

## CONHECIMENTOS ESPECÍFICOS

A respeito de redes WAN (*wide area network*), julgue os itens a seguir.

- 61 A tecnologia *frame relay*, embora com capacidade de transmissão em alta velocidade, não é adequada para uso em WANs.
- 62 Nas WANs, as linhas de transmissão podem utilizar fios metálicos e fibras ópticas, entre outros meios.
- 63 O protocolo PPP pode ser usado nas conexões em uma rede WAN.

O projeto de cabeamento estruturado de um condomínio com vários edifícios deve prever a instalação de mais de 500 pontos de rede para transmissão de dados e voz.

Acerca desse projeto e a respeito de cabeamento estruturado, em geral, julgue os itens seguintes.

- 64 Caso a interconexão de alguns concentradores da referida rede requeira cabos com comprimento superior a 500 m, será recomendável a utilização de fibras ópticas em vez de cabos do tipo UTP, inadequados para essa interconexão.
- 65 Cabos do tipo UTP de categoria 5 constituem meio de transmissão capaz de suportar taxas de transmissão de até 10 Gbps.
- 66 Os painéis de conexão (*patch panel*) facilitam a identificação dos pontos de rede e podem ser utilizados como intermediários entre os computadores e um concentrador de rede, como, por exemplo, um *switch*.
- 67 Considere que, nos edifícios do projeto em questão, não exista tubulação específica para o cabeamento da rede de dados e que o cabeamento de energia elétrica instalado não possua blindagem. Nessas condições, para reduzir custos, é adequado instalar, na tubulação em que esteja o cabeamento elétrico dos edifícios, pares trançados de categoria 5, sem blindagem, uma vez que a corrente alternada nos cabos de energia elétrica certamente não causará interferência relevante na transmissão de dados.

A respeito de redes locais sem fio nas quais sejam utilizados os padrões IEEE 802.11, julgue os itens de 68 a 73.

- 68 Na arquitetura do tipo *ad hoc*, os computadores da rede deverão estar, necessariamente, conectados a um *access point* para que seja possível o envio de dados entre eles.
- 69 O padrão IEEE 802.11g, para rede local sem fio, especifica uma técnica de transmissão que opera em 2,4 GHz.
- 70 Em uma organização onde exista uma rede sem fio no padrão IEEE 802.11a, com velocidade máxima de 11 Mbps, caso seja necessário adaptar a rede para operar com transmissões superiores a 110 Mbps, a fim de atender demandas de acesso a aplicações contendo vídeos e arquivos com grandes volumes de dados, essa nova demanda poderá ser atendida com a troca dos equipamentos de rede atuais por equipamentos que utilizem o padrão IEEE 802.11n.

- 71 Um sistema de telefonia sem fio que opere em 2,4 GHz e uma rede sem fio no padrão IEEE 802.11b não sofrem interferência mútua, pois esse tipo de rede não opera em 2,4 GHz.
- 72 As redes sem fio no padrão IEEE 802.11 não utilizam detecção de colisão, mas possuem recursos para evitá-la, como o de detectar se o canal de transmissão está ocioso para, só então, realizar a transmissão.
- 73 Os *access points* que concentram as conexões dos terminais de usuários de uma rede sem fio não transmitem o SSID por *broadcast*.

Acerca do serviço VoIP, julgue os seguintes itens.

- 74 O protocolo H.323, com controle de admissão e *codecs*, é uma alternativa ao SIP utilizada em audioconferências e videoconferências.
- 75 O RTP (*real-time transport protocol*) tem capacidade para transportar dados de um serviço VoIP sobre o protocolo UDP (*user datagram protocol*).
- 76 O SIP (*session initiation protocol*), que provê mecanismos para suporte de tráfego de voz, necessita de outros protocolos para estabelecer e encerrar chamadas em uma rede IP.

A respeito das tecnologias ADSL, julgue os itens que se seguem.

- 77 O *modem* ADSL tem a função de converter o fluxo de *bits* entregue por um dispositivo (um computador, por exemplo) a ele conectado em um sinal com características apropriadas para trafegar pela linha telefônica, juntamente com um eventual sinal de voz de uma ligação telefônica.
- 78 O serviço ADSL opera basicamente com dados que são enviados e recebidos por meio de um computador, e, para isso, necessita utilizar um ou mais protocolos para transportar os dados através da rede telefônica; um deles é o protocolo IPX (*internetwork packet exchange*) que é orientado a conexão.
- 79 A primeira geração do ADSL permite acessos com velocidades de *download* de até 50 Mbps, quando são usadas linhas telefônicas de qualidade, com comprimento máximo de 2 km; para velocidades superiores a essa, é necessário o uso do padrão ADSL2.
- 80 O padrão ADSL2+ apresenta como vantagem a possibilidade de preservação do investimento, pois pode operar na mesma infraestrutura física instalada para uso dos padrões ADSL e ADSL2.
- 81 Entre os componentes de uma rede ADSL, encontram-se os divisores de potência, cuja função é concentrar o tráfego de várias linhas telefônicas em um único *modem* ADSL, por meio do qual é feito o acesso à rede de dados.

Julgue os itens subsequentes, relativos a *gateways* de aplicação pertencentes a um sistema de *firewall* cuja função seja proteger a rede interna de uma organização contra ataques oriundos da Internet.

- 82 Para filtrar o acesso a conteúdos que exibam vídeos no padrão MPEG na Internet, deve-se utilizar um filtro de aplicação, que inspeciona o tráfego na camada de aplicação; um filtro de pacotes é inadequado para essa função, visto que esse tipo de filtro realiza basicamente a filtragem de endereços IPs de origem e destino, tipos de protocolo e estados de conexão, entre outros.
- 83 Em um mesmo *gateway*, não é possível utilizar, em conjunto, os recursos de filtragem de aplicação e filtragem de pacotes, sendo necessário implementá-los em equipamentos distintos, caso se deseje utilizar ambos os recursos.
- 84 Um filtro de pacote que possua recurso de inspeção de estado tem a capacidade de substituir um filtro de aplicação no equipamento de *gateway*.

Acerca do NAT (*network address translation*) em um *gateway* com a função de conectar a rede interna de uma organização à Internet, julgue os itens seguintes.

- 85 Se o *gateway* for configurado no modo *bridge* (ponte), uma estação de trabalho que utilize o IP privado 192.168.0.100, com máscara de rede 255.255.255.0, poderá acessar a Internet sem a intervenção do recurso NAT, isto é, sem que ocorra a tradução de endereço no *gateway*.
- 86 O endereço e a porta de origem inscritos nos pacotes que, provenientes da Internet, passam pelo *gateway* com destino a uma estação de trabalho na rede interna podem ser alterados pela variante do NAT conhecida como NAPT (*network address and port translation*).
- 87 O *gateway* encarregado de fazer o NAT para o tráfego originado na rede interna e destinado à Internet armazena, em uma tabela NAT, as informações acerca das conexões correntes. Caso uma pane ocasione perda dos dados dessa tabela, as conexões TCP não serão destruídas, pois esse protocolo tem recursos para preservar as conexões nessa situação.
- 88 Por padrão o NAT funciona adequadamente com os protocolos TCP e UDP. Caso seja criado um protocolo de transporte diferente para acesso a uma aplicação, que necessite atravessar o *gateway* para ser acessada, cujo tráfego sofra o processo de NAT, o acesso a essa aplicação falhará.
- 89 As estações de trabalho da rede interna podem acessar a Internet utilizando endereços IPs privados. Para isso, é necessário que as estações de trabalho tenham, em suas configurações de rede, o endereço do equipamento de *gateway* e este deve ter a capacidade de trocar nos pacotes encaminhados à Internet o endereço privado por um endereço público.

A respeito de roteamento, julgue os itens a seguir.

- 90 Considere que um roteador em rede suporte circuitos virtuais e identifique a ocorrência de congestionamento, isto é, de tráfego de rede superior ao que ele suporta, o que prejudica o desempenho da rede. Nesse caso, para reduzir o congestionamento, pode-se utilizar o controle de acesso: um novo circuito virtual não será montado até que a rede tenha capacidade de transportar o tráfego sem ficar congestionada.
- 91 O campo TTL, existente no pacote IP, evita que pacotes fiquem presos em *loops* infinitos, devido a erros de configuração nas tabelas de roteamento: ao passar por um roteador, o valor do TTL é subtraído de um e, quando atinge zero, o pacote é descartado pelo roteador.
- 92 O VRRP (*virtual router redundancy protocol*) permite a utilização de pares de roteadores, operando um roteador do par como *master* e o outro como *backup*, que somente entra em operação se o *master* falhar.
- 93 Quando ocorre grande crescimento da tabela de roteamento de um roteador, em consequência aumenta o consumo de tempo de CPU e memória do roteador, para que os pacotes possam ser tratados.
- 94 Um roteador que utiliza a técnica de *flooding* (inundação) de roteamento envia cópias de cada pacote recebido para todas as suas interfaces de saída, exceto para a interface pela qual o pacote chegou.
- 95 Quando um roteador que esteja sofrendo congestionamento utiliza a técnica de corte de carga para solucionar o congestionamento, ele notifica os transmissores, por meio de um pacote regulador, para que pausem o envio de pacotes.

Julgue os itens a seguir, relativos ao STP (*spanning tree protocol*), um protocolo muito utilizado em redes com *switches*.

- 96 O STP possibilita a criação de dois *switches* do tipo raiz, que fazem balanceamento de carga e são capazes de fazer agregação de *links* quando existe um *loop* físico.
- 97 No STP, o *hello time* indica o tempo de transmissão da mensagem *hello* de um *switch* para outros *switches*.
- 98 No STP, o parâmetro *forward delay timer* monitora o tempo gasto por uma porta nos estados de aprendizagem e de escuta.
- 99 O STP permite redundância de caminhos e evita a criação de *loops* indesejáveis.
- 100 Quando o STP está em funcionamento em uma rede do tipo *fast ethernet*, ele prevê, nessa situação, dois caminhos ativos entre duas estações que estejam se comunicando.

A respeito das características gerais dos concentradores, dispositivos normalmente utilizados em redes de comunicação, julgue os itens que se seguem.

- 101** A velocidade do concentrador deve ser baixa, de modo que ele possa receber mensagens de vários terminais de baixa velocidade simultaneamente.
- 102** Em ambiente onde um concentrador recebe sinal de vários terminais ao mesmo tempo, durante o encaminhamento da mensagem também é enviada a identificação do terminal que gerou a mensagem.
- 103** Um concentrador de camada 2 deve ter capacidade de atender a mudanças nas velocidades de transmissão, formatos, códigos e protocolos de transmissão.
- 104** Um concentrador de camada 2, dispositivo com *buffer* de armazenamento, altera a velocidade de transmissão das mensagens.
- 105** Os concentradores não têm capacidade de processamento local.

Acerca das técnicas de multiplexação e de suas características gerais, julgue os itens subsequentes.

- 106** Em um sistema DWDM, entre os pontos de multiplexagem e demultiplexagem, um único comprimento de onda é transmitido.
- 107** Em um sistema DWDM, o ADM (*optical add/drop multiplexers*) é um dispositivo que pode remover e inserir comprimentos de onda em determinado caminho.
- 108** Multiplexadores e demultiplexadores ativos são baseados na combinação de elementos passivos com filtros e devem minimizar o efeito *cross-talk*.

Em engenharia de tráfego, é comum a otimização da transmissão por meio de técnicas que envolvam qualidade de serviço — *quality of service* (QoS) —, utilizando-se, para isso, diversos protocolos e tecnologias. A esse respeito, julgue os itens de **109** a **113**.

- 109** Com o protocolo RSVP (*resource reservation protocol*) a aplicação não é capaz de notificar antecipadamente de que recurso da rede ela necessitará. Apenas roteadores intermediários fazem essa notificação.
- 110** O *DiffServ*, modelo de serviços diferenciados, implementa QoS com base na definição de tipos de serviços.
- 111** O modelo de serviços diferenciados é caracterizado pela reserva de recursos.

- 112** Em uma rede com RSVP (*resource reservation protocol*), os receptores escolhem o nível de recursos a serem reservados e, de maneira geral, a rede responde explicitamente se admite ou rejeita as requisições de reserva de recurso.
- 113** Em redes com arquitetura de serviços integrados, existe, entre domínios adjacentes, um acordo — o SLA (*service level agreement*) — que estabelece os serviços que serão disponibilizados entre esses mesmos domínios.

Diversos dispositivos são utilizados para interconectar redes de comunicação embasadas em comutação de pacotes. Julgue os itens a seguir, acerca desses dispositivos e protocolos, considerando o modelo OSI como referência.

- 114** Um *hub*, quando dotado do princípio de encaminhamento do quadro baseado no endereço MAC e IP, trabalha nas camadas 2 e 3.
- 115** Uma *bridge* — dispositivo que faz a segmentação entre duas ou mais redes — atua na camada 2.
- 116** Um *switch*, que é dotado de encaminhamento rápido de quadros, encontra-se na camada 2.
- 117** Um roteador que se situe na camada 3 é responsável, entre outras funcionalidades, por interligar redes com endereços de rede IP diferentes.
- 118** O protocolo HTTP, amplamente utilizado na Internet, situa-se na camada 4.

A respeito do TCP/IP e do conjunto de protocolos que fazem parte da pilha, julgue os próximos itens.

- 119** No cabeçalho do protocolo ARP, o campo denominado *protocol type* tem 16 *bits* e corresponde ao endereço de alto nível provido pela rede de comunicação. No caso de uso em *frame relay*, esse campo retorna o número do canal virtual utilizado.
- 120** O campo *protocol* no cabeçalho do IP indica um valor numérico do protocolo que está fazendo uso do pacote IP no momento da transmissão.
- 121** O protocolo ICMP possui uma estrutura de dados em que o *checksum* é um campo obrigatório em implementações TCP/IP e possui 16 *bytes* de tamanho.
- 122** O TCP possui campos próprios em que estão definidos os estados da conexão, tais como SYN, ACK e FYN.

```

C:\ >nslookup
Default Server: ns.meudns.com.br
Address: 10.1.0.2

> server a.root.net
DNS request timed out.
  timeout was 2 seconds.
*** Can't find address for server a.root.net: Timed out
> set type=ns
> unb.br
Default Server: ns.meudns.com.br
Address: 10.1.0.2

Non-authoritative answer:
unb.br nameserver = dns2.unb.br
unb.br nameserver = dns3.unb.br
unb.br nameserver = server1.pop-df.rnp.br
unb.br nameserver = dns1.unb.br

server1.pop-df.rnp.br internet address = 200.19.119.125
> set type=mx
> unb.br
Default Server: ns.meudns.com.br
Address: 10.1.0.2

DNS request timed out.
  timeout was 2 seconds.
*** Request to ns.meudns.com.br timed-out
> set type=mx
> unb.br
Default Server: ns.meudns.com.br
Address: 10.1.0.2

Non-authoritative answer:
unb.br MX preference = 5, mail exchanger = mxd.unb.br
unb.br MX preference = 10, mail exchanger = mx.unb.br
unb.br MX preference = 10, mail exchanger = mx3.unb.br
unb.br MX preference = 5, mail exchanger = mxc.unb.br

unb.br nameserver = server1.pop-df.rnp.br
unb.br nameserver = dns1.unb.br
unb.br nameserver = dns2.unb.br
unb.br nameserver = dns3.unb.br
mxc.unb.br      internet address = 164.41.101.96
mxd.unb.br      internet address = 164.41.101.97
mx.unb.br       internet address = 164.41.101.16
mx3.unb.br      internet address = 164.41.101.112
dns1.unb.br     internet address = 164.41.101.3
dns2.unb.br     internet address = 164.41.101.6
dns3.unb.br     internet address = 164.41.101.8
server1.pop-df.rnp.br internet address = 200.19.119.125
>

```

Considerando o trecho de código mostrado acima, que descreve algumas consultas a um servidor DNS em busca de algumas respostas na Internet, julgue os itens a seguir.

- 123** Houve *time out* em uma consulta e as respostas dadas foram não autoritativas, ou seja, não foi o servidor DNS responsável pelo domínio `unb.br` que forneceu as respostas.
- 124** Infere-se do trecho de código que o endereço IP do cliente que fez as consultas a `ns.meudns.com.br` é `10.1.0.2`.
- 125** O trecho de código mostra que foi feita uma consulta acerca do name server responsável pelo domínio `unb.br`.
- 126** O trecho de código mostra que foi feita uma pesquisa acerca do *canonical name* do responsável pelo domínio `unb.br`.

As redes de computadores recebem, atualmente, ataques de diversos tipos, com os mais diversos propósitos. Acerca de tipos de ataques a redes e da segurança dessas redes, julgue os itens a seguir.

- 127** Intrusão ocorre quando um atacante consegue explorar alguma vulnerabilidade remota do computador — por exemplo, por meio de estouro de pilha — e consegue obter um *shell* remoto.
- 128** Em rede local, no ataque do tipo *man in the middle*, o atacante é capaz de desviar o fluxo normal da informação para a origem e para o destino em um processo de comunicação.
- 129** Ataques do tipo *syn flooding* consistem no envio seguido de requisições UDP, de tal forma que o computador atacado não consiga responder as requisições UDP, causando uma negação de serviço.
- 130** Ataques de inserção SQL (*SQL injection*) podem ocorrer com o protocolo HTTP; no entanto, o protocolo HTTPS não permite ataques desse tipo.