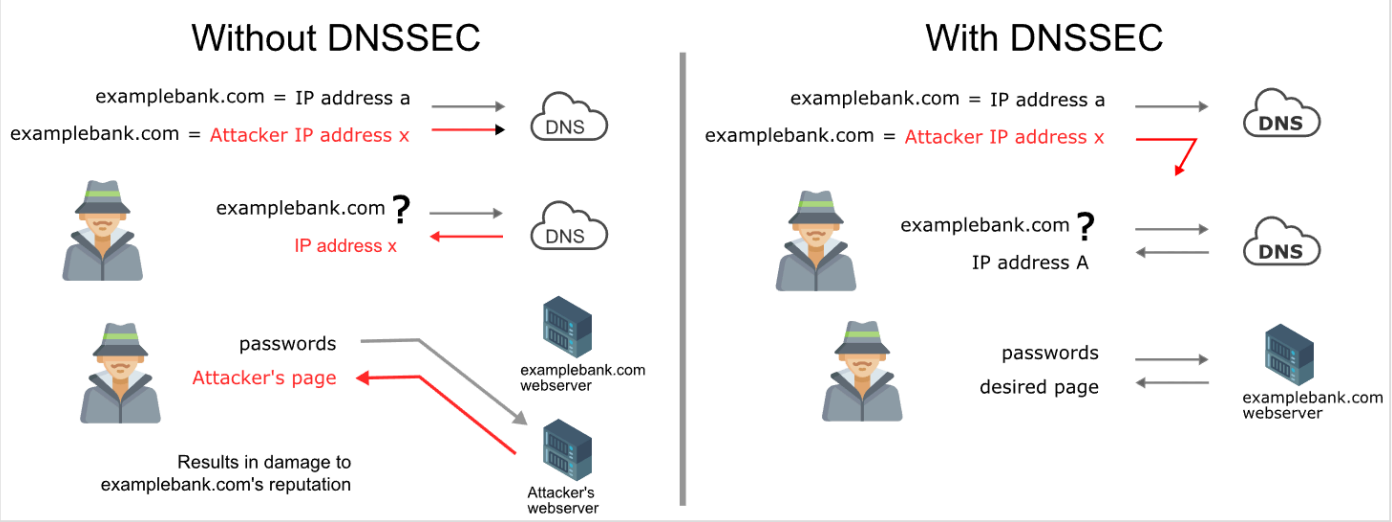
a) Query: é uma mensagem enviada pelo cliente para um servidor DNS, solicitando informações sobre um determinado nome de domínio.
b) Response: é a mensagem de resposta do servidor DNS ao cliente que contém as informações solicitadas. No DNSSEC, a resposta é assinada digitalmente para garantir a autenticidade e integridade das informações.
c) RRSIG: é uma mensagem que contém a assinatura digital dos registros DNS associados a um nome de domínio. Ela é usada para verificar a autenticidade das informações DNS.
d) KEY: é uma mensagem que contém a chave pública usada para verificar a assinatura digital em um registro RRSIG.
e) DS: é uma mensagem usada para distribuir a chave pública de um servidor de nome DNS para um servidor pai. Ela é usada para estabelecer uma cadeia de confiança na autenticidade das informações DNS.

f) NSEC/NSEC3: são mensagens usadas para proteger contra ataques de falsificação de nomes de domínio. Elas são usadas para provar que um nome de domínio não existe no DNS.

Abaixo, temos algumas imagens que representam esse processo de troca de chaves entre os clientes e os servidores de resolução de nomes.




Nesta segunda imagem, temos uma representação bem simplista, basicamente do processo com e sem DNSEC:




Ainda, quero trazer para vocês a visibilidade do conceito dos RRSET's. O primeiro passo para proteger uma zona com DNSSEC é agrupar todos os registros de mesmo tipo em um conjunto de registros de recursos (RRSet). Por exemplo, se você tivesse três registros AAAA em sua zona no mesmo rótulo (por exemplo, rótulo.example.com), todos seriam agrupados em um único RRSet AAAA.

Recomendo fortemente a leitura deste artigo que explicada detalhadamente muitos parâmetros e informações do DNSSEC:

https://www.cloudflare.com/pt-br/dns/dnssec/how-dnssec-works/

FGV - 2018 - Banestes - Analista em Tecnologia da Informação - Suporte e Infraestrutura

Para implementar uma resolução de nomes mais segura, foi desenvolvido o padrão DNSSEC.

Basicamente ele serve para:

A assinar digitalmente os registros DNS, o que permite fornecer proteção completa contra ataques do tipo DoS;

B permitir um acesso seguro a consultas DNS, através de criptografia simétrica;

C permitir uma assinatura na transferência de zonas entre servidores DNS primários e secundários;

D garantir a confidencialidade do conjunto de registros de recursos, o Resource Record Set (RRset);

E evitar que dados de DNS sejam forjados ou manipulados, porém sem fornecer confidencialidade, pois as respostas DNSSEC são autenticadas, mas não criptografadas.

Comentário:

Vamos aos itens, pessoal:

a) De fato, ele permite as assinaturas digitais. Entretanto, o seu propósito não é a disponibilidade frente a ataques de DOS, mas sim a autenticidade e integridade para ataques do tipo cache poisoning. INCORRETO

b) A criptografia utilizada é a assimétrica, e não a simétrica. E, de fato, é para permitir um acesso seguro às consultas. INCORRETO

c) Seu foco não é no processo de replicação de zonas. INCORRETO

d) Não se trata do princípio da confidencialidade, muito menos de criptografia específica pra essa finalidade. INCORRETO

e) Na linha do que comentamos em todos os itens anteriores. CORRETO

Gabarito: E

FGV - 2024 - CVM - Infraestrutura e Segurança em TI

Após uma determinada rede receber ataques de DNS spoofing, foi sugerida a implantação do DNSsec. Acerca desse assunto, é correto afirmar que:

(A) sigilo é um serviço oferecido, pois todas as informações no DNS são consideradas privadas;

(B) o DNSsec também admite alguns tipos de registros. O registro CERT pode ser usado para armazenar certificados;

(C) DNSsec oferece três serviços, que são a prova onde os dados se originaram, distribuição de chave privada e autenticação de transação e solicitação;

(D) o segundo entre os novos tipos de registros é o registro SIG. Ele contém o hash assinado de acordo com o algoritmo especificado no registro ALG;

(E) os registros DNS são agrupados, em conjuntos chamados RRreg, com todos aqueles que têm o mesmo nome e o mesmo tipo.

Comentários:

Vamos aos itens:

a) DNSsec não oferece sigilo, mas sim integridade e autenticidade dos dados. As informações no DNS ainda são públicas. INCORRETO.

b) Conforme vimos na seção dos registros. CORRETO

c) DNSsec oferece prova da origem dos dados e integridade, mas não trata da distribuição de chave privada diretamente. A autenticação de transação e solicitação também não é um serviço direto do DNSsec. INCORRETO

d) O correto seria RRSIG. INCORRETO

e) O correto seria RRSET. INCORRETO

Gabarito: B

FGV - 2024 - CVM - Infraestrutura e Segurança em TI

Analise os registros a seguir.

cvm.com 86400 IN A 35.1.4.5

cvm.com 86400 IN KEY 36367503A8B848F527225B7EF...

cvm.com 86400 IN SIG 86947503A8B848F527225850C6...

Em relação a esses registros, é correto afirmar que o:

(A) registro KEY é a chave privada de cvm;

(B) registro do tipo A contém um endereço IPv4 ou IPv6;

(C) registro SIG contém o hash assinado do servidor *com* de nível superior dos registros A e KEY;

(D) tempo de vida fornece uma indicação de estabilidade do registro, que, no caso acima, é de 60 dias;

(E) tempo de vida fornece uma indicação de estabilidade do registro, que, no caso acima, é de 60 horas.

Comentários:

Vamos aos itens:

a) O mais correto seria DNSKEY, e este armazena a chave pública e não a privada. INCORRETO.

b) O registro do tipo A contém um endereço IPv4. Para IPv6, seria um registro AAAA.. INCORRETO

c) O mais adequado seria RRSIG. Mas como vocês viram, também é referenciado meramente como SIG. CORRETO

d) O tempo de vida (TTL) de 86400 segundos é de 24 horas, não 60 dias.. INCORRETO

e) Mesma da anterior. INCORRETO

Gabarito: C

*Referências:*

1. *Kurose - Redes de Computadores e a Internet - Uma abordagem Top Down - 6ª Edição - Oficial*
2. *Tanenbaum - Redes de Computadores - 5ª Edição*
3. *Forouzan - Comunicação de Dados e Redes de Computadores 4ª Edição*
4. *teleco.com.br*
5. *https://cert.br/*
6. *gta.ufrj.br*
7. https://www.cloudflare.com/pt-br/dns/dnssec/how-dnssec-works/

# QUESTÕES COMENTADAS – DNS - CESPE

1. CEBRASPE (CESPE) - AIS (EMPREL)/EMPREL/Redes/2023

O registro DNS que aponta um nome de domínio (um alias) para outro domínio é do tipo

a) AAAA.

b) NS.

c) CNAME.

d) MX.

e) PTR.

Comentários:

Vimos os diversos tipos de registros que se traduzem em serviços por parte do DNS. Lembrando:

Registro AAAA: usado para mapear um nome de domínio para um endereço IPv6.

Registro NS: usado para mapear um nome de domínio para seus servidores de nomes.

Registro CNAME: usado para mapear um nome de domínio (um alias) para outro domínio.

Registro MX: usado para mapear um nome de domínio para seus servidores de e-mail.

Registro PTR: usado para mapear um endereço IP para um nome de domínio, em um processo reverso ao mais comum.

No contexto do CNAME, por exemplo, se você possui o nome de domínio www.exemplo.com e deseja que ele aponte para www.exemplo.net, você criaria um registro CNAME com o seguinte valor:

www.exemplo.com CNAME www.exemplo.net

Gabarito: C

2. CEBRASPE (CESPE) - Per Crim (POLC AL)/POLC AL/Análise de Sistemas, Ciências da Computação, Informática. Processamento de Dados ou Sistemas da Informação/2023

O DNS (domain naming system) utiliza um esquema hierárquico de atribuição de nomes com base no domínio e um sistema de bancos de dados distribuídos para mapear nomes de hosts em endereços IP.

Comentários:

Vimos vários exemplos de composição de nomes de domínio em nossa teoria, mantendo o modelo hierárquico de nomenclatura e responsabilidade sobre os domínios.

Vimos também que essa estrutura mundial é mantida de forma distribuída entre vários servidores.

Gabarito: Certo

3. CESPE / CEBRASPE - 2022 - TCE-SC - Auditor Fiscal de Controle Externo - Ciência da Computação

Cabe ao CGIbr estabelecer diretrizes na execução do registro de nomes de domínio, bem como na alocação de endereço IP.

Comentários:

Essas são, sem dúvida, competências do CGI.br. Lembrando que sua operacionalização e subsídio técnico acontece pelo NIC.Br, que está vinculado ao CGI.BR.

Gabarito: B

4. CESPE / CEBRASPE - 2022 - TCE-SC - Auditor Fiscal de Controle Externo - Ciência da Computação

É prevista a participação de representantes da comunidade científica e tecnológica no Comitê Gestor da Internet (CGI.BR), entre cujas atribuições e responsabilidades se inclui o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil.

Comentários:

Questão bem específica, que nos leva a trazer o conteúdo de forma pontual. Vejam que no próprio SIte do CGI.BR, temos:

https://www.cgi.br/membros/


Gabarito: C

5. (CESPE – TCE-PR/Analista de Controle – Área TI/2016) Uma consulta DNS inicial típica, originada de uma máquina de usuário e encaminhada ao servidor de nomes local para um nome de domínio externo não armazenado em cache DNS, será do tipo

A) raiz.

B) domínio de alto nível.

C) iterativa.

D) recursiva.

E) direta.

Comentários:

Pessoal, vimos que o modo típico utilizado é o recursivo, ok?

Gabarito: D

6. (CESPE - ANCINE/Área II/2013) O DNS (domain name system) está relacionado a esquema hierárquico de atribuição de nomes embasado no domínio de um sistema de banco de dados distribuído para implementar esse esquema de nomenclatura.

Comentários:

Questão bem tranquila com um resumo bem objetivo do protocolo DNS.

Gabarito: C

7. (CESPE - ANATEL/Arquitetura de Soluções de Tecnologia da Informação e Comunicação/2014) O DNS (domain name system) organiza o espaço de nomes em uma estrutura hierárquica que permite descentralizar as responsabilidades envolvidas na atribuição de nomes, podendo usar os serviços do UDP ou TCP por meio da porta-padrão 53.

Comentários:

Perfeito né pessoal. A descentralização pode ser feita através da criação de zonas. Além disso, utiliza-se o UDP para consultas simples e comuns e utiliza-se o TCP para respostas com mais de 512 bytes ou transferência de zonas.

Gabarito: C

8. (CESPE - ANATEL/Suporte e Infraestrutura de Tecnologia da Informação/2014) Em uma zona DNS, ao se utilizar o registro de recurso do tipo MX, informa-se o registro reverso de nome para endereço IP.

Comentários:

Pessoal, vimos que o tipo MX é para resolução de nomes de email. O tipo para registro reverso é o PTR.

Gabarito: E

9. (CESPE - ANATEL/Engenharia/2014) O DNS (domain name system) é uma base de dados distribuída, armazenada em uma hierarquia de servidores, responsável pela tradução de identificadores mnemônicos de hosts, como, por exemplo, cespe.unb.br, para endereços IP, já que estes são necessários para os roteadores encaminharem corretamente os pacotes.

Comentários:

Questão certinha, não é pessoal? Os roteadores e dispositivos precisam conhecer endereços IP para envio e roteamento dos pacotes. Dessa forma, o DNS traduz os nomes de registro em endereços IP.

Gabarito: C

10. (CESPE – TRE-RJ/Técnico Judiciário/2012) A resolução do nome www.google.com.br para o endereço IP 74.125.234.120 é realizada pelo protocolo de navegação HTTP.

Comentários:

Esse é um tipo de resolução DNS da forma direta, ou seja, de um nome para um endereço IP. Não há o que se falar de HTTP.

Gabarito: E

11. (CESPE – TRE-RJ/Técnico Judiciário/2012) Suponha que, após a execução do comando ping 127.0.0.1, seja apresentada como reposta que o tempo limite do pedido tenha se esgotado. Nessa situação, é correto afirmar que houve falha de DNS e, para solucionar o problema, deve-se executar o comando ipconfig /flushdns.

Comentários:

O comando flushdns server para limpar a tabela de registros e mapeamento de endereços IP e nomes no host. Entretanto, a questão só aborda o comando ping em um endereço IP já definido, ou seja, não há necessidade de tradução de nome em endereço IP, independendo, portanto, do serviço DNS.

Gabarito: E

12. (CESPE – Câmara dos Deputados/Analista – Engenharia Eletrônica/2012) O sistema de DNS caracteriza-se por um banco de dados distribuído de registros de recursos (RRs — resource records), no qual cada registro de recurso possui um campo de TTL (time to livE) que indica o tempo que a entrada deve ser mantida no servidor de nomes autoritativos antes de sua exclusão.

Comentários:

Exclusão nos servidores de nomes autoritativos não né pessoa? O campo TTL indica o prazo de validade do registro armazenado em cache, ou seja, em servidores não autoritativos para aquela mensagem.

Gabarito: E

13. (CESPE - Ana MPU/Tecnologia da Informação e Comunicação/Suporte e Infraestrutura/2013) O DNS utiliza o UDP em consultas, mas não em transferências de zona. Para esta operação, é utilizado o TCP.

Comentários:

Para consolidarmos o que vimos. Lembremos que ambos ocorrem na porta 53, mudando apenas o protocolo da camada de transporte.

Gabarito: C

14. (CESPE - TJ STF/Apoio Especializado/Tecnologia da Informação/2013) Na aplicação DNS (Domain Name System), o UDP fornece controle preciso dos fluxos de pacotes, erros ou sincronização.

Comentários:

Pessoal, discordo do gabarito da Banca pois o protocolo da camada de transporte que fornece controle preciso dos fluxos de pacotes, erros ou sincronização é o TCP, orientado à conexão.

Gabarito: C (Gabarito Professor: E)

15. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013)

```
C:\>nslookup
Servidor Padrão: UnKnown
Address: 192.168.1.1
> set type=ptr
> www.google.com
Servidor: UnKnown
Address: 192.168.1.1

google.com

primary name server = ns1.google.com
responsible mail addr = dns-admin.google.com
serial = 1507969
refresh = 7200 (2 hours)
retry = 1800 (30 mins)
expire = 1209600 (14 days)
default TTL = 300 (5 mins)

>
```

Com base no trecho de código acima, que se refere a uma consulta realizada na Internet, julgue o item que se segue.

Não há indício de que a consulta realizada tenha retornado o endereço de ponteiro do domínio www.google.com.

Comentários:

Pessoal, como vimos, o nslookup é um comando para verificar informações de um servidor, podendo inclusive realizar consultas parciais. Na questão, definiu-se o tipo de consulta para DNS reverso através do set type=ptr.

Entretanto, como vimos, nas consultas reversas, fornece-se um endereço IP para se obter o nome de registro. Entretanto, no código da questão foi fornecido a url www.google.com, obtendo apenas informações a respeito desse servidor como nameserver e email administrativo, porém, não obtivemos a resposta do nome de registro.

Gabarito: C

16. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) Com base no trecho de código acima da questão anterior, que se refere a uma consulta realizada na Internet, julgue o item que se segue.
O TTL correspondente a 300 foi o tempo que a consulta levou para ser armazenada, em cache, no roteador que gerou a última rota do pacote.

Comentários:

Pessoal, vimos que o campo TTL diz respeito ao prazo de validade da informação obtida. Essa regra se aplica aos servidores secundários que obtiveram essas respostas para armazenamento em cache. Além disso, não há o que se falar de roteador, mas sim, servidores DNS e consultas realizadas.

Gabarito: E

17. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O endereço 192.168.1.1 refere-se a um servidor DNS que não é do tipo autoritativo do domínio consultado.

Comentários:

Vimos que o servidor que respondeu diretamente ao cliente foi o endereço 192.168.1.1 .Esse endereço pertence a um servidor DNS da rede local inclusive sem nome de servidor DNS mapeado (unknown), o que já nos leva a excluir a possibilidade deste ser autoritativo. Além disso, vemos que o nome do servidor primário que é o servidor autoritativo corresponde a ns1.google.com, sendo um dos servidores autoritativos para o endereço www.google.com.

Gabarito: C

18. (CESPE - TJ STF/Analista Judiciário/2013) Considerando que uma organização possua uma intranet com servidor web e servidor de correio eletrônico, julgue o item a seguir.

Tanto no caso do servidor web como no do servidor de correio eletrônico, é necessário haver um serviço DNS para converter nomes em endereços IPs.

Comentários:

Pessoal, questão bem complicada. Na prática, todos os servidores WEB e de correio eletrônico são conhecidos pelos hosts e mapeados com registros de nome e para tanto, necessitam de servidores DNS para resolução dos nomes. Entretanto, eles podem ser acessados diretamente via endereçamento IP, independendo, portanto, de servidores DNS.

Gabarito: C (gabarito professor: E)

19. (CESPE – Telebrás/Especialista em Gestão de Telecomunicações – Analista em TI/2013) Quando um usuário, em sua estação de trabalho, tenta acessar o sítio da Web representado pelo endereço www.xyz.com.br, que está associado a um endereço IP na Internet, o acesso será conseguido em razão de o serviço DNS fazer resoluções diretas de nomes para o endereço IP.

Comentários:

Bem tranquilo não é pessoal? A característica da resolução direta diz respeito ao sentido normal da tradução, ou seja, de um nome DNS para um endereço IP. A indireta é o que conhecemos como resolução reversa, ou seja, de um endereço IP para um nome DNS.

Gabarito: C

20. (CESPE – TJ-RO/Analista Judiciário – Análise de Sistemas/2012) Considere que um administrador de rede tendo disponibilizado um servidor de correio eletrônico com o nome mail.empresa.com.br associado a determinado endereço IP. Considere, ainda, que o administrador tendo configurado o recurso de resolução reversa de endereçamento IP, visto que outros servidores de correio eletrônico podem recusar a entrega das mensagens de e-mail, devido a falta desse recurso. O registro de recurso no servidor DNS que faz corretamente a resolução reversa do endereço IP é o

A) A.

B) MX

C) TXT.

D) CNAME.

E) PTR

Comentários:

Como já vimos, o tipo PTR é responsável por resoluções de nomes na forma reversa.

Gabarito: E

21. (CESPE - ANATEL/Suporte e Infraestrutura de Tecnologia da Informação/2014) Na estrutura hierárquica de funcionamento do serviço DNS, ao receber uma requisição para resolução de nome, o servidor local de nomes DNS verifica se o nome está no cache DNS local ou se consta do seu banco de dados. Se o encontrar, retorna o endereço IP

correspondente ao solicitante; caso contrário, o servidor DNS local repassa a consulta a um servidor DNS de nível mais alto.

Comentários:

Pessoal, a questão não entrou no mérito de diferenciar o servidor DNS local ou resolver. Independente disso, caso não haja a resposta no servidor preferencial, este necessariamente precisará repassar a consulta para obter a informação. Lembremos que essa é a estrutura de um sistema recursivo.

Gabarito: C

22. (CESPE – TCU/Analista de Controle Interno – TI/2008) O administrador da rede pediu a um analista orientações quanto a técnicas para reduzir o volume de dados que trafegam entre os seus servidores de DNS. Diante desse pedido, o analista solicitou ao administrador que verificasse se o sistema está realizando a transferência incremental de zona entre servidores DNS e esclareceu que, devido à transferência incremental de zona, quando um escravo de uma zona precisa atualizar os seus registros RR, ele envia uma solicitação ao mestre da zona, que pode responder enviando para o escravo apenas os valores dos RR que estejam desatualizados no escravo. Nessa situação, os esclarecimentos e orientações do analista foram adequados, considerando-se a demanda do administrador.

Comentários:

Pessoal, vimos que o método incremental (IXFR) gera um menor consumo de banda justamente por tratar apenas dos registros desatualizados. Dessa forma, o esclarecimento referido na questão está correto.

Gabarito: C

23. (CESPE – DEPEN/Agente Penitenciário – Área 7/2015) Seja para impedir que determinados computadores em uma rede local possam consultar servidores DNS na Internet, seja para controlar esses computadores na saída da rede por um firewall para o serviço de DNS, o firewall deve bloquear o uso do protocolo UDP na porta padrão 53.

Comentários:

Temos aqui uma questão polêmica. De fato, as consultas padrões do DNS ocorrem por intermédio do protocolo UDP na porta 53. Entretanto, vimos que algumas consultas podem utilizar o protocolo TCP, quando temos mensagens maiores que 512 bytes. Por esse motivo, vemos que tal procedimento não é suficiente.

Entretanto, como sempre digo, é importante termos em mente tal entendimento do CESPE. Quando não é abordado tal características explicitamente, devemos considerar apenas as consultas simples em UDP/53.

Gabarito: C (Gabarito do Professor: E)

24. (CESPE – TRE-GO/Técnico Judiciário – Programação de Sistemas/2015) Quando o cliente de um serviço DNS (domain name system) envia um pedido de resolução de nomes a um servidor, esse pedido é transportado pelo TCP, que se encarrega de buscar os servidores DNS primário e secundário.

Comentários:

O problema da questão está em afirmar que será utilizado o protocolo TCP, quando sabemos que em regra, será utilizado o protocolo UDP, exceto os casos de consultas que geram respostas grandes. Aí, nesse caso, será usado o TCP, bem como na transferência de zonas. Percebam que a questão trouxe o que uma possibilidade como sendo uma verdade.

Gabarito: E

25. (CESPE – STJ/Analista Judiciário – Suporte em TI/2015) O uso de um servidor DNS de encaminhamento central para a resolução de nomes da Internet pode reduzir o desempenho da rede, tornando complexo o processo de solução de problemas, além de ser uma prática não recomendada em termos de segurança.

Comentários:

Pessoal, o servidor de DNS de encaminhamento central é aquele que quando não é capaz de resolver um nome a partir da sua base de dados, encaminha a consulta para outros servidores externos com o objetivo de obter a devida informação. Na prática, é justamente essa capacidade de encaminhar consultas e obter informações externas que permite a navegação na Internet, pois o gerenciamento e atualização de nomes de forma local seria simplesmente inviável. Em termos de segurança, é muito mais recomendável concentrar as consultas em um servidor DNS da rede com encaminhamento de consultas do que deixar a cargo dos diversos hosts realizarem suas próprias consultas a servidores externos diretamente.

Gabarito: E

26. (CESPE – TRE/RS / Técnico Judiciário – Área 7/2015 - ADAPTADA) O DNS define dois tipos de servidores: primários e secundários. O servidor secundário não cria nem atualiza os arquivos de zona. Se for necessária a atualização, ela deve ser feita pelo servidor primário, que transmite uma versão atualizada para o secundário.

Comentários:

Exatamente isso pessoal. Em cada zona, devemos ter sempre apenas um primário, que será responsável pela atualização das entradas e múltiplos secundários, que terão suas bases replicadas a partir do servidor primário.

Gabarito: C

27. (CESPE – TRE/RS / Técnico Judiciário – Área 7/2015 - ADAPTADA) Por exigir que, na árvore de seu espaço de nome, os filhos de um nó tenham labels distintos, o DNS é considerado um espaço de nomes planos.

Comentários:

O DNS utiliza o conceito de espaço de nomes hierarquizados e não planos.

Gabarito: E

# QUESTÕES COMENTADAS – DNS - FCC

1. (FCC - TJ TRT18/TRT 18/Apoio Especializado/Tecnologia da Informação/2023)

Considere as seguintes afirmações sobre os protocolos DNS e DHCPv4:

I. Por padrão, servidor DNS escuta na porta 53/TCP e o servidor DHCPv4 na 68/TCP.

II. As solicitações de endereços IPs e resolução de endereços são encaminhadas pelos clientes por meio de endereços de multicast.

III. Um registro DNS do tipo A vincula o nome de domínio a um endereço IPv4.

IV. Em resposta a um DHCPOFFER, um cliente responde com uma mensagem DHCPREQUEST.

Está correto o que se afirma APENAS em

a) I, III e IV.

b) II e III.

c) I e II.

d) III e IV.

e) I, II e IV.

Comentários:

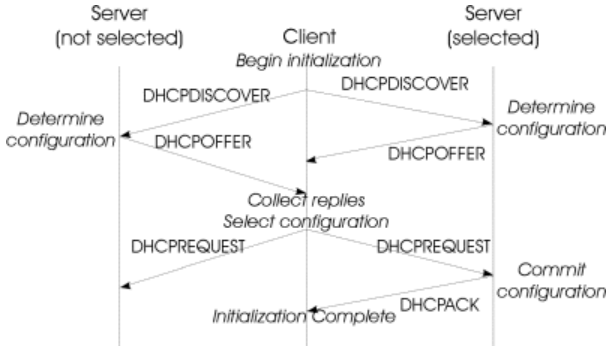
Vamos aos itens:

I. Incorreto. O servidor DNS escuta na porta 53, tanto para TCP quanto para UDP. No entanto, o servidor DHCPv4 escuta na porta 67/TCP e o cliente DHCPv4 na porta 68/TCP. Lembrando do fluxo bidirecional de mensagens no 4-way-handshake.

II. Incorreto. As solicitações de endereços IP feitas por um cliente DHCP são enviadas para um endereço de broadcast (255.255.255.255) ou multicast (224.0.0.1), dependendo da configuração. Então aqui já temos um erro, diante da afirmativa restritiva da questão. Entretanto, levando em consideração o DNS, pois o enunciado contemplou ambos, as solicitações de resolução de nomes DNS são normalmente enviadas para o endereço unicast do servidor DNS.

III. Correto. Sem dúvida. Principal tipo de registro do DNS.

IV. Correto. Estamos falando da segunda e terceira mensagens, conforme nossa imagem a seguir:




Gabarito: D

2. (FCC – CNMP/Analista de Suporte/2015) O serviço de nome de domínios (DNS) possui uma arquitetura do tipo cliente/servidor na qual a base de dados é distribuída por toda internet. Nessa arquitetura, o acesso ao servidor DNS para buscar o relacionamento IP/Domínio é feito pelo cliente que é o

A) Browser.

B) DNS Cache.

C) DNS Resolver.

D) DNS Searcher.

E) Gateway

Comentários:

Como vimos, o elemento responsável por efetivamente resolver o nome é chamado de DNS Resolver. Lembremos que este pode estar no próprio equipamento do cliente ou em um servidor a parte.

Gabarito: C

3. (FCC – Prefeitura de São Paulo – SP/Auditor Fiscal do Município/2012) O sistema hierárquico e distribuído de gerenciamento de nomes utilizado por computadores conectados à Internet, que é utilizado para a resolução ou conversão de nomes de domínios como arpanet.com em endereços IP como 173.254.213.241, é chamado de

A) Gateway.

B) DNS.

C) Roteador.

D) Switch.

E) HTTP.

Comentários:

Questão bem tranquila, certo? Falou de tradução de endereços a partir de nomes de domínio para IP's, teremos o protocolo DNS. Vale lembrar que o DNS possui diversas implementações e diversos tipos de tradução de nomes.

Gabarito: B

4. (FCC – TRT – 6ªRegião (PE)/Analista Judiciário – TI/2012) O Domain Name System pode ser visto como uma base de dados onde é possível consultar, entre outras coisas,

A) a lista dos serviços disponíveis em um certo domínio.

B) os servidores HTTP responsáveis por servir as páginas WWW de um certo domínio.

C) os servidores NTP responsáveis por manter o sincronismo de um certo domínio.

D) os servidores DHCP responsáveis por atribuir números IP às máquinas que se conectam dinamicamente a um certo domínio.

E) os servidores de e-mail responsáveis por receber as mensagens endereçadas a um certo domínio.

Comentários:

Questão polêmica. Quando digitamos um endereço na URL, temos que o DNS é responsável por traduzir esse nome em um endereço IPv4 através do tipo de registro "A". Esse tipo não se restringe a servidores HTTP conforme apontado pela alternativa B, o que levou muitos candidatos ao erro. Poderá retornar, por exemplo, o endereço de um servidor FTP.

Os serviços que possui entrada específica no DNS é o serviço de email através do registro MX. Dessa forma, quando um host ou servidor busca a informação do endereço IP a partir de um nome, tem-se que será fornecido de fato os endereços de servidores de email.

Serviços como NTP e DHCP não possuem entradas específicas nos registros e tipos do protocolo DNS.

Gabarito: E

5. (FCC - TCE-AP/Analista de Controle Externo – TI/2012) As mensagens DNS possuem um cabeçalho com tamanho fixo de

A) 8 bytes, sendo que os dois últimos tratam o número de informações adicionais.

B) 8 bytes, sendo que os dois últimos tratam o número de respostas.

C) 12 bytes, sendo que os dois últimos tratam o número de respostas.

D) 12 bytes, sendo que os dois últimos tratam o número de informações adicionais.

E) 16 bytes, sendo que os dois últimos tratam o número de autoridades.

Comentários:

Conforme vimos, seu cabeçalho possui um tamanho de 12 bytes, dos quais os dois últimos são utilizados para definir a quantidade de informações adicionais.

Gabarito: D

6. (FCC – TRT – 2ª Região (SP)/Técnico Judiciário – TI/2014) O sistema de nomes de domínios (DNS), possui 3 macros componentes:

I. São especificações para uma estrutura em árvore dos nomes e dados associados a estes nomes.

II. Servidores que guardam a informação sobre as árvores de nomes.

III. Programas que extraem a informação dos servidores em reposta à requisição dos clientes.

Estes componentes são, correta e respectivamente, denominados:

A) DOMAIN NAME SPACE / RESOURCE RECORDS - NAME SERVERS - RESOLVERS

B) NAME SERVERS - RESOLVERS - CLIENT PROGRAMS

C) DNS MODULES - DNS SERVERS - NAME SERVERS

D) RESOLVERS - CLIENT PROGRAMS - DNS MODULES

E) NAME SERVERS - DNS MODULES - DOMAIN NAME SPACE / RESOURCE RECORDS

Comentários:

A estrutura em árvore apresenta na teoria possui como termo técnico definido pela RFC de DOMAIN NAME SPACE. As informações vinculadas a cada um dos nós dessa árvore é conhecido como Resources Records.

Além disso, vimos ainda que o NAME SERVER é responsável por prover informações a respeitos do registros e domínios. Possui uma identificação própria de NS nos tipos de registros.

E por último, temos os resolvers. São os responsáveis por efetivar as consultas em busca de respostas nos servidores de domínio espalhados pela rede.

Gabarito: A

7. (FCC – TRT – 16ªRegião (MA)/Analista Judiciário – TI/2014) O serviço de rede DNS possui uma arquitetura hierárquica que inclui clientes e servidores, com bases de dados distribuídos, que se comunicam por meio dos protocolos definidos para o DNS. Dentre os três tipos de mensagens definidas no protocolo, a mensagem utilizada para a troca de informações entre os servidores DNS é do tipo

A) consulta.

B) resposta.

C) busca.

D) atualização.

E) sincronização.

Comentários:

Existem três tipos de mensagens: Consultas e Respostas que acontecem do cliente para o servidor, e as atualizações, que acontecem entre servidores.

Gabarito: D

8. (FCC – MPE-MA/Analista Ministerial – Rede e Infraestrutura/2013) Em um serviço de nomes de domínios (DNS), tipos de campos são utilizados em registros de recursos. É correto afirmar que dentre estes tipos se inclua

A) MFD.

B) NIL.

C) QINFO.

D) KWS.

E) SOA.

Comentários:

Vimos que o tipo de registro SOA (Start of Autority) corresponde a um tipo de registro de servidores autoritativos. Temos assim a representação de que este é a melhor fonte de informações para determinado registro.

Gabarito: E

9. (FCC – TRE-CE/Analista Judiciário – Análise de Sistemas/2012) Nome de domínio que especifica a sua localização exata na hierarquia da árvore do Domain Name System - DNS. Trata-se de

A) SNMP.

B) FQDN.

C) OSPF.

D) SDN.

E) RTPC.

Comentários:

A navegação pelos diversos nós da estrutura em árvore do DNS permite a composição de um nome único (registro) de identificação dos nós na rede. Vimos que cada dispositivo que deseja ser identificado deve possuir um nome que permite a sua localização exata na estrutura. Chamamos esse nome de FQDN (Fully Qualified Domain Name).

Gabarito: B

10. (FCC – TRE-CE/Técnico Judiciário/2012) A utilização de Sistemas de Nomes de Domínios (Domain Name System) para mapear um endereço IP em um nome de domínio é chamado de DNS

A) reverso.

B) secundário.

C) autoritativo.

D) raiz.

E) cache.

Comentários:

Em regra, na maioria absoluta das consultas DNS, temos que SE busca descobrir o endereço IP a partir de um nome DNS. Entretanto, o protocolo DNS também permite a realização da operação no sentido contrário, ou seja, a partir de um endereço IP, obter-se o nome de registro. Esse serviço é conhecido como DNS reverso e é mapeado pelo tipo de registro PTR.

Gabarito: A

11. (FCC – MPE-PE/Técnico Ministerial – Telecomunicações/2012) Trata-se de um sistema de gerenciamento de nomes, hierárquico e distribuído, define a sintaxe dos nomes usados na Internet e os associa a um endereço IP:

A) TCP - TransmissionControlProtocol

B) NFS - Network File System

C) SMTP - Simple Mail TransferProtocol

D) URN - UniformResourceName

E) DNS - Domain Name System

Comentários:

Questão bem tranquila, certo pessoal? O DNS é o responsável pelas traduções de nomes em um modelo distribuído e hierárquico.

Gabarito: E

12. (FCC – TJ-RJ/Analista Judiciário – Analista de Sistemas/2012) Base de dados distribuída, organizada hierarquicamente, é uma descrição sucinta do

a) Network File System (NFS).

B) Dynamic Host Configuration Protocol (DHCP).

C) Remote Desktop Protocol (RDP).

D) Peer to Peer (P2P).

E) Domain Name System (DNS).

Comentários:

Mais uma definição extremamente genérica a respeito do protocolo DNS.

Gabarito: E

# Questões Comentadas – DNS - FGV

1. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

O analista Daniel administra o serviço de Domain Name System (DNS) da DPE/RS. Foi solicitado que Daniel atualize a configuração de DNS reverso, de forma que o endereço IP 200.198.128.255, da Defensoria, seja resolvido para o nome de domínio www23.defensoria.rs.def.br.

Para atender à solicitação, Daniel deve proceder com a inserção de um novo registro de recurso DNS do tipo:

a) A;

b) PTR;

c) CAA;

d) AAAA;

e) NAPTR.

Comentários:

Muita atenção meus amigos. Vejam a palavra chave no enunciado (REVERSO). Ou seja, a partir de um endereço IP, busca-se o respectivo nome ou URL. Essa é a característica do PTR.

Alguns alunos acabam focando somente no endereço IPv4, e acabam marcando erradamente a letra A, como se fosse a resolução de nomes no formato tradicional.

Gabarito: B

2. FGV - 2022 - Senado Federal - Consultor Legislativo - Comunicação e Tecnologia da Informação

Em setembro de 2022, o Domínio .br, operado pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), ultrapassou 5 milhões de nomes registrados. O funcionamento do .br prevê diversas alternativas para que um nome registrado possa ter semântica embutida.

Entre elas, estão

A por DNSSEC obrigatório, como é o caso dos meios de comunicação com os domínios TVsec.br; radiosec.br e infsec.br.

B por tipo de aplicação, sendo o blog.br, destinado aos blogs de textos e o vlog.br, aos de fotos e vídeos desenvolvidos exclusivamente por pessoas jurídicas.

C por geolocalização, mas os registros cidade.br só podem ser usados por pessoas jurídicas.

D por tipo de atividade, sendo o com.br destinado preferencialmente a atividades comerciais desenvolvidas por pessoas físicas ou jurídicas.

E por atividades de profissionais liberais constituídos como pessoa física ou jurídica, a exceção dos especialistas em Tecnologia da Informação (eti.br), que só podem ser pessoa jurídica.

Comentários:

Temos a definição e orquestração do domínio .br feita pelo NIC.Br. A partir do próprio NIC.Br, vimos também que há uma definição de finalidades específicas para cada tipo de domínio e, justamente o .com.br, o principal domínio para o Brasil, contempla as pessoas físicas e jurídicas de uma forma geral para atividades comerciais.

Ainda, em relação aos itens:

a) Não há uma relação do DNSSEC, que é uma extensão de segurança os nomes de domínio com os tipos de domínio.

b) Não há essa restrição, e, inclusive, vimos que os domínios são abertos a pessoas físicas e jurídicas.

c) Não há classificação por geolocalização interna no país.

e) Os domínios são abertos conforme mencionamos no início da questão.

Gabarito: D

3. FGV - 2018 - MPE-AL - Analista do Ministério Público - Administrador de Rede

A rede da empresa Kanguroo Tec apresenta problemas com a conexão de uma estação de trabalho aos servidores DNS. Foi identificado que o problema encontrava-se na camada de transporte. Para resolver o problema deve ser verificado se o protocolo de transporte utilizado está correto e se a porta do servidor DNS está aceitando conexões.

O protocolo de transporte e a porta padrão utilizada pelo DNS, são, respectivamente,

A UDP e 50.

B TCP e 25.

C UDP e 443.

D TCP e 22.

E UDP e 53.

Comentários:

Conforme vimos, em que pese haja outras possibilidades de uso com o TCP, mas a essência é na porta UDP/53.

Gabarito: E

4. FGV - 2021 - Câmara de Aracaju - SE - Técnico de Tecnologia da Informação

Um técnico incumbido da instalação de software nos computadores de uma empresa pediu ao responsável pelos serviços da empresa o endereço do servidor de e-mail corporativo, e lhe foi informado o endereço mail.empresa.com.br. O técnico concluiu a instalação do software e verificou rapidamente que o servidor de e-mail estava localizado no endereço IP 192.168.16.30. A localização do servidor (internet ou intranet) e o recurso utilizado para descobrir o endereço IP a partir daquele informado pelo responsável pelos serviços foram, respectivamente:

A Intranet; ARP;

B Internet; IPX;

C Intranet; DNS;

D Internet; VPN;

E Internet; NAT.

Comentários:

A primeira parte da questão nos traz uma cobrança tradicional do assunto de IP. Lembrando que as faixas privadas contemplam as redes internas ou intranets para uso.

Bom, mas o que nos interessa é a segunda parte da questão, onde se busca descobrir o endereço IP a partir do recurso informado pelo responsável. O que vale destacar nessa questão, é que não há restrição do tipo de recurso. Pois há vários modos de se solicitar o endereço IP. Veremos ainda ao longo dessa aula tais tipos.

Gabarito: C

5. FGV - 2022 - MPE-GO - Assistente Programador

Uma equipe de suporte de redes foi chamada para resolver um problema de conectividade de um computador que se comunica normalmente com os demais dispositivos da rede, mas falha em navegar na Internet. A equipe verificou, porém, que quando se digita o endereço IP dos sites, a navegação ocorre normalmente. A experiente equipe de suporte de redes concluiu que houve uma desconfiguração no endereço do servidor

A User Datagram Protocol.

B Transmission Control Protocol.

C Windows Internet Name Service.

D Domain Name System.

E Dynamic Host Configuration Protocol.

Comentários:

Temos nesse enunciado a descrição clássica de um problema associado ao protocolo DNS. Se o usuário em questão conseguiu acessar e navegar pelo endereço IP, indica-se que não há problema de conectividade, mas sim, de tradução do nome para acesso e recuperação do endereço IP para navegação.

Gabarito: D

FGV - 2018 - MPE-AL - Analista do Ministério Público - Administrador de Rede

O Bind é um software Open Source que implementa o serviço de DNS.

Considerando a implementação de um DNS autoritativo, com Bind a partir da versão 9 (estável e superiores), assinale a afirmativa correta.

A O servidor DNS, que opera como primário para algumas zonas, não pode operar como secundário para outras zonas.

B O servidor DNS secundário é o local onde é mantida a cópia principal de uma zona.

C O servidor DNS não pode operar como recursivo para um grupo de clientes locais.

D O servidor DNS primário precisa ter dois ou mais servidores secundários para realizar a tradução reversa.

E O servidor DNS secundário recebe o conteúdo de uma zona de outro servidor, por meio de um processo de sincronização.

Comentários:

Em que pese a questão traga os conceitos associados ao BIND em seu enunciado, mas temos que as características básicas são do próprio DNS.

Vamos aos itens:

a) É possível ele atuar como primário e secundário, normalmente, a depender das zonas. INCORRETO

b) O erro está em dizer que o DNS secundário armazena a cópia principal da zona, em vez de ser a réplica. INCORRETO

c) Não há qualquer restrição quanto à sua configuração dos modos recursivo ou interativo. Veremos esse conceito mais à frente. INCORRETO

d) Não há essa vinculação. Como fora destacado inclusive pelo Forouzan, trata-se de um recurso de redundância, e organização das zonas. INCORRETO

e) Exatamente pessoal. Esse é o termo mais adequado para o processo. CORRETO

Gabarito: E

6. FGV - 2022 - TJ-DFT - Analista Judiciário - Suporte em Tecnologia da Informação

Andréa administra o DNS (Domain Name System) do órgão onde trabalha e precisa gerenciar vários registros de domínio para um endereço único de domínio.

De forma a permitir esse tipo de apontamento, Andréa configurou um registro CNAME, apontando-o para o:

A nome real do hospedeiro;

B endereço IP do hospedeiro;

C endereço IP do servidor DNS autoritativo daquele registro;

D nome do cliente DNS utilizado na consulta;

E nome do servidor DNS autoritativo daquele registro.

Comentários:

O CNAME criado é utilizado para criar um alias ou um nome alternativo. Agora, obviamente, a sua referência e apontamento precisa indicar para o nome real do hospedeiro, para manter esse relacionamento.

Gabarito: A

7. FGV - 2018 - Banestes - Analista em Tecnologia da Informação - Suporte e Infraestrutura

Para implementar uma resolução de nomes mais segura, foi desenvolvido o padrão DNSSEC.

Basicamente ele serve para:

A assinar digitalmente os registros DNS, o que permite fornecer proteção completa contra ataques do tipo DoS;

B permitir um acesso seguro a consultas DNS, através de criptografia simétrica;

C permitir uma assinatura na transferência de zonas entre servidores DNS primários e secundários;

D garantir a confidencialidade do conjunto de registros de recursos, o Resource Record Set (RRset);

E evitar que dados de DNS sejam forjados ou manipulados, porém sem fornecer confidencialidade, pois as respostas DNSSEC são autenticadas, mas não criptografadas.

Comentário:

Vamos aos itens, pessoal:

a) De fato, ele permite as assinaturas digitais. Entretanto, o seu propósito não é a disponibilidade frente a ataques de DOS, mas sim a autenticidade e integridade para ataques do tipo cache poisoning. INCORRETO

b) A criptografia utilizada é a assimétrica, e não a simétrica. E, de fato, é para permitir um acesso seguro às consultas. INCORRETO

c) Seu foco não é no processo de replicação de zonas. INCORRETO

d) Não se trata do princípio da confidencialidade, muito menos de criptografia específica pra essa finalidade. INCORRETO

e) Na linha do que comentamos em todos os itens anteriores. CORRETO

Gabarito: E

# Lista de Questões – DNS - CESPE

1. CEBRASPE (CESPE) - AIS (EMPREL)/EMPREL/Redes/2023

O registro DNS que aponta um nome de domínio (um alias) para outro domínio é do tipo

a) AAAA.

b) NS.

c) CNAME.

d) MX.

e) PTR.

2. CEBRASPE (CESPE) - Per Crim (POLC AL)/POLC AL/Análise de Sistemas, Ciências da Computação, Informática. Processamento de Dados ou Sistemas da Informação/2023

O DNS (domain naming system) utiliza um esquema hierárquico de atribuição de nomes com base no domínio e um sistema de bancos de dados distribuídos para mapear nomes de hosts em endereços IP.

3. CESPE / CEBRASPE - 2022 - TCE-SC - Auditor Fiscal de Controle Externo - Ciência da Computação

Cabe ao CGIbr estabelecer diretrizes na execução do registro de nomes de domínio, bem como na alocação de endereço IP.

4. CESPE / CEBRASPE - 2022 - TCE-SC - Auditor Fiscal de Controle Externo - Ciência da Computação

É prevista a participação de representantes da comunidade científica e tecnológica no Comitê Gestor da Internet (CGI.BR), entre cujas atribuições e responsabilidades se inclui o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil.

5. (CESPE – TCE-PR/Analista de Controle – Área TI/2016) Uma consulta DNS inicial típica, originada de uma máquina de usuário e encaminhada ao servidor de nomes local para um nome de domínio externo não armazenado em cache DNS, será do tipo

A) raiz.

B) domínio de alto nível.

C) iterativa.

D) recursiva.

E) direta.

6. (CESPE - ANCINE/Área II/2013) O DNS (domain name system) está relacionado a esquema hierárquico de atribuição de nomes embasado no domínio de um sistema de banco de dados distribuído para implementar esse esquema de nomenclatura.

7. (CESPE - ANATEL/Arquitetura de Soluções de Tecnologia da Informação e Comunicação/2014) O DNS (domain name system) organiza o espaço de nomes em uma estrutura hierárquica que permite descentralizar as responsabilidades envolvidas na atribuição de nomes, podendo usar os serviços do UDP ou TCP por meio da porta-padrão 53.

8. (CESPE - ANATEL/Suporte e Infraestrutura de Tecnologia da Informação/2014) Em uma zona DNS, ao se utilizar o registro de recurso do tipo MX, informa-se o registro reverso de nome para endereço IP.

9. (CESPE - ANATEL/Engenharia/2014) O DNS (domain name system) é uma base de dados distribuída, armazenada em uma hierarquia de servidores, responsável pela tradução de identificadores mnemônicos de hosts, como, por exemplo, cespe.unb.br, para endereços IP, já que estes são necessários para os roteadores encaminharem corretamente os pacotes.

10. (CESPE – TRE-RJ/Técnico Judiciário/2012) A resolução do nome www.google.com.br para o endereço IP 74.125.234.120 é realizada pelo protocolo de navegação HTTP.

11. (CESPE – TRE-RJ/Técnico Judiciário/2012) Suponha que, após a execução do comando ping 127.0.0.1, seja apresentada como reposta que o tempo limite do pedido tenha se esgotado. Nessa situação, é correto afirmar que houve falha de DNS e, para solucionar o problema, deve-se executar o comando ipconfig /flushdns.

12. (CESPE – Câmara dos Deputados/Analista – Engenharia Eletrônica/2012) O sistema de DNS caracteriza-se por um banco de dados distribuído de registros de recursos (RRs — resource records), no qual cada registro de recurso possui um campo de TTL (time to livE) que indica o tempo que a entrada deve ser mantida no servidor de nomes autoritativos antes de sua exclusão.

13. (CESPE - Ana MPU/Tecnologia da Informação e Comunicação/Suporte e Infraestrutura/2013) O DNS utiliza o UDP em consultas, mas não em transferências de zona. Para esta operação, é utilizado o TCP.

14. (CESPE - TJ STF/Apoio Especializado/Tecnologia da Informação/2013) Na aplicação DNS (Domain Name System), o UDP fornece controle preciso dos fluxos de pacotes, erros ou sincronização.

15. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013)

```
C:\>nslookup
Servidor Padrão: UnKnown
Address: 192.168.1.1
> set type=ptr
> www.google.com
Servidor: UnKnown
Address: 192.168.1.1

google.com

primary name server = ns1.google.com
responsible mail addr = dns-admin.google.com
serial = 1507969
refresh = 7200 (2 hours)
retry = 1800 (30 mins)
expire = 1209600 (14 days)
default TTL = 300 (5 mins)

>
```

Com base no trecho de código acima, que se refere a uma consulta realizada na Internet, julgue o item que se segue.

Não há indício de que a consulta realizada tenha retornado o endereço de ponteiro do domínio www.google.com.

16. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) Com base no trecho de código acima da questão anterior, que se refere a uma consulta realizada na Internet, julgue o item que se segue.
O TTL correspondente a 300 foi o tempo que a consulta levou para ser armazenada, em cache, no roteador que gerou a última rota do pacote.

17. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O endereço 192.168.1.1 refere-se a um servidor DNS que não é do tipo autoritativo do domínio consultado.

18. (CESPE - TJ STF/Analista Judiciário/2013) Considerando que uma organização possua uma intranet com servidor web e servidor de correio eletrônico, julgue o item a seguir.

Tanto no caso do servidor web como no do servidor de correio eletrônico, é necessário haver um serviço DNS para converter nomes em endereços IPs.

19. (CESPE – Telebrás/Especialista em Gestão de Telecomunicações – Analista em TI/2013) Quando um usuário, em sua estação de trabalho, tenta acessar o sítio da Web representado pelo endereço www.xyz.com.br, que está associado a um endereço IP na Internet, o acesso será conseguido em razão de o serviço DNS fazer resoluções diretas de nomes para o endereço IP.

20. (CESPE – TJ-RO/Analista Judiciário – Análise de Sistemas/2012) Considere que um administrador de rede tendo disponibilizado um servidor de correio eletrônico com o nome mail.empresa.com.br associado a determinado endereço IP. Considere, ainda, que o administrador tendo configurado o recurso de resolução reversa de endereçamento IP, visto que outros servidores de correio eletrônico podem recusar a entrega das mensagens de e-mail, devido a falta desse recurso. O registro de recurso no servidor DNS que faz corretamente a resolução reversa do endereço IP é o

A) A.

B) MX

C) TXT.

D) CNAME.

E) PTR

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

22. (CESPE – TCU/Analista de Controle Interno – TI/2008) O administrador da rede pediu a um analista orientações quanto a técnicas para reduzir o volume de dados que trafegam entre os seus servidores de DNS. Diante desse pedido, o analista solicitou ao administrador que verificasse se o sistema está realizando a transferência incremental de zona entre servidores DNS e esclareceu que, devido à transferência incremental de zona, quando um escravo de uma zona precisa atualizar os seus registros RR, ele envia uma solicitação ao mestre da zona, que pode responder enviando para o escravo apenas os valores dos RR que estejam desatualizados no escravo. Nessa situação, os esclarecimentos e orientações do analista foram adequados, considerando-se a demanda do administrador.

23. (CESPE – DEPEN/Agente Penitenciário – Área 7/2015) Seja para impedir que determinados computadores em uma rede local possam consultar servidores DNS na Internet, seja para controlar esses computadores na saída da rede por um firewall para o serviço de DNS, o firewall deve bloquear o uso do protocolo UDP na porta padrão 53.

24. (CESPE – TRE-GO/Técnico Judiciário – Programação de Sistemas/2015) Quando o cliente de um serviço DNS (domain name system) envia um pedido de resolução de nomes a um servidor, esse pedido é transportado pelo TCP, que se encarrega de buscar os servidores DNS primário e secundário.

25. (CESPE – STJ/Analista Judiciário – Suporte em TI/2015) O uso de um servidor DNS de encaminhamento central para a resolução de nomes da Internet pode reduzir o desempenho da rede, tornando complexo o processo de solução de problemas, além de ser uma prática não recomendada em termos de segurança.

26. (CESPE – TRE/RS / Técnico Judiciário – Área 7/2015 - ADAPTADA) O DNS define dois tipos de servidores: primários e secundários. O servidor secundário não cria nem atualiza os

arquivos de zona. Se for necessária a atualização, ela deve ser feita pelo servidor primário, que transmite uma versão atualizada para o secundário.

27. (CESPE – TRE/RS / Técnico Judiciário – Área 7/2015 - ADAPTADA) Por exigir que, na árvore de seu espaço de nome, os filhos de um nó tenham labels distintos, o DNS é considerado um espaço de nomes planos.

## GABARITO

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

*Questão 23, gabarito do professor: E

* Questão 18, gabarito do professor: E

* Questão 14, gabarito do professor: E

# Lista de Questões – DNS - FCC

1. (FCC - TJ TRT18/TRT 18/Apoio Especializado/Tecnologia da Informação/2023)

Considere as seguintes afirmações sobre os protocolos DNS e DHCPv4:

I. Por padrão, servidor DNS escuta na porta 53/TCP e o servidor DHCPv4 na 68/TCP.

II. As solicitações de endereços IPs e resolução de endereços são encaminhadas pelos clientes por meio de endereços de multicast.

III. Um registro DNS do tipo A vincula o nome de domínio a um endereço IPv4.

IV. Em resposta a um DHCPOFFER, um cliente responde com uma mensagem DHCPREQUEST.

Está correto o que se afirma APENAS em

a) I, III e IV.

b) II e III.

c) I e II.

d) III e IV.

e) I, II e IV.

2. (FCC – CNMP/Analista de Suporte/2015) O serviço de nome de domínios (DNS) possui uma arquitetura do tipo cliente/servidor na qual a base de dados é distribuída por toda internet. Nessa arquitetura, o acesso ao servidor DNS para buscar o relacionamento IP/Domínio é feito pelo cliente que é o

A) Browser.

B) DNS Cache.

C) DNS Resolver.

D) DNS Searcher.

E) Gateway

3. (FCC – Prefeitura de São Paulo – SP/Auditor Fiscal do Município/2012) O sistema hierárquico e distribuído de gerenciamento de nomes utilizado por computadores conectados à

Internet, que é utilizado para a resolução ou conversão de nomes de domínios como arpanet.com em endereços IP como 173.254.213.241, é chamado de

A) Gateway.

B) DNS.

C) Roteador.

D) Switch.

E) HTTP.

4. (FCC – TRT – 6ªRegião (PE)/Analista Judiciário – TI/2012) O Domain Name System pode ser visto como uma base de dados onde é possível consultar, entre outras coisas,

A) a lista dos serviços disponíveis em um certo domínio.

B) os servidores HTTP responsáveis por servir as páginas WWW de um certo domínio.

C) os servidores NTP responsáveis por manter o sincronismo de um certo domínio.

D) os servidores DHCP responsáveis por atribuir números IP às máquinas que se conectam dinamicamente a um certo domínio.

E) os servidores de e-mail responsáveis por receber as mensagens endereçadas a um certo domínio.

5. (FCC - TCE-AP/Analista de Controle Externo – TI/2012) As mensagens DNS possuem um cabeçalho com tamanho fixo de

A) 8 bytes, sendo que os dois últimos tratam o número de informações adicionais.

B) 8 bytes, sendo que os dois últimos tratam o número de respostas.

C) 12 bytes, sendo que os dois últimos tratam o número de respostas.

D) 12 bytes, sendo que os dois últimos tratam o número de informações adicionais.

E) 16 bytes, sendo que os dois últimos tratam o número de autoridades.

6. (FCC – TRT – 2ª Região (SP)/Técnico Judiciário – TI/2014) O sistema de nomes de domínios (DNS), possui 3 macros componentes:

I. São especificações para uma estrutura em árvore dos nomes e dados associados a estes nomes.

II. Servidores que guardam a informação sobre as árvores de nomes.

III. Programas que extraem a informação dos servidores em reposta à requisição dos clientes.

Estes componentes são, correta e respectivamente, denominados:

A) DOMAIN NAME SPACE / RESOURCE RECORDS - NAME SERVERS - RESOLVERS

B) NAME SERVERS - RESOLVERS - CLIENT PROGRAMS

C) DNS MODULES - DNS SERVERS - NAME SERVERS

D) RESOLVERS - CLIENT PROGRAMS - DNS MODULES

E) NAME SERVERS - DNS MODULES - DOMAIN NAME SPACE / RESOURCE RECORDS

7. (FCC – TRT – 16ªRegião (MA)/Analista Judiciário – TI/2014) O serviço de rede DNS possui uma arquitetura hierárquica que inclui clientes e servidores, com bases de dados distribuídos, que se comunicam por meio dos protocolos definidos para o DNS. Dentre os três tipos de mensagens definidas no protocolo, a mensagem utilizada para a troca de informações entre os servidores DNS é do tipo

A) consulta.

B) resposta.

C) busca.

D) atualização.

E) sincronização.

8. (FCC – MPE-MA/Analista Ministerial – Rede e Infraestrutura/2013) Em um serviço de nomes de domínios (DNS), tipos de campos são utilizados em registros de recursos. É correto afirmar que dentre estes tipos se inclua

A) MFD.

B) NIL.

C) QINFO.

D) KWS.

E) SOA.

9. (FCC – TRE-CE/Analista Judiciário – Análise de Sistemas/2012) Nome de domínio que especifica a sua localização exata na hierarquia da árvore do Domain Name System - DNS. Trata-se de

A) SNMP.

B) FQDN.

C) OSPF.

D) SDN.

E) RTPC.

10. (FCC – TRE-CE/Técnico Judiciário/2012) A utilização de Sistemas de Nomes de Domínios (Domain Name System) para mapear um endereço IP em um nome de domínio é chamado de DNS

A) reverso.

B) secundário.

C) autoritativo.

D) raiz.

E) cache.

11. (FCC – MPE-PE/Técnico Ministerial – Telecomunicações/2012) Trata-se de um sistema de gerenciamento de nomes, hierárquico e distribuído, define a sintaxe dos nomes usados na Internet e os associa a um endereço IP:

A) TCP - TransmissionControlProtocol

B) NFS - Network File System

C) SMTP - Simple Mail TransferProtocol

D) URN - UniformResourceName

E) DNS - Domain Name System

12. (FCC – TJ-RJ/Analista Judiciário – Analista de Sistemas/2012) Base de dados distribuída, organizada hierarquicamente, é uma descrição sucinta do

A) Network File System (NFS).

B) Dynamic Host Configuration Protocol (DHCP).

C) Remote Desktop Protocol (RDP).

D) Peer to Peer (P2P).

E) Domain Name System (DNS).

# GABARITO

| 01 | 02 | 03 | 04 | 05 | 06 |
|---|---|---|---|---|---|
| D | C | B | E | D | A |
| 07 | 08 | 09 | 10 | 11 | 12 |
| D | E | B | A | E | E |

# Lista de Questões – DNS - FGV

1. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

O analista Daniel administra o serviço de Domain Name System (DNS) da DPE/RS. Foi solicitado que Daniel atualize a configuração de DNS reverso, de forma que o endereço IP 200.198.128.255, da Defensoria, seja resolvido para o nome de domínio www23.defensoria.rs.def.br.

Para atender à solicitação, Daniel deve proceder com a inserção de um novo registro de recurso DNS do tipo:

a) A;

b) PTR;

c) CAA;

d) AAAA;

e) NAPTR.

2. FGV - 2022 - Senado Federal - Consultor Legislativo - Comunicação e Tecnologia da Informação

Em setembro de 2022, o Domínio .br, operado pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), ultrapassou 5 milhões de nomes registrados. O funcionamento do .br prevê diversas alternativas para que um nome registrado possa ter semântica embutida.

Entre elas, estão

A) por DNSSEC obrigatório, como é o caso dos meios de comunicação com os domínios TVsec.br; radiosec.br e infsec.br.

B) por tipo de aplicação, sendo o blog.br, destinado aos blogs de textos e o vlog.br, aos de fotos e vídeos desenvolvidos exclusivamente por pessoas jurídicas.

C) por geolocalização, mas os registros cidade.br só podem ser usados por pessoas jurídicas.

D) por tipo de atividade, sendo o com.br destinado preferencialmente a atividades comerciais desenvolvidas por pessoas físicas ou jurídicas.

E) por atividades de profissionais liberais constituídos como pessoa física ou jurídica, a exceção dos especialistas em Tecnologia da Informação (eti.br), que só podem ser pessoa jurídica.

3. FGV - 2018 - MPE-AL - Analista do Ministério Público - Administrador de Rede

A rede da empresa Kanguroo Tec apresenta problemas com a conexão de uma estação de trabalho aos servidores DNS. Foi identificado que o problema encontrava-se na camada de transporte. Para resolver o problema deve ser verificado se o protocolo de transporte utilizado está correto e se a porta do servidor DNS está aceitando conexões.

O protocolo de transporte e a porta padrão utilizada pelo DNS, são, respectivamente,

A) UDP e 50.

B) TCP e 25.

C) UDP e 443.

D) TCP e 22.

E) UDP e 53.

4. FGV - 2021 - Câmara de Aracaju - SE - Técnico de Tecnologia da Informação

Um técnico incumbido da instalação de software nos computadores de uma empresa pediu ao responsável pelos serviços da empresa o endereço do servidor de e-mail corporativo, e lhe foi informado o endereço mail.empresa.com.br. O técnico concluiu a instalação do software e verificou rapidamente que o servidor de e-mail estava localizado no endereço IP 192.168.16.30. A localização do servidor (internet ou intranet) e o recurso utilizado para descobrir o endereço IP a partir daquele informado pelo responsável pelos serviços foram, respectivamente:

A) Intranet; ARP;

B) Internet; IPX;

C) Intranet; DNS;

D) Internet; VPN;

E) Internet; NAT.

5. FGV - 2022 - MPE-GO - Assistente Programador

Uma equipe de suporte de redes foi chamada para resolver um problema de conectividade de um computador que se comunica normalmente com os demais dispositivos da rede, mas falha em navegar na Internet. A equipe verificou, porém, que quando se digita o endereço IP dos sites, a navegação ocorre normalmente. A experiente equipe de suporte de redes concluiu que houve uma desconfiguração no endereço do servidor

A) User Datagram Protocol.

B) Transmission Control Protocol.

C) Windows Internet Name Service.

D) Domain Name System.

E) Dynamic Host Configuration Protocol.

6. FGV - 2018 - MPE-AL - Analista do Ministério Público - Administrador de Rede

O Bind é um software Open Source que implementa o serviço de DNS.

Considerando a implementação de um DNS autoritativo, com Bind a partir da versão 9 (estável e superiores), assinale a afirmativa correta.

A) O servidor DNS, que opera como primário para algumas zonas, não pode operar como secundário para outras zonas.

B) O servidor DNS secundário é o local onde é mantida a cópia principal de uma zona.

C) O servidor DNS não pode operar como recursivo para um grupo de clientes locais.

D) O servidor DNS primário precisa ter dois ou mais servidores secundários para realizar a tradução reversa.

E) O servidor DNS secundário recebe o conteúdo de uma zona de outro servidor, por meio de um processo de sincronização.

7. FGV - 2022 - TJ-DFT - Analista Judiciário - Suporte em Tecnologia da Informação

Andréa administra o DNS (Domain Name System) do órgão onde trabalha e precisa gerenciar vários registros de domínio para um endereço único de domínio.

De forma a permitir esse tipo de apontamento, Andréa configurou um registro CNAME, apontando-o para o:

A) nome real do hospedeiro;

B) endereço IP do hospedeiro;

C) endereço IP do servidor DNS autoritativo daquele registro;

D) nome do cliente DNS utilizado na consulta;

E) nome do servidor DNS autoritativo daquele registro.

8. FGV - 2018 - Banestes - Analista em Tecnologia da Informação - Suporte e Infraestrutura

Para implementar uma resolução de nomes mais segura, foi desenvolvido o padrão DNSSEC.

Basicamente ele serve para:

A) assinar digitalmente os registros DNS, o que permite fornecer proteção completa contra ataques do tipo DoS;

B) permitir um acesso seguro a consultas DNS, através de criptografia simétrica;

C) permitir uma assinatura na transferência de zonas entre servidores DNS primários e secundários;

D) garantir a confidencialidade do conjunto de registros de recursos, o Resource Record Set (RRset);

E) evitar que dados de DNS sejam forjados ou manipulados, porém sem fornecer confidencialidade, pois as respostas DNSSEC são autenticadas, mas não criptografadas.

# GABARITO

| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 |
|---|---|---|---|---|---|---|---|
| B | D | E | C | D | E | A | E |

# ESSA LEI TODO MUNDO CONHECE:
# PIRATARIA É CRIME.

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

1. 

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

2. 

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

3. 

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

4. 

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

5. 

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

6. 

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

7. 

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

8. 

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

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