[**Informações do teste**](https://uniritter.blackboard.com/webapps/assessment/take/launch.jsp?course_assessment_id=_2945968_1&course_id=_732490_1&content_id=_18760494_1&step=null)

|  |  |
| --- | --- |
| Descrição |  |
| Instruções | Caso necessite a utilização do "EXCEL" clique no link ao lado -----------> [excel.xlsx](https://uniritter.blackboard.com/bbcswebdav/pid-18760494-dt-content-rid-84766551_1/xid-84766551_1) |
| Várias tentativas | Não permitido. Este teste só pode ser feito uma vez. |
| Forçar conclusão | Este teste pode ser salvo e retomado posteriormente. |

Expandir Estado de Conclusão da Pergunta:

**PERGUNTA 1**

1. Assim como o endereço IP, a máscara de rede é composta por 32 *bits* , com 4 números decimais separados por pontos. Na estrutura da máscara de rede, os *bits* com valor 1 se referem à rede e os *bits* 0 se referem ao *host* . Ela é utilizada exatamente para isso, para que a máquina saiba a qual classe o IP pertence e qual o tamanho da sua rede. No caso das sub-redes, definir a máscara correta é fundamental para que os dispositivos da sub-rede se comuniquem entre si nessa sub-rede em específico e não estejam conectados a sub-redes diferentes.  
   Nesse contexto, relacione as máscaras *default* para cada classe:

|  |  |
| --- | --- |
| 1.      Classe A | (  ) 255.255.0.0 |
| 2.      Classe B | (  ) 255.255.255.0 |
| 3.      Classe C | (  ) 255.0.0.0 |

1. A ordem correta de associação das classes com suas máscaras *default* é:

|  |  |  |
| --- | --- | --- |
|  |  | .3, 1, 2. |
|  |  | .3, 2, 1. |
|  |  | .2, 3, 1. |
|  |  | .2, 1, 3. |
|  |  | .1, 2, 3. |

**1 pontos**

**PERGUNTA 2**

1. O protocolo da camada de aplicação da web, está no coração da web. O HTTP é executado em dois programas: um cliente e outro servidor. Os dois, executados em sistemas finais diferentes, conversam entre si por meio da troca de mensagens HTTP. O HTTP define a estrutura dessas mensagens e o modo como o cliente e o servidor as trocam.  
   Nesse contexto, podemos definir o protocolo HTTP como sendo:

|  |  |  |
| --- | --- | --- |
|  |  | .Um protocolo simples que permite que a aplicação envie dados encapsulados em pacotes até o destino. |
|  |  | .Uma linguagem de código utilizada para desenvolver páginas web. |
|  |  | .Um protocolo utilizado para controle de transmissão de pacote de dados entre duas aplicações. |
|  |  | .Um protocolo que define como os pacotes devem ser transmitidos entre servidores web. |
|  |  | .O protocolo que define os padrões e as regras para troca de informações entre servidores que abrigam sites e computadores. |

**1 pontos**

**PERGUNTA 3**

1. O FTP é um protocolo que tem por objetivo transferir arquivos. Um exemplo de como isso é feito, de modo geral, é quando o FTP cria um canal de comunicação entre o computador (cliente FTP) e o servidor que hospeda o seu *site* . Assim, você pode enviar os arquivos que deseja ou fazer modificações no arquivo. No entanto, apenas o FTP não oferece serviços de segurança. Para isso, existe o FTPS.  
   Nesse contexto, sobre o FTPS, analise as asserções a seguir:  
   I. O FTPS utiliza a tecnologia SSL ( *Secure Socket Layer* ) para prover segurança na transferência de arquivos.  
   PORQUE  
   II. O SSL fornece segurança na comunicação através da implementação de criptografia.  
   A respeito dessas asserções, analise suas relações e assinale a opção correta.

|  |  |  |
| --- | --- | --- |
|  |  | As asserções I e II são proposições verdadeiras, e a II é uma justificativa correta da primeira. |
|  |  | A asserção I é uma proposição falsa, e a II é uma proposição verdadeira. |
|  |  | A asserção I é uma proposição verdadeira, e a II é uma proposição falsa. |
|  |  | As asserções I e II são proposições verdadeiras, mas a II não é uma justificativa correta da I. |
|  |  | As asserções I e II são proposições falsas. |

**1 pontos**

**PERGUNTA 4**

1. O protocolo permite que um cliente liste os usuários um a um e em seguida envie uma única cópia de uma mensagem para todos os usuários da lista. Isto é, um cliente envia “Eu tenho uma mensagem de correio para o usuário A” e o servidor responde “OK” ou “O usuário não existe aqui”. Na verdade, cada mensagem ao servidor desse protocolo começa com um código numérico, algo como “250 OK” ou “550 O usuário não existe aqui”.  
   De qual protocolo estamos falando?

|  |  |  |
| --- | --- | --- |
|  |  | FTP. |
|  |  | SMTP. |
|  |  | TFTP. |
|  |  | MIME. |
|  |  | POP. |

**1 pontos**

**PERGUNTA 5**

1. Devido ao esgotamento de endereços disponíveis do IPv4, foi necessário começar a criar, no início da década de 1990, uma nova versão do endereço IP, chamada de IPv6. Enquanto o IPv4 possui 32 *bits* , o IPv6 possui 128 *bits* , o que permite um número de endereços absurdamente maior, resolvendo de vez o problema de limitação de endereços IP na internet. O IPv6 não trabalha com octetos em decimal como o IPv4, em vez disso, trabalha com números em hexadecimal. Além disso, o IPv6 acrescenta as funcionalidades de criptografia de pacotes que garantem a integridade, confidencialidade e autenticidade, avançando no quesito segurança na internet.  
   Nesse contexto, o IPv6 é formado por:

|  |  |  |
| --- | --- | --- |
|  |  | . 16 quartetos de 2 *bytes*, representados por 16 *bits*. |
|  |  | . 8 quartetos de 16 *bits*, representados por 16 *bytes*. |
|  |  | . 8 octetos de 16 *bits*, representados por 8 *bytes*. |
|  |  | . 8 blocos de 4 *bits*, representados por 126 *bits*. |
|  |  | . 4 octetos de 8 *bytes*, representados por 32 *bytes*. |

**1 pontos**

**PERGUNTA 6**

1. Antes de surgir o protocolo DHCP, era utilizado o servidor BOOTP ( *Bootstrap Protocol* ), que usava uma atribuição de endereço fixo na qual o servidor tinha um banco de dados de endereço IPv4 que deveria ser atribuído a cada *host*na rede. O servidor BOOTP precisava de uma administração manual, na qual o administrador de rede deveria configurar o servidor para conhecer o endereço IP do computador. Com o tempo houve a necessidade de mudar esse conceito, evoluindo para o DHCP (COMER, 2016).  
   COMER, D. E. **Redes de computadores e internet** . 6. ed. Porto Alegre: Bookman, 2016.  
   Sobre o DHCP, analise as asserções e a relação entre elas:  
   I.          O DHCP tem como conceito oportunizar que um computador obtenha um endereço IP automaticamente.  
   PORQUE  
   II.       O DHCP é um servidor em que o administrador precisa configurar de forma manual para obter o endereço de IP de um computador.  
   Agora, assinale a alternativa correta.

|  |  |  |
| --- | --- | --- |
|  |  | .As asserções I e II são proposições verdadeiras, e a II é uma justificativa correta da I. |
|  |  | .As asserções I e II são proposições verdadeiras, mas a II não é uma justificativa correta da primeira. |
|  |  | .A asserção I é uma proposição verdadeira, e a II é uma proposição falsa. |
|  |  | .A asserção I é uma proposição falsa, e a II é uma proposição verdadeira. |
|  |  | .As asserções I e II são proposições falsas. |

**1 pontos**

**PERGUNTA 7**

1. Quando uma rede de computadores está sendo configurada, é preciso atribuir endereços IP de forma individual às interfaces de *hosts* e roteadores. O administrador de rede pode configurar os endereços IP no roteador de forma remota através de um *software* de gerenciamento de rede. Apesar dessa tarefa de configuração de endereços IP poder ser feita de forma manual, atualmente, é comumente feita através da configuração de um DHCP.  
   Sobre o protocolo DHCP, analise as asserções:  
   I.                    O administrador de rede pode configurar o DHCP para que um *host*  
   receba um único endereço IP cada vez que se conectar.  
   II.                 O administrador de rede pode configurar o DHCP para receber um endereço diferente sempre que se conectar, porém, que seja temporário.  
   III.              O DHCP permite descobrir a máscara de sub-rede a qual está conectada.  
   IV.              O DHCP permite descobrir o endereço do roteador *default gateway* da rede.  
   V.                O DHCP permite descobrir o DNS de todos os dispositivos conectados à rede.  
   Agora, assinale a alternativa que apresenta as asserções corretas.

|  |  |  |
| --- | --- | --- |
|  |  | . III, IV e V. |
|  |  | .I, II e III. |
|  |  | .II, IV e V. |
|  |  | .I, III e IV. |
|  |  | . I, II, III e IV. |

**1 pontos**

**PERGUNTA 8**

1. Quando servidores web são replicados, um conjunto de endereços IP fica associado a um único nome canônico e contido no banco de dados do DNS. Quando clientes consultam um nome mapeado para um conjunto de endereços, o DNS responde com o conjunto inteiro de endereços IP, mas faz um rodízio da ordem deles dentro de cada resposta.  
   Como um cliente em geral envia sua mensagem de requisição HTTP ao endereço IP que ocupa o primeiro lugar no conjunto, o rodízio de DNS distribui o tráfego entre os servidores replicados. Essa definição se refere ao serviço oferecido pelo DNS de:

|  |  |  |
| --- | --- | --- |
|  |  | .Apelidos de servidor de correio, quando é atribuído um apelido para um endereço de e-mail. |
|  |  | Nome canônico, que faz a distribuição de apelidos para um nome difícil de lembrar. |
|  |  | .*Aliasing*, definindo nomes diferentes para cada nome canônico de servidores diversos. |
|  |  | .Apelido de hosts, quando um apelido é necessário para atribuir ao host, pois o nome canônico é maior e mais complicado. |
|  |  | .Distribuição de carga, necessária quando páginas web movimentadas são replicadas em vários servidores. |

**1 pontos**

**PERGUNTA 9**

1. O protocolo IP atua na camada de internet do modelo TCP-IP e permite que sejam elaborados e transportados os datagramas IP, isto é, os pacotes de dados. O protocolo IP define a representação de um datagrama, seu encaminhamento e seu envio, considerando que os datagramas IP são independentes. Os datagramas são dados encapsulados, que incluem informações sobre seu transporte, tal como a informação do endereço IP de origem e de destino. Quem analisa esses datagramas são os roteadores para, então, encaminhá-los pela rede. A tabela a seguir mostra como o datagrama aparece.

|  |
| --- |
| **32 *bits*** |

|  |  |  |  |
| --- | --- | --- | --- |
| Versão (4 *bits* ) | Comprimento do cabeçalho (4 *bits* ) | Tipo de serviço (8 *bits* ) | Comprimento total (16 *bits* ) |

|  |  |  |
| --- | --- | --- |
| Identificação (16 *bits* ) | Bandeira (3 *bits* ) | Desfasamento de fragmento (13 *bits* ) |
| Duração de vida (8 *bits* ) | Protocolo (8 *bits* ) | Soma de controle de cabeçalho ( *checksum* ) (16 *bits* ) |

|  |
| --- |
| Endereço IP de origem (32 *bits* ) |
| Endereço de IP de destino (32 *bits* ) |
| Dados |

1. Fonte: Elaborado pela autora, 2019.  
   Sobre o formato do endereço IP que faz parte da estrutura de um datagrama, escolha a alternativa que apresenta o formato correto do IPv4.

|  |  |  |
| --- | --- | --- |
|  |  | .O IPv4 é formado por 6 blocos de 2 *bytes*, representados por 32 *bytes*. |
|  |  | .O IPv4 é formado por 4 octetos de 16 *bits*, representados por 8 *bytes*. |
|  |  | . O IPv4 é formado por 4 octetos de 8 *bits*, representados por 4 *bytes*. |
|  |  | .O IPv4 é formado por 8 blocos de 4 *bits*, representados por 32 *bits*. |
|  |  | .O IPv4 é formado por 14 octetos de 2 *bytes*, representados por 16 *bits*. |

**1 pontos**

**PERGUNTA 10**

1. HTTP é um sistema de mão única. Os arquivos são transportados do servidor para o navegador do cliente. Somente o conteúdo da página web é transferido para exibição no navegador. Após essa transferência em determinada requisição, o servidor HTTP tem determinado comportamento e por isso o HTTP é chamado de protocolo sem estado. Nesse contexto, analise as asserções a seguir:  
      
   (1)   Os arquivos são transferidos, mas não baixados, de modo que não são copiados para a memória do dispositivo receptor.  
   PORQUE  
   (2)   O servidor não tem memória, por isso não guarda o objeto que recebe.  
      
   Agora, sobre as asserções, assinale a alternativa correta:

|  |  |  |
| --- | --- | --- |
|  |  | .A asserção I é uma proposição verdadeira, e a II é uma proposição falsa. |
|  |  | .As asserções I e II são proposições verdadeiras, mas a II não é uma justificativa correta da primeira. |
|  |  | .As asserções I e II são proposições falsas. |
|  |  | .A asserção I é uma proposição falsa, e a II é uma proposição verdadeira. |
|  |  | .As asserções I e II são proposições verdadeiras, e a II é uma justificativa correta da I. |