

1) A representação de um endereço IPv6 requer:

- a) 32 bits.
- b) 48 bits.
- c) 64 bits.
- d) 127 bits.
- e) 128 bits.

2) Quando um *host* configurado para uso de DHCP falha na obtenção de endereço IP, haverá o uso do recurso de *Automatic Private IP Addressing* (APIPA). Em qual das faixas de endereços o *host* receberá um IP quando ocorrer a falha no DHCP?

- a) 169.254.1.0 até 169.254.254.255.
- b) 192.168.0.0 até 192.168.0.255.
- c) 10.0.0.1 até 10.255.255.254.
- d) 192.168.0.1 até 192.168.0.254.
- e) 172.0.0.1 até 172.255.255.255.

3) São ferramentas utilizadas para verificação da rota dos pacotes na rede:

- a) ping e netstat.
- b) iperf e netstat.
- c) traceroute e mtr.
- d) traceroute e htop.
- e) ping e ifconfig.

4) Assinale a alternativa, com base na norma **NBR 14565**, que apresenta a sequência **CORRETA** de cores dos fios quando é realizada uma conectorização no padrão **T568A**.

- a) Branco Verde, Verde, Laranja, Branco Laranja, Azul, Branco Azul, Marrom, Branco Marrom.
- b) Branco Verde, Verde, Branco Laranja, Azul, Branco Azul, Laranja, Branco Marrom, Marrom.
- c) Branco Laranja, Laranja, Branco Verde, Verde, Azul, Branco Azul, Branco Marrom, Marrom.
- d) Branco Laranja, Verde, Branco Verde, Laranja, Azul, Branco Azul, Branco Marrom, Marrom.
- e) Branco Azul, Verde, Branco Laranja, Laranja, Azul, Branco Verde, Branco Marrom, Marrom.

5) Assinale a alternativa **FALSA**.

- a) RIP e OSPF são exemplos de protocolos de roteamento intra-domínio.
- b) BGP é um protocolo de roteamento inter-domínio.
- c) OSPF utiliza um algoritmo de estado de enlace.
- d) RIP utiliza um algoritmo de vetor distância.
- e) O RIP converge mais rapidamente que o OSPF.

6) De acordo com a norma **NBR 14565**, deverá haver um padrão para identificação de pontos de telecomunicações no projeto da rede. Assinale a alternativa que apresenta o formato **CORRETO** determinado pela norma.

- a) PT XX XXX, sendo PT “ponto de telecomunicações”, XX “representa o pavimento onde está localizada a tomada” e XXX “representa um número sequencial da tomada”.
- b) PT XX XXX, sendo PT “ponto de telecomunicações”, XX “representa o tipo de cabo” e XXX “representa um número sequencial da tomada”.
- c) PT XX XXX, sendo PT “ponto de telecomunicações”, XX “representa um número sequencial da tomada” e XXX “representa o pavimento onde está localizada a tomada”.
- d) TC XX XXX, sendo TC “tomada de cabo”, XX “representa o pavimento onde está localizada a tomada” e XXX “representa um número sequencial da tomada”.
- e) PT XX XXX, sendo PT “ponto de telecomunicações”, XX “representa o pavimento onde está localizada a tomada” e XXX “representa o tipo de cabeamento”.

7) Assinale a alternativa **CORRETA**.

- a) A distância máxima recomendada para uso com cabos UTP é de 120 metros.
- b) Não há problemas de interferência ao utilizar no mesmo duto cabos UTP sem blindagem e cabeamento elétrico.
- c) Em *racks* para uso de equipamentos ativos de rede a medida padrão de largura esperada para os dispositivos é de 17 polegadas.
- d) A aplicação de curvatura do cabeamento de rede lógica fora do padrão estabelecido na norma poderá aumentar a atenuação do sinal e causar perdas de pacotes.
- e) O processo de crimpagem de conectores machos RJ-45 utiliza alicates de tipo *punch-down*.

8) Sobre redes sem fios do padrão IEEE 802.11n, assinale a alternativa onde são apresentados os **três** canais de comunicação que não possuem sobreposição entre si.

- a) 2, 8, 12.
- b) 1, 7, 11.
- c) 1, 2, 3.
- d) 1, 6, 11.
- e) 1, 6, 9.

9) Assinale a alternativa onde **TODAS** as opções listadas são mecanismos de segurança em redes do padrão IEEE 802.11.

- a) PAT, WPA, WPA2.
- b) HTP, WEP, RTP.
- c) WEP, WPA, WPA2.
- d) VPN, IPSEC, ICMP.
- e) WEP, WISP, WPA.

10) Assinale a alternativa **INCORRETA**.

- a) O protocolo ARP tem como função principal realizar a descoberta de endereços MAC a partir de um endereço IP na rede local diretamente conectada.
- b) O protocolo IPSEC atua na camada de rede e é utilizado para a criação de VPNs.
- c) Os protocolos DHCP, SNMP e NTP utilizam o protocolo UDP para realizar o transporte de pacotes.
- d) O uso do protocolo TELNET é recomendado para acesso a dispositivos em redes públicas não-confiáveis.
- e) O protocolo SCP é um subsistema do protocolo SSH e permite a cópia de arquivos e pastas de forma segura.

11) A funcionalidade “DHCP Snooping” é encontrada em *switches* gerenciáveis. Assinale a alternativa que descreve o conceito desta funcionalidade.

- a) Serve para limitar o número de pacotes *multicast* em determinada porta de um *switch*.
- b) Serve para gerar endereços IP para *hosts* ligados a determinada porta de um *switch*.
- c) Serve para bloquear servidores DHCP não-autorizados em determinadas portas de um *switch*.
- d) Serve para limitar o número de pacotes *unicast* em determinada porta de um *switch*.
- e) Serve para permitir que os *hosts* conectados ao *switch* possam realizar descoberta de dispositivos.

12) Assinale a alternativa onde estão listadas duas ferramentas que servem para realizar testes e diagnóstico de problemas em servidores de DNS.

- a) iperf e ping.
- b) ping e traceroute.
- c) netstat e nslookup.
- d) nslookup e dig.
- e) nmap e ping.

13) O uso de VLANs é fundamental para organização e melhoria da segurança em uma rede de computadores. Em relação ao conceito e uso de VLANs, assinale a alternativa **CORRETA**.

- a) A identificação das VLANs (VID) é baseada em um campo de 16 bits.
- b) Uma porta de um *switch* gerenciável configurada em modo “acesso” é utilizada para conectar *hosts* que não interpretam as marcações de VLAN dos pacotes.
- c) Uma porta de um *switch* em modo “trunk” (tronco), obrigatoriamente, deverá repassar todas as VLANs configuradas no *switch*.
- d) Por padrão, a identificação da VLAN de gerenciamento em *switches* possui o VID “5”.
- e) O conceito de portas “tagged” é similar ao conceito de portas em modo “acesso”.

14) Em um servidor de *firewall* usando o sistema operacional Linux, deverá ser criada uma regra de *firewall* para liberar o acesso do IP 10.15.90.4 para o banco de dados MySQL que está hospedado no IP de endereço 200.18.76.10. Sendo o *firewall* com Iptables usando a política “DROP” na *chain* “FORWARD”, a porta do banco de dados MySQL padrão e a interface de entrada “eth1”, assinale a alternativa que possui a regra correta para realizar a liberação.

- a) iptables -I FORWARD -i eth1 -p tcp -s 10.15.90.4/32 -d 200.18.76.10/32 --dport 3306 -j ACCEPT
- b) iptables -I FORWARD -i eth1 -p tcp -s 10.15.90.4/32 -d 200.18.76.10/32 --dport 5432 -j ACCEPT
- c) iptables -I FORWARD -i eth1 -p tcp -s 200.18.76.10/32 -d 10.15.90.4/32 --dport 5432 -j ACCEPT
- d) iptables -I FORWARD -i eth0 -p tcp -s 200.18.76.10/32 -d 10.15.90.4/32 --dport 3306 -j ACCEPT
- e) iptables -D FORWARD -i eth1 -p tcp -s 10.15.90.4/32 -d 200.18.76.10/32 --dport 5432 -j ACCEPT

15) Com base no modelo TCP/IP é **CORRETO** afirmar que roteadores, *bridges* e *switches* de camada L2 operam, respectivamente, nas camadas de:

- a) rede, enlace e enlace.
- b) enlace, rede e enlace.
- c) enlace, rede e rede.
- d) rede, rede e enlace.
- e) rede, enlace e transporte.

16) O envio de pacotes em modo *broadcast* tem como destino todos os *hosts* pertencentes à rede diretamente conectada ao *host* emissor. Em uma rede LAN, um determinado *host* possui o IP 192.168.1.10/24 e uma aplicação neste *host* envia um pacote em *broadcast*. Assinale a alternativa **CORRETA** que lista os endereçamentos de destino na camada de enlace de dados e na camada de rede do pacote emitido pelo *host* 192.168.1.10 .

- a) Camada de Enlace de Dados: 00:00:00:00:00:00
Camada de Rede: 0.0.0.0
- b) Camada de Enlace de Dados: FF:FF:FF:FF:FF:FF
Camada de Rede: 192.168.0.255
- c) Camada de Enlace de Dados: FF:FF:FF:FF:FF:FF
Camada de Rede: 192.168.1.255
- d) Camada de Enlace de Dados: 00:00:00:00:00:00
Camada de Rede: 192.168.0.255
- e) Camada de Enlace de Dados: 00:00:00:00:00:00
Camada de Rede: 255.255.255.255

17) Em determinada empresa, um usuário relatou ao suporte de redes que o seu computador não estava com acesso à Internet. O atendente do suporte, ao solicitar ao usuário qual o endereço IP estava configurado no computador, foi relatado o endereço 10.0.0.10. Sendo o endereçamento IP configurado na rede da empresa 172.26.0.0/16 e distribuído de forma dinâmica, assinale a alternativa que apresenta a causa mais provável do problema relatado pelo usuário.

- a) Problemas no serviço de DNS.
- b) Existência de um servidor de DHCP não-autorizado na rede da empresa.
- c) Cabo desconectado no computador do usuário.
- d) Sistema operacional não atualizado.
- e) *Firewall* do computador desabilitado.

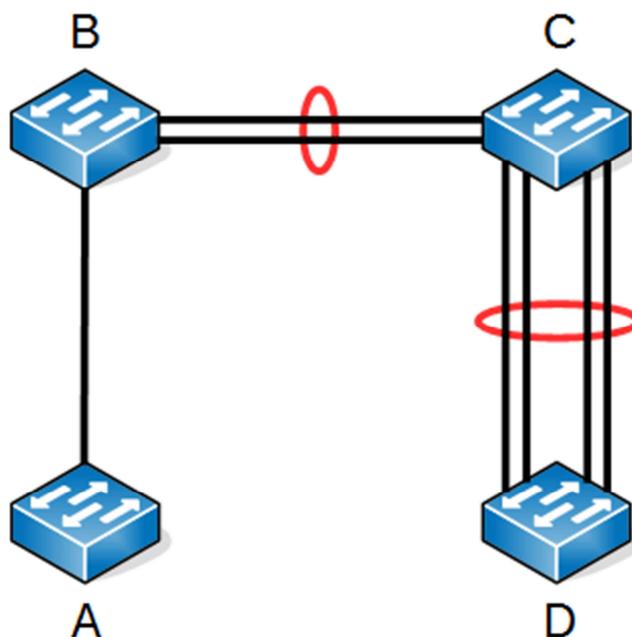
18) Sobre endereçamento IPv6, a alternativa que está **INCORRETA** é?

- a) O endereçamento IPv6 pode ser dividido em três tipos: *unicast*, *anycast* e *multicast*.
- b) 2001:0db8:015d:0000:0000:0000:0130:0001 pode ser representado por 2001:db8:15d::130:1.
- c) 2001:0db8:j0a0:bebe:cafe::1 representa um formato correto de endereço IPv6.
- d) 2001:0db8:f00f:0000:0192:0168:0000:0010 não pode ser representado por 2001:db8:ff:0:192:168:0:10.
- e) Os endereços considerados *Link Local* são representados pelo bloco fe80::/10.

19) Sobre a rede 192.168.96.0/23, pode-se concluir que:

- a) 192.168.96.255 é o endereço de *broadcast*.
- b) 192.168.97.0 é um endereço inválido para *host*.
- c) 192.166.97.255 é o endereço de *broadcast*.
- d) 192.168.96.0 é um endereço válido para *host*.
- e) 192.168.97.255 é o endereço de *broadcast*.

20) Observe o diagrama a seguir.



Sabendo que a comunicação entre os *switches* está estabilizada e totalmente operante, com base no protocolo LACP (*Link Aggregation Control Protocol*) e suas características, pode-se concluir que:

- a) ao todo, o diagrama apresenta dois LAG (*Link Aggregation Group*): um entre os *switches* B e C; e um entre os *switches* C e D.
- b) existem dois LAG (*Link Aggregation Group*), distintos, entre os *switches* C e D.
- c) se uma das portas do *switch* B ficar indisponível, B e C perdem a comunicação entre eles.
- d) o protocolo LACP permite o uso de três modos de operação: ativo, passivo e alternado.
- e) o protocolo LACP bloqueia todas as portas, deixando apenas uma ativa para cada enlace, a fim de evitar *looping* na rede local.

21) Sobre SNMP e suas características, assinale a alternativa **INCORRETA**.

- a) GET e SET são comandos utilizados no protocolo SNMP.
- b) É possível efetuar a alteração de valores em dispositivos gerenciados utilizando o comando SET.
- c) O gerente SNMP (cliente) responde às requisições do agente SNMP (servidor).
- d) O agente SNMP (servidor) responde às requisições do gerente SNMP (cliente).
- e) A versão 3 do protocolo SNMP é a mais segura, permitindo a autenticação, o controle de acesso e a privacidade nas transações feitas entre cliente-servidor.

22) Sobre o padrão IEEE 802.11 (WLAN) e suas variações, é correto afirmar que:

- a) os padrões 802.11b/g/n operam somente na frequência de 5GHz.
- b) o padrão 802.11ac possui desempenho inferior ao padrão 802.11g.
- c) equipamentos que operam na frequência de 2.4GHz não causam interferência nas WLANs que utilizam os padrões 802.11b e 802.11g.
- d) o padrão 802.11ac possui as larguras de banda 20, 40, 80 e 160MHz disponíveis para uso.
- e) o padrão 802.11a opera somente na frequência de 2.4GHz.

23) Assinale a alternativa que apresenta um protocolo utilizado para o envio de arquivos na atualização de *firmware* em *switches*.

- a) ARP.
- b) TFTP.
- c) DNS.
- d) Radius.
- e) SNTP.

24) Com relação às camadas do modelo OSI, assinale a alternativa que contém o correto ordenamento considerando como ponto inicial a camada mais baixa.

- a) Física, Enlace, Rede, Transporte, Apresentação, Sessão, Aplicação.
- b) Física, Rede, Enlace, Transporte, Sessão, Apresentação, Aplicação.
- c) Física, Transporte, Rede, Enlace, Apresentação, Sessão, Aplicação.
- d) Física, Enlace, Transporte, Rede, Sessão, Aplicação, Apresentação.
- e) Física, Enlace, Rede, Transporte, Sessão, Apresentação, Aplicação.

25) A seguir são apresentados comandos e resultados da ferramenta *traceroute*:

Comando 1) *traceroute -q 1 -T www.furg.br*

Resultado 1) *traceroute to www.furg.br (200.19.254.110), 30 hops max, 60 byte packets*
 1 10.113.0.1 (10.113.0.1) 14.295 ms
 2 c915c001.virtua.com.br (201.21.192.1) 14.795 ms
 3 c915c00a.virtua.com.br (201.21.192.10) 40.079 ms
 4 *
 5 *
 6 *
 7 200.19.255.70 (200.19.255.70) 20.033 ms
 8 *
 9 furg.br (200.19.254.110) 20.273 ms

Comando 2) *traceroute -q 1 -m 9 www.furg.br*

Resultado 2) *traceroute to www.furg.br (200.19.254.110), 9 hops max, 60 byte packets*
 1 10.113.0.1 (10.113.0.1) 64.509 ms
 2 c915c001.virtua.com.br (201.21.192.1) 70.085 ms
 3 c915c00a.virtua.com.br (201.21.192.10) 68.811 ms
 4 as2716.portoalegre.rs.ix.br (200.219.143.1) 64.362 ms
 5 mlxe8.tche.br (200.19.246.5) 74.855 ms
 6 furg-ve-35-mlxe8.tche.br (200.19.240.18) 69.280 ms
 7 200.19.255.70 (200.19.255.70) 70.195 ms
 8 200.19.255.213 (200.19.255.213) 75.075 ms
 9 *

Em relação ao acima exposto é correto afirmar que:

I – no comando 1) o parâmetro *-q* indica o número de requisições que serão enviadas para cada *hop*.

II – no resultado 2) o destino *furg.br (200.19.254.110)* estava indisponível.

III – no comando 2) o parâmetro *-m* define o tamanho das mensagens enviadas.

IV – no comando 1) o parâmetro *-T* indica que as mensagens serão enviadas utilizando TLS.

V – no resultado 2) o endereço *200.19.255.213* respondeu com mensagens ICMP do tipo *TIME_EXCEEDED*.

Assinale a alternativa que apresenta as afirmações **VERDADEIRAS**.

- a) Apenas I e V.
- b) Apenas I, II e V
- c) Apenas II, III e IV
- d) Apenas II e III
- e) Apenas I, III e V