

Questões Comentadas com Resolução Assistida

Comunicação de Dados

OSI, TCP/IP, Topologias, Cabeamento

1. Os serviços de controle de diálogo, gerenciamento de token e sincronização pertencem à camada de

- A. Rede.
- B. Enlace de Dados.
- C. Sessão.
- D. Apresentação.
- E. Transporte.

1.Os serviços de controle de diálogo, gerenciamento de token e sincronização pertencem à camada de

A. Rede.

B. Enlace de Dados.



C. Sessão.

D. Apresentação.

E. Transporte.

2.A topologia de uma rede local de computadores determina a forma pela qual as diversas estações estarão interconectadas. Em relação às topologias de redes locais, analise as afirmativas a seguir:

I - Em uma topologia em anel todos os nós (ou estações) são ligados a um nó central através do qual todos os dados passam.

II - Uma rede organizada em estrela é configurada por uma série de estações ligadas em série, formando uma malha fechada.

III - Na topologia em barramento, quando um computador estiver a transmitir um sinal, toda a rede fica ocupada; se outro computador tentar enviar outro sinal ao mesmo tempo, ocorre uma colisão e é preciso reiniciar a transmissão.

Está correto o que se afirma em:

- A. somente I;
- B. somente II;
- C. somente III;
- D. somente I e III;
- E. I, II e III.

Está correto o que se afirma em:

A. somente I;

B. somente II;

 C. somente III;

D. somente I e III;

E. I, II e III.

3.A troca de estrutura de dados feita de forma abstrata, em conjunto com uma codificação padrão, possibilita a comunicação entre computadores com representações distintas de dados.

A camada do modelo de referência OSI (Open Systems Interconnection), que está relacionada à sintaxe e à semântica das informações transmitidas, é a camada de

- A. transmissão
- B. adaptação
- C. apresentação
- D. transformação
- E. compatibilidade

3.A troca de estrutura de dados feita de forma abstrata, em conjunto com uma codificação padrão, possibilita a comunicação entre computadores com representações distintas de dados.

A camada do modelo de referência OSI (Open Systems Interconnection), que está relacionada à sintaxe e à semântica das informações transmitidas, é a camada de

- A. transmissão
- B. adaptação
-  C. apresentação
- D. transformação
- E. compatibilidade

4. Os cabos de cobre blindados melhoram o desempenho das redes de dados quando amenizam o efeito das interferências, reduzindo o volume de quadros corrompidos e retransmissões. Os cabos da categoria STP (Shielded Twisted Pair) reduzem o crosstalk e melhoram a tolerância à distância, pois

- A. usam uma blindagem individual para cada par de cabos.
- B. envolvem todos os pares do cabo com uma blindagem única.
- C. usam uma blindagem individual para cada par de cabos e também envolvem todos os pares do cabo com uma blindagem única.
- D. separam todos os pares do cabo com um separador plástico maleável.
- E. aumentam a espessura de todos os pares do cabo.

4.Os cabos de cobre blindados melhoram o desempenho das redes de dados quando amenizam o efeito das interferências, reduzindo o volume de quadros corrompidos e retransmissões. Os cabos da categoria STP (Shielded Twisted Pair) reduzem o crosstalk e melhoram a tolerância à distância, pois



- A. usam uma blindagem individual para cada par de cabos.
- B. envolvem todos os pares do cabo com uma blindagem única.
- C. usam uma blindagem individual para cada par de cabos e também envolvem todos os pares do cabo com uma blindagem única.
- D. separam todos os pares do cabo com um separador plástico maleável.
- E. aumentam a espessura de todos os pares do cabo.

Cabos Blindados

- FTP (Foiled Twisted Pair)
 - Blindagem envolve todos os pares do cabo



- STP (Shielded Twisted Pair)
 - Blindagem individual para cada par de cabos



- SSTP (Screened Shielded Twisted Pair)
 - blindagem individual para cada par de cabos com uma segunda blindagem externa



5.No modelo de referência ISO OSI, as camadas que formam a sub-rede de comunicação são

- A. Enlace de Dados, Rede, Física.
- B. Enlace de Dados, Rede, Transporte.
- C. Transporte, Sessão, Física.
- D. Sessão, Transporte, Rede.
- E. Sessão, Rede, Física.

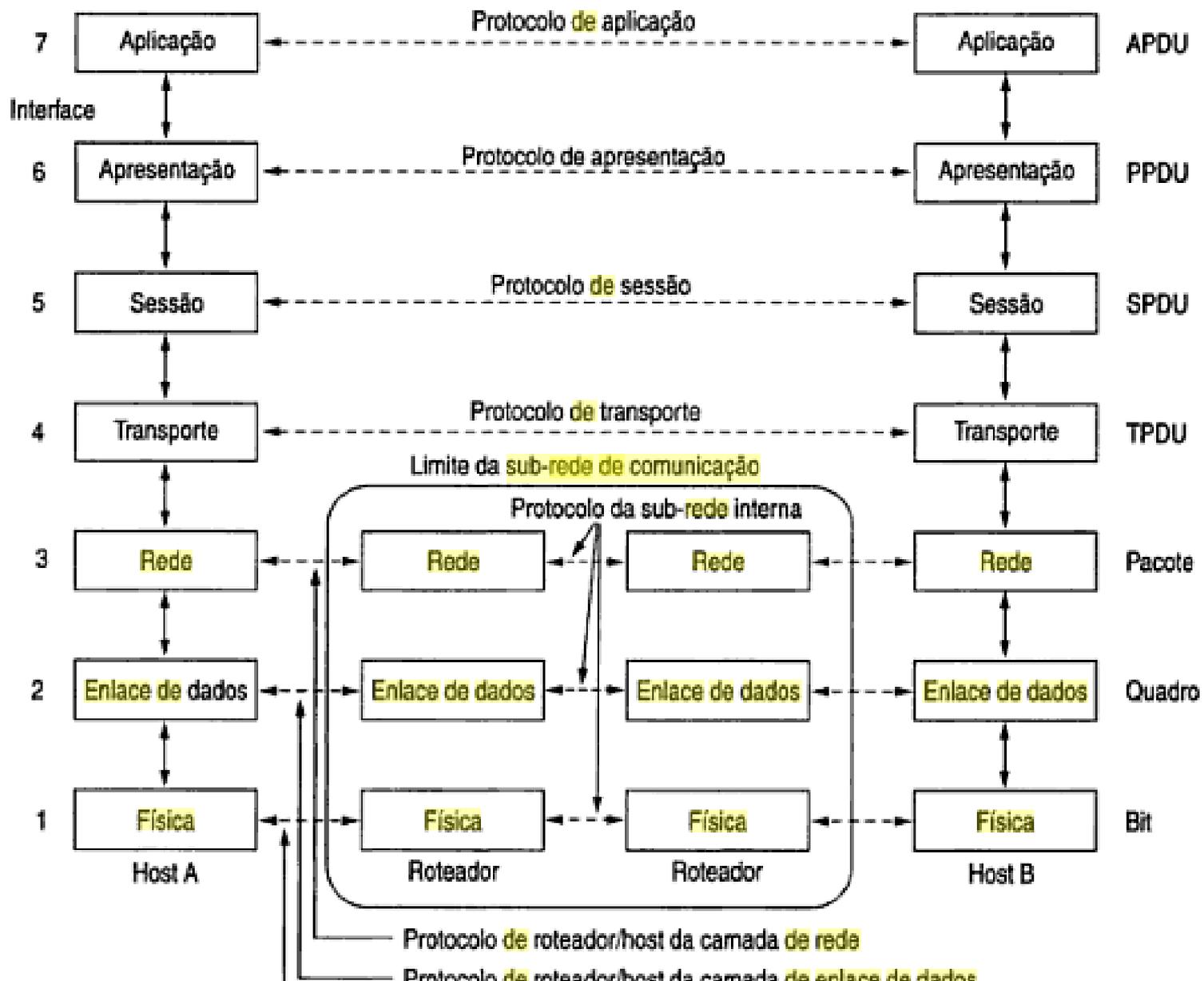
5.No modelo de referência ISO OSI, as camadas que formam a sub-rede de comunicação são



- A. Enlace de Dados, Rede, Física.
- B. Enlace de Dados, Rede, Transporte.
- C. Transporte, Sessão, Física.
- D. Sessão, Transporte, Rede.
- E. Sessão, Rede, Física.

Camada

Nome da unidade intercambiada



6. São camadas do modelo de referência TCP/IP:

- A. Apresentação, Transporte.
- B. Rede, Enlace de Dados.
- C. Host/rede, Inter-redes.
- D. Transporte, Física.
- E. Aplicação, Sessão.

6. São camadas do modelo de referência TCP/IP:

A. Apresentação, Transporte.

B. Rede, Enlace de Dados.



C. Host/rede, Inter-redes.

D. Transporte, Física.

E. Aplicação, Sessão.

<http://www.itnerante.com.br/profiles/blogs/afinal-o-tcp-ip-possui-quantas-camadas>

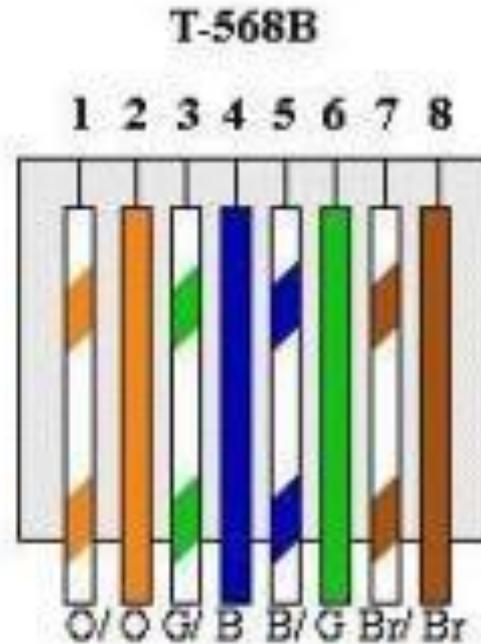
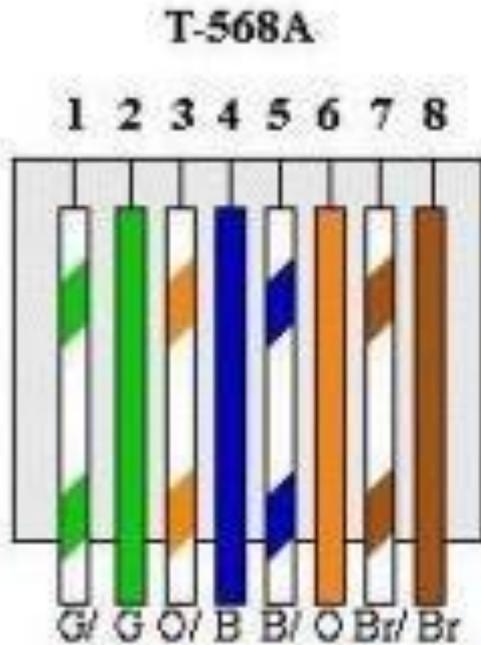
7. Deseja-se construir um segmento de cabo de rede de 5 m, utilizando cabo de pares trançados CAT-5 com terminação T568A da norma TIA/EIA 568, em ambas as extremidades. Nesse caso, a sequência de cores dos fios, iniciando-se no pino 1 até o pino 8 do conector RJ45, é:

- A. branco/laranja, laranja, branco/azul, verde, branco/verde, azul, branco/marrom e marrom.
- B. branco/laranja, laranja, branco/verde, azul, branco/azul, verde, branco/marrom e marrom.
- C. branco/laranja, laranja, branco/verde, verde, branco/azul, azul, branco/marrom e marrom.
- D. branco/verde, verde, branco/laranja, azul, branco/azul, laranja, branco/marrom e marrom.
- E. branco/verde, verde, branco/laranja, laranja, branco/azul, azul, branco/marrom e marrom.

7. Deseja-se construir um segmento de cabo de rede de 5 m, utilizando cabo de pares trançados CAT-5 com terminação T568A da norma TIA/EIA 568, em ambas as extremidades. Nesse caso, a sequência de cores dos fios, iniciando-se no pino 1 até o pino 8 do conector RJ45, é:

- A. branco/laranja, laranja, branco/azul, verde, branco/verde, azul, branco/marrom e marrom.
- B. branco/laranja, laranja, branco/verde, azul, branco/azul, verde, branco/marrom e marrom.
- C. branco/laranja, laranja, branco/verde, verde, branco/azul, azul, branco/marrom e marrom.
-  D. branco/verde, verde, branco/laranja, azul, branco/azul, laranja, branco/marrom e marrom.
- E. branco/verde, verde, branco/laranja, laranja, branco/azul, azul, branco/marrom e marrom.

T-568A e T-568B



8. Uma das camadas do modelo de referência OSI (Open Systems Interconnection) é a responsável por oferecer o controle de diálogo, que visa a determinar quem deve transmitir em cada momento; o gerenciamento de token, que visa a impedir que duas partes tentem executar a mesma operação crítica ao mesmo tempo; e o controle de sincronização, que visa a possibilitar a continuidade da comunicação a partir do ponto onde ocorreu uma falha.

A camada que oferece essas funcionalidades é a camada de

- A. aplicação
- B. apresentação
- C. sessão
- D. transporte
- E. rede

8. Uma das camadas do modelo de referência OSI (Open Systems Interconnection) é a responsável por oferecer o controle de diálogo, que visa a determinar quem deve transmitir em cada momento; o gerenciamento de token, que visa a impedir que duas partes tentem executar a mesma operação crítica ao mesmo tempo; e o controle de sincronização, que visa a possibilitar a continuidade da comunicação a partir do ponto onde ocorreu uma falha.

A camada que oferece essas funcionalidades é a camada de

- A. aplicação
- B. apresentação
-  C. sessão
- D. transporte
- E. rede

9. Dois computadores que se encontram a uma distância de 10 metros um do outro estão conectados por um único enlace cuja taxa de transmissão é 56 kbps. Um pacote de tamanho L bits é enviado de um computador para o outro através desse enlace.

O tempo de transmissão do pacote, em segundos, é

A. $L / 56$

B. $L / (10 * 56)$

C. $L / (56 * 1000)$

D. $(10 * L) / (56 * 1000)$

E. $(1000 * L) / (10 * 56)$

9. Dois computadores que se encontram a uma distância de 10 metros um do outro estão conectados por um único enlace cuja taxa de transmissão é 56 kbps. Um pacote de tamanho L bits é enviado de um computador para o outro através desse enlace.

O tempo de transmissão do pacote, em segundos, é

A. $L / 56$

B. $L / (10 * 56)$

 C. $L / (56 * 1000)$

D. $(10 * L) / (56 * 1000)$

E. $(1000 * L) / (10 * 56)$

10.O Modelo OSI (Open Systems Interconnection) é um modelo de referência que sintetiza, de modo abstrato, a estrutura funcional dos elementos envolvidos na comunicação entre sistemas abertos de comunicação de dados. Esse modelo é dividido em sete camadas sobrepostas, de modo que cada camada executa um conjunto bem definido de funções. A utilização de algoritmos de roteamento para determinar rotas apropriadas para transferência de unidades de dados entre endereços de rede é função da camada:

- A. transporte;
- B. sessão;
- C. enlace;
- D. rede;
- E. física.

10.O Modelo OSI (Open Systems Interconnection) é um modelo de referência que sintetiza, de modo abstrato, a estrutura funcional dos elementos envolvidos na comunicação entre sistemas abertos de comunicação de dados. Esse modelo é dividido em sete camadas sobrepostas, de modo que cada camada executa um conjunto bem definido de funções. A utilização de algoritmos de roteamento para determinar rotas apropriadas para transferência de unidades de dados entre endereços de rede é função da camada:

- A. transporte;
- B. sessão;
- C. enlace;
-  D. rede;
- E. física.

11.O Modelo de Referência ISO OSI (Open Systems Interconnection) trata da interconexão de sistemas abertos. A camada do modelo OSI responsável pelo gerenciamento de token é a camada de

- A. Gerenciamento.
- B. Transporte.
- C. Apresentação.
- D. Aplicação.
- E. Sessão.

11.0 Modelo de Referência ISO OSI (Open Systems Interconnection) trata da interconexão de sistemas abertos. A camada do modelo OSI responsável pelo gerenciamento de token é a camada de

A. Gerenciamento.

B. Transporte.

C. Apresentação.

D. Aplicação.

 E. Sessão.

12.A função do nível físico do modelo OSI é

- A. fornecer mecanismos de verificação utilizados pelo nível posterior.
- B. permitir o fluxo de bits agregados segundo critérios estabelecidos pela topologia da rede.
- C. permitir o envio de uma cadeia de bytes pela rede, verificando seu significado e sua composição em bits.
- D. controlar o envio de mensagens pela rede, preocupando-se com o seu significado e com a forma como esses bits são agregados.
- E. permitir o envio de uma cadeia de bits pela rede sem se preocupar com o seu significado ou com a forma como esses bits são agregados.

12.A função do nível físico do modelo OSI é

- A. fornecer mecanismos de verificação utilizados pelo nível posterior.
- B. permitir o fluxo de bits agregados segundo critérios estabelecidos pela topologia da rede.
- C. permitir o envio de uma cadeia de bytes pela rede, verificando seu significado e sua composição em bits.
- D. controlar o envio de mensagens pela rede, preocupando-se com o seu significado e com a forma como esses bits são agregados.
-  E. permitir o envio de uma cadeia de bits pela rede sem se preocupar com o seu significado ou com a forma como esses bits são agregados.

13.O técnico de informática do Tribunal de Contas foi incumbido de realizar o cabeamento, utilizando cabo UTP, entre a sala de comunicação e o novo computador, localizados no mesmo andar. Considerando a Norma TIA/EIA 568B, o máximo comprimento do trecho de cabo permitido para essa instalação é, em metros,

- A. 5.
- B. 10.
- C. 50.
- D. 90.
- E. 200.

13.O técnico de informática do Tribunal de Contas foi incumbido de realizar o cabeamento, utilizando cabo UTP, entre a sala de comunicação e o novo computador, localizados no mesmo andar. Considerando a Norma TIA/EIA 568B, o máximo comprimento do trecho de cabo permitido para essa instalação é, em metros,

A. 5.

B. 10.

C. 50.

 D. 90.

E. 200.

GABARITO



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

Questões Comentadas com Resolução Assistida

Tecnologia e Protocolos de Redes
Locais e Redes sem Fio

Ethernet, IEEE 802.11

1. Após a instalação do novo Access Point, o administrador de uma rede local de computadores foi incumbido de atualizar o esquema de segurança de todos os Access Points padrão IEEE 802.11g. Considerando o WPA e o WPA2, o administrador deve escolher o

- A. WPA2 devido à maior segurança oferecida pelo uso do AES.
- B. WPA2 devido ao melhor algoritmo de segurança utilizado, que é o RC4.
- C. WPA2 devido ao menor tempo de processamento requerido se comparado com o WPA.
- D. WPA devido ao maior tamanho permitido para a chave se comparado ao WPA2.
- E. WPA, pois utiliza o esquema de chaves dinâmicas enquanto o WPA2 utiliza o esquema de chaves fixas.

1. Após a instalação do novo Access Point, o administrador de uma rede local de computadores foi incumbido de atualizar o esquema de segurança de todos os Access Points padrão IEEE 802.11g. Considerando o WPA e o WPA2, o administrador deve escolher o



- A. WPA2 devido à maior segurança oferecida pelo uso do AES.
- B. WPA2 devido ao melhor algoritmo de segurança utilizado, que é o RC4.
- C. WPA2 devido ao menor tempo de processamento requerido se comparado com o WPA.
- D. WPA devido ao maior tamanho permitido para a chave se comparado ao WPA2.
- E. WPA, pois utiliza o esquema de chaves dinâmicas enquanto o WPA2 utiliza o esquema de chaves fixas.

2.O quadro Ethernet (IEEE 802.3) contém dois endereços, um para o destino e um para a origem. Para um quadro ser aceito por todas as estações da rede local, o endereço destino deve conter o endereço de difusão (broadcast), representado em hexadecimal como

- A. 00:00:00:00:00:00
- B. 11:11:11:11:11:11
- C. 01:01:01:01:01:01
- D. 1F:1F:1F:1F:1F:1F
- E. FF:FF:FF:FF:FF:FF

2.O quadro Ethernet (IEEE 802.3) contém dois endereços, um para o destino e um para a origem. Para um quadro ser aceito por todas as estações da rede local, o endereço destino deve conter o endereço de difusão (broadcast), representado em hexadecimal como

A. 00:00:00:00:00:00

B. 11:11:11:11:11:11

C. 01:01:01:01:01:01

D. 1F:1F:1F:1F:1F:1F

E. FF:FF:FF:FF:FF:FF

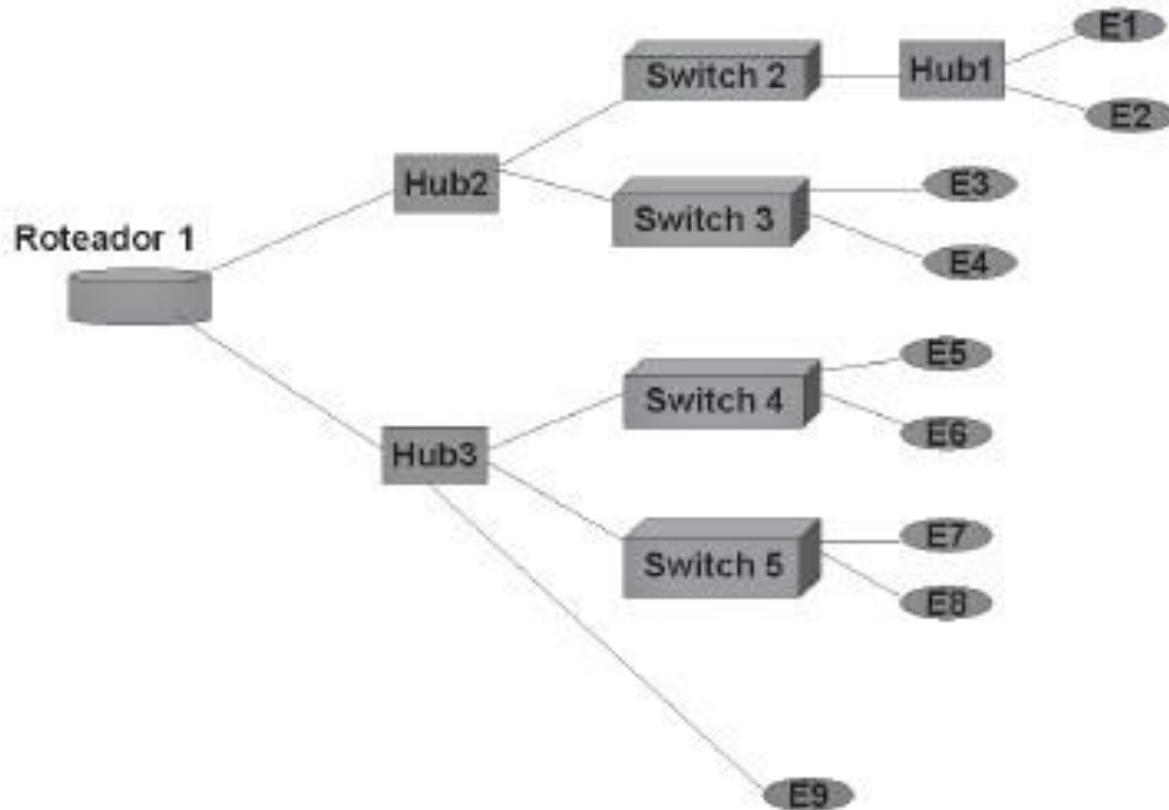
3. Um ponto de acesso de rede sem fio, configurado como ponte, está ligado fisicamente a uma porta de um comutador Fast-Ethernet. Nesse ambiente, o tamanho máximo dos dados dentro de um quadro Fast-Ethernet que o ponto de acesso consegue interpretar é:

- A. 576 bytes;
- B. 768 bytes;
- C. 1500 bytes;
- D. 2048 bytes;
- E. 4000 bytes.

3. Um ponto de acesso de rede sem fio, configurado como ponte, está ligado fisicamente a uma porta de um comutador Fast-Ethernet. Nesse ambiente, o tamanho máximo dos dados dentro de um quadro Fast-Ethernet que o ponto de acesso consegue interpretar é:

- A. 576 bytes;
- B. 768 bytes;
-  C. 1500 bytes;
- D. 2048 bytes;
- E. 4000 bytes.

4. Seja uma rede Ethernet utilizando roteador, switches (que funcionam como ponte) e hubs para conectar as estações (identificadas por E1 até E9), montada com a seguinte topologia:



4.Com base no esquema acima indicado, quantos domínios de colisão e quantos domínios de broadcast podem ser identificados, respectivamente, nessa rede?

A. 2 e 7

B. 2 e 9

C. 4 e 6

D. 7 e 2

E. 9 e 2

4.Com base no esquema acima indicado, quantos domínios de colisão e quantos domínios de broadcast podem ser identificados, respectivamente, nessa rede?

A. 2 e 7

B. 2 e 9

C. 4 e 6

D. 7 e 2

 E. 9 e 2

5.A Ethernet de gigabit foi ratificada pelo IEEE em 1998, com o nome 802.3z. A Ethernet de gigabit com 4 pares de UTP categoria 5 e distância máxima de segmento de 100m é denominada

- A. 1000Base-CX.
- B. 1000Base-T.
- C. 1000Base-LX.
- D. 1000Base-UTP.
- E. 1000Base-SX.

5.A Ethernet de gigabit foi ratificada pelo IEEE em 1998, com o nome 802.3z. A Ethernet de gigabit com 4 pares de UTP categoria 5 e distância máxima de segmento de 100m é denominada

A. 1000Base-CX.



B. 1000Base-T.

C. 1000Base-LX.

D. 1000Base-UTP.

E. 1000Base-SX.

6.O uso do protocolo WEP para proteger uma rede sem fio não é recomendável porque

- A. esse protocolo só permite utilizar chaves simétricas de até 40 bits de tamanho.
- B. os vetores de inicialização do protocolo WEP possuem tamanho limitado (24 bits).
- C. esse protocolo utiliza o algoritmo RC4 de criptografia, reconhecidamente vulnerável.
- D. a informação sobre o SSID da rede não é criptografada pelo WEP.
- E. esse protocolo armazena no ponto de acesso (access point) a chave privada do usuário.

6.O uso do protocolo WEP para proteger uma rede sem fio não é recomendável porque

- A. esse protocolo só permite utilizar chaves simétricas de até 40 bits de tamanho.
-  B. os vetores de inicialização do protocolo WEP possuem tamanho limitado (24 bits).
- C. esse protocolo utiliza o algoritmo RC4 de criptografia, reconhecidamente vulnerável.
- D. a informação sobre o SSID da rede não é criptografada pelo WEP.
- E. esse protocolo armazena no ponto de acesso (access point) a chave privada do usuário.

7.A Seção 3 do atual padrão IEEE 802.3 é derivada dos adendos IEEE 802.3ab e IEEE 802.3z. Segundo essa parte do padrão, conhecida como Gigabit Ethernet, há duas famílias de interfaces físicas Gigabit Ethernet: 1000BASE-T e 1000BASE-X. A família 1000BASE-X é composta por três opções: 1000BASE-SX, 1000BASE-LX e 1000BASE-CX.

Para as opções 1000BASE-SX e 1000BASE-LX pode-se utilizar as fibras

A.

1000BASE-SX	1000BASE-LX
monomodo, apenas	multimodo, apenas

B.

multimodo, apenas	monomodo, apenas
-------------------	------------------

C.

multimodo, apenas	monomodo e multimodo
-------------------	----------------------

D.

monomodo e multimodo	monomodo, apenas
----------------------	------------------

E.

monomodo e multimodo	monomodo e multimodo
----------------------	----------------------

7.A Seção 3 do atual padrão IEEE 802.3 é derivada dos adendos IEEE 802.3ab e IEEE 802.3z. Segundo essa parte do padrão, conhecida como Gigabit Ethernet, há duas famílias de interfaces físicas Gigabit Ethernet: 1000BASE-T e 1000BASE-X. A família 1000BASE-X é composta por três opções: 1000BASE-SX, 1000BASE-LX e 1000BASE-CX.

Para as opções 1000BASE-SX e 1000BASE-LX pode-se utilizar as fibras

A.

1000BASE-SX	1000BASE-LX
monomodo, apenas	multimodo, apenas

B.

multimodo, apenas	monomodo, apenas
-------------------	------------------

C.

multimodo, apenas	monomodo e multimodo
-------------------	----------------------

D.

monomodo e multimodo	monomodo, apenas
----------------------	------------------

E.

monomodo e multimodo	monomodo e multimodo
----------------------	----------------------



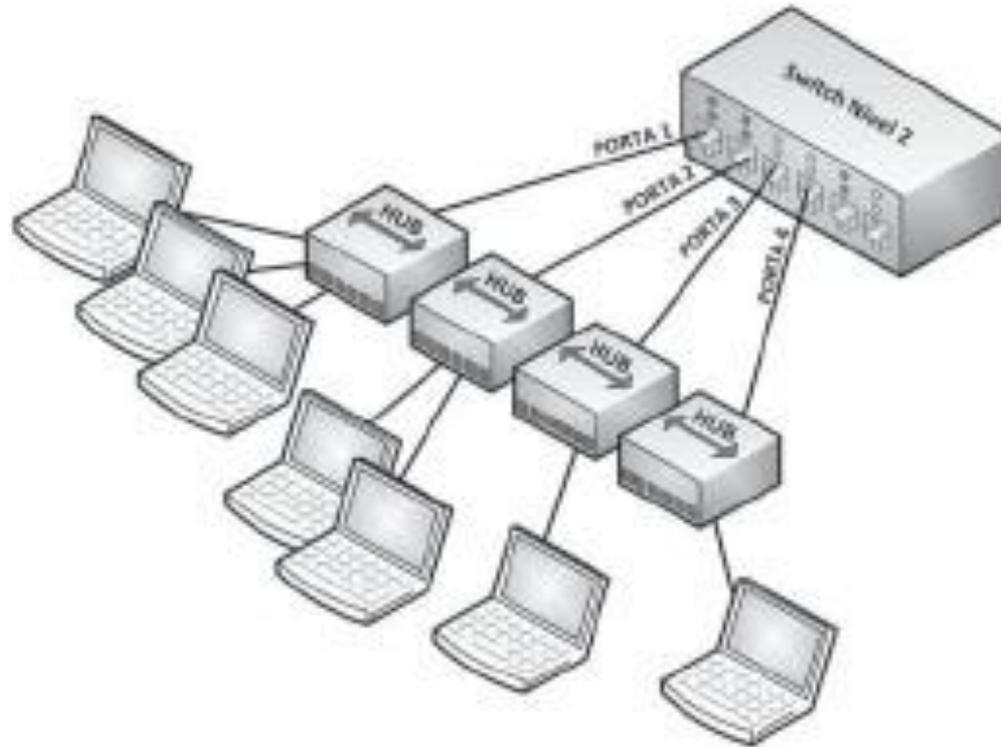
8.No quadro Ethernet,

- A. o campo de dados (10 a 46 bytes) carrega o endereço TCP.
- B. a finalidade do campo verificação de equivalência cíclica (CEC) é permitir que o adaptador receptor, o adaptador P, detecte quadros equivalentes.
- C. a finalidade do campo verificação de redundância cíclica (CRC) é permitir que o adaptador receptor, o adaptador B, detecte se algum erro foi introduzido no quadro.
- D. o campo de endereço (46 a 3500 bytes) carrega o verificador de login.
- E. a finalidade do campo verificação de redundância compartilhada (SRC) é verificar o compartilhamento do quadro B.

8.No quadro Ethernet,

- A. o campo de dados (10 a 46 bytes) carrega o endereço TCP.
- B. a finalidade do campo verificação de equivalência cíclica (CEC) é permitir que o adaptador receptor, o adaptador P, detecte quadros equivalentes.
-  C. a finalidade do campo verificação de redundância cíclica (CRC) é permitir que o adaptador receptor, o adaptador B, detecte se algum erro foi introduzido no quadro.
- D. o campo de endereço (46 a 3500 bytes) carrega o verificador de login.
- E. a finalidade do campo verificação de redundância compartilhada (SRC) é verificar o compartilhamento do quadro B.

9. Em uma determinada empresa, uma rede local foi construída utilizando a configuração da Figura abaixo.



9.O Switch de Nível 2 foi configurado de forma que as portas 1 e 2 estão associadas à VLAN 12, enquanto as demais portas estão associadas à VLAN 15.

As quantidades de domínios de colisão e de difusão nessa rede são, respectivamente,

A. 7 e 6

B. 6 e 6

C. 4 e 4

D. 4 e 2

E. 2 e 2

9.O Switch de Nível 2 foi configurado de forma que as portas 1 e 2 estão associadas à VLAN 12, enquanto as demais portas estão associadas à VLAN 15.

As quantidades de domínios de colisão e de difusão nessa rede são, respectivamente,

A. 7 e 6

B. 6 e 6

C. 4 e 4

 D. 4 e 2

E. 2 e 2

10.O padrão IEEE 802.3 prevê, ao longo de seu texto e das várias opções especificadas, dois modos de operação: o half-duplex e o full-duplex.

As opções de interface 100BASE-T, 1000BASE-T, 10GBASE-T, 10GBASE-LX preveem, respectivamente, o uso dos modos

- A. tanto half-duplex como full-duplex para todas as opções
- B. tanto half-duplex como full-duplex para as três primeiras opções e apenas full-duplex para a quarta opção
- C. tanto half-duplex como full-duplex para as duas primeiras opções e apenas full-duplex para as outras duas opções
- D. apenas half-duplex para a primeira opção, tanto halfduplex como full-duplex para a segunda opção e apenas full-duplex para a terceira e quarta opções.
- E. apenas half-duplex para a primeira opção, tanto half- -duplex como full-duplex para a segunda e terceira opções, e apenas full duplex para a quarta opção.

10.O padrão IEEE 802.3 prevê, ao longo de seu texto e das várias opções especificadas, dois modos de operação: o half-duplex e o full-duplex.

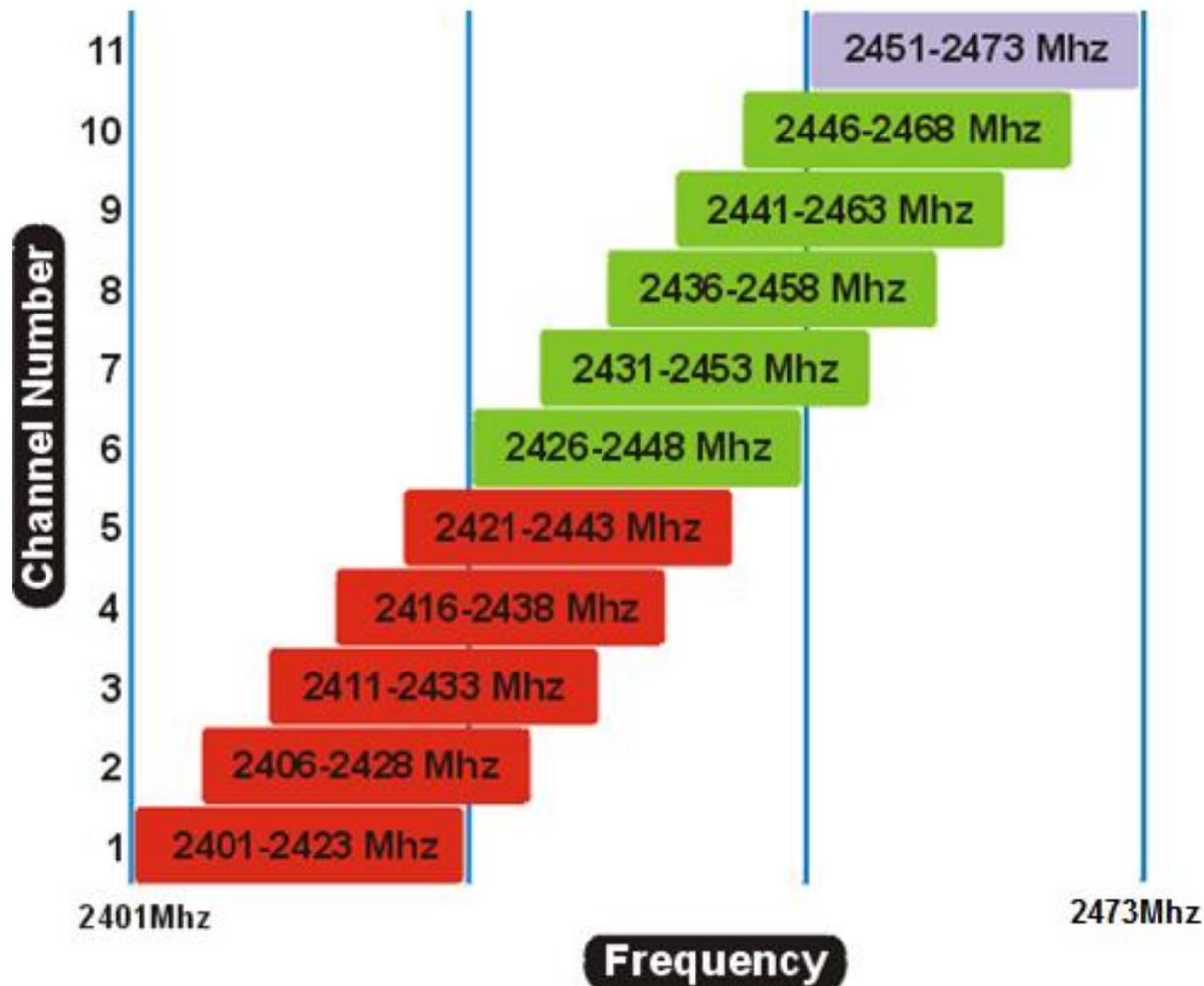
As opções de interface 100BASE-T, 1000BASE-T, 10GBASE-T, 10GBASE-LX preveem, respectivamente, o uso dos modos

- A. tanto half-duplex como full-duplex para todas as opções
- B. tanto half-duplex como full-duplex para as três primeiras opções e apenas full-duplex para a quarta opção
-  C. tanto half-duplex como full-duplex para as duas primeiras opções e apenas full-duplex para as outras duas opções
- D. apenas half-duplex para a primeira opção, tanto halfduplex como full-duplex para a segunda opção e apenas full-duplex para a terceira e quarta opções.
- E. apenas half-duplex para a primeira opção, tanto half- -duplex como full-duplex para a segunda e terceira opções, e apenas full duplex para a quarta opção.

11.O administrador de uma rede local de computadores deve instalar um novo Access Point, padrão IEEE 802.11g, em um andar da empresa com 10 salas, para melhorar a qualidade do sinal de acesso. Sabendo-se que no local já existem dois Access Points instalados nas extremidades do conjunto de salas, um configurado para o canal 1 e outro para o canal 6, o novo Access Point, a ser instalado entre os dois Access Points, deve ser configurado para utilizar o canal

- A. 3.
- B. 5.
- C. 8.
- D. 11.
- E. 15.

Canais Wi-Fi



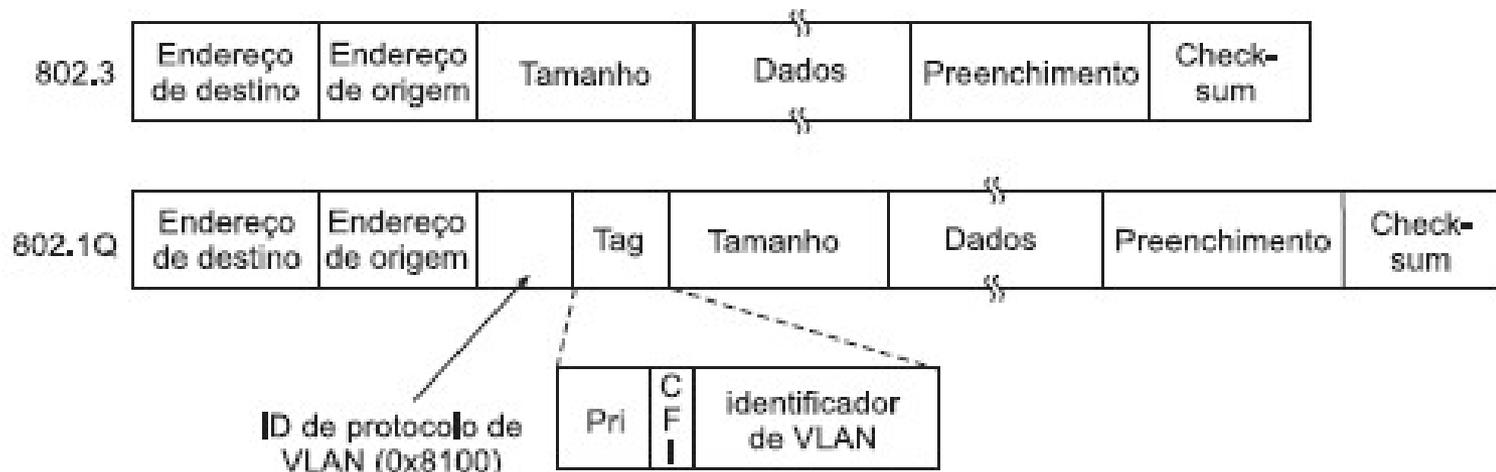
11.O administrador de uma rede local de computadores deve instalar um novo Access Point, padrão IEEE 802.11g, em um andar da empresa com 10 salas, para melhorar a qualidade do sinal de acesso. Sabendo-se que no local já existem dois Access Points instalados nas extremidades do conjunto de salas, um configurado para o canal 1 e outro para o canal 6, o novo Access Point, a ser instalado entre os dois Access Points, deve ser configurado para utilizar o canal

- A. 3.
- B. 5.
- C. 8.
-  D. 11.
- E. 15.

12.O padrão IEEE-802.1Q usa um mecanismo denominado tagging que insere um campo tag de 4 bytes no frame original, entre os campos endereço de origem e tamanho. Nesse contexto, a figura mostra os formatos de quadros Ethernet 802.3 e 802.1q. O campo Identificador de VLAN tem 12 bits e identifica, de forma única, a VLAN à qual o frame pertence. Ao campo Identificador de VLAN, deve ser atribuído, exclusivamente, qualquer valor na faixa $0 \leq M \leq K$.

Então, K é igual a

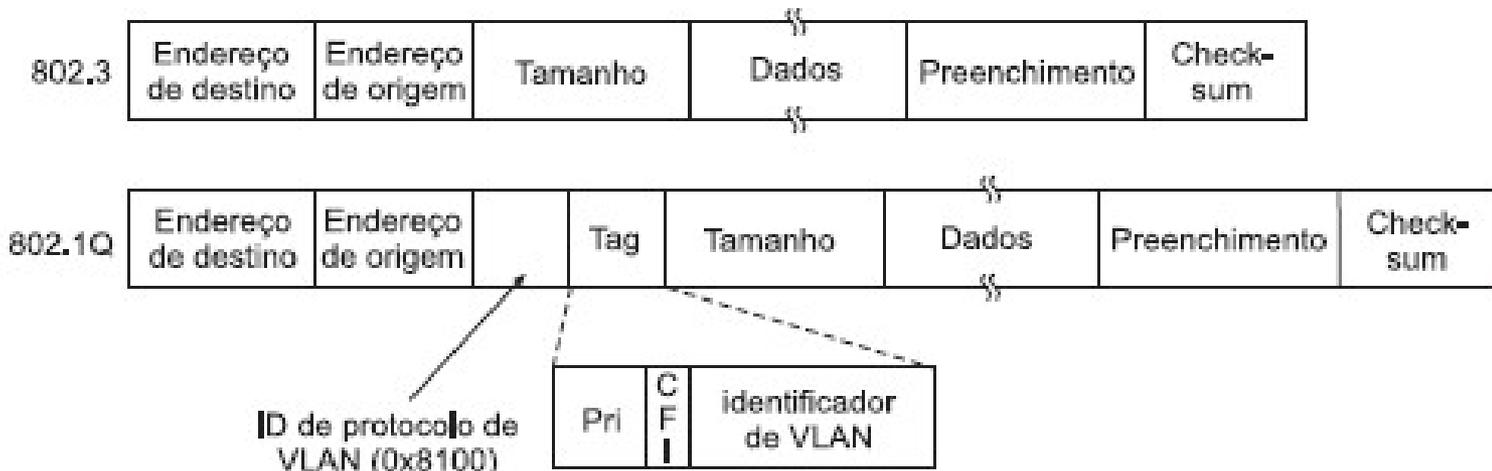
- A. 255
- B. 511
- C. 1023
- D. 2047
- E. 4095



12.O padrão IEEE-802.1Q usa um mecanismo denominado tagging que insere um campo tag de 4 bytes no frame original, entre os campos endereço de origem e tamanho. Nesse contexto, a figura mostra os formatos de quadros Ethernet 802.3 e 802.1q. O campo Identificador de VLAN tem 12 bits e identifica, de forma única, a VLAN à qual o frame pertence. Ao campo Identificador de VLAN, deve ser atribuído, exclusivamente, qualquer valor na faixa .

Então, K é igual a

- A. 255
- B. 511
- C. 1023
- D. 2047
- E. 4095



13. Redes IEEE-802.11 podem ser usadas de dois modos, descritos a seguir.

Cada cliente está associado a um ponto de acesso, que, por sua vez, está conectado a outra rede. Vários pontos de acesso podem ser conectados, normalmente por um sistema de distribuição, para formar uma rede estendida.

Não existe ponto de acesso. É uma coleção de computadores que estão associados de maneira que possam enviar quadros diretamente uns aos outros.

Esses modos são, respectivamente, de

- A. acesso múltiplo e rede anycast
- B. acesso múltiplo e rede ad hoc
- C. infraestrutura e rede multicast
- D. infraestrutura e rede ad hoc
- E. infraestrutura e rede anycast

13. Redes IEEE-802.11 podem ser usadas de dois modos, descritos a seguir.

Cada cliente está associado a um ponto de acesso, que, por sua vez, está conectado a outra rede. Vários pontos de acesso podem ser conectados, normalmente por um sistema de distribuição, para formar uma rede estendida.

Não existe ponto de acesso. É uma coleção de computadores que estão associados de maneira que possam enviar quadros diretamente uns aos outros.

Esses modos são, respectivamente, de

- A. acesso múltiplo e rede anycast
- B. acesso múltiplo e rede ad hoc
- C. infraestrutura e rede multicast
- D. infraestrutura e rede ad hoc
- E. infraestrutura e rede anycast



GABARITO



1. A
2. E
3. C
4. E
5. B
6. B
7. C
8. C
9. D

10. C
11. D
12. E
13. D

Questões Comentadas com Resolução Assistida

Elementos de Interconexão e
Roteamento

Hub, Switch, Bridge, Roteador
OSPF, RIP, BGP

1. O OSPF é um protocolo criado em resposta à demanda por tabelas de roteamento dinâmicas. Nele, o roteamento é realizado dentro e não entre sistemas autônomos.

Por suas características, esse protocolo é considerado roteamento

- A. intradomínio e estado de enlace
- B. intradomínio e vetor distância
- C. intradomínio e vetor de rota
- D. interdomínio e estado de enlace
- E. interdomínio e vetor distância

1. O OSPF é um protocolo criado em resposta à demanda por tabelas de roteamento dinâmicas. Nele, o roteamento é realizado dentro e não entre sistemas autônomos.

Por suas características, esse protocolo é considerado roteamento

-  A. intradomínio e estado de enlace
- B. intradomínio e vetor distância
- C. intradomínio e vetor de rota
- D. interdomínio e estado de enlace
- E. interdomínio e vetor distância

2.Repetidores, pontes e roteadores são dispositivos de comutação de uso comum em redes de computadores. Em relação a esses dispositivos de comutação, analise as afirmativas a seguir:

I. Repetidores operam na camada física e não reconhecem quadros, pacotes ou cabeçalhos, somente volts.

II. Um roteador opera na camada de transporte e tem várias linhas de entrada que ele conecta eletricamente. Os quadros de dados que chegam em quaisquer dessas linhas são enviados a todas as outras.

III. Pontes operam na camada de enlace de dados e são utilizadas para conectar duas ou mais LANs.

Está correto o que se afirma em:

- A. somente I;
- B. somente II;
- C. somente III;
- D. somente I e III;
- E. I, II e III.

Está correto o que se afirma em:

A. somente I;

B. somente II;

C. somente III;

 D. somente I e III;

E. I, II e III.

3. Os dispositivos de rede que baseiam seu roteamento em endereços de quadro são:

- A. Gateways e switches.
- B. Switches e pontes.
- C. Repetidores e switches.
- D. Roteadores e pontes.
- E. Roteadores e hubs.

3. Os dispositivos de rede que baseiam seu roteamento em endereços de quadro são:

A. Gateways e switches.



B. Switches e pontes.

C. Repetidores e switches.

D. Roteadores e pontes.

E. Roteadores e hubs.

4.O objetivo de um protocolo de roteamento é suprir a informação necessária para o roteador fazer o roteamento quando o destino não é diretamente alcançável. O Routing Information Protocol (RIP) é um protocolo de roteamento que opera com base no algoritmo de

- A. inundação
- B. estado de enlace
- C. vetor de distância
- D. shortest path first
- E. dijkstra

4.O objetivo de um protocolo de roteamento é suprir a informação necessária para o roteador fazer o roteamento quando o destino não é diretamente alcançável. O Routing Information Protocol (RIP) é um protocolo de roteamento que opera com base no algoritmo de

A. inundação

B. estado de enlace

 C. vetor de distância

D. shortest path first

E. dijkstra

5.É um dispositivo utilizado em redes de computadores para reencaminhar módulos (frames) entre os diversos nós. Além disso, segmenta a rede internamente, sendo que a cada porta corresponde um domínio de colisão diferente, o que significa que não haverá colisões entre os pacotes de segmentos diferentes. Este dispositivo é o

- A. Roteador.
- B. Hub.
- C. Switch.
- D. Concentrador.
- E. Ponte.

5. É um dispositivo utilizado em redes de computadores para reencaminhar módulos (frames) entre os diversos nós. Além disso, segmenta a rede internamente, sendo que a cada porta corresponde um domínio de colisão diferente, o que significa que não haverá colisões entre os pacotes de segmentos diferentes. Este dispositivo é o

- A. Roteador.
- B. Hub.
-  C. Switch.
- D. Concentrador.
- E. Ponte.

6. Uma vantagem comum a todos os switches com funcionalidades de camada 3, em relação a dispositivos de camada 2, é

- A. realizar o controle de envio de mensagens broadcast.
- B. disponibilizar uma grande variedade de interfaces para conexão, como, por exemplo, ATM, TokenRing e Ethernet.
- C. permitir a configuração remota do switch, acessando seu endereço IP.
- D. permitir a implementação de NAT (Network Address Translation).
- E. permitir o roteamento de mensagens com base na definição da aplicação.

6. Uma vantagem comum a todos os switches com funcionalidades de camada 3, em relação a dispositivos de camada 2, é



- A. realizar o controle de envio de mensagens broadcast.
- B. disponibilizar uma grande variedade de interfaces para conexão, como, por exemplo, ATM, TokenRing e Ethernet.
- C. permitir a configuração remota do switch, acessando seu endereço IP.
- D. permitir a implementação de NAT (Network Address Translation).
- E. permitir o roteamento de mensagens com base na definição da aplicação.

7. Analise as situações de interconexões em rede a seguir.

I. Dois escritórios são ligados por equipamento atuando na camada de enlace do modelo OSI, sendo sua presença transparente para os computadores presentes na rede.

II. Vários departamentos estão ligados por um equipamento que faz filtragem de tráfego, isolando os pacotes broadcast de um departamento para outro.

III. Dois equipamentos estão ligados, via rede sem fio, a grande distância, por meio de um equipamento que estende o sinal no nível físico.

Os equipamentos usados nos itens I, II e III são, respectivamente,

- A. roteador, switch e hub.
- B. comutador, hub e repetidor.
- C. ponte, roteador e repetidor.
- D. roteador, ponte e switch.
- E. repetidor, roteador e hub.

7. Analise as situações de interconexões em rede a seguir.

I. Dois escritórios são ligados por equipamento atuando na camada de enlace do modelo OSI, sendo sua presença transparente para os computadores presentes na rede.

II. Vários departamentos estão ligados por um equipamento que faz filtragem de tráfego, isolando os pacotes broadcast de um departamento para outro.

III. Dois equipamentos estão ligados, via rede sem fio, a grande distância, por meio de um equipamento que estende o sinal no nível físico.

Os equipamentos usados nos itens I, II e III são, respectivamente,

- A. roteador, switch e hub.
- B. comutador, hub e repetidor.
-  C. ponte, roteador e repetidor.
- D. roteador, ponte e switch.
- E. repetidor, roteador e hub.

8.Quando se comparam switches de níveis 2 e 3, observa-se que, por suas funcionalidades, eles são referenciados em camadas diferentes do modelo OSI/ISO e encaminham frames ou pacotes utilizando tipos distintos de endereços.

Nesse contexto, os switches de nível 2 atuam numa camada e utilizam endereços conhecidos, denominados, respectivamente,

- A. enlace e IP
- B. enlace e MAC
- C. rede e IP
- D. rede e MAC
- E. transporte e MAC

8.Quando se comparam switches de níveis 2 e 3, observa-se que, por suas funcionalidades, eles são referenciados em camadas diferentes do modelo OSI/ISO e encaminham frames ou pacotes utilizando tipos distintos de endereços.

Nesse contexto, os switches de nível 2 atuam numa camada e utilizam endereços conhecidos, denominados, respectivamente,

A. enlace e IP



B. enlace e MAC

C. rede e IP

D. rede e MAC

E. transporte e MAC

9.Os protocolos de roteamento podem ser classificados em interiores, quando são utilizados para trocar informações dentro de Sistemas Autônomos (AS), ou exteriores, quando realizam conexões entre AS.

Um importante protocolo exterior é o

A. EIGRP

B. OSPF

C. IGRP

D. RIP

E. BGP

9.Os protocolos de roteamento podem ser classificados em interiores, quando são utilizados para trocar informações dentro de Sistemas Autônomos (AS), ou exteriores, quando realizam conexões entre AS.

Um importante protocolo exterior é o

A. EIGRP

B. OSPF

C. IGRP

D. RIP

E. BGP

10.O Modelo de Referência para Interconexão de Sistemas Abertos (RM-OSI ou, simplesmente, modelo OSI) da International Organization for Standardization (ISO) é dividido em 7 camadas ou níveis.

Com base nesse modelo, considerando-se um switch de camada 2 (layer 2) e um switch de camada 3 (layer 3), tem-se que

- A. apenas o switch de camada 2 possui a possibilidade de configuração de VLANs.
- B. apenas o switch de camada 3 pode fazer roteamento.
- C. apenas o switch de camada 3 possui a possibilidade de configuração de VLANs.
- D. ambos podem realizar roteamento.
- E. nenhum deles pode realizar roteamento.

10.O Modelo de Referência para Interconexão de Sistemas Abertos (RM-OSI ou, simplesmente, modelo OSI) da International Organization for Standardization (ISO) é dividido em 7 camadas ou níveis.

Com base nesse modelo, considerando-se um switch de camada 2 (layer 2) e um switch de camada 3 (layer 3), tem-se que

- A. apenas o switch de camada 2 possui a possibilidade de configuração de VLANs.
-  B. apenas o switch de camada 3 pode fazer roteamento.
- C. apenas o switch de camada 3 possui a possibilidade de configuração de VLANs.
- D. ambos podem realizar roteamento.
- E. nenhum deles pode realizar roteamento.

11.O padrão utilizado na internet atualmente é o modelo de camadas TCP/IP, ou como alguns autores o chamam, modelo internet. A arquitetura do modelo de camadas TCP/IP é composta por cinco camadas, sendo cada uma responsável por um serviço, e com as suas funções específicas. Numa transmissão de dados, por exemplo, o envio dos dados das eleições, que é feito via internet, cada uma das camadas tem a sua importância e seu respectivo protocolo responsável por cada ação realizada nessas transmissões. Na camada de rede encontram-se os protocolos de roteamento, e dois protocolos têm sido os mais utilizados para o roteamento dentro de um sistema autônomo na internet, conhecidos como IGP (Internet Gateway Protocols - Protocolos de Roteadores Internos).

11. Sobre esses dois protocolos, assinale a alternativa correta.

- A. OSPF (Open Shortest Path File) e BGP (Border Gateway Protocol).
- B. RIP (Routing Information Protocol) e OSPF (Open Shortest Path File).
- C. BGP (Border Gateway Protocol) e IS-IS (Intermediate-System-to-Intermediate-System).
- D. IS-IS (Intermediate-System-to-Intermediate-System) e RIP (Routing Information Protocol).

11.Sobre esses dois protocolos, assinale a alternativa correta.

- A. OSPF (Open Shortest Path File) e BGP (Border Gateway Protocol).
-  B. RIP (Routing Information Protocol) e OSPF (Open Shortest Path File).
- C. BGP (Border Gateway Protocol) e IS-IS (Intermediate-System-to-Intermediate-System).
- D. IS-IS (Intermediate-System-to-Intermediate-System) e RIP (Routing Information Protocol).

12. Switches de nível 2 empregam tecnologia Fast Ethernet na camada link de dados, operam com base em um determinado tipo de endereço e permitem tráfego de dados até uma velocidade máxima específica. O tipo de endereço e a velocidade máxima desses switches são, respectivamente,

- A. IP/lógico e 1 Gbps
- B. IP/lógico e 100 Mbps
- C. MAC/físico e 10 Gbps
- D. MAC/físico e 100 Mbps
- E. MAC/físico e 1 Gbps

12. Switches de nível 2 empregam tecnologia Fast Ethernet na camada link de dados, operam com base em um determinado tipo de endereço e permitem tráfego de dados até uma velocidade máxima específica. O tipo de endereço e a velocidade máxima desses switches são, respectivamente,

- A. IP/lógico e 1 Gbps
- B. IP/lógico e 100 Mbps
- C. MAC/físico e 10 Gbps
-  D. MAC/físico e 100 Mbps
- E. MAC/físico e 1 Gbps

13. Protocolo de roteamento “open”, publicamente disponível, usa algoritmo Link State, com disseminação de pacote LS, mapa de topologia em cada nó e cálculo de rota usando Algoritmo de Dijkstra. Assinale a alternativa que contempla corretamente o protocolo de roteamento que se encaixa na especificação acima.

- A. HELLO.
- B. OSPF - Open Shortest Path First.
- C. IGP - Internet Gateway Protocol.
- D. RIP - Routing Information Protocol.
- E. IGRP - Internet Router Gateway Protocol.

13. Protocolo de roteamento “open”, publicamente disponível, usa algoritmo Link State, com disseminação de pacote LS, mapa de topologia em cada nó e cálculo de rota usando Algoritmo de Dijkstra. Assinale a alternativa que contempla corretamente o protocolo de roteamento que se encaixa na especificação acima.

A. HELLO.

 B. OSPF - Open Shortest Path First.

C. IGP - Internet Gateway Protocol.

D. RIP - Routing Information Protocol.

E. IGRP - Internet Router Gateway Protocol.

14. Uma empresa comprou um equipamento de conexão de rede, mas ele não funcionou corretamente.

O equipamento deveria atender às seguintes especificações:

- fazer uso do sistema de endereçamento lógico;
- permitir interligações de redes com arquiteturas diferentes (por exemplo, rede Token Ring com uma rede Ethernet) e com a internet;
- trabalhar na camada três do modelo OSI/ISO e com a fragmentação dos datagramas recebidos.

O equipamento que deveria ser comprado para atender a essas características é um (a)

- A. hub
- B. roteador
- C. ponte
- D. repetidor
- E. switch simples

14. Uma empresa comprou um equipamento de conexão de rede, mas ele não funcionou corretamente.

O equipamento deveria atender às seguintes especificações:

- fazer uso do sistema de endereçamento lógico;
- permitir interligações de redes com arquiteturas diferentes (por exemplo, rede Token Ring com uma rede Ethernet) e com a internet;
- trabalhar na camada três do modelo OSI/ISO e com a fragmentação dos datagramas recebidos.

O equipamento que deveria ser comprado para atender a essas características é um (a)

- A. hub
- B. roteador
- C. ponte
- D. repetidor
- E. switch simples



15.O protocolo de roteamento que funciona transformando o conjunto de redes, roteadores e linhas reais em um grafo orientado, no qual se atribui um custo (distância, retardo etc.) a cada arco, para, em seguida, calcular o caminho mais curto com base nos pesos dos arcos é o

- A. IP.
- B. OSPF.
- C. AODV.
- D. IPX.
- E. RIP.

15.O protocolo de roteamento que funciona transformando o conjunto de redes, roteadores e linhas reais em um grafo orientado, no qual se atribui um custo (distância, retardo etc.) a cada arco, para, em seguida, calcular o caminho mais curto com base nos pesos dos arcos é o

A. IP.

 B. OSPF.

C. AODV.

D. IPX.

E. RIP.

GABARITO



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

13. B
14. B
15. B

Questões Comentadas com Resolução Assistida

Nível de Rede TCP/IP

IPv4, IPv6, Mascaramento, Classes

1. Quantos hosts VÁLIDOS estão disponíveis em cada subrede do endereço 192.168.11.0 máscara 255.255.255.192?

A. 26

B. 62

C. 64

D. 63

1. Quantos hosts VÁLIDOS estão disponíveis em cada subrede do endereço 192.168.11.0 máscara 255.255.255.192?

A. 26

B. 62

C. 64

D. 63

$$10000000 = 128$$

$$2^1 = 2$$

$$11000000 = 192$$

$$2^2 = 4$$

$$11100000 = 224$$

$$2^3 = 8$$

$$11110000 = 240$$

$$2^4 = 16$$

$$11111000 = 248$$

$$2^5 = 32$$

$$11111100 = 252$$

$$2^6 = 64$$

$$11111110 = 254$$

$$2^7 = 128$$

$$11111111 = 255$$

$$2^8 = 256$$

1. Quantos hosts VÁLIDOS estão disponíveis em cada subrede do endereço 192.168.11.0 máscara 255.255.255.192?

A. 26

 B. 62

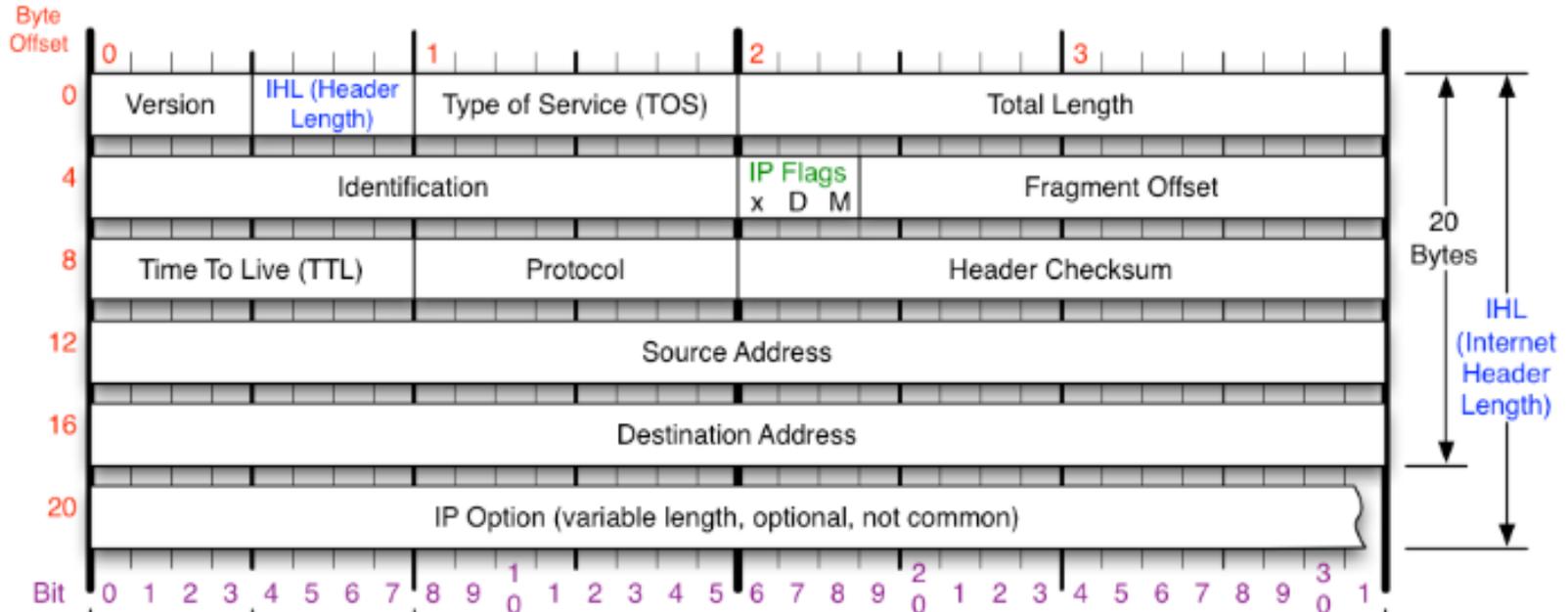
C. 64

D. 63

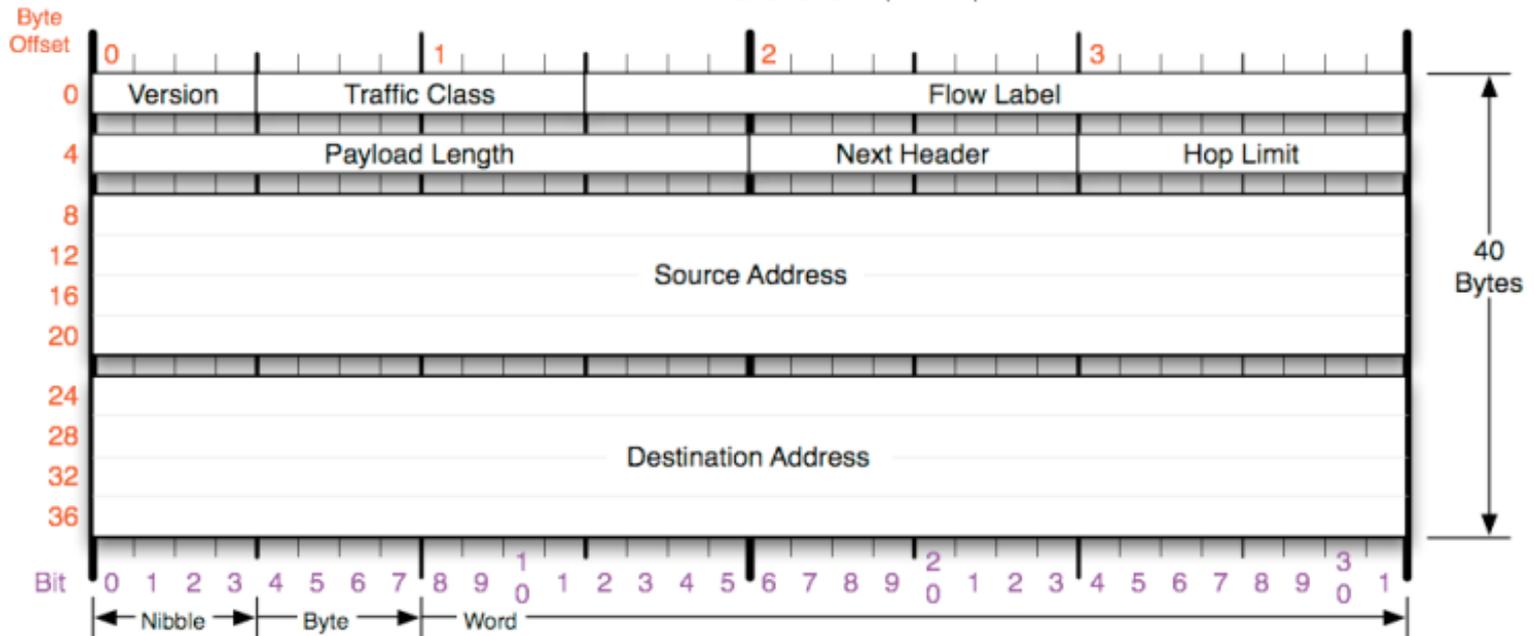
2.Com o crescimento de dispositivos conectados à internet, o número de endereços IPv4 disponíveis está praticamente esgotado. Algumas empresas ainda possuem alguns blocos de endereços IPv4, mas comercialmente já está difícil conseguir algum bloco para aquisição. Há muito já se fala nesse problema e, por isso, foi criado um novo protocolo, oIPv6, que deverá se tornar o padrão de fato para a internet e as redes em geral. Com a entrada do IPv6 uma das mudanças está no tamanho do endereço, passando dos atuais 32 bits para 128 bits. O IPv4 utiliza quatro octetos,agrupados três a três, ao passo que o IPv6 utiliza caracteres hexadecimais, agrupados em oito conjuntos de quatro caracteres. Um data grama IPv6 possui algumas diferenças, se comparado com o seu antecessor. Alguns campos foram suprimidos no IPv6, tornando o data grama mais simples. São campos do novo data grama IPv6, EXCETO:

- A. Versão e classe de tráfego.
- B. Próximo cabeçalho e limite de saltos.
- C. Rótulo de fluxo e comprimento de carga útil.
- D. Fragmentação/remontagem e soma de verificação do cabeçalho.

IPv4 Header



IP Header (version 6)



2.Com o crescimento de dispositivos conectados à internet, o número de endereços IPv4 disponíveis está praticamente esgotado. Algumas empresas ainda possuem alguns blocos de endereços IPv4, mas comercialmente já está difícil conseguir algum bloco para aquisição. Há muito já se fala nesse problema e, por isso, foi criado um novo protocolo, oIPv6, que deverá se tornar o padrão de fato para a internet e as redes em geral. Com a entrada do IPv6 uma das mudanças está no tamanho do endereço, passando dos atuais 32 bits para 128 bits. O IPv4 utiliza quatro octetos,agrupados três a três, ao passo que o IPv6 utiliza caracteres hexadecimais, agrupados em oito conjuntos de quatro caracteres. Um data grama IPv6 possui algumas diferenças, se comparado com o seu antecessor. Alguns campos foram suprimidos no IPv6, tornando o data grama mais simples. São campos do novo data grama IPv6, EXCETO:

- A. Versão e classe de tráfego.
- B. Próximo cabeçalho e limite de saltos.
- C. Rótulo de fluxo e comprimento de carga útil.
- D. Fragmentação/remontagem e soma de verificação do cabeçalho.



3.O cabeçalho do IPv6, ocasionalmente, precisa de alguns dos campos ausentes do IPv4. Desta forma, o IPv6 introduziu o conceito de cabeçalho de extensão. São cabeçalhos de extensão, EXCETO:

- A. Routing.
- B. Hop limit.
- C. Hop-by-hop options.
- D. Encrypted security payload.

3.O cabeçalho do IPv6, ocasionalmente, precisa de alguns dos campos ausentes do IPv4. Desta forma, o IPv6 introduziu o conceito de cabeçalho de extensão. São cabeçalhos de extensão, EXCETO:

A. Routing.

 B. Hop limit.

C. Hop-by-hop options.

D. Encrypted security payload.

<http://www.itnerante.com.br/profiles/blogs/ipv4-vs-ipv6-principais-mudan-as>

4.No conjunto de protocolos TCP/IP, o IP (Internet Protocol) é utilizado para o endereçamento dos dispositivos de rede e o roteamento das mensagens e, para facilitar o roteamento, o endereço IP é dividido em Classes. Um endereço IPv4 é identificado como de Classe B quando, no endereço IP,

- A. o primeiro bit à esquerda é 0.
- B. os dois primeiros bits à esquerda são 1 e 0.
- C. os dois primeiros bits à esquerda são 1 e 1.
- D. os dois primeiros bits à direita são 1 e 1.
- E. os três primeiros bits à direita são 1, 0 e 0.

Classes IP

Class	First Octet Range	Max Hosts	Format
A	1-126	16M	<p>NETID HOSTID</p> <p>0 </p> <p>1 Octet 3 Octets</p>
B	128-191	64K	<p>NETID HOSTID</p> <p>1 0 </p> <p>2 Octets 2 Octets</p>
C	192-223	254	<p>NETID HOSTID</p> <p>1 1 0 </p> <p>3 Octets 1 Octet</p>
D	224-239	N/A	<p>Multicast Address</p> <p>1 1 1 0</p>
E	240-255	N/A	<p>Experimental</p> <p>1 1 1 1</p>

4.No conjunto de protocolos TCP/IP, o IP (Internet Protocol) é utilizado para o endereçamento dos dispositivos de rede e o roteamento das mensagens e, para facilitar o roteamento, o endereço IP é dividido em Classes. Um endereço IPv4 é identificado como de Classe B quando, no endereço IP,

- A. o primeiro bit à esquerda é 0.
-  B. os dois primeiros bits à esquerda são 1 e 0.
- C. os dois primeiros bits à esquerda são 1 e 1.
- D. os dois primeiros bits à direita são 1 e 1.
- E. os três primeiros bits à direita são 1, 0 e 0.

5.A rede de dados de uma empresa utilizava a máscara de subendereço 255.255.255.224. Em determinado momento, o administrador da rede resolveu alterar a máscara para 255.255.255.192 em toda a rede da empresa.

Devido a essa mudança, a quantidade total de sub-redes disponíveis

- A. aumentará, e a quantidade total de endereços IP disponíveis por sub-rede também.
- B. aumentará, e a quantidade total de endereços IP disponíveis por sub-rede diminuirá.
- C. diminuirá, e a quantidade total de endereços IP disponíveis por sub-rede aumentará.
- D. diminuirá, e a quantidade total de endereços IP disponíveis por sub-rede também.
- E. permanecerá inalterada.

5.A rede de dados de uma empresa utilizava a máscara de subendereço 255.255.255.224. Em determinado momento, o administrador da rede resolveu alterar a máscara para 255.255.255.192 em toda a rede da empresa.

Devido a essa mudança, a quantidade total de sub-redes disponíveis

- A. aumentará, e a quantidade total de endereços IP disponíveis por sub-rede também.
- B. aumentará, e a quantidade total de endereços IP disponíveis por sub-rede diminuirá.
-  C. diminuirá, e a quantidade total de endereços IP disponíveis por sub-rede aumentará.
- D. diminuirá, e a quantidade total de endereços IP disponíveis por sub-rede também.
- E. permanecerá inalterada.

6. Em uma determinada rede local de computadores, os computadores possuem endereços IPs Classe C fixos e reais, ou seja, não é utilizado o recurso de NAT nessa rede. Considerando que o IP: 133.108.201.120 é um endereço válido nessa rede, outro IP válido é:

- A. 103.138.102.1.
- B. 133.108.101.120.
- C. 133.108.201.1.
- D. 133.208.201.120.
- E. 233.108.201.1.

6. Em uma determinada rede local de computadores, os computadores possuem endereços IPs Classe C fixos e reais, ou seja, não é utilizado o recurso de NAT nessa rede. Considerando que o IP: 133.108.201.120 é um endereço válido nessa rede, outro IP válido é:

A. 103.138.102.1.

B. 133.108.101.120.



C. 133.108.201.1.

D. 133.208.201.120.

E. 233.108.201.1.

7. Dividir uma rede de computadores em sub-rede é uma prática para lidar com limitações topológicas, para simplificar administração de redes ou, por vezes, para representar uma estrutura organizacional.

Considere que a seguinte máscara de sub-rede 255.255.252.0 foi utilizada para implementar a divisão em sub-redes. O número máximo de sub-redes é:

- A. 128
- B. 64
- C. 32
- D. 16
- E. 8

7. Dividir uma rede de computadores em sub-rede é uma prática para lidar com limitações topológicas, para simplificar administração de redes ou, por vezes, para representar uma estrutura organizacional.

Considere que a seguinte máscara de sub-rede 255.255.252.0 foi utilizada para implementar a divisão em sub-redes. O número máximo de sub-redes é:

- A. 128
-  B. 64
- C. 32
- D. 16
- E. 8

<http://www.itnerante.com.br/profiles/blogs/descontar-ou-n-o-descontar-duas-sub-redes-eis-a-quest-o>

8. Redes de computadores com acesso à internet operam com base nos protocolos da arquitetura TCP/IP.

O IP versão 4 emprega classes, dentre as quais a B que engloba endereços cujo primeiro octeto está enquadrado numa faixa que se inicia em 128 e termina em

- A. 143
- B. 159
- C. 175
- D. 191
- E. 223

Classes IP

Class	First Octet Range	Max Hosts	Format
A	1-126	16M	<p>NETID HOSTID</p> <p>0 </p> <p>1 Octet 3 Octets</p>
B	128-191	64K	<p>NETID HOSTID</p> <p>1 0 </p> <p>2 Octets 2 Octets</p>
C	192-223	254	<p>NETID HOSTID</p> <p>1 1 0 </p> <p>3 Octets 1 Octet</p>
D	224-239	N/A	<p>Multicast Address</p> <p>1 1 1 0</p>
E	240-255	N/A	<p>Experimental</p> <p>1 1 1 1</p>

8. Redes de computadores com acesso à internet operam com base nos protocolos da arquitetura TCP/IP.

O IP versão 4 emprega classes, dentre as quais a B que engloba endereços cujo primeiro octeto está enquadrado numa faixa que se inicia em 128 e termina em

A. 143

B. 159

C. 175

 D. 191

E. 223

9.O IPv6 trouxe novos protocolos em relação ao IPv4, como o Neighbor Discovery Protocol (NDP), que substitui a funcionalidade, presente no IPv4, do protocolo:

- A. DHCP;
- B. ARP;
- C. DNS;
- D. ICMP;
- E. RARP.

9.O IPv6 trouxe novos protocolos em relação ao IPv4, como o Neighbor Discovery Protocol (NDP), que substitui a funcionalidade, presente no IPv4, do protocolo:

A. DHCP;



B. ARP;

C. DNS;

D. ICMP;

E. RARP.

10.A camada de inter-rede da arquitetura TCP/IP pode emitir mensagens de sinalização que visam a informar sobre erros relacionados ao encaminhamento ou recebimento de pacotes. Essas mensagens fazem parte do

- A. Network Status Message Protocol
- B. Network Error Message Protocol
- C. Internet Error Message Protocol
- D. Internet Group Message Protocol
- E. Internet Control Message Protocol

10.A camada de inter-rede da arquitetura TCP/IP pode emitir mensagens de sinalização que visam a informar sobre erros relacionados ao encaminhamento ou recebimento de pacotes. Essas mensagens fazem parte do

- A. Network Status Message Protocol
- B. Network Error Message Protocol
- C. Internet Error Message Protocol
- D. Internet Group Message Protocol
-  E. Internet Control Message Protocol

11.No protocolo TCP/IP, as classes de endereços IP foram criadas para facilitar a distribuição dos endereços IP. Qual é o número máximo de dispositivos que a classe C de endereços IP pode endereçar, se descontados os endereços reservados?

A. 16.777.216

B. 65.536

C. 1.024

D. 254

E. 256

11.No protocolo TCP/IP, as classes de endereços IP foram criadas para facilitar a distribuição dos endereços IP. Qual é o número máximo de dispositivos que a classe C de endereços IP pode endereçar, se descontados os endereços reservados?

A. 16.777.216

B. 65.536

C. 1.024

 D. 254

E. 256

12. Na rede de microcomputadores de uma empresa, foi observado que há falta de endereços IPv4 para acesso à internet. Para solucionar esse problema, o responsável técnico pela rede decidiu implantar o recurso NAT, por meio do intervalo de endereços privados de classe B. Considerando que, conforme a notação CIDR, na classe B o intervalo é 172.16.0.0 - 172.31.255.255/12, qual a máscara de rede padrão nesse caso?

- A. 255.224.0.0
- B. 255.240.0.0
- C. 255.255.0.0
- D. 255.255.255.240
- E. 255.255.255.224

12. Na rede de microcomputadores de uma empresa, foi observado que há falta de endereços IPv4 para acesso à internet. Para solucionar esse problema, o responsável técnico pela rede decidiu implantar o recurso NAT, por meio do intervalo de endereços privados de classe B. Considerando que, conforme a notação CIDR, na classe B o intervalo é 172.16.0.0 - 172.31.255.255/12, qual a máscara de rede padrão nesse caso?

- A. 255.224.0.0
-  B. 255.240.0.0
- C. 255.255.0.0
- D. 255.255.255.240
- E. 255.255.255.224

13.No TCP/IP, o endereçamento é especificado pelo protocolo IP. De acordo com esse protocolo, cada nó da rede possui um endereço que, na versão IPv4, é composto por 32 bits. Comumente, tais endereços são divididos em cinco classes. O endereço IPv4, em notação decimal, 130.55.6.3 refere- -se à classe de endereço

- A. A
- B. B
- C. C
- D. D
- E. E

13.No TCP/IP, o endereçamento é especificado pelo protocolo IP. De acordo com esse protocolo, cada nó da rede possui um endereço que, na versão IPv4, é composto por 32 bits. Comumente, tais endereços são divididos em cinco classes. O endereço IPv4, em notação decimal, 130.55.6.3 refere- -se à classe de endereço

- A. A
- B. B
- C. C
- D. D
- E. E

14. Assinale a opção correta.

- A. O datagrama IP é encapsulado fora do quadro de camada de enlace para ser transportado de um roteador até o roteador seguinte.
- B. O datagrama IP não pode ser fragmentado em datagramas IP menores.
- C. O datagrama BSP pode ser fragmentado em dois datagramas BSM menores.
- D. O datagrama TCP/IP pode ser adicionado ao datagrama TMS.
- E. O datagrama IP é encapsulado dentro do quadro de camada de enlace para ser transportado de um roteador até o roteador seguinte.

14. Assinale a opção correta.

- A. O datagrama IP é encapsulado fora do quadro de camada de enlace para ser transportado de um roteador até o roteador seguinte.
- B. O datagrama IP não pode ser fragmentado em datagramas IP menores.
- C. O datagrama BSP pode ser fragmentado em dois datagramas BSM menores.
- D. O datagrama TCP/IP pode ser adicionado ao datagrama TMS.
-  E. O datagrama IP é encapsulado dentro do quadro de camada de enlace para ser transportado de um roteador até o roteador seguinte.

15. Um gerente de redes deseja configurar um servidor DHCP usando a faixa de endereços reservados para redes privadas da classe C entre 192.168.0.1 e 192.168.0.254, dividida em 4 sub-redes que não devem interferir entre si.

Que valores correspondem, respectivamente, ao endereço e à máscara de sub-rede, para a sub-rede que inclui o endereço 192.168.0.84 e que atendem a essa especificação?

- A. 192.168.0.64 e 255.255.255.0
- B. 192.168.0.64 e 255.255.255.128
- C. 192.168.0.64 e 255.255.255.192
- D. 192.168.0.65 e 255.255.255.128
- E. 192.168.0.65 e 255.255.255.192

15. Um gerente de redes deseja configurar um servidor DHCP usando a faixa de endereços reservados para redes privadas da classe C entre 192.168.0.1 e 192.168.0.254, dividida em 4 sub-redes que não devem interferir entre si.

Que valores correspondem, respectivamente, ao endereço e à máscara de sub-rede, para a sub-rede que inclui o endereço 192.168.0.84 e que atendem a essa especificação?

- | | | | |
|----|--------------------------------|----------------|-------------|
| A. | 192.168.0.64 e 255.255.255.0 | 10000000 = 128 | $2^1 = 2$ |
| B. | 192.168.0.64 e 255.255.255.128 | 11000000 = 192 | $2^2 = 4$ |
| C. | 192.168.0.64 e 255.255.255.192 | 11100000 = 240 | $2^3 = 8$ |
| D. | 192.168.0.65 e 255.255.255.128 | 11110000 = 248 | $2^4 = 16$ |
| E. | 192.168.0.65 e 255.255.255.192 | 11111000 = 252 | $2^5 = 32$ |
| | | 11111100 = 254 | $2^6 = 64$ |
| | | 11111110 = 254 | $2^7 = 128$ |
| | | 11111111 = 255 | $2^8 = 256$ |

15. Um gerente de redes deseja configurar um servidor DHCP usando a faixa de endereços reservados para redes privadas da classe C entre 192.168.0.1 e 192.168.0.254, dividida em 4 sub-redes que não devem interferir entre si.

Que valores correspondem, respectivamente, ao endereço e à máscara de sub-rede, para a sub-rede que inclui o endereço 192.168.0.84 e que atendem a essa especificação?

- A. 192.168.0.64 e 255.255.255.0
- B. 192.168.0.64 e 255.255.255.128
-  C. 192.168.0.64 e 255.255.255.192
- D. 192.168.0.65 e 255.255.255.128
- E. 192.168.0.65 e 255.255.255.192

16.No endereçamento IP, para implementar a divisão em sub-redes, o roteador principal precisa de uma máscara de sub-rede que indique a divisão entre:

- A. número de rede e a sub-rede adjacente.
- B. número de rede e a sub-rede subjacente.
- C. número de rede mais sub-rede e o host.
- D. número de rede e o host.
- E. número de sub-rede e o host.

16.No endereçamento IP, para implementar a divisão em sub-redes, o roteador principal precisa de uma máscara de sub-rede que indique a divisão entre:

- A. número de rede e a sub-rede adjacente.
- B. número de rede e a sub-rede subjacente.
-  C. número de rede mais sub-rede e o host.
- D. número de rede e o host.
- E. número de sub-rede e o host.

17.O Protocolo da Internet (IP) é responsável pelo repasse e endereçamento de pacotes. Dentre as características mais importantes introduzidas no protocolo IPv6, está a(o)

- A. expansão da capacidade de endereçamento
- B. flexibilização do comprimento do cabeçalho
- C. compatibilização com o HTTPS
- D. acomodação do IMAP
- E. acoplamento ao protocolo TCP

17.O Protocolo da Internet (IP) é responsável pelo repasse e endereçamento de pacotes. Dentre as características mais importantes introduzidas no protocolo IPv6, está a(o)

-  A. expansão da capacidade de endereçamento
- B. flexibilização do comprimento do cabeçalho
- C. compatibilização com o HTTPS
- D. acomodação do IMAP
- E. acoplamento ao protocolo TCP

18. Em uma rede de endereço 172.16.0.0/25, quais são os endereços de rede e broadcast da primeira sub-rede?

- A. 172.16.0.0 e 172.16.0.127
- B. 172.16.0.0 e 172.16.0.254
- C. 172.16.0.128 e 172.16.0.255
- D. 172.16.0.1 e 172.16.0.255

18. Em uma rede de endereço 172.16.0.0/25, quais são os endereços de rede e broadcast da primeira sub-rede?



- A. 172.16.0.0 e 172.16.0.127
- B. 172.16.0.0 e 172.16.0.254
- C. 172.16.0.128 e 172.16.0.255
- D. 172.16.0.1 e 172.16.0.255

GABARITO



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

13. B
14. E
15. C
16. C
17. A
18. A

Questões Comentadas com Resolução Assistida

Nível de Transporte TCP/IP

TCP, UDP, NAT

1.O protocolo sem conexão e não-confiável, destinado a aplicações que não querem controle de fluxo nem manutenção da sequência das mensagens enviadas é o

A. SMTP.

B. OSPF.

C. FTP.

D. TCP.

E. UDP.

1.O protocolo sem conexão e não-confiável, destinado a aplicações que não querem controle de fluxo nem manutenção da sequência das mensagens enviadas é o

A. SMTP.

B. OSPF.

C. FTP.

D. TCP.

 E. UDP.

2.O TCP (Transmission Control Protocol) foi projetado especificamente para oferecer um fluxo de bytes fim a fim confiável em uma inter-rede não confiável. O controle de fluxo no TCP é administrado por meio de

- A. memória compartilhada
- B. contador de datagramas
- C. contador de pacotes
- D. temporizador de pacotes
- E. janela deslizante

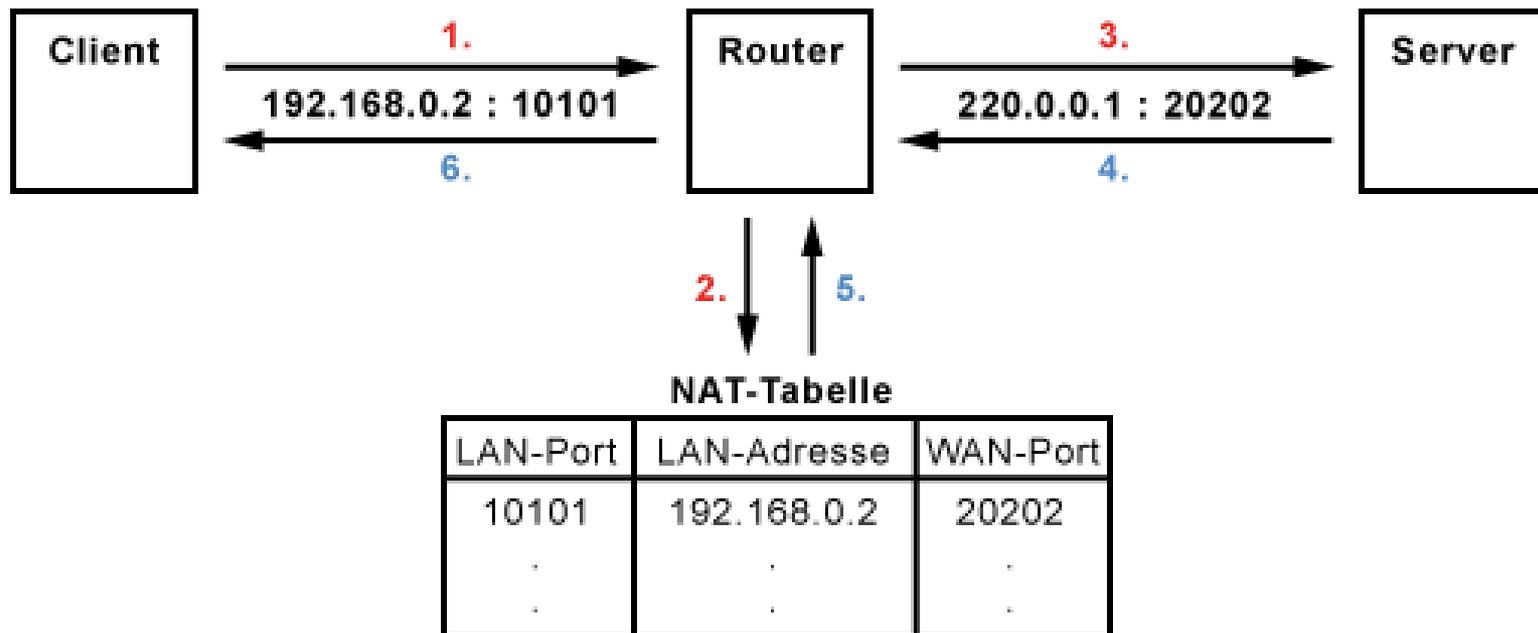
2.O TCP (Transmission Control Protocol) foi projetado especificamente para oferecer um fluxo de bytes fim a fim confiável em uma inter-rede não confiável. O controle de fluxo no TCP é administrado por meio de

- A. memória compartilhada
- B. contador de datagramas
- C. contador de pacotes
- D. temporizador de pacotes
-  E. janela deslizante

3. Para melhorar a segurança de uma rede local de computadores (LAN), é possível utilizar o serviço NAT (Network Address Translation), que não expõe o computador da LAN para acesso externo direto. Na estrutura do NAT, o relacionamento entre o computador da LAN e a mensagem gerada por esse computador e enviada para a WAN é realizado por meio da informação inserida

- A. em um cabeçalho adicional do IPSec.
- B. no campo Porta destino do TCP.
- C. no campo Porta origem do TCP.
- D. no campo Type do frame Ethernet.
- E. no espaço reservado Options do IP.

NAT



3. Para melhorar a segurança de uma rede local de computadores (LAN), é possível utilizar o serviço NAT (Network Address Translation), que não expõe o computador da LAN para acesso externo direto. Na estrutura do NAT, o relacionamento entre o computador da LAN e a mensagem gerada por esse computador e enviada para a WAN é realizado por meio da informação inserida

- A. em um cabeçalho adicional do IPSec.
- B. no campo Porta destino do TCP.
-  C. no campo Porta origem do TCP.
- D. no campo Type do frame Ethernet.
- E. no espaço reservado Options do IP.

4.As conexões TCP são do tipo:

- A. Full-duplex e multidifusão.
- B. Duplex e multidifusão.
- C. Full-duplex e ponto a ponto.
- D. Duplex e difusão.
- E. Simplex e ponto a ponto.

4.As conexões TCP são do tipo:

A. Full-duplex e multidifusão.

B. Duplex e multidifusão.

 C. Full-duplex e ponto a ponto.

D. Duplex e difusão.

E. Simplex e ponto a ponto.

5. Analise as seguintes afirmações relacionadas ao protocolo TCP/IP:

I. O UDP é um protocolo orientado a conexão, com garantia de entrega.

II. O TCP é um protocolo que trata adequadamente pacotes recebidos fora de ordem ou duplicados.

III. ICMP é um protocolo que não admite fragmentação de seus pacotes devido ao handshake de conexão.

Está correto somente o que se afirma em:

A. I;

B. II;

C. III;

D. I e II;

E. I e III.

5. Analise as seguintes afirmações relacionadas ao protocolo TCP/IP:

I. O UDP é um protocolo orientado a conexão, com garantia de entrega.

II. O TCP é um protocolo que trata adequadamente pacotes recebidos fora de ordem ou duplicados.

III. ICMP é um protocolo que não admite fragmentação de seus pacotes devido ao handshake de conexão.

Está correto somente o que se afirma em:

A. I;

 B. II;

C. III;

D. I e II;

E. I e III.

6.Quanto ao Protocolo TCP, é correto afirmar que

- A. exige um serviço de rede confiável para operar.
- B. um socket identifica biunivocamente um usuário TCP em toda inter-rede.
- C. as conexões são half-duplex, ou seja transportam dados em apenas uma direção.
- D. foi projetado para funcionar em um serviço de rede conectado e com confirmações.
- E. foi projetado para funcionar em um serviço de rede sem conexão e sem confirmação.

6.Quanto ao Protocolo TCP, é correto afirmar que

- A. exige um serviço de rede confiável para operar.
- B. um socket identifica biunivocamente um usuário TCP em toda inter-rede.
- C. as conexões são half-duplex, ou seja transportam dados em apenas uma direção.
- D. foi projetado para funcionar em um serviço de rede conectado e com confirmações.
-  E. foi projetado para funcionar em um serviço de rede sem conexão e sem confirmação.

7. Uma empresa tem um conjunto de máquinas locais que deseja ligar à Internet, usando IPv4, mas não conseguiu obter suficientes endereços IP válidos. A solução será conectar essas máquinas utilizando:

- A. IPSEC;
- B. SNMP;
- C. NAT;
- D. NDP;
- E. ARP.

7. Uma empresa tem um conjunto de máquinas locais que deseja ligar à Internet, usando IPv4, mas não conseguiu obter suficientes endereços IP válidos. A solução será conectar essas máquinas utilizando:

A. IPSEC;

B. SNMP;

 C. NAT;

D. NDP;

E. ARP.

8.O TCP (Transmission Control Protocol) da camada de transporte da arquitetura TCP/IP garante a entrega fim a fim de mensagens da camada de aplicação. Para isso, esse protocolo utiliza técnicas para controle de fluxo e controle de erro conhecidas como

- A. janela de fluxo e janela de confirmação
- B. janela de fluxo e reconhecimento
- C. janela deslizante e reconhecimento
- D. janela deslizante e janela de confirmação
- E. janela de congestionamento e janela de confirmação

8.O TCP (Transmission Control Protocol) da camada de transporte da arquitetura TCP/IP garante a entrega fim a fim de mensagens da camada de aplicação. Para isso, esse protocolo utiliza técnicas para controle de fluxo e controle de erro conhecidas como

A. janela de fluxo e janela de confirmação

B. janela de fluxo e reconhecimento

 C. janela deslizante e reconhecimento

D. janela deslizante e janela de confirmação

E. janela de congestionamento e janela de confirmação

9.O UDP é um protocolo de transporte da Internet que tem alguns usos específicos, como interações cliente/servidor e multimídia. Em relação a esse protocolo, é correto afirmar que:

- A. as conexões são estabelecidas por meio do handshake de três vias;
- B. realiza controle de fluxo, controle de erros ou retransmissão após a recepção de um segmento incorreto;
- C. foi projetado especificamente para oferecer um fluxo de bytes fim a fim confiável em uma inter-rede não confiável;
- D. oferece um meio para as aplicações enviarem datagramas IP encapsulados sem que seja necessário estabelecer uma conexão;
- E. transmite segmentos que consistem em um cabeçalho de 128 bytes, seguido pela carga útil.

9.O UDP é um protocolo de transporte da Internet que tem alguns usos específicos, como interações cliente/servidor e multimídia. Em relação a esse protocolo, é correto afirmar que:

- A. as conexões são estabelecidas por meio do handshake de três vias;
- B. realiza controle de fluxo, controle de erros ou retransmissão após a recepção de um segmento incorreto;
- C. foi projetado especificamente para oferecer um fluxo de bytes fim a fim confiável em uma inter-rede não confiável;
-  D. oferece um meio para as aplicações enviarem datagramas IP encapsulados sem que seja necessário estabelecer uma conexão;
- E. transmite segmentos que consistem em um cabeçalho de 128 bytes, seguido pela carga útil.

10. Para estabelecer uma conexão, o módulo TCP da camada de transporte do cliente executa o procedimento do 3-way handshake com o módulo TCP da camada de transporte do servidor. Esse handshake é caracterizado pela troca de três mensagens, na seguinte ordem:

- A. SYN, ACK e FIN
- B. SYN, SYN-ACK e FIN
- C. SYN, SYN-ACK e ACK
- D. SYN-ACK, SYN-ACK e ACK
- E. SYN-ACK, ACK e FIN

10. Para estabelecer uma conexão, o módulo TCP da camada de transporte do cliente executa o procedimento do 3-way handshake com o módulo TCP da camada de transporte do servidor. Esse handshake é caracterizado pela troca de três mensagens, na seguinte ordem:

- A. SYN, ACK e FIN
- B. SYN, SYN-ACK e FIN
-  C. SYN, SYN-ACK e ACK
- D. SYN-ACK, SYN-ACK e ACK
- E. SYN-ACK, ACK e FIN

11. Um computador que obtém acesso à Internet compartilhada através de um NAT precisa ser acessado remotamente a partir da Internet pela Porta TCP 5900. Para que esse acesso seja possível, é necessário que

- A. o computador que atua como rota padrão (gateway) encaminhe as requisições na Porta TCP 5900 para o computador que precisa ser acessado remotamente.
- B. o endereço de difusão (broadcast) da rede na qual o computador a ser acessado está configurado seja utilizado para efetuar a conexão.

- C. a Porta TCP seja alterada para uma porta baixa, isto é, cujo número seja inferior a 1024, pois apenas essas portas podem ser acessadas remotamente por intermédio de um NAT.
- D. um firewall seja ativado na Porta TCP 5900 no computador que precisa ser acessado remotamente.
- E. um proxy HTTP seja instalado no computador que atua como rota padrão (gateway), para permitir o acesso remoto aos computadores da rede.

11. Um computador que obtém acesso à Internet compartilhada através de um NAT precisa ser acessado remotamente a partir da Internet pela Porta TCP 5900. Para que esse acesso seja possível, é necessário que

-  A. o computador que atua como rota padrão (gateway) encaminhe as requisições na Porta TCP 5900 para o computador que precisa ser acessado remotamente.
- B. o endereço de difusão (broadcast) da rede na qual o computador a ser acessado está configurado seja utilizado para efetuar a conexão.

GABARITO



1. E

2. E

3. C

4. C

5. B

6. E

7. C

8. C

9. D

10. C

11. A

Questões Comentadas com Resolução Assistida

Nível de Aplicação TCP/IP

DNS, SMTP, POP, IMAP, DHCP

1.A arquitetura TCP/IP dispõe de um conjunto de protocolos para comunicação entre computadores em rede. Em relação aos protocolos de comunicação, analise as afirmativas a seguir:

I. TFTP é um protocolo de terminal virtual que permite ao usuário de um sistema acessar um sistema remoto através de uma sessão de terminal, operando como se estivesse conectado diretamente à aquele sistema.

II. O FTP provê serviços de transferência, renomeação e remoção de arquivos e também de criação, remoção e modificação de diretórios.

III. O TCP é o protocolo responsável por mapear os nomes de hosts para seus respectivos endereços de rede.

1. Está correto o que se afirma em:

- A. somente I;
- B. somente II;
- C. somente III;
- D. somente I e II;
- E. I, II e III.

1. Está correto o que se afirma em:

A. somente I;

 B. somente II;

C. somente III;

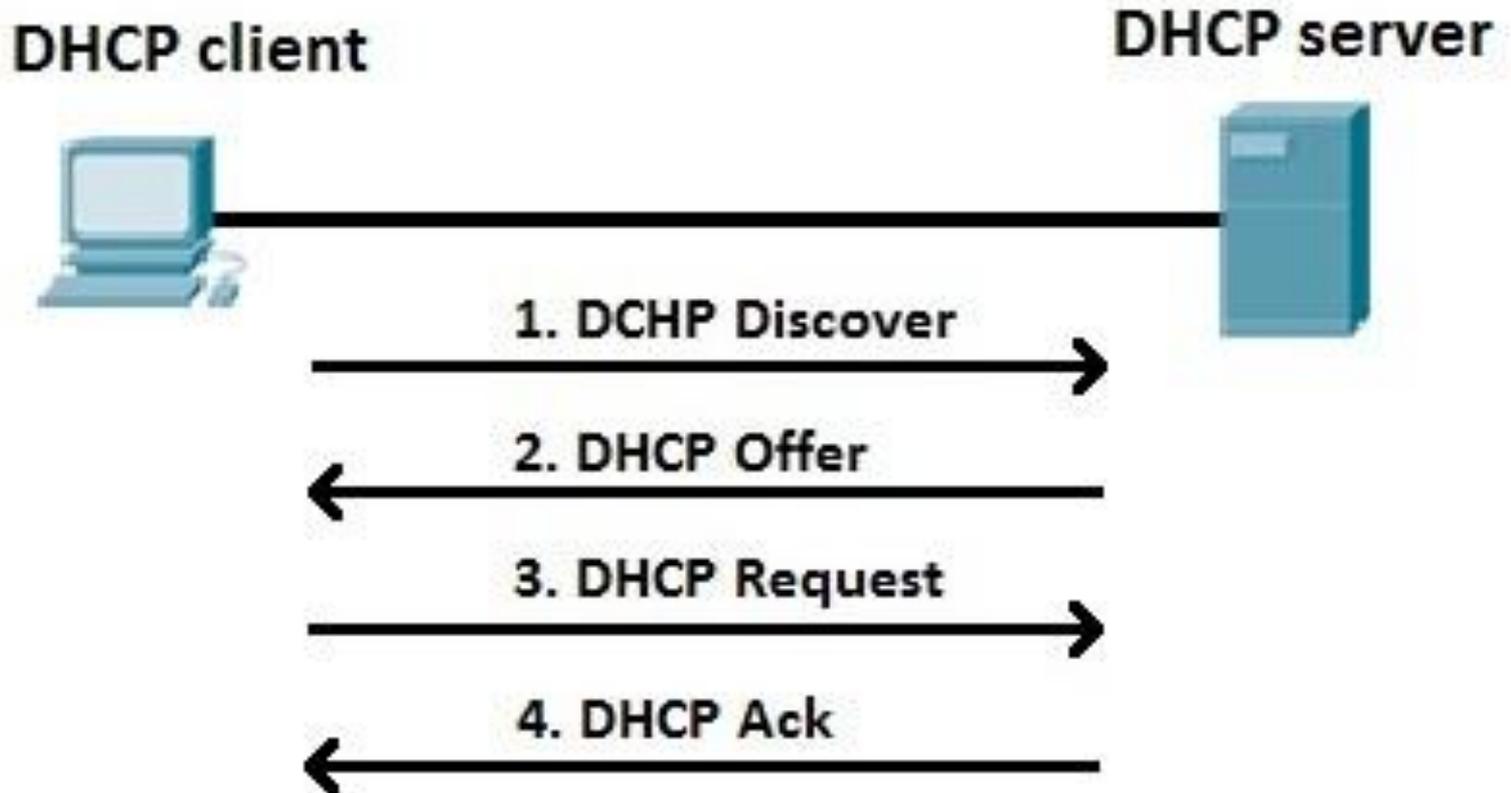
D. somente I e II;

E. I, II e III.

2.Segundo a RFC 2131, que define o funcionamento do protocolo DHCP para redes IPv4, após o recebimento da mensagem DHCPDISCOVER, o servidor DHCP oferece um endereço IP ao cliente por meio da mensagem

- A. DHCPACK.
- B. DHCPINFORM.
- C. DHCPOFFER.
- D. DHCPREQUEST.
- E. DHCPSEND.

DHCP - Mensagens



2.Segundo a RFC 2131, que define o funcionamento do protocolo DHCP para redes IPv4, após o recebimento da mensagem DHCPDISCOVER, o servidor DHCP oferece um endereço IP ao cliente por meio da mensagem

A. DHCPACK.

B. DHCPINFORM.

 C. DHCPOFFER.

D. DHCPREQUEST.

E. DHCPSEND.

3. Um dos principais tipos de registros de recursos do DNS para o IPv4 é o:

A. AIP.

B. NSS.

C. MMX.

D. PTA.

E. SOA.

DNS - Registros

- **SOA** – Start of Authority
 - Início dos dados de um domínio
- **A** – Address
 - Endereço IPv4
 - **AAAA** – IPv6
- **CNAME** – Canonical Name
 - Alias/Apelido
- **PTR** – Pointer
 - DNS Reverso
- **NS** - Name Server
 - Servidor de nomes
- **MINFO** - Mailbox Info
 - Email dos responsáveis pelo domínio
- **HINFO** – Host Info
 - Informações sobre o host
- **MX** - Mail Exchange
 - Servidor de e-mails
- **TXT** - Text
 - SPF - Sender Policy Framework

3. Um dos principais tipos de registros de recursos do DNS para o IPv4 é o:

A. AIP.

B. NSS.

C. MMX.

D. PTA.

 E. SOA.

4. Assinale a opção correta.

- A. O protocolo SMTP restringe apenas o cabeçalho de todas as mensagens de correio ao simples formato ASCII de 7 bits.
- B. O protocolo HTTP é implementado em três programas: um programa cliente, um programa servidor e um programa misto.
- C. O protocolo SMTP restringe o corpo de todas as mensagens de correio ao simples formato ASCII de 15 bits.
- D. O protocolo STP2 implementa mensagens de correio no formato HEXA de 7 bits.
- E. O protocolo HTTP é implementado em dois programas: um programa cliente e outro servidor.

4. Assinale a opção correta.

- A. O protocolo SMTP restringe apenas o cabeçalho de todas as mensagens de correio ao simples formato ASCII de 7 bits.
- B. O protocolo HTTP é implementado em três programas: um programa cliente, um programa servidor e um programa misto.
- C. O protocolo SMTP restringe o corpo de todas as mensagens de correio ao simples formato ASCII de 15 bits.
- D. O protocolo STP2 implementa mensagens de correio no formato HEXA de 7 bits.
-  E. O protocolo HTTP é implementado em dois programas: um programa cliente e outro servidor.

5.No desenvolvimento de aplicações Web, o desenvolvedor deverá certamente utilizar o protocolo HTTP, devendo escolher entre duas maneiras de solicitar informação do servidor, indicadas pelos comandos GET e POST do protocolo. A diferença básica entre eles é que o

- A. GET envia os parâmetros da solicitação codificados na URL, o POST os envia como parte do corpo da requisição.
- B. GET não permite enviar parâmetros, o POST permite.
- C. GET só funciona com navegadores, o POST, com qualquer tipo de aplicação Web.
- D. POST envia os parâmetros da solicitação codificados na URL, o GET os envia como parte do corpo da requisição.
- E. POST não permite enviar parâmetros, o GET permite.

5.No desenvolvimento de aplicações Web, o desenvolvedor deverá certamente utilizar o protocolo HTTP, devendo escolher entre duas maneiras de solicitar informação do servidor, indicadas pelos comandos GET e POST do protocolo. A diferença básica entre eles é que o



- A. GET envia os parâmetros da solicitação codificados na URL, o POST os envia como parte do corpo da requisição.
- B. GET não permite enviar parâmetros, o POST permite.
- C. GET só funciona com navegadores, o POST, com qualquer tipo de aplicação Web.
- D. POST envia os parâmetros da solicitação codificados na URL, o GET os envia como parte do corpo da requisição.
- E. POST não permite enviar parâmetros, o GET permite.

6. Assinale a opção correta.

- A. O protocolo POP3 provê meios para um usuário criar pastas remotas e designar mensagens a pastas.
- B. O protocolo POP3 é definido no RFC 1939.
- C. Em uma transação POP3, o controlador emite comandos e o servidor, uma demanda única para todos eles.
- D. O protocolo POP3 é definido no RSC 1949.
- E. O protocolo POP3 provê meios para um usuário criar janelas remotas e atribuir mensagens a pastas clientes.

6. Assinale a opção correta.

- A. O protocolo POP3 provê meios para um usuário criar pastas remotas e designar mensagens a pastas.
-  B. O protocolo POP3 é definido no RFC 1939.
- C. Em uma transação POP3, o controlador emite comandos e o servidor, uma demanda única para todos eles.
- D. O protocolo POP3 é definido no RSC 1949.
- E. O protocolo POP3 provê meios para um usuário criar janelas remotas e atribuir mensagens a pastas clientes.

7. Um administrador de rede precisa criar o registro DNS para o servidor de correio eletrônico de entrada do seu domínio. Para isso, o administrador deve acrescentar, no mapa da zona do seu domínio, o Registro de Recurso (RR)

- A. MX - Mail Exchanger
- B. MR - Mail Receiver
- C. MS - Mail Server
- D. IM - Incoming Mailer
- E. DM - Domain Mailer

7. Um administrador de rede precisa criar o registro DNS para o servidor de correio eletrônico de entrada do seu domínio. Para isso, o administrador deve acrescentar, no mapa da zona do seu domínio, o Registro de Recurso (RR)



- A. MX - Mail Exchanger
- B. MR - Mail Receiver
- C. MS - Mail Server
- D. IM - Incoming Mailer
- E. DM - Domain Mailer

8. Os servidores DNS (Domain Name System) contêm

- A. o banco de dados do DNS com o mapeamento entre os domínios de acesso e o respectivo número APS.
- B. o banco de dados do DNS com o mapeamento entre os nomes DNS e o respectivo número IP.
- C. os programas do DNS com a transformação dos nomes DNS em números no padrão IP-S.
- D. o banco de operações do DNS com o mapeamento entre os usuários DNS e os mecanismos de suporte Active Device.
- E. o banco de dados do DNS com as relações entre plug-ins DNS e o respectivo meio de acesso IP.

8. Os servidores DNS (Domain Name System) contêm

- A. o banco de dados do DNS com o mapeamento entre os domínios de acesso e o respectivo número APS.
-  B. o banco de dados do DNS com o mapeamento entre os nomes DNS e o respectivo número IP.
- C. os programas do DNS com a transformação dos nomes DNS em números no padrão IP-S.
- D. o banco de operações do DNS com o mapeamento entre os usuários DNS e os mecanismos de suporte Active Device.
- E. o banco de dados do DNS com as relações entre plug-ins DNS e o respectivo meio de acesso IP.

9. Ao tentar acessar um servidor, um usuário obtém a seguinte mensagem: “404 Not Found: documento requisitado não existe no servidor”.

No modelo de referência TCP/IP, que protocolo da camada de aplicação é responsável por emitir a mensagem acima?

- A. FTP
- B. HTTP
- C. SMTP
- D. TELNET
- E. SSH

9. Ao tentar acessar um servidor, um usuário obtém a seguinte mensagem: “404 Not Found: documento requisitado não existe no servidor”.

No modelo de referência TCP/IP, que protocolo da camada de aplicação é responsável por emitir a mensagem acima?

A. FTP

 B. HTTP

C. SMTP

D. TELNET

E. SSH

10. Uma configuração bastante efetiva contra abusos em correio eletrônico é a de reservar a porta 25/TCP somente para troca de mensagens entre MTAs e usar outra porta para mensagens enviadas por um cliente para o seu MTA. Essa nova porta, para uso de MSA (Mail Submission Agent), é definida como sendo

- A. TCP/465.
- B. TCP/587.
- C. TCP/993.
- D. TCP/995.
- E. TCP/2049.

10. Uma configuração bastante efetiva contra abusos em correio eletrônico é a de reservar a porta 25/TCP somente para troca de mensagens entre MTAs e usar outra porta para mensagens enviadas por um cliente para o seu MTA. Essa nova porta, para uso de MSA (Mail Submission Agent), é definida como sendo

A. TCP/465.



B. TCP/587.

C. TCP/993.

D. TCP/995.

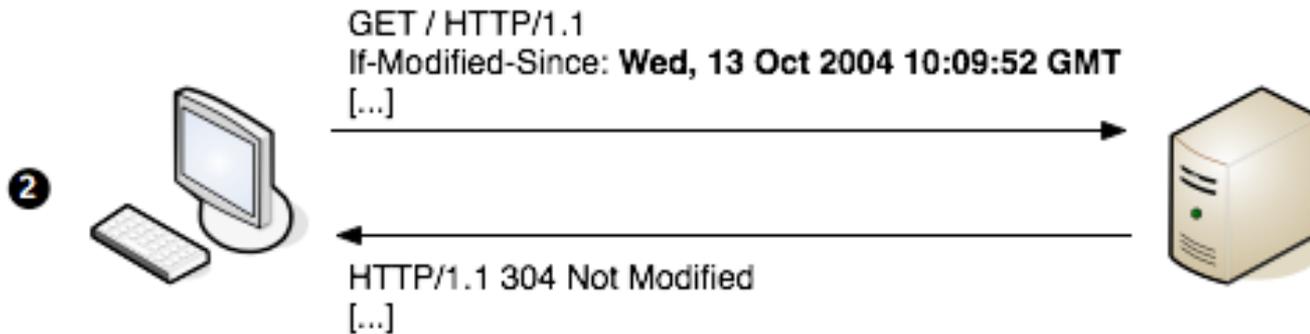
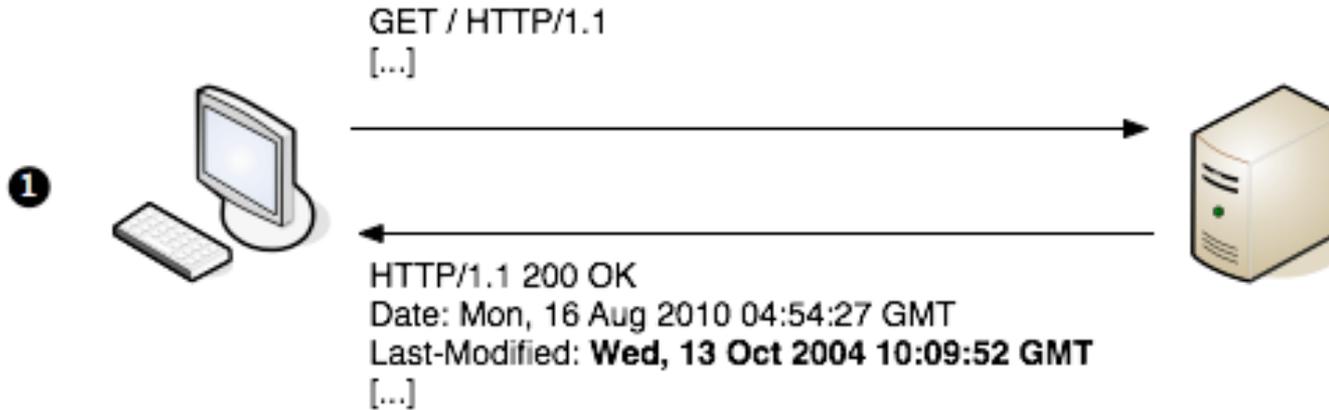
E. TCP/2049.

11.O HTTP (HyperText Transfer Protocol) permite que o cliente envie uma requisição condicional para o servidor para otimizar a recuperação de itens, evitando, assim, transferências desnecessárias.

O cabeçalho que deve ser incluído na mensagem HTTP para evitar a transferência de um item a menos que este tenha sido atualizado é

- A. If-Time-And-Date-Modified
- B. If-Modified-Since
- C. Accept-If-Modified
- D. Content-Modified
- E. Content-Updated

HTTP Cache



11.O HTTP (HyperText Transfer Protocol) permite que o cliente envie uma requisição condicional para o servidor para otimizar a recuperação de itens, evitando, assim, transferências desnecessárias.

O cabeçalho que deve ser incluído na mensagem HTTP para evitar a transferência de um item a menos que este tenha sido atualizado é

- A. If-Time-And-Date-Modified
-  B. If-Modified-Since
- C. Accept-If-Modified
- D. Content-Modified
- E. Content-Updated

12. Em um servidor DNS, são necessários alguns registros de recursos para seu adequado funcionamento. Um registro SOA, por exemplo, fornece o nome da principal fonte de informações sobre a zona do servidor de nome, como: o endereço de correio eletrônico do administrador, um número de série exclusivo, alguns flags e seus timeouts. Qual dos tipos de registro listados a seguir permite a criação de nomes alternativos?

- A. CNAME
- B. ANAME
- C. MX
- D. NS
- E. SRV

12. Em um servidor DNS, são necessários alguns registros de recursos para seu adequado funcionamento. Um registro SOA, por exemplo, fornece o nome da principal fonte de informações sobre a zona do servidor de nome, como: o endereço de correio eletrônico do administrador, um número de série exclusivo, alguns flags e seus timeouts. Qual dos tipos de registro listados a seguir permite a criação de nomes alternativos?



- A. CNAME
- B. ANAME
- C. MX
- D. NS
- E. SRV

13.O Domain Name System (DNS) é um sistema de gerenciamento de nomes hierárquico e distribuído que permite resolver nomes de domínios em endereços de rede.

No Windows Server 2003, o DNS reverso

- A. é uma cópia de segurança do servidor DNS primário.
- B. é um servidor secundário para o nível raiz do DNS.
- C. é o nível secundário da hierarquia DNS, estando logo abaixo do nível raiz.
- D. resolve o endereço IP, buscando o nome de domínio associado ao host.
- E. estabelece os mecanismos de armazenamento temporário com vistas à melhoria da eficiência das consultas.

13.O Domain Name System (DNS) é um sistema de gerenciamento de nomes hierárquico e distribuído que permite resolver nomes de domínios em endereços de rede.

No Windows Server 2003, o DNS reverso

- A. é uma cópia de segurança do servidor DNS primário.
- B. é um servidor secundário para o nível raiz do DNS.
- C. é o nível secundário da hierarquia DNS, estando logo abaixo do nível raiz.
-  D. resolve o endereço IP, buscando o nome de domínio associado ao host.
- E. estabelece os mecanismos de armazenamento temporário com vistas à melhoria da eficiência das consultas.

14. Em relação ao serviço FTP, analise as afirmativas a seguir:

I. Como forma de aumentar a velocidade de transferência de arquivos, o FTP utiliza o protocolo de transporte UDP como padrão.

II. O FTP utiliza duas conexões TCP/IP para realizar transferência de arquivos, uma servindo de controle e outra para enviar os dados.

III. O modo passivo do FTP foi criado para permitir a transferência de arquivos binários.

Está correto somente o que se afirma em:

A. I;

B. II;

C. III;

D. I e II;

E. I e III.

14. Em relação ao serviço FTP, analise as afirmativas a seguir:

I. Como forma de aumentar a velocidade de transferência de arquivos, o FTP utiliza o protocolo de transporte UDP como padrão.

II. O FTP utiliza duas conexões TCP/IP para realizar transferência de arquivos, uma servindo de controle e outra para enviar os dados.

III. O modo passivo do FTP foi criado para permitir a transferência de arquivos binários.

Está correto somente o que se afirma em:

A. I;

 B. II;

C. III;

D. I e II;

E. I e III.

15. Os protocolos HTTP e SMTP são utilizados para a transferência de informações entre dois hospedeiros, porém possuem algumas diferenças entre si.

Dentre essas diferenças, está a(o)

- A. codificação exigida para os dados transmitidos.
- B. capacidade de lidar com subredes virtuais.
- C. camada de rede à que pertencem.
- D. dependência do DNS.
- E. tipo de conexão que usam (UDP e TCP, respectivamente).

15. Os protocolos HTTP e SMTP são utilizados para a transferência de informações entre dois hospedeiros, porém possuem algumas diferenças entre si.

Dentre essas diferenças, está a(o)



A. codificação exigida para os dados transmitidos.

B. capacidade de lidar com subredes virtuais.

C. camada de rede à que pertencem.

D. dependência do DNS.

E. tipo de conexão que usam (UDP e TCP, respectivamente).

16. Um tipo de consulta ao serviço DNS (Domain Name System) permite mapear um endereço IP em um nome de domínio.

Esse tipo de consulta é chamado de

- A. mapeamento dinâmico
- B. mapeamento reverso
- C. mapeamento direto
- D. consulta direta
- E. consulta estática

16. Um tipo de consulta ao serviço DNS (Domain Name System) permite mapear um endereço IP em um nome de domínio.

Esse tipo de consulta é chamado de

A. mapeamento dinâmico



B. mapeamento reverso

C. mapeamento direto

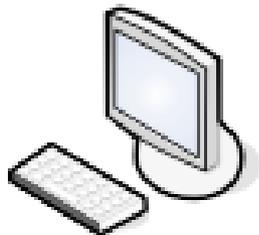
D. consulta direta

E. consulta estática

17.O protocolo HTTP aceita operações chamadas métodos. De acordo com a versão 1.1 desse protocolo de transferência utilizado em toda a World Wide Web, o método recomendado para se obter a data da última modificação feita em determinada página é:

- A. HEAD
- B. CONNECT
- C. READ
- D. PUSH
- E. TRACE

1



GET / HTTP/1.1
[...]



HTTP/1.1 200 OK
Date: Mon, 16 Aug 2010 04:54:27 GMT
Last-Modified: **Wed, 13 Oct 2004 10:09:52 GMT**
[...]



17.O protocolo HTTP aceita operações chamadas métodos. De acordo com a versão 1.1 desse protocolo de transferência utilizado em toda a World Wide Web, o método recomendado para se obter a data da última modificação feita em determinada página é:



- A. HEAD
- B. CONNECT
- C. READ
- D. PUSH
- E. TRACE

18. Um analista de segurança precisa liberar, para um servidor interno, as portas TCP em um firewall de borda.

Para permitir o acesso aos protocolos HTTP, HTTPS, SMTP, IMAP e POP, as portas (default) liberadas devem ser, respectivamente,

- A. 80, 443, 25, 143 e 110
- B. 80, 443, 110, 25 e 143
- C. 80, 8080, 25, 161 e 110
- D. 80, 8080, 161, 143 e 25
- E. 443, 80, 110, 25 e 143

18. Um analista de segurança precisa liberar, para um servidor interno, as portas TCP em um firewall de borda.

Para permitir o acesso aos protocolos HTTP, HTTPS, SMTP, IMAP e POP, as portas (default) liberadas devem ser, respectivamente,



A. 80, 443, 25, 143 e 110

B. 80, 443, 110, 25 e 143

C. 80, 8080, 25, 161 e 110

D. 80, 8080, 161, 143 e 25

E. 443, 80, 110, 25 e 143

19. Em uma reunião técnica sobre a implantação de um novo website, um analista de suporte fez as seguintes afirmativas:

I - pacotes IP podem seguir por diferentes caminhos entre a origem e o destino;

II - para maior agilidade, o servidor HTTP deve ser executado via UDP, em vez do TCP;

III - para maior flexibilidade e facilidade para os usuários, o endereço IP do novo website deverá ser divulgado, em vez de seu nome.

Está(ão) correta(s) a(s) afirmativa(s)

- A. I, apenas.
- B. II, apenas.
- C. III, apenas.
- D. I e II, apenas.
- E. I, II e III.

19. Em uma reunião técnica sobre a implantação de um novo website, um analista de suporte fez as seguintes afirmativas:

I - pacotes IP podem seguir por diferentes caminhos entre a origem e o destino;

II - para maior agilidade, o servidor HTTP deve ser executado via UDP, em vez do TCP;

III - para maior flexibilidade e facilidade para os usuários, o endereço IP do novo website deverá ser divulgado, em vez de seu nome.

Está(ão) correta(s) a(s) afirmativa(s)



- A. I, apenas.
- B. II, apenas.
- C. III, apenas.
- D. I e II, apenas.
- E. I, II e III.

20. Os servidores raiz são parte crucial da Internet porque eles são o primeiro passo em traduzir nomes para endereços IP e são usados para comunicação entre hosts. Devido aos limites do DNS no tamanho dos pacotes UDP (User Datagram Protocol) em 512 bytes, o número de endereços dos servidores raiz que são acomodados nas pesquisas de nome do DNS é limitado. Esse limite determina que atualmente o número de servidores raiz seja:

- A. 5.
- B. 8.
- C. 13.
- D. 16.
- E. 64.

20. Os servidores raiz são parte crucial da Internet porque eles são o primeiro passo em traduzir nomes para endereços IP e são usados para comunicação entre hosts. Devido aos limites do DNS no tamanho dos pacotes UDP (User Datagram Protocol) em 512 bytes, o número de endereços dos servidores raiz que são acomodados nas pesquisas de nome do DNS é limitado. Esse limite determina que atualmente o número de servidores raiz seja:

- A. 5.
- B. 8.
-  C. 13.
- D. 16.
- E. 64.

21.O HTTP (Hypertext Transfer Protocol) é o protocolo básico da World Wide Web (WWW) e pode ser utilizado em qualquer aplicação cliente/servidor. Os dados transferidos pelo protocolo podem ser texto puro, hipertexto, áudio, imagens ou qualquer informação acessível pela Internet. Esses dados são transferidos em texto claro, o que possibilita a sua inspeção ao longo do caminho percorrido. Para garantir segurança das mensagens HTTP, o cliente e o servidor podem utilizar o HTTPS, que é

- A. uma nova versão do protocolo HTTP (HTTP Secure) com recursos de segurança para garantia de integridade, autenticidade e sigilo de todas as mensagens do HTTP.

- B. uma nova versão do protocolo HTTP (HTTP Secure) com recursos de segurança para garantia de integridade, autenticidade e sigilo de parte das mensagens do HTTP.

- C. uma nova versão do protocolo HTTP utilizado sobre a SSL (Secure Socket Layer) que oferece recursos de segurança para garantia de integridade, autenticidade e sigilo de parte das mensagens do HTTP.

- D. o próprio protocolo HTTP utilizado sobre a SSL (Secure Socket Layer) que oferece recursos de segurança para garantia de integridade, autenticidade e sigilo de parte das mensagens do HTTP.

- E. o próprio protocolo HTTP utilizado sobre a SSL (Secure Socket Layer) que oferece recursos de segurança para garantia de integridade, autenticidade e sigilo de todas as mensagens do HTTP.

- C. uma nova versão do protocolo HTTP utilizado sobre a SSL (Secure Socket Layer) que oferece recursos de segurança para garantia de integridade, autenticidade e sigilo de parte das mensagens do HTTP.
- D. o próprio protocolo HTTP utilizado sobre a SSL (Secure Socket Layer) que oferece recursos de segurança para garantia de integridade, autenticidade e sigilo de parte das mensagens do HTTP.
- E.  o próprio protocolo HTTP utilizado sobre a SSL (Secure Socket Layer) que oferece recursos de segurança para garantia de integridade, autenticidade e sigilo de todas as mensagens do HTTP.

22.Em relação aos tipos de servidores de correio eletrônico, analise as afirmativas a seguir:

I - Servidores SMTP atuam como agentes para envio das mensagens de correio eletrônico para a Internet. O servidor SMTP manipula a caixa de saída do correio eletrônico.

II - Servidores IMAP mantêm as mensagens de correio eletrônico até que o usuário verifique sua caixa de entrada e, nesse ponto, as mensagens são transferidas para o computador do usuário.

III - Servidores POP3 permitem trabalhar com mensagens de correio eletrônico sem baixá-las para o computador primeiro. É possível visualizar, excluir e organizar mensagens diretamente no servidor de correio eletrônico e cópias são armazenadas no servidor até que o usuário opte por excluí-las.

22. Está correto o que se afirma em:

- A. somente I;
- B. somente II;
- C. somente III;
- D. somente I e III;
- E. I, II e III.

22. Está correto o que se afirma em:



A. somente I;

B. somente II;

C. somente III;

D. somente I e III;

E. I, II e III.

23.O SMTP (Simple Mail Transfer Protocol) é um dos serviços prestados pela camada de aplicação da Arquitetura Internet e costuma estar presente em qualquer implementação TCP/IP. Em relação ao conjunto de comandos do protocolo SMTP, considere V para a(s) afirmativa(s) verdadeira(s) e F para a(s) falsa(s).

() As funções de abertura e fechamento de um canal de transmissão são realizadas por meio dos comandos HELO e QUIT.

() A transação para transmissão de mensagens é iniciada com o comando MAIL e o argumento deste comando corresponde à rota de retorno que pode ser usada para notificar ao originador quando ocorre um erro com o roteamento da mensagem.

() A lista dos destinatários da mensagem a ser transmitida é especificada como argumento do comando RCPT.

23.A sequência correta é:

A. F - V - F;

B. F - V - V;

C. V - F - F;

D. V - V - F;

E. F - F - V.

23. A sequência correta é:

A. F - V - F;

B. F - V - V;

C. V - F - F;

 D. V - V - F;

E. F - F - V.

GABARITO



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

13. D
14. B
15. A
16. B
17. A
18. A
19. A
20. C
21. E
22. A
23. D

Questões Comentadas com Resolução Assistida

Voz sobre IP

Qualidade de Serviço

1. São requisitos de Qualidade de Serviço (QoS - Quality of Service):

- A. Capacidade, Jitter, Sincronização, Banda estável.
- B. Confiabilidade, Retardo, Flutuação no Jitter, Largura de Banda.
- C. Capacidade do enlace, Jitter, Sincronização, Banda variável.
- D. Confiabilidade, Retardo, Flutuação do tempo de transmissão, Largura de Banda.
- E. Capacidade, Retardo, Flutuação no Jitter, Banda estável.

Requisitos de QoS

- Confiabilidade (Perda de pacotes)
 - Integridade dos dados
- Largura de banda (Vazão ou Througput)
 - Velocidade de transmissão
- Atraso (Latência, Retardo ou Delay)
 - Soma de todos os atrasos no caminho
- Variação do atraso (Flutuação ou Jitter)
 - Atraso variável entre pacotes

1. São requisitos de Qualidade de Serviço (QoS - Quality of Service):

- A. Capacidade, Jitter, Sincronização, Banda estável.
- B. Confiabilidade, Retardo, Flutuação no Jitter, Largura de Banda.
- C. Capacidade do enlace, Jitter, Sincronização, Banda variável.
-  D. Confiabilidade, Retardo, Flutuação do tempo de transmissão, Largura de Banda.
- E. Capacidade, Retardo, Flutuação no Jitter, Banda estável.

2.O SIP (Session Initiation Protocol) é um protocolo de texto modelado sobre o HTTP. Uma parte envia mensagem em texto ASCII, que consiste em um nome do método na primeira linha, seguido por linhas adicionais contendo cabeçalhos para passagem de parâmetros. Seis métodos são definidos pela especificação do núcleo. Relacione adequadamente os métodos às respectivas características.

- | | |
|--------------|---|
| 1. INVITE. | () Solicita o término de uma sessão. |
| 2. ACK. | () Solicita o início de uma sessão. |
| 3. BYE. | () Informa um servidor de redirecionamento sobre a localização atual do usuário. |
| 4. OPTIONS. | () Cancela uma solicitação pendente. |
| 5. CANCEL. | () Consulta um host sobre seus recursos. |
| 6. REGISTER. | () Confirma que uma sessão foi iniciada. |

2.A sequência está correta em

A. 2, 4, 6, 1, 3, 5.

B. 4, 2, 3, 6, 5, 1.

C. 3, 1, 6, 5, 4, 2.

D. 6, 3, 5, 2, 1, 4.

2.A sequência está correta em

A. 2, 4, 6, 1, 3, 5.

B. 4, 2, 3, 6, 5, 1.

 C. 3, 1, 6, 5, 4, 2.

D. 6, 3, 5, 2, 1, 4.

3. Na pilha de protocolos H.323, há um protocolo para estabelecer e encerrar conexões, fornecer tons de discagem, gerar sons de chamada e o restante da telefonia padrão. Este protocolo é o:

- A. ITU Q.931.
- B. H.245.
- C. RTCP.
- D. PSTN.
- E. H.225.

3. Na pilha de protocolos H.323, há um protocolo para estabelecer e encerrar conexões, fornecer tons de discagem, gerar sons de chamada e o restante da telefonia padrão. Este protocolo é o:

 A. ITU Q.931.

B. H.245.

C. RTCP.

D. PSTN.

E. H.225.

4. Em uma rede VoIP que utiliza o protocolo H.323, o dispositivo denominado de MCU (Multipoint Control Unit) tem como função principal

- A. proporcionar uma interface entre canais VoIP e canais com sinalização tradicional.
- B. enviar mensagens de controle de todos os gatekeepers da rede.
- C. realizar uma monitoração centralizada de chamadas para terminais registrados na sua zona.
- D. gerenciar chamadas do tipo conferência.
- E. enviar mensagens do tipo broadcasting.

4. Em uma rede VoIP que utiliza o protocolo H.323, o dispositivo denominado de MCU (Multipoint Control Unit) tem como função principal

- A. proporcionar uma interface entre canais VoIP e canais com sinalização tradicional.
- B. enviar mensagens de controle de todos os gatekeepers da rede.
- C. realizar uma monitoração centralizada de chamadas para terminais registrados na sua zona.
-  D. gerenciar chamadas do tipo conferência.
- E. enviar mensagens do tipo broadcasting.

5.Comparando o H.323 com o SIP, observa-se que

- A. o primeiro tem arquitetura modular, enquanto o segundo tem arquitetura monolítica.
- B. o primeiro tem endereçamento pelo número de host ou telefone, enquanto o segundo tem endereçamento pela URL.
- C. o primeiro não tem conferência de multimídia, enquanto o segundo tem.
- D. o primeiro tem formato de mensagens ASCII, enquanto o segundo tem formato de mensagens binário.
- E. o primeiro não tem compatibilidade com PSTN, enquanto o segundo tem compatibilidade restrita.

5. Comparando o H.323 com o SIP, observa-se que

- A. o primeiro tem arquitetura modular, enquanto o segundo tem arquitetura monolítica.
-  B. o primeiro tem endereçamento pelo número de host ou telefone, enquanto o segundo tem endereçamento pela URL.
- C. o primeiro não tem conferência de multimídia, enquanto o segundo tem.
- D. o primeiro tem formato de mensagens ASCII, enquanto o segundo tem formato de mensagens binário.
- E. o primeiro não tem compatibilidade com PSTN, enquanto o segundo tem compatibilidade restrita.

6. Em uma rede onde a política de QoS fim-a-fim existente é a de melhor esforço (“best effort”), pode-se afirmar que nessa situação:

- A. não há diferenciação entre os fluxos da rede;
- B. existe reserva absoluta dos recursos de rede para tráfegos específicos;
- C. pacotes prioritários sofrem marcação ;
- D. está sendo usado Traffic Shaping para reserva de tráfego;
- E. está sendo usado tráfego isócrona via protocolo RSVP.

6. Em uma rede onde a política de QoS fim-a-fim existente é a de melhor esforço (“best effort”), pode-se afirmar que nessa situação:

-  A. não há diferenciação entre os fluxos da rede;
- B. existe reserva absoluta dos recursos de rede para tráfegos específicos;
- C. pacotes prioritários sofrem marcação ;
- D. está sendo usado Traffic Shaping para reserva de tráfego;
- E. está sendo usado tráfego isócrono via protocolo RSVP.

7.Uma das vantagens do IPv6 sobre o IPv4 é que, ao implementar QoS, os roteadores podem identificar o tipo de fluxo bastando consultar um campo do cabeçalho do pacote IPv6, sem precisar analisá-lo de forma mais aprofundada. Esse campo é marcado pelo nó de origem do pacote, e tem o nome de:

- A. Flow label;
- B. Type of service;
- C. Traffic class;
- D. Diffserv field;
- E. Intserv field.

7.Uma das vantagens do IPv6 sobre o IPv4 é que, ao implementar QoS, os roteadores podem identificar o tipo de fluxo bastando consultar um campo do cabeçalho do pacote IPv6, sem precisar analisá-lo de forma mais aprofundada. Esse campo é marcado pelo nó de origem do pacote, e tem o nome de:



- A. Flow label;
- B. Type of service;
- C. Traffic class;
- D. Diffserv field;
- E. Intserv field.

8.O algoritmo em que cada host está conectado à rede por uma interface que contém uma fila interna finita e, se um pacote chegar à fila quando ela estiver cheia, o pacote será descartado, é o:

- A. Algoritmo de balde cheio (Full bucket).
- B. Algoritmo de roteamento finito (Finite routing).
- C. Algoritmo de fila finita (Finite Queue).
- D. Algoritmo de balde de símbolos (Token bucket).
- E. Algoritmo de balde furado (Leaky bucket).

8.O algoritmo em que cada host está conectado à rede por uma interface que contém uma fila interna finita e, se um pacote chegar à fila quando ela estiver cheia, o pacote será descartado, é o:

- A. Algoritmo de balde cheio (Full bucket).
- B. Algoritmo de roteamento finito (Finite routing).
- C. Algoritmo de fila finita (Finite Queue).
- D. Algoritmo de balde de símbolos (Token bucket).
-  E. Algoritmo de balde furado (Leaky bucket).

9. Em uma rede orientada a conexões, os pacotes que pertencem a um fluxo seguem a mesma rota, enquanto que, em uma rede não orientada a conexões, esses pacotes podem seguir rotas diferentes. As necessidades de cada fluxo são definidas por quatro parâmetros que determinam a qualidade de serviço (QoS).

Esses parâmetros são, respectivamente,

- A. largura de sinal, atenuação, sincronismo e perda
- B. tipo de sinal, atraso, sincronismo e perda
- C. largura de sinal, atenuação, flutuação e distância
- D. tipo de sinal, atenuação, sincronismo e distância
- E. largura de banda, atraso, flutuação e perda .

9. Em uma rede orientada a conexões, os pacotes que pertencem a um fluxo seguem a mesma rota, enquanto que, em uma rede não orientada a conexões, esses pacotes podem seguir rotas diferentes. As necessidades de cada fluxo são definidas por quatro parâmetros que determinam a qualidade de serviço (QoS).

Esses parâmetros são, respectivamente,

- A. largura de sinal, atenuação, sincronismo e perda
- B. tipo de sinal, atraso, sincronismo e perda
- C. largura de sinal, atenuação, flutuação e distância
- D. tipo de sinal, atenuação, sincronismo e distância
- E. largura de banda, atraso, flutuação e perda .



10. Fazem parte da pilha de protocolos H.323:

- A. TCP, G723, RTP, H.229.
- B. Protocolo de enlace, IP, RTP, H.248.
- C. TCP, Protocolo de Aplicação, RPP, H.245.
- D. UDP, IP, G724, H.328.
- E. UDP, IP, RTCP, H.225.

10. Fazem parte da pilha de protocolos H.323:

- A. TCP, G723, RTP, H.229.
- B. Protocolo de enlace, IP, RTP, H.248.
- C. TCP, Protocolo de Aplicação, RPP, H.245.
- D. UDP, IP, G724, H.328.
-  E. UDP, IP, RTCP, H.225.

11. Uma das diferenças entre o algoritmo de balde de símbolos (token bucket algorithm) e o algoritmo de balde furado (leaky bucket algorithm) se verifica quando o "balde" enche. Nesse momento,

- A. os dois descartam símbolos.
- B. o primeiro algoritmo descarta pacotes, enquanto que o segundo descarta símbolos.
- C. os dois descartam pacotes.
- D. o primeiro algoritmo nunca descarta pacotes, enquanto que o segundo descarta.
- E. o primeiro algoritmo descarta pacotes, enquanto que o segundo não descarta.

11. Uma das diferenças entre o algoritmo de balde de símbolos (token bucket algorithm) e o algoritmo de balde furado (leaky bucket algorithm) se verifica quando o "balde" enche. Nesse momento,

- A. os dois descartam símbolos.
- B. o primeiro algoritmo descarta pacotes, enquanto que o segundo descarta símbolos.
- C. os dois descartam pacotes.
-  D. o primeiro algoritmo nunca descarta pacotes, enquanto que o segundo descarta.
- E. o primeiro algoritmo descarta pacotes, enquanto que o segundo não descarta.

GABARITO



1. D

2. C

3. A

4. D

5. B

6. A

7. A

8. E

9. E

10. E

11. D