

CONHECIMENTO ESPECÍFICO

01. Suponha um usuário acessando a Internet por meio de um enlace de 256K bps.
O tempo mínimo necessário para transferir um arquivo de 1M byte é da ordem de
- A) 4 segundos.
 - B) 32 segundos.
 - C) 1 segundos.
 - D) 262 segundos.
 - E) 1024 segundos.
02. Um roteador na Internet deve obrigatoriamente processar os seguintes protocolos:
- A) IP, TCP e UDP.
 - B) IP e TCP.
 - C) IP apenas.
 - D) IP, TCP, UDP e HTTP.
 - E) IP, TCP, UDP e todos os protocolos de aplicação.
03. Não é um endereço IP versão 4:
- A) 200.128.100.254
 - B) 200.129.257.12
 - C) 1.100.45.2
 - D) 43.157.23.11
 - E) 153.91.188.242
04. A partir do endereço de rede 200.182.40.0/24 foi aplicada a máscara 255.255.255.252.
Quantos hosts são possíveis em cada nova rede criada?
- A) 8
 - B) 6
 - C) 2
 - D) 12
 - E) 62
05. O endereço de broadcast da rede 192.128.64.0/18 é:
- A) 192.128.127.255
 - B) 192.128.255.255
 - C) 192.128.64.255
 - D) 192.255.255.255
 - E) 192.128.128.255
06. Em um switch Ethernet foram criadas 5 VLANs.
Para projetar o endereçamento IP para estas VLANs:
- A) O acesso à Internet pode ser feito sem endereços IP.
 - B) Todas as VLANs podem compartilhar um mesmo prefixo de rede.
 - C) O endereçamento será definido automaticamente.
 - D) Deve ser criado um prefixo de rede diferente para cada VLAN.
 - E) Podem ser atribuídos endereços IP aleatoriamente para os hosts em cada VLAN.
07. A função de um painel de manobras (patch panel) é:
- A) Processar os pacotes e envia para a porta de destino correspondente.
 - B) Atuar como um multi-repetidor.
 - C) Reconstituir o sinal e transmite para o elemento de destino.
 - D) Realizar a gerência da rede pelo protocolo SNMP.
 - E) Proporcionar organização e flexibilidade na gerência do cabeamento.
08. Um switch (comutador) Ethernet:
- A) Implementa as operações de controle de acesso e segurança em uma rede.
 - B) É um elemento que processa pacotes na camada 3, montando tabelas com os endereços IP dos hosts conectados em cada porta.
 - C) Retransmite o sinal observado em uma porta para todas as outras.
 - D) Tem como função principal objetivo organizar o cabeamento da rede.
 - E) É um elemento que processa pacotes na camada 2, montando tabelas com os endereços de hardware dos hosts conectados em cada porta.
09. Um Hub Ethernet:
- A) Tem como função principal objetivo organizar o cabeamento da rede.
 - B) É um elemento que processa pacotes na camada 2, montado tabelas com os endereços de hardware dos hosts conectados em cada porta.
 - C) É um elemento que processa pacotes na camada 3, montado tabelas com os endereços IP dos hosts conectados em cada porta.
 - D) Retransmite o sinal observado em uma porta para todas as outras.
 - E) Implementa as operações de controle de acesso e segurança em uma rede.
10. O endereço de loopback em uma rede IP é:
- A) 255.255.255.255
 - B) 0.0.0.0
 - C) 127.0.0.1
 - D) 10.0.0.0
 - E) 192.168.1.1
11. O endereço de broadcast geral em uma rede IP é:
- A) 255.255.255.255
 - B) 10.255.255.255
 - C) 127.0.0.1
 - D) 192.168.255.255
 - E) 172.168.255.255

12. A distância máxima entre o armário de telecomunicações e uma tomada (rede secundária) considerando-se um sistema de cabeamento estruturado utilizando cabos UTP categoria 5 é dado por:
- A) 90m
 - B) 150m
 - C) 200m
 - D) 120m
 - E) 50m
13. Em um sistema de cabeamento estruturado, a distância máxima de um cabo de fibra óptica multimodo 62,5/125 na rede primária é:
- A) 7000m
 - B) 2000m
 - C) 10000m
 - D) 50000m
 - E) Indiferente
14. Uma empresa contratou um provedor de acesso à Internet e recebeu o endereço válido 200.140.32.0/24. No entanto, essa empresa possui 5 redes locais com 15 hosts em cada rede. É necessário aplicar uma nova máscara para obter novos endereços de rede. Qual máscara pode ser aplicada para resolver o problema?
- A) 255.255.255.224
 - B) 255.255.255.128
 - C) 255.255.255.252
 - D) 255.255.255.0
 - E) 255.255.255.255
15. O endereço de rede e máscara para ser utilizado para criação da rota default é:
- A) Endereço 10.0.0.0 com máscara 255.0.0.0
 - B) Endereço 0.0.0.0 com máscara 255.255.255.255
 - C) Endereço 255.255.255.255 com máscara 0.0.0.0
 - D) Endereço 255.255.255.255 com máscara 255.255.255.255
 - E) Endereço 0.0.0.0 com máscara 0.0.0.0
16. Com relação ao roteamento utilizado na Internet, é correto afirmar:
- A) Todo ele é feito com protocolo OSPF.
 - B) Todo ele é feito com protocolo RIP.
 - C) Todo ele é feito com protocolo BGP.
 - D) Não é possível implementar roteamento automático em toda a Internet.
 - E) Não é necessário definir rotas na Internet.
17. Qual dos endereços abaixo é um endereço de rede reservado para uso privativo, por exemplo, quando o endereçamento da rede privativa é projetada para utilizar o NAT (Network Address Translation)
- A) 136.12.1.0/24
 - B) 200.172.0.0/16
 - C) 192.168.0.0/16
 - D) 132.16.1.0/24
 - E) 11.192.0.0/16
18. Em um sistema Unix o controle permissões de acesso a um arquivo contempla:
- A) Permissão de leitura, escrita e execução para o dono, grupo e todos.
 - B) Permissão de leitura, escrita e execução para uma lista de usuários.
 - C) Permissão de leitura, escrita e execução para o dono, e uma lista de grupos.
 - D) Permissão de leitura, escrita, execução, controle total e modificação para o dono, grupo e todos.
 - E) Permissão de leitura, escrita, execução, controle total e modificação para uma lista de usuários.
19. Em um sistema Windows com NTFS, o controle de permissões de acesso a um arquivo contempla:
- A) Uma lista de permissões (como Controle Total, Exclusão, Execução, etc.) atribuída a um usuário ou grupo apenas.
 - B) Apenas permissão de leitura, escrita e execução para o dono, grupo e todos.
 - C) Uma lista de permissões (como Controle Total, Exclusão, etc.) atribuído uma lista de usuários ou grupos
 - D) Apenas permissão de leitura, escrita e execução para uma lista de usuários/grupos.
 - E) O NTFS não possibilita a atribuição de permissões de acesso a um arquivo.
20. Um hacker teve acesso a uma linha de transmissão de dados e interceptou os dados transmitidos entre um usuário e o site de um banco. Infelizmente para ele, a transmissão estava criptografada utilizando o algoritmo IDEA (chaves de 128 bits). Imediatamente o hacker iniciou uma tentativa de descoberta da chave utilizando o método da força bruta utilizando um PC. É correto afirmar que:
- A) Ele irá conseguir decifrar a mensagem rapidamente em virtude de um bug amplamente conhecido do algoritmo IDEA.
 - B) Provavelmente o hacker irá descobrir a chave e decifrar as mensagens em algumas horas.
 - C) Provavelmente o hacker irá descobrir a chave e decifrar as mensagens em alguns dias.
 - D) O hacker pode utilizar os dados para fazer uma transmissão fazendo-se passar pelo usuário.
 - E) É praticamente impossível que seja quebrada a segurança apenas com as informações a que o hacker teve acesso.

21. A gerência de redes utilizando o protocolo SNMP (Simple Network Management Protocol):
- A) Opera na camada de transporte da rede gerenciada.
 - B) Necessita de uma rede de gerência, implementada em paralelo com a rede gerenciada.
 - C) Opera na camada de rede da rede gerenciada.
 - D) Opera na camada de aplicação da rede gerenciada.
 - E) Opera na camada de sessão da rede gerenciada.
22. O sistema de resolução de nomes utilizado na Internet é o DNS (Domain Name Service), que é:
- A) uma base de dados distribuída e hierárquica.
 - B) uma base de dados central única.
 - C) uma base de dados distribuída que opera com consultas SQL.
 - D) baseado no arquivo hosts, disponível em sistemas Unix e Windows.
 - E) uma base de dados distribuída implementada com CORBA.
23. Uma VPN (Virtual Private Network) é:
- A) Uma interligação entre redes utilizando recursos de segurança do protocolo ATM sobre IP.
 - B) Uma rede particular de propriedade privada, dentro de uma região geográfica definida pelos limites da organização.
 - C) Um conceito similar ao conceito da VLAN (Virtual Local Area Network) das redes Ethernet, mas implementado na camada 4.
 - D) Um recurso exclusivo do IP versão 6 para melhorar o desempenho das redes privativas.
 - E) O tráfego de uma rede tunelado por outra rede, com recursos de criptografia e segurança.
24. Os endereços do protocolo IP versão 6 possuem as seguintes características corretas:
- A) 128 bits e é sempre incompatível com IP versão 4.
 - B) 128 bits e a integração com IP versão 4 é sempre transparente e não exige mecanismos de mapeamento.
 - C) 128 bits e a integração com IP versão 4 exige mecanismos de mapeamento.
 - D) 32 bits e seu uso se tornou obrigatório no Brasil a partir de fevereiro de 2004.
 - E) 32 bits e seu uso é opcional para quem deseja se integrar à Internet.
25. Assinale a alternativa correta sobre o protocolo IP:
- A) É baseado no conceito de datagrama confiável.
 - B) É baseado no conceito de datagrama não confiável.
 - C) É baseado no conceito de circuito virtual.
 - D) É um protocolo baseado em conexão.
 - E) Implementa controle de fluxo e erros.
26. Assinale a alternativa correta sobre o processo de conexão do protocolo TCP:
- A) Realiza a atribuição de números de circuito virtual para o controle de erros.
 - B) Realiza a troca de números de porta aleatórios entre cliente e o servidor.
 - C) Realiza a troca de números de seqüência aleatórios entre o cliente e o servidor.
 - D) Serve apenas para realizar o controle de fluxo entre os elementos transmissor e receptor.
 - E) Não tem função e deve ser retirado na próxima revisão do protocolo.
27. O protocolo de camada de transporte mais apropriado a ser utilizado por uma transmissão em tempo real é:
- A) RR TCP
 - B) TCP
 - C) SMB
 - D) ICMP
 - E) UDP
28. Um administrador de rede está configurando as regras em um firewall localizado no roteador que interliga a rede da empresa com a Internet. Para evitar que os usuários da rede da empresa realizem o acesso à redes Peer to Peer (P2P), pode-se proceder da seguinte forma:
- A) A configuração de regras de acesso por portas é insuficiente neste caso.
 - B) Configurar regras para permitir o acesso apenas às portas conhecidas (como 80 para Web, 25 para correio, etc.) impede o acesso a sistemas P2P.
 - C) Não permitir o acesso às portas que o sistema Peer to Peer normalmente utilizam, o que irá impedir o acesso a sistemas P2P.
 - D) Configurar regras para permitir o acesso apenas a aplicativos que utilizam protocolo TCP irá impedir o acesso a sistemas P2P.
 - E) Habilitar apenas o acesso à porta 80 irá impedir o acesso a sistemas P2P.
29. Um dos conceitos cada vez mais necessários à rede IP é a implementação de mecanismos de qualidade de serviço (QoS). Sobre a QoS no IP, pode-se afirmar:
- A) Os mecanismos que implementam QoS no IP são experimentais e não podem ser utilizados com confiança.
 - B) Apenas o IP versão 6 suporta QoS.
 - C) O IP possui diversos mecanismos que permitem a implementação de QoS.
 - D) As tentativas de implementação de QoS no IP não tiveram sucesso.
 - E) Existem mecanismos para implementação de QoS, mas eles não são eficientes por causa da integração com a rede Ethernet.

30. As sete camadas do modelo OSI são, respectivamente:
- A) Física, Rede, Transporte, Enlace, Sessão, Apresentação e Aplicação.
 - B) Física, Enlace, Rede, Transporte, Sessão, Apresentação e Aplicação.
 - C) Física, Modulação, Sessão, Transporte, Rede, Apresentação e Aplicação.
 - D) Física, Rede, Transporte, Sessão, Apresentação, Aplicação e Web.
 - E) Transmissão, Modulação, Enlace, Roteamento, Apresentação, Aplicação e Web.
31. O objetivo do protocolo Spanning Tree é:
- A) Garantir uma topologia livre de loops em uma rede local interligada por bridges.
 - B) Permitir a transmissão segura sobre a Internet.
 - C) É o protocolo que implementa uma VPN (Virtual Private Network).
 - D) Permite o balanceamento de carga da rede ATM.
 - E) Gerencia um sistema de transmissão baseada em árvores binárias na rede.
32. Suponha que um erro de configuração de rotas estáticas criou um loop fechado entre roteadores IP para uma determinada rede de destino. Nesse caso, é correto afirmar:
- A) Esse problema será detectado e corrigido pelo protocolo TCP.
 - B) A rede irá parar de funcionar devido a esse problema.
 - C) O algoritmo Spanning Tree irá detectar e corrigir o problema automaticamente.
 - D) O sistema de roteamento estático irá detectar e corrigir esse problema automaticamente.
 - E) A rede irá continuar a funcionar graças ao mecanismo de prevenção implementado com o campo TTL do protocolo IP.
33. Sobre o protocolo RIP (Routing Information Protocol), indique qual das alternativas abaixo, está **INCORRETA**:
- A) O RIP exige a transmissão periódica de broadcasts com a tabela de rotas do roteador.
 - B) O protocolo RIP possui um limite de 15 saltos.
 - C) O RIP leva em consideração conceitos de áreas e limites hierárquicos.
 - D) O RIP versão 1 não trata máscaras de rede. A máscara é inferida da classe do endereço pela análise do primeiro octeto do endereço.
 - E) O objetivo do RIP é configurar rotas de maneira automática.
34. Qual a informação correta sobre o protocolo OSPF (Open Shortest Path First):
- A) Não possui limitação no número de saltos.
 - B) Possui um limite de 15 saltos.
 - C) Não é compatível com máscaras de rede variáveis.
 - D) O objetivo do protocolo é implementar políticas de qualidade de serviço (QoS).
 - E) O objetivo do protocolo é realizar a autenticação de usuários nos roteadores.
35. Para mostrar os processos em execução em um sistema Linux, deve ser executado o comando:
- A) show process
 - B) ls -ls
 - C) grep ps
 - D) ps -ef
 - E) ln -p
36. O IPSec é um protocolo padrão projetado pelo IETF que oferece transferência segura de informações fim a fim pela rede IP pública ou privada. Assinale a alternativa **INCORRETA**:
- A) O IPSec implementa um protocolo de transporte seguro para ser utilizado em VPN.
 - B) O IPSec foi projetado para suportar múltiplos protocolos de criptografia.
 - C) O IPSec permite a implementação de uma VPN.
 - D) O IPSec Fonece mecanismos para autenticação.
 - E) O IpSec Opera na camada de rede.
37. O protocolo SMTP é responsável por:
- A) Transferência de hipertexto na Internet.
 - B) Gerência de redes.
 - C) Transferência de correio eletrônico.
 - D) Compartilhamento de arquivos.
 - E) Execução de procedimentos remotos.
38. O objetivo do protocolo ARP é:
- A) Evitar a geração de broadcasts na rede.
 - B) Transformar um nome (ex. www.google.com) em um endereço IP.
 - C) Encontrar o endereço de hardware correspondente a um endereço de camada 3.
 - D) Registrar um host no servidor DHCP.
 - E) Compartilhar arquivos em uma rede com sistemas Unix.

39. Um hacker instalou um analisador de protocolos em um desktop na rede de uma empresa. Sabe-se que a empresa utiliza uma rede Ethernet operando com switches 10/100 como elemento central. Indique a alternativa correta:
- A) Ele terá acesso apenas ao tráfego transmitido em broadcast e multicast.
 - B) Ele terá acesso ao tráfego total produzido pelos computadores conectados ao switch onde o seu computador está conectado.
 - C) Ele terá acesso ao tráfego total produzido pelos computadores conectados a todos os switches da rede.
 - D) Ele terá acesso ao tráfego transmitido em broadcast e o que for gerado ou tiver como destino o computador onde foi instalado o analisador de protocolo.
 - E) Ele não terá acesso a qualquer tipo de transmissão.
40. O TCP é um dos protocolos de camada de transporte mais utilizados na Internet. Suas funções são:
- A) Multiplexação lógica, controle de erros, controle de fluxo, controle de congestionamento e seqüenciação.
 - B) Multiplexação lógica, controle de erros, conversões de tipo e gerência da sessão.
 - C) Endereçamento e encaminhamento seguro de pacotes.
 - D) Estabelecimento de conexões e controle de janelas apenas.
 - E) Transferência de arquivos em formato hipertexto na Internet.