

CONHECIMENTOS ESPECÍFICOS

Com relação aos protocolos e conceitos de *ethernet*, julgue os itens a seguir.

- 51 10Base2, ou *thin ethernet*, é uma das implementações de *ethernet*. Ela requer a utilização de topologia em barramento, mas o comprimento de cada segmento não deverá ultrapassar 20 metros em razão do alto grau de atenuação do cabo coaxial utilizado para transmissão.
- 52 O padrão *ethernet* requereu que fossem impostas restrições tanto no comprimento mínimo como no máximo de um *frame*.
- 53 A sequência 06:1M:02:BB:2C é um exemplo de endereço *ethernet* na notação hexadecimal.
- 54 No padrão *ethernet*, o endereço de destino *unicast* é um caso especial do endereço *multicast*, no qual todos os *bits* do endereço são setados em 1.

A *ethernet* padrão de 10 Mbps passou por várias mudanças antes de suportar velocidades mais altas. Essas mudanças permitiram a evolução da *ethernet* para torná-la compatível com LANs de alta velocidade de transmissão de dados. Acerca dos novos padrões da *ethernet*, julgue os itens que se seguem.

- 55 A camada física no 10 *gigabit ethernet* foi desenvolvida para uso apenas com cabos de fibra óptica em grandes distâncias. As implementações mais comuns desse padrão são: 10Gbase-S, com comprimento máximo de 1 km; 10Gbase-L, com comprimento máximo de 10 km; e 10Gbase-E, com comprimento máximo de 20 km.
- 56 No *fast ethernet*, a autonegociação permite que dois dispositivos negociem o modo ou a taxa de dados da operação.
- 57 Na evolução da *ethernet* de 10 Mbps para 100 Mbps manteve-se inalterada a camada física, a fim de que se garantisse a compatibilidade com as versões anteriores da *ethernet* padrão.
- 58 No modo *full-duplex* do *gigabit ethernet*, não existem colisões. O comprimento máximo do cabo é determinado em função da atenuação do sinal no cabo.

Para interligar LANs, ou segmentos de LANs, são usados elementos que podem operar em diferentes camadas da arquitetura TCP/IP. A respeito de elementos de interconexão, julgue os próximos itens.

- 59 O roteador é um dispositivo de três camadas que direciona pacotes com base em seus endereços físicos (endereçamento *host-host*).
- 60 Em uma *bridge* transparente, as estações desconhecem completamente a sua existência, todavia, se uma *bridge* for acrescentada ou eliminada do sistema, é necessário reconfigurar as estações.
- 61 Um *hub* passivo é, simplesmente, um conector que interliga os cabos provenientes de diferentes ramificações.
- 62 Um repetidor é um dispositivo que opera apenas na camada física. Ele recebe um sinal e, antes do sinal se tornar muito fraco ou corrompido, regenera o padrão de *bits* original. Assim, uma de suas funções é interligar diferentes LANs.

Julgue os itens seguintes, acerca de elementos de interconexão.

- 63 Um *gateway* é um dispositivo que opera em todas as camadas de uma rede e é capaz de atuar nas cinco camadas da arquitetura TCP/IP e nas sete camadas do modelo OSI.
- 64 Uma *bridge* possibilita que uma rede desenvolvida para usar o modelo OSI possa ser conectada a uma rede que utiliza o modelo TCP/IP.
- 65 Um *hub* ativo opera tanto na camada física quanto na camada de enlace de dados. Como um dispositivo da camada física, ele regenera o sinal que recebe. Ao atuar como um dispositivo da camada de enlace de dados, ele é capaz de verificar os endereços MAC (origem e destino) contidos no *frame*.

Na comunicação dos computadores pela Internet, é necessário um esquema de endereçamento global. Consoante os conceitos e as regras para os endereços IPs, julgue os próximos itens.

- 66 Um provedor de acesso à Internet que receba um bloco de endereços iniciado em 190.100.0.0/16 tem 65.536 endereços para serem atribuídos aos seus clientes.
- 67 A sequência 75.45.301.14 é um exemplo de endereço IPv4 válido.
- 68 O endereço 00000001 00001011 00001011 11101111, mostrado na notação binária, pertence a classe A de endereços IPv4.
- 69 Considere que um bloco de endereços IPs tenha sido concedido ao Banco da Amazônia S.A. e que um dos endereços pertencentes ao bloco seja 205.16.37.39/28. Nesse caso, é correto afirmar que o último endereço do bloco concedido é 205.16.37.47.

Apesar de todas as soluções de curto prazo, como endereçamento sem classes, o esgotamento de endereços IPs é um problema para a Internet. Com relação aos conceitos e protocolos da família TCP/IP, julgue os itens subsequentes.

- 70 O DHCP (*dynamic host configuration protocol*) permite a alocação estática e dinâmica de endereços, a qual pode ser manual ou automática.
- 71 As três sequências abaixo são representações válidas de um mesmo endereço IPv6.
FDEC:0074:0000:0000:0000:B0FF:0000:FFFF
FDEC:74:0:0:0:B0FF:0:FFFF
FDEC:74: :B0FF:0:FFFF
- 72 No protocolo IPv6, assim como no protocolo IPv4, os únicos tipos de endereços que existem são *unicast* e *multicast*.
- 73 Suponha que um computador que utilize IPv6 precise enviar uma mensagem a outro computador que também utilize IPv6, mas a mensagem precisa passar por uma parte da rede que esteja operando em IPv4. Nessa situação, deve ser usado um endereço compatível, cujo prefixo de tipo é 0000 0000.
- 74 Uma conexão TCP (*transmission control protocol*) envolve um único endereço IP de destino e de origem. Uma associação no SCTP (*stream control transmission protocol*) suporta serviços *multihoming*, ou seja, os *hosts* emissor e receptor podem definir vários endereços IP em cada ponto final.

Acerca de técnicas de comutação de circuitos, pacotes e mensagens, julgue os próximos itens.

- 75 Uma rede de circuitos virtuais é uma união entre uma rede de comutação de circuitos e uma rede de datagramas, pois apresenta características de ambas as redes que formam essa união.
- 76 Na comutação de circuitos, os recursos precisam ser reservados durante a fase de estabelecimento da conexão. Todavia, os recursos não precisam permanecer dedicados por toda a duração da transferência de dados.
- 77 Na comutação de células, a alocação de banda de transmissão é feita dinamicamente, tendo por base a demanda.

Em uma rede comutada, parte dos nós é diretamente conectada aos sistemas finais e outra parte é utilizada apenas para roteamento. Com base nos conceitos e nas técnicas de comutação, julgue os itens que se seguem.

- 78 A comutação de células opera com blocos de tamanho variável, e geralmente esses blocos são de tamanho reduzido, por isso são chamados de células.
- 79 A comutação na Internet é realizada usando-se a metodologia de datagramas para a comutação de pacotes na camada de redes.
- 80 Na comutação de circuitos, os dados a serem transferidos são empacotados e quebrados em unidades cujo tamanho é determinado pela camada de rede.

A respeito de conceitos e características do protocolo MPLS (*multiprotocol label switching*), julgue os itens seguintes.

- 81 Um quadro melhorado com MPLS somente pode ser enviado entre roteadores habilitados para MPLS ou habilitados para IP.
- 82 O cabeçalho MPLS deve ser inserido entre os cabeçalhos da camada de rede e da camada de transporte.
- 83 Nas redes MPLS, os pacotes percorrem a rede pública por meio de caminhos estáticos do tipo circuito, que são a base para redes virtuais privadas (VPNs).
- 84 O MPLS provê uma forma simples de implementar engenharia de tráfego porque ele tem a capacidade de repassar pacotes por rotas impossíveis de se utilizar com protocolos padronizados de roteamento IP.
- 85 Diferentemente da rede de telefonia de comutação de circuitos, as redes MPLS são redes de comutação de pacotes por circuitos virtuais.

Acerca de padrões da família 802.11, julgue os itens a seguir.

- 86 As tecnologias e os protocolos IEEE 802.11b e IEEE 802.11g usam ou podem usar a faixa de frequência de 2,4 GHz, que também é empregada nas tecnologias *bluetooth* e *ZigBee*, todas de comunicação em redes locais que utilizam meios não guiados.
- 87 Ao se usar o DSSS (*direct sequence spread spectrum*) em uma rede padrão IEEE 802.11, torna-se desnecessário utilizar canais distintos para diferentes pontos de acesso que estejam fisicamente próximos e configurados no modo de infraestrutura, uma vez que o espalhamento espectral reduz as interferências entre os canais.
- 88 A baixa interferência entre redes IEEE 802.11b e IEEE 802.11g é facilitada devido ao fato de que as duas usam diferentes esquemas de modulação, apesar de usarem a mesma faixa de frequência e canalização.
- 89 As tecnologias de rede IEEE 802.11a e IEEE 802.11b usam modulação DSSS e OFDM, respectivamente, sendo que a modulação DSSS permite ao protocolo IEEE 802.11a funcionar com uma velocidade de até 54 Mbps, enquanto IEEE 802.11b é limitado a 11 Mbps.

Com relação aos conceitos básicos de funcionamento e segurança de tecnologias e protocolos de rede sem fio, julgue os itens subsequentes.

- 90 A característica de WPS (*Wi-Fi protected setup*) foi introduzida no modelo de segurança WPA e é inexistente no protocolo WEP. Essa característica contribuiu significativamente para reduzir a vulnerabilidade das redes sem fio a ataques de força bruta para realizar associação indevida à rede.
- 91 O *upgrade* do *firmware* de um dispositivo IEEE 802.11 é uma das formas mais comuns de correção de vulnerabilidades de segurança encontradas nesse dispositivo.
- 92 A escolha de um protocolo de segurança que usa a técnica de CRC (*cyclic redundancy check*), em vez de outro que emprega a técnica MAC (*message authentication code*), contribui para reduzir a vulnerabilidade de ataques à autenticidade em uma rede sem fio.
- 93 Entre os complexos desafios ao gerenciamento de chaves em um ambiente de redes sem fio, encontra-se o problema da distribuição de chaves. Nesse tipo de problema, o uso de protocolos de troca de chave do tipo Diffie-Hellman possibilita a troca de chaves de forma *out-of-band*.
- 94 Em uma configuração de rede IEEE 802.11 com WPA2, uma das razões para escolha da segurança AES-based CCMP (*advanced encryption standard based counter cipher mode with block chaining message authentication code protocol*), em vez de TKIP (*temporal key integrity protocol*), é a maior compatibilidade com equipamentos legados, especialmente com *hardware* aderente ao WEP (*wired equivalent protocol*).
- 95 Em uma configuração de rede IEEE 802.11 com WPA2-Enterprise faz-se necessária a instalação de um serviço Kerberos, para fins de autenticação, autorização e contabilização.
- 96 A arquitetura de uma rede WPA-2 com autenticação embasada no protocolo IEEE 802.1X, também conhecido como encapsulamento EAPOL (*extensible authentication protocol over local area network*), é composta por três partes: um solicitante, um servidor de autenticação e um autenticador. Nessa arquitetura, o autenticador é que deve possuir maior inteligência, isto é, conhecimento dos detalhes, do processo de autenticação.
- 97 Em uma rede TCP/IP que se baseia em enlaces IEEE 802.11 com segurança 128-bit WEP ao se registrar uma chave com *X bits*, concatenada com *Y bits* de um vetor de inicialização, resulta em uma chave completa cuja soma *X+Y* é igual a 128 bits.
- 98 Em uma rede TCP/IP baseada em enlaces IEEE 802.11 com segurança 128-bit WEP, uma chave criptográfica de tamanho fixo é usada como semente para um cifrador de fluxo RC4, visando gerar uma chave criptográfica de fluxo (*keystream*) que será aplicada apenas ao *payload* dos pacotes IP que trafegam nessa rede.
- 99 Uma rede IEEE 802.11 que usa segurança embasada no protocolo WPA2 apresenta menor vulnerabilidade que uma com base no WEP, entre outras coisas, porque esquemas de cifragem empregados no WPA2 são mais avançados que aqueles empregados no WEP.
- 100 Considerando-se um ponto de acesso para uma rede 64-bit WEP, o uso de uma máscara ASCII com limite de 5 caracteres na digitação da chave deixa a rede mais vulnerável a ataque por meio de força bruta, quando comparada a uma máscara de entrada de dados com limite de 10 dígitos hexadecimais.

A respeito de noções de administração de dados na plataforma de sistemas operacionais Windows ou Linux, julgue os itens seguintes.

- 101** A opção por uso de fita magnética para *backup* dos dados de um serviço *online*, em detrimento de uso de discos rígidos, se torna cada vez mais atraente quanto mais importante forem as necessidades de preservação dos dados a longo prazo, isto é, para finalidades arquivísticas.
- 102** O uso de sistemas de arquivo no padrão NTFS, em detrimento do FAT32, oferece, entre algumas vantagens na administração de dados, o suporte a arquivos que podem exceder 1 *terabyte* de tamanho e suporte a nomes de arquivos que excedem 256 caracteres.

Julgue os próximos itens com relação a serviços de diretório AD (Active Directory) e LDAP (*lightweight directory access protocol*), no âmbito dos sistemas operacionais Windows ou Linux.

- 103** O protocolo LDAP é implementado pelo OpenLDAP, *software* livre de código aberto, disponível na plataforma Linux e compatível com Windows, que provê suporte a operações básicas do LDAP, as quais permitem, entre outras, autenticação, busca por entradas, adição, remoção e modificação de entradas (nós).
- 104** Caso executada com sucesso em um domínio X de um serviço de diretório no Active Directory, a consulta LDAP (`objectCategory=computer`) (`!description=*`) retornaria uma lista com todos os computadores do domínio X que não possuem descrição.
- 105** Uma das desvantagens do Active Directory, com relação a implementações como o OpenLDAP, é que o Active Directory não suporta replicação de bancos de dados nem a criação de cadeias de confiança.
- 106** Uma instalação do Active Directory em ambiente heterogêneo Windows e Linux dispensa o uso de serviços como o NIS (*network information system*), uma vez que, na hierarquia do Active Directory, é possível o armazenamento centralizado ou distribuído de bancos de dados contendo dados de autenticação de usuários.
- 107** O protocolo de autenticação TACACS é usualmente uma solução empregada para suporte à autenticação em uma instalação de Active Directory ou LDAP.
- 108** Em uma rede na qual funciona um serviço de diretório aderente ao protocolo LDAP, a porta de serviço que recebe requisição dos clientes é a 389, TCP. Sendo assim, os pacotes IP que circulam nessa rede, relacionados ao uso do serviço LDAP, contêm em seu cabeçalho a indicação de que 389 é o número da porta de origem ou o da porta de destino.

Acerca de interoperabilidade de dados, julgue os itens subsecutivos.

- 109** O uso de *middleware* em um ambiente de TI tem como efeito principal o aumento da interoperabilidade desse ambiente.
- 110** O padrão XML (*extensible markup language*) é mais adequado à obtenção de interoperabilidade no nível sintático, quando comparado ao padrão RDF (*resource description framework*), este último de nível semântico.
- 111** DTD (*document type definition*) e XSD (*XML schema description*) são dois formatos de interoperabilidade de dados usados no escopo do padrão XML, e, de modo geral, um documento DTD é semanticamente menos expressivo que seu equivalente XSD.
- 112** A arquitetura ANSI SPARC é um modelo de interoperabilidade de dados, voltado para o domínio de sistemas de gerenciamento de bases de dados (SGBDs). O modelo em questão é organizado em três níveis, dos quais um é o nível conceitual, mais semântico; e outro é o nível físico ou interno, mais sintático.
- 113** Um documento codificado em ASCII possui maior expressividade e interoperabilidade semântica que um similar codificado em UTF-8.
- 114** O aumento da interoperabilidade semântica de determinada plataforma computacional reduz as chances de preservação digital de um documento.

Com relação a ferramentas automatizadas de gestão da infraestrutura de ambientes de TIC, julgue os itens que se seguem.

- 115** Uma ferramenta de virtualização de *storage* tem como um de seus benefícios centrais o ganho de mobilidade no armazenamento.
- 116** Uma ferramenta de gerência de ativos provê melhoria imediata na eficiência do processo de registro de incidentes e menos impacto sobre o gerenciamento de níveis de serviço.
- 117** A contratação de um serviço de computação em nuvem do tipo PaaS (*platform as a service*) demandará do adquirente do serviço maior conhecimento de ferramentas automatizadas de gestão da infraestrutura, especialmente as relacionadas à administração de dados, quando comparada à contratação de um serviço do tipo SaaS (*software as a service*).
- 118** Eventos produzidos por SNMP *traps* são insumos de elevada relevância para uma ferramenta automatizada de gerenciamento de disponibilidade.
- 119** Simuladores de carga são ferramentas tipicamente mais bem empregadas no provisionamento de serviços de TI que no gerenciamento e planejamento de capacidade de uma infraestrutura de TI.
- 120** Uma ferramenta de gestão de relacionamento com clientes impacta de forma mais direta o gerenciamento de mudanças, e de forma menos direta o gerenciamento de acordos de níveis de serviço.