****

**TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS**

MATERIAL INSTRUCIONAL ESPECÍFICO

**TOMO 14**

**CQA/UNIP – Comissão de Qualificação e Avaliação da UNIP**

**TECNOLOGIA EM ANÁLISE E**

**DESENVOLVIMENTO DE SISTEMAS**

MATERIAL INSTRUCIONAL ESPECÍFICO

**TOMO 14**

# Christiane Mazur Doi

Doutora em Engenharia Metalúrgica e de Materiais, Mestra em Ciências - Tecnologia Nuclear, Especialista em Língua Portuguesa e Literatura, Engenheira Química e Licenciada em Matemática, com Aperfeiçoamento em Estatística. Professora titular da Universidade Paulista.

**José Carlos Morilla**

Doutor em Engenharia de Materiais, Mestre em Engenharia de Materiais e em Engenharia de Produção, Especialista em Engenharia Metalúrgica e Física e Engenheiro Mecânico, com MBA em Gestão de Empresas. Professor adjunto da Universidade Paulista.

**Tiago Guglielmeti Correale**

Doutor em Engenharia Elétrica, Mestre em Engenharia Elétrica e Engenheiro Elétrico (ênfase em Telecomunicações). Professor titular da Universidade Paulista.

*Material instrucional específico, cujo conteúdo integral ou parcial não pode ser reproduzido ou utilizado sem autorização expressa, por escrito, da CQA/UNIP – Comissão de Qualificação e Avaliação da UNIP – UNIVERSIDADE PAULISTA.*

**Questão 1**

**Questão 1.**[[1]](#footnote-1)

Leia o texto a seguir.

*Um ponto de acesso é um dispositivo de camada 2 que funciona como um hub 802.3 Ethernet. A rádio frequência é um meio compartilhado, e pontos de acesso escutam todo o tráfego de rádio. Assim como no padrão IEEE 802.3 Ethernet, dispositivos que operam no padrão IEEE 802.11 WLAN também disputam o meio para transmitir. Apesar disso, diferentemente das placas de rede Ethernet, dispositivos de rádio em vez de detectarem colisões são criados para evitá-las.*

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet: uma abordagem top-down*. 5 ed. São Paulo: Addison Wesley, 2010.

Sobre a operação dos padrões IEEE 802.3 e 802.11, avalie as afirmativas.

1. O padrão IEEE 802.3 permite detecção de colisão.
2. O método de acesso para o padrão 802.3 é o CSMA/CD, enquanto o padrão 802.11 faz uso de CSMA/CA.
3. O padrão IEEE 802.11 usa o CSMA/CD como protocolo de acesso múltiplo ao meio.
4. O quadro 802.11, assim como o quadro 802.3, inclui uma verificação de redundância cíclica (CRC).
5. A transmissão no padrão IEEE 802.11 inicia-se assim que a estação percebe que o canal está ocioso.

É correto apenas o que se afirma em

1. I e II.
2. II e III.
3. III e IV.
4. I, II e IV.
5. I, III e IV.

**1. Introdução teórica**

**Redes sem fio e protocolos de acesso múltiplo**

Inicialmente, para poder utilizar uma rede sem fio de infraestrutura, um computador precisava associar-se a um ponto de acesso. Para facilitar tal acesso, uma rede deve ter uma identificação, chamada de SSID (Service Set Identifier).

As frequências utilizadas em redes de computadores são padronizadas, sendo também divididas em diversos canais, o que facilita a existência de redes sem fio “vizinhas” (ou seja, fisicamente próximas). Diferentes canais podem ser utilizados por redes próximas, ou seja, trata-se de uma forma de tentar diminuir a interferência entre as redes. Evidentemente, em um cenário em que existam muitas redes fisicamente próximas, especialmente se esse número for muito superior ao número de canais disponíveis, sabemos que deve ocorrer interferência e perda de performance.

A popularização das redes sem fio levou a muitas adições e melhorias dos padrões associados. Por exemplo, o padrão 802.11 foi sendo melhorado ao longo do tempo, tendo inicialmente velocidades na faixa de 1Mbps, que foram sendo ampliadas, como no caso do padrão 801.11b, um padrão superior, com velocidade de 11Mbps (TANENBAUM e WETHERALL, 2011).

Quando criamos uma rede de comunicação sem fio, um dos primeiros problemas que podemos identificar está no acesso ao meio de comunicação. Em uma rede cabeada, o meio de comunicação corresponde aos fios que servem de suporte para a propagação dos sinais (tensões e correntes) associados à transmissão dos bits. É possível criar uma rede cabeada na qual evitamos que máquinas diferentes compartilhem o mesmo meio de comunicação; com essa finalidade, colocamos cabos individuais para cada máquina. Também é possível fazer uma rede cabeada na qual exista o compartilhamento do meio, o que inclusive foi bastante comum no passado. Contudo, em uma rede sem fio típica, o meio de comunicação é o ar (ou o espaço, se considerarmos um satélite), que é compartilhado por todos os dispositivos que compõem a rede. No sentido aqui empregado, o termo “compartilhado” refere-se ao fato de dois equipamentos podem atuar no meio ao mesmo tempo, enviando sinais simultaneamente. Esse processo pode levar a uma série de problemas, pois trata-se de uma situação equivalente a duas ou mais pessoas tentando falar ao mesmo tempo: com todas as pessoas falando simultaneamente, é impossível entender o que alguém está falando.

Outro fator complicador é que os diversos equipamentos que fazem parte da rede não sabem o momento em que vai existir uma transmissão. Em um caso geral, cada máquina executa os seus próprios programas, não sendo possível saber exatamente quando vai ocorrer a transmissão, nem por quanto tempo ela vai ocorrer.

Existem diversas formas de resolver esse tipo de problema. Inicialmente, devemos ter em mente que a sua gravidade está ligada ao número de máquinas que devem acessar e utilizar o meio simultaneamente. Por exemplo, em uma situação “ponto a ponto”, com apenas duas máquinas se comunicando, tal problema pode ser facilmente sanado. O problema é diferente da situação na qual existe um transmissor enviando dados para uma grande quantidade de receptores. Nesses casos, apenas um equipamento transmite dados, enquanto as demais apenas recebem os dados enviados. Nesse contexto, o uso do meio compartilhado é bastante adequado, uma vez que a maioria das máquinas utiliza o meio apenas para “ouvir”, e não para “falar”.

O problema torna-se maior quando diversas máquinas podem enviar e receber dados. Esse é o cenário típico de uma rede de computadores, em que os usuários enviam e recebem dados de acordo com o seu fluxo de trabalho. Em tais cenários, devemos utilizar um “protocolo de acesso múltiplo” para permitir a organização do processo de comunicação (KUROSE e ROSS, 2010).

Quando dispomos de um meio compartilhado, podemos empregar basicamente três estratégias para o problema do acesso múltiplo (KUROSE e ROSS, 2010, p.332):

* protocolos de divisão de canal;
* protocolos de acesso aleatório;
* protocolos de revezamento.

De uma forma bastante simplificada, podemos pensar nos protocolos de divisão de canal de uma forma similar (mas não igual!) a uma rádio FM (ou mesmo a uma rádio AM). Em uma rádio FM, temos apenas uma antena, mas existem várias rádios. Quando queremos escutar a nossa rádio favorita, devemos sintonizar a rádio, normalmente utilizando um botão ou um controle. Todas as rádios transmitem ao mesmo tempo, mas cada uma transmite em uma frequência diferente. Ao sintonizarmos o nosso aparelho, escolhemos ouvir uma rádio específica e filtramos (eliminamos) todas as demais. O meio (no caso, o ar) é compartilhado por todas as rádios, mas as diferentes frequências são alocadas de modo que o processo de “seleção e filtragem” permita que escutemos apenas a rádio desejada. Cada rádio tem uma fração do espectro associada e, idealmente, não deve trasmitir ou interferir nos sinais transmitidos por outras rádios.

Em uma rede de computadores, o processo é mais complexo, pois, ao contrário de um receptor FM que não transmite nenhuma informação (apenas recebe os sinais enviados das rádios), os diversos computadores de uma rede devem ser capazes de enviar e receber informações. Contudo, a ideia básica é similar: o canal de comunicação é dividido de alguma maneira entre os diversos equipamentos, e cada um utiliza apenas uma parcela da banda disponível. A vantagem desse processo é tornar possível a comunicação simultânea de vários equipamentos. Voltando à analogia das rádios, várias pessoas podem escutar diferentes rádios ao mesmo tempo, sem interferir umas nas outras. Contudo, existem também algumas desvantagens, como o problema de como alocar as frequências para cada rádio, algo que deve ser feito previamente (normalmente, por alguma agência governamental). Se isso fosse feito em uma rede de computadores, o processo seria bem mais complexo, pois o número de máquinas pode ser muito grande. Outro aspecto a ser considerado é que cada equipamento pode utilizar apenas uma fração da banda total disponível. Em alguns casos, isso pode não ser um grande problema, como na telefonia celular, que usa diversos protocolos para a divisão de canal, como (KUROSE e ROSS, 2010):

* o TDM, que utiliza a divisão por tempo;
* o FDM, que utiliza a divisão por frequência;
* o CDMA, que utiliza a divisão por código.

Uma abordagem diferente dos protocolos de divisão de canal são os protocolos de acesso aleatório. Aqui, a estratégia é que cada máquina utilize tada a banda disponível do canal para transmitir dados (KUROSE e ROSS, 2010). Supondo que uma máquina não trasmita continuamente dados o tempo todo, é possível que exista espaço para que todas as máquinas consigam transmitir dados utilizando o mesmo canal de forma “exclusiva”, ainda que não ao mesmo tempo. Evidentemente, há a probabilidade (muitas vezes considerável) da existência de “colisão”, em que duas máquinas tentem transmitir informações simultaneamente. Isso gera sinais distorcidos e outros problemas de comunicação. Mesmo empregando técnicas de correção de erros, podem ocorrer situações nas quais as informações transmitidas são completamente perdidas em virtude da colisão. Para evitar essas situações de colisão e a eventual perda de dados, alguns protocolos da categoria costumam especificar que as máquinas devem parar de transmitir pacotes (essencialmente, desistindo de transmitir) e esperar um tempo variável e aleatório até tentar uma nova transmissão, monitorando o meio e aguardando a ociosidade do canal.

Quando pensamos nos protocolos de acesso aleatório, devemos ter em mente que podemos ter uma rede de computadores relativamente grande e complexa, em que cada uma das máquinas da rede não sabe quando vai ocorrer uma transmissão das outras máquinas. Isso significa que a ocorrência da colisão não pode ser previamente determinada em todas as situações. Dessa forma, uma estratégia interessante é aquela na qual a maioria das máquinas deve “ouvir” o canal de comunicação para determinar quando é o melhor momento de transmitir (o que acontece quando o canal fica ocioso). Até mesmo quando uma ociosidade é detectada, ainda existe o risco de colisão, devido aos atrasos de propagação dos sinais e aos problemas na detecção dos sinais e no seu processamento.

As ideias apresentadas são utilizadas em diversos protocolos de acesso aleatório, como o ALOHA e o CSMA (KUROSE e ROSS, 2010). O CSMA ou “Carrier-sense muliple access” (também chamado de “Acesso múltiplo com detecção de portadora”) é um protocolo de acesso ao meio que tem como objetivo diminuir a probabilidade de colisão (FOROUZAN, 2008), especificando que o meio deve ser monitorado antes de ser feita uma transmissão. Para aprimorar mais seu desempenho, o protocolo CSMA foi melhorado com a incorporação de um mecanismo de tratamento das colisões, o que deu origem ao protocolo CSMA/CD ou “Carrier-sense muliple access with collision detection” (CSMA com detecção de colisão).

Outra melhoria no protocolo CSMA refere-se à inclusão de mais métodos para se evitar ao máximo as colisões, o que ocorre no CSMA/CA (“Carrier-sense muliple access with collision avoidance” ou “CSMA com prevenção de colisão”). Nessa variação, são incorporados mecanismos diversos, como aquele que cólica um tempo de espera na trasmissão dos dados, mesmo quando o canal está ocioso, chamado de “interframe space” ou IFS. Há, também, o uso de janelas de conteção (“contention window”) e de confirmações de recebimento dos dados (FOROUZAN, 2008). Todos esses métodos são especialmente úteis e necessários em redes sem fio, nas quais as probabilidades de interferência e colisões são muitos maiores do que nas redes cabeadas (ainda que também possam ocorrer, dependendo da tecnologia utilizada).

Como a criação de redes sem fio envole uma série de desafios ainda maiores do que aqueles encontrados em uma rede tradicional cabeada, foram desenvolvidos adicionalmente outros mecanismos para tratar de situações mais complexas. No caso dos protocolos de acesso ao meio, um exemplo é o protocolo MACAW (“Multiple access collision avoidance wireless”), utilizado para evitar colisões mesmo em situações nas quais existem estações ocultas (CARISSIMI *et al.*, 2009).

**2. Análise das afirmativas**

I – Afirmativa correta.

JUSTIFICATIVA. O padrão IEEE 802.3 utilizava originalmente o protocolo CSMA/CD (Carrier Sense Multiple Access with Collision Detection), que é capaz de detectar colisões.

II – Afirmativa correta.

JUSTIFICATIVA. O problema do terminal oculto pode dificultar o uso do método de acesso CSMA/CD para redes sem fio, de forma que é necessário utilizar um método de acesso diferente, que busca evitar as colisões, chamado de CSMA/CA (Carrier Sense Multiple Access with Collision Detection).

III – Afirmativa incorreta.

JUSTIFICATIVA. O padrão IEEE 802.11 utiliza o padrão CSMA/CA, e não o padrão CSMA/CD.

IV – Afirmativa correta.

JUSTIFICATIVA. Ambos os padrões precisam de um mecanismo para detecção de erro, que pode ser causado por efeito de ruídos ou colisões.

V – Afirmativa incorreta.

JUSTIFICATIVA. Mesmo quando o canal de comunicação é percebido como ocioso por um transmissor, é possível que ocorreram colisões, pois a detecção de ociosidade pode estar equivocada. Para diminuir a chance de ocorrência de colisões, uma estratégia é monitorar o meio por determinado intervalo de tempo antes de começar a transmissão, o que deve ser feito apenas caso o meio tenha permanecido ocioso durante todo o período de monitoração. Esse intervalo de tempo não deve ser muito longo, pois isso levaria a um atraso muito grande na comunicação. Esse período é chamado de “Espaçamento de Interquadros Distribuído”, ou “Distributed Interframe Space – DIFS” (KUROSE e ROSS, 2010).

Alternativa correta: D.

**3. Indicações bibliográficas**

* CARISSIMI, A. S.; ROCHOL, J.; GRANVILLE, L . Z. *Redes de computadores*. Porto Alegre: Bookman, 2009.
* COMER, D. E. *Redes de computadores e internet*. Porto Alegre: Bookman, 2007.
* FOROUZAN, B. A. *Comunicação de dados e redes de computadores*. 4. ed. Porto Alegre: AMGH, 2008.
* KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet: uma abordagem top-down*. 5. ed. São Paulo: Addison Wesley, 2010.
* TANENBAUM, A. S.; WETHERALL, D. *Redes de computadores*. São Paulo: Pearson, 2011.

**Questão 2**

**Questão 2.**[[2]](#footnote-2)

Os Sistemas Operacionais de Redes (SOR) são uma extensão dos Sistemas Operacionais Locais (SOL), voltados para tornar transparente o uso dos recursos compartilhados, com funções de gerenciamento do acesso ao sistema de comunicação e às estações remotas para utilização de recursos de hardware e software remotos.

Com relação aos SOR, avalie as afirmativas a seguir.

1. A extensão do sistema operacional das estações é feita por meio de um módulo redirecionador que funciona interceptando as chamadas das aplicações ao sistema operacional local, desviando aquelas que dizem respeito a recursos remotos para o módulo do sistema operacional de rede, que providencia o acesso ao dispositivo remoto.
2. A interface entre as aplicações e o sistema operacional baseia-se em interações solicitação/resposta. A aplicação solicita um serviço, por meio de uma chamada ao sistema operacional que executa o serviço solicitado e responde, informando o status da operação e transferindo os dados resultantes da execução para a aplicação quando for o caso.
3. A interação cliente-servidor constitui-se no modo básico dos sistemas operacionais de redes. As estações que disponibilizam seus recursos a outras estações devem possuir a entidade (ou módulo) servidor. As estações que permitem que suas aplicações utilizem recursos compartilhados com outras estações devem possuir a entidade (ou módulo) cliente.
4. Pode-se classificar os módulos de um SOR instalados nas estações em dois tipos: SORC (módulo cliente) e SORS (módulo servidor do sistema operacional).

É correto o que se afirma em

1. I, apenas.
2. I e II, apenas.
3. III e IV, apenas.
4. II, III e IV, apenas.
5. I, II, III e IV.
6. **Introdução teórica**

**Sistemas operacionais de rede**

Pode parecer curioso para as pessoas mais jovens, mas a disponibilidade de interconexões com redes não foi uma característica sempre presente em sistemas operacionais. Durante muito tempo, cada computador era essencialmente uma “ilha” isolada de recursos e não havia muitas formas de comunicação ou compartilhamento de arquivos, com exceções de alguma forma primitiva de comunicação via modem (como as antigas BBS) ou de compartilhamento de alguma mídia (como um disquete).

Em virtude do surgimento e da popularização das redes de computadores, muitos sistemas operacionais que já existiam foram modificados, com diversas funcionalidades de rede adicionadas posteriormente. Um exemplo dessa situação ocorreu no sistema operacional DOS (especialmente o MS-DOS e o DR-DOS) que, nas suas primeiras versões, não incluía nativamente nenhuma forma de suporte a redes. Isso proporcionou o lançamento de produtos de terceiros, como o Novell Netware, que possibilitavam o uso de redes de computadores para certas tarefas, como o compartilhamento de discos rígidos em máquinas remotas e o compartilhamento de impressoras.

Um dos motivos das limitações dos primeiros sistemas operacionais estava nas restrições de hardware das máquinas disponíveis no mercado, especialmente com relação à quantidade de memória RAM. Durante boa parte da década de 1980, a quantidade de memória RAM típica de um microcomputador era tão pequena (inferior a 1MB) que os sistemas operacionais tinham que ser muito pequenos. Isso limitava bastante muitas das funcionalidades desses sistemas operacionais; uma das funcionalidades sacrificadas, pelo menos inicialmente, foram as relacionadas às redes de computadores. Naquela época, apenas máquinas mais caras e poderosas, chamadas de “workstations”, tinham memória suficiente e sistemas operacionais capazes de trabalhar em redes de computadores mais sofisticadas.

Com a rápida evolução dos computadores, especialmente no final da década de 1980 e na década de 1990, somada à crescente popularização das redes de computadores em empresas, a maioria dos sistemas passou a disponibilizar módulos típicos de redes, especialmente redes TCP/IP. Dessa forma, muitos dos sistemas operacionais que utilizamos hoje suportam redes de computadores, tanto sistemas operacionais que rodam em telefones celulares quanto sistemas embarcados.

Machado e Maia (2013, p.21) definem um sistema operacional de rede (SOR) como um sistema operacional que “permite que um host compartilhe seus recursos, como uma impressora ou um diretório, com os demais hosts da rede”.

Do ponto de vista da arquitetura desses sistemas operacionais, eles costumam ser classificados como sistemas fracamente acoplados. Isso significa que cada computador deve gerenciar os seus recursos de forma isolada, mas compartilhando algumas funcionalidades com outras máquinas por meio de uma rede de comunicação de dados (MACHADO e MAIA, 2013, p.21)

É importante observarmos que um sistema operacional de rede não é a mesma coisa que um sistema operacional distribuído. Em um sistema distribuído, o usuário não percebe diretamente que está utilizando recursos em diferentes máquinas, o que é chamado de “imagem única do sistema” (MACHADO e MAIA, 2013). Em um sistema operacional de rede, o usuário percebe de modo claro que está se comunicando com diferentes computadores, especialmente se considerarmos que esse processo é mediado pelo uso de um usuário e uma senha.

É importante observarmos, ainda que a maioria dos sistemas operacionais modernos seja capaz de prover serviços de compartilhamento de diretórios e impressoras, a diferença entre os sistemas operacionais tipicamente feitos para trabalhar como cliente e sistemas operacionais de servidores. No último caso, o sistema operacional deve estar preparado para gerenciar um número muito grande de conexões simultâneas, um elevado volume de tráfego de rede e hardware de excelente desempenho. Já nos sistemas clientes, o foco está mais no consumo de serviços por um usuário, ainda que possam existir servidores rodando localmente nessas máquinas.

Finalmente, é bastante comum diferenciarmos sistemas operacionais voltados para máquinas, que devem atuar como servidores em uma rede, daqueles que devem trabalhar em máquinas que serão utilizadas como clientes. Em um sistema operacional voltado para o uso em servidores, é fundamental que haja:

* suporte para gerenciamento remoto;
* grande capacidade de lidar com elevado número de conexões simultâneas;
* utilização de hardware mais sofisticado e de maior desempenho.

Em um sistema operacional que visa a ser utilizado em máquinas clientes, o foco pode ser diferente, especialmente caso ele seja voltado para o mercado doméstico. Nesse caso, outras questões, como a usabilidade e a disponibilidade de programas para o entretenimento, costumam ser enfatizadas. Assim, essas máquinas devem atuar como clientes de outros servidores.

Contudo, tanto no caso dos sistemas operacionais para clientes quanto no caso dos sistemas operacionais para servidores, uma série de funcionalidades de rede devem ser devidamente providas pelos seus respectivos sistemas operacionais, uma vez que ambos devem ser capazes de se comunicar por meio de uma rede de dados.

1. **Análise das afirmativas**

I – Afirmativa correta.

JUSTIFICATIVA. Para que o processo seja o mais transparente possível para o usuário final, o sistema operacional deve saber diferenciar (automaticamente) os recursos locais dos recursos remotos.

II – Afirmativa correta.

JUSTIFICATIVA. A interface de um sistema operacional é um aspecto crucial da sua arquitetura. É importante que as aplicações tenham apenas conhecimento da interface em si, e não dos detalhes particulares de implementação.

III e IV – Afirmativas corretas.

JUSTIFICATIVA. Toda estação que tiver um módulo servidor pode atuar, de fato, como um servidor. De forma equivalente, toda estação que tiver um módulo cliente pode atuar como um cliente de algum serviço. Contudo, devemos ter em mente que algumas máquinas são construídas especificamente para proverem serviços a outras máquinas e, nesse caso, chamamos essas máquinas de “servidores”. Outras máquinas, cujo foco está em consumir esses serviços, podem ser chamadas de clientes ou workstations (estações de trabalho).

Alternativa correta: E.

1. **Indicações bibliográficas**

* FOROUZAN, A. B. *Comunicação de dados e redes de computadores*. São Paulo: McGraw-Hill, 2008.
* MACHADO, F. B.; MAIA, L. P. *Arquitetura de sistemas operacionais*. 5. ed. Rio de Janeiro: LTC, 2013.
* SILBERSCHATZ, A.; GALVIN, P. B.; GAGNE, G. *Operating system concepts.* 9. ed. Hoboken: Wiley, 2013.
* TANENBAUM, A. S.; WHETHERALL, D. J. *Redes de computadores.* São Paulo: Pearson Prentice Hall, 2011.

**Questão 3**

**Questão 3.**[[3]](#footnote-3)

A Qualidade de Serviço (QoS) é muito importante para as redes convergentes, tornando-as capazes de transportar, de maneira bem próxima ao ideal, os mais diversos tráfegos, como vídeo, voz e dados; de modo simultâneo e sem interferências mútuas. A QoS apresenta duas soluções para redes IP: Serviços Integrados (IntServ) e Serviços Diferenciados (DiffServ).

Em relação a essas soluções, é correto afirmar que

1. o DiffServ é mais adequado em redes locais e intradomínio.
2. O IntServ é mais adequado para ser utilizado no núcleo da rede.
3. O IntServ estabelece priorização de tráfego baseado em classes de fluxo, seguindo as características de tráfego das aplicações.
4. o DiffServ e o IntServ fornecem melhor tratamento aos fluxos das aplicações quando comparadas com fluxos que seguem o modelo best-effort.
5. o DiffServ estabelece reservas de recursos ao longo de um caminho de rede, oferecendo valores absolutos de largura de banda, atraso e perda de pacotes para as aplicações.

**1. Introdução teórica**

**1.1. Garantia de qualidade de serviço**

Para entendermos os conceitos envolvidos na qualidade de serviço, é interessante termos em mente a evolução da Internet. Nos seus primórdios, a Internet apresentava um tráfego muito menor do que o observado na atualidade, que era constituído principalmente por troca de arquivos entre diferentes computadores (especialmente arquivos de texto simples, de pequeno tamanho). A forma de comunicação não era de tempo real, havendo um grande atraso de comunicação entre as diversas máquinas. Contudo, o seu crescimento, explosivo especialmente durante o final da década de 1990, e a popularização dos serviços de banda larga levaram a um uso muito mais intenso e a aplicações que não eram originalmente planejadas, como a transmissão de vídeos e comunicação via voz. Enfim, esse aumento do consumo e a ampliação dos serviços ocasionaram um crescimento exponencial do tráfego de dados, o que gerou um problema similar aos engarrafamentos de automóveis que ocorrem no trânsito de grandes cidades.

O crescimento da Internet também não foi apenas um crescimento no volume de dados: houve, também, uma ampliação do seu uso para diversos tipos de comunicação. Por exemplo, os serviços de transmissão de vídeos pela Internet têm um perfil de uso específico. A utilização de programas de vídeo conferência também apresenta peculiaridades diferentes da mera cópia de arquivos entre dois servidores.

Dessa forma, as empresas evolvidas na comunicação pela Internet tiveram que o resolver o seguinte problema: como atender às necessidades de alguns usuários específicos (como, por exemplo, usuários que precisam utilizar serviços de telefonia IP) sem ter que superdimensionar a rede de computadores (o que tornaria o seu custo proibitivo)? Isso levou à criação de uma série de estratégias de gerenciamento do tráfego em uma rede.

Quatro parâmetros básicos são utilizados para caracterizar o tipo de tráfego e as necessidades da comunicação (TANENBAUM e WETHERALL, 2011):

* confiabilidade;
* retardo;
* flutuação;
* banda.

Esses quatro parâmetros caracterizam a qualidade de serviço, em inglês, chamada de “Quality of Service” ou apenas QoS. (TANENBAUM e WETHERALL, 2011).

Uma das estratégias para garantir a qualidade de serviço é conhecida como “Serviços Integrados” ou apenas Intserv. Nesse caso, a estratégia envolve fazer uma espécie de reserva de recursos ao longo da rede. Utiliza-se um protocolo denominado RSVP (“Resource Reservation Protocol”) para que as reservas necessárias de bandas sejam comunicadas aos equipamentos da rede (TANENBAUM e WETHERALL, 2011).

Vale notar que esse protocolo foca no problema da reserva de recursos, e não no envio de dados (TANENBAUM e WETHERALL, 2011). Isso faz sentido, já que o protocolo para o envio de dados vai depender da rede e da aplicação em questão.

Devemos ter em mente que, para o uso de serviços integrados garantir a QoS, é necessário que exista uma arquitetura sofisticada e específica configurada entre os roteadores. Isso adiciona custos para a empresa fornecedora dos serviços de comunicação. Outra abordagem possível para garantir a QoS engloba a criação de classes de pacotes diferentes. Uma analogia seria imaginar que os pacotes recebem “etiquetas” contendo a sua classe e, dependendo dessa classe, podem receber tratamento melhores ou piores. Assim, clientes que pagam serviços mais caros terão pacotes etiquetados com uma classe “superior”, recebendo uma espécie de tratamento especial. Serviços mais baratos terão pacotes etiquetados com uma classe mais simples, e os roteadores aplicarão um tratamento trivial. Essa estratégia é a ideia básica existente no chamado “Differentiated Services”, “Serviços Diferenciados” em português, ou apenas Diffserv.

Uma das vantagens do Diffserv em relação ao Intserv é a simplicidade (TANENBAUM e WETHERALL, 2011). Para o seu uso, existem basicamente dois elementos funcionais (KUROSE e ROSS, 2010):

* a função de borda;
* a função central.

A função de borda é basicamente o processo de “etiquetagem” do tráfego gerado por um cliente, por exemplo. Os pacotes devem ser identificados com a sua classe, o que vai definir o seu tratamento posteriormente na rede (KUROSE e ROSS, 2010).

A função central de envio corresponde ao comportamento dos roteadores centrais, de acordo com a classe dos pacotes. Esses roteadores encaminham os pacotes seguindo diretrizes definidas apenas pelas suas classes. Isso simplifica o processo: os roteadores não precisam memorizar estados especiais dependendo do fluxo de comunicação e tomam as decisões de controle da comunicação, como a definição da largura de banda, apenas na classe do pacote recebido, o que é facilmente identificado (KUROSE e ROSS, 2010). Observe que isso é diferente do Intserv, no qual é necessário utilizar algoritmos que levem em conta todo o fluxo.

Outro aspecto utilizado na implementação do Diffserv está relacionado ao chamado “comportamento por salto” dos roteadores, ou “per-hop behavior”. Ele especifica como o roteador deve se comportar de acordo com a classe dos pacotes. Nesse caso, existem duas categorias:

* repasse acelerado;
* repasse assegurado.

No repasse acelerado, pacotes especialmente marcados trafegam como se não houvesse outros pacotes na rede (TANENBAUM e WETHERALL, 2011), ou seja, “passam na frente” dos demais pacotes. Obviamente, isso só pode funcionar de modo adequado se a minoria do total de pacotes for “privilegiada”; caso contrário, a estratégia não funcionaria mais.

O repasse assegurado é um pouco diferente do anterior: nele, há a criação de uma série de prioridades entre pacotes associados a classes específicas e busca-se garantir um mínimo de banda para os pacotes de acordo com a sua classe.

Do ponto de vista comercial, a ideia é que as empresas fornecedoras de serviços de telecomunicações possam cobrar por esses serviços de diferentes formas, como, por exemplo, limitando o número de pacotes de acordo com o produto contratado pelo cliente ou criando uma tarifação baseada em volume de pacotes (TANENBAUM e WETHERALL, 2011). Contudo, devemos ter em mente que algumas pessoas e organizações criticam tais tipos de tratamento e de cobrança.

**2. Análise das alternativas**

A – Alternativa incorreta.

JUSTIFICATIVA. O uso de Diffserv não é adequado em uma rede local, pois precisamos lembrar que os pacotes devem ser classificados e receber um “rótulo” com a sua classe, o que normalmente acontece nos roteadores de borda (KUROSE e ROSS, 2010). Por esse motivo, ele deve ser utilizado no núcleo da rede.

B – Alternativa incorreta.

JUSTIFICATIVA. O IntServ não é exclusivo para o núcleo da rede, podendo ser utilizado inclusive em conjunto com o DiffServ, esse sim executado no núcleo da rede, como proposto na RFC 2998.

C – Alternativa incorreta.

JUSTIFICATIVA. É a arquitetura DiffServ que fornece um serviço diferenciado baseado em classes.

D – Alternativa correta.

JUSTIFICATIVA. Uma característica do modelo de “Best Effort” é que ele não diferencia o tipo de tráfego da rede. Ainda que essa característica possa ser considerada bastante democrática, o desempenho de alguns tipos de aplicações pode se tornar muito ruim, especialmente em situações nas quais a rede se encontra com elevado tráfego (EVANS e FILSFILS, 2010). Isso é especialmente verificado no caso de aplicações como as transmissões de voz e de vídeo. Uma analogia possível seria o tráfego de automóveis nas ruas, em que alguns veículos (como ambulâncias e carros de polícia) devem ter tratamentos diferenciados.

E – Alternativa incorreta.

JUSTIFICATIVA. A descrição corresponde ao IntServ, e não ao DiffServ.

Alternativa correta: D.

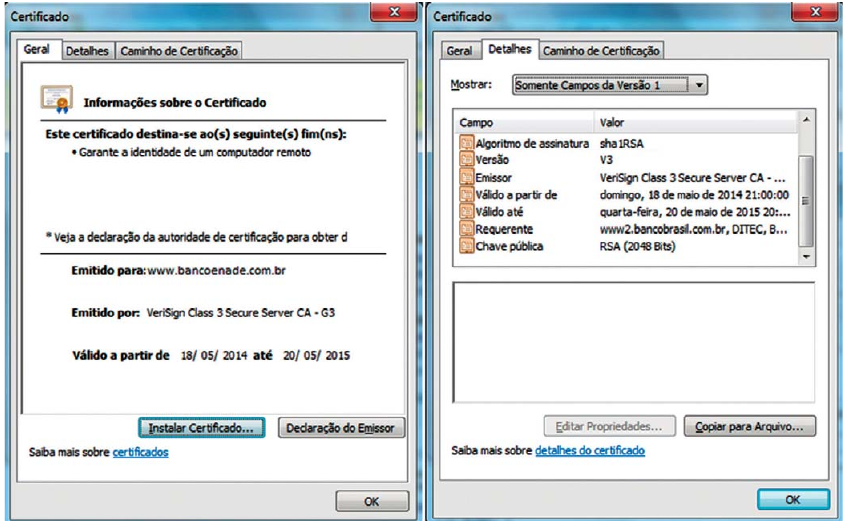
**3. Indicações bibliográficas**

* AGARWAL, M.; MAJUMDAR, A. Design of a minimal signaling BAS1 - Bandwidth Brokering Protocol. In *Smart Networks: IFIP TC6/WG6. 7 Seventh International Conference on Intelligence in Networks (SmartNet 2002)* Saariselkä: Springer Science & Business Media, 2002.
* EVANS, J.; FILSFILS, C. *Deploying IP and MPLS QOS for Multiservice Networks*. San Francisco: Morgan Kaufmann, 2010.
* KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet: uma abordagem top-down*. São Paulo: Pearson, 2010.
* RFC 2998. BERNET, Y. *et al*. "A Framework for Integrated Services Operation over Diffserv Networks". RFC 2998, nov. 2000.
* TANENBAUM, A. S.; WETHERALL, D. *Redes de computadores*. São Paulo: Pearson, 2011.

**Questão 4**

**Questão 4.**[[4]](#footnote-4)

Uma empresa deseja estabelecer um novo canal de negócios utilizando a internet. Para isso, desenvolveu uma aplicação para internet - um portal - e criou um mecanismo de segurança, com base no uso do protocolo SSL (Secure Socket Layer) e de certificados digitais, de forma a proteger as informações de seus clientes durante o acesso. Parte do certificado digital dessa empresa aparece na imagem abaixo.



Em relação aos aspectos de segurança da informação, faça o que se pede nos itens a seguir.

1. Conceitue criptografia simétrica e criptografia assimétrica.
2. Utilizando o certificado digital mostrado na figura, indique: quem o assina, a quem se destina, o algoritmo de *hash* da assinatura desse certificado, o algoritmo de criptografia pública da assinatura desse certificado e o tamanho da chave pública utilizada.
3. Explique o processo de geração da assinatura digital desse site.

**1. Introdução teórica**

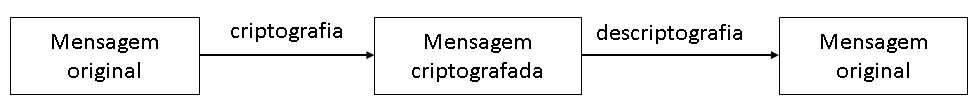
**Criptografia simétrica e assimétrica**

Frequentemente, é necessária a troca de informações por meios inseguros, o que significa que o tráfego de informação pode ser interceptado. Nesses casos, não queremos que um terceiro seja capaz de compreender o conteúdo da mensagem, mesmo tendo acesso aos bits transmitidos. Esse controle é feito por meio da criptografia, que pode ser encarada, de forma extremamente simplificada, como o embaralhamento da mensagem a ser transmitida de forma a impedir que um terceiro entenda o seu conteúdo mesmo tendo sido capaz de interceptar a sua transmissão.

Formatos primitivos de criptografia utilizavam apenas técnicas que dependiam de um algoritmo fixo para a construção da mensagem criptografada. Dessa forma, qualquer pessoa que conhecesse o funcionamento do algoritmo poderia ser capaz de decifrar o conteúdo da mensagem. Nessas circunstâncias, é fundamental o sigilo do algoritmo: a única forma de prevenir que uma pessoa não autorizada seja capaz de ler a mensagem é o desconhecimento do processo de criptografia (KOŚCIELNY, KURKOWSKI e SREBRNY, 2013).

Essa abordagem sofre de vários problemas. Como o sigilo do algoritmo é fundamental, cada grupo de pessoas que precisa se comunicar de forma privativa deve ter um algoritmo em particular. Como esse algoritmo deve ser secreto, ele não pode ser analisado pela comunidade acadêmica, uma vez que a sua divulgação tornaria o algoritmo inútil (KOŚCIELNY, KURKOWSKI e SREBRNY, 2013). Além disso, se uma das pessoas do grupo de comunicação tiver de ser excluída por algum motivo, como demissão, o processo perde seu valor e um novo algoritmo deve ser desenvolvido.

Para resolver o problema anteriormente ilustrado, foi criado o sistema de criptografia utilizando chaves. Observe o diagrama (simplificado) de um sistema de comunicação que utiliza criptografia sem chaves, como ilustrado na figura 1.

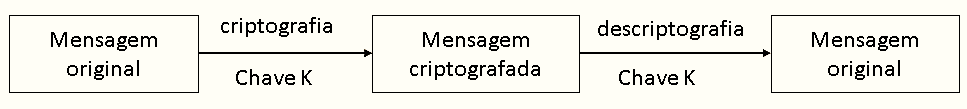


**Figura 1.** Processo de criptografia e descriptografia sem chaves.

**Fonte.** KOŚCIELNY, KURKOWSKI e SREBRNY, 2013 (com adaptações).

Na figura 1, a mensagem original deve ser criptografada por um algoritmo, transmitida e, finalmente, descriptografada por outro algoritmo no receptor.

Podemos melhorar consideravelmente a segurança do processo ao incorporarmos uma chave: uma cadeia de bits que é utilizada para a encriptação e descriptação da mensagem. Dessa forma, tanto no lado que vai transmitir a informação quanto no lado que vai recebê-la, é necessário que se conheça não apenas o algoritmo de criptografia, mas também a chave. Quando utilizamos a mesma chave no processo de encriptação e no processo de descriptação, dizemos que trabalhamos com criptografia simétrica. Esse mecanismo é ilustrado na figura 2.



**Figura 2.** Processo de criptografia e descriptografia simétrica.

**Fonte.** KOŚCIELNY, KURKOWSKI e SREBRNY, 2013 (com adaptações).

É possível modificar o esquema da criptografia simétrica, utilizando chaves diferentes para a encriptação e para a descriptação, como ilustrado na figura 3. Em muitos casos, a chave K1 é divulgada, e por isso é chamada de chave pública. Por outro lado, a chave K2 deve ser conhecida apenas pela pessoa que vai ler a mensagem, sendo chamada de chave privada.



**Figura 3.** Processo de criptografia e processo de descriptografia assimétrica.

**Fonte.** KOŚCIELNY, KURKOWSKI e SREBRNY, 2013 (com adaptações).

Tanto no processo de criptografia simétrica quanto no processo de criptografia assimétrica, é fundamental que a chave (privada, no segundo caso) seja guardada de forma segura. No entanto, o algoritmo pode ser totalmente conhecido, avaliado pela comunidade acadêmica e implementado por empresas terceiras. Uma vez que as chaves não sejam conhecidas, apenas o conhecimento do algoritmo não afeta a qualidade e a segurança do processo de criptografia.

Para provar que determinada pessoa é a “dona” de uma chave pública, utiliza-se um certificado digital. Nesse caso, uma entidade terceira tem responsabilidade legal em associar uma chave a uma pessoa (ou empresa) e emitir o certificado digital.

**2. Padrão de Resposta do Inep**

**Parte A.**

*Algoritmos de criptografia de chave simétrica utilizam a mesma chave tanto para criptografar quanto para descriptografar a mensagem. Esses algoritmos costumam ser mais rápidos que os utilizados na criptografia assimétrica, o que é uma vantagem, porém, como a chave é a mesma tanto para o remetente quanto para o destinatário, sua divulgação torna-se um ponto crítico do processo.*

*Algoritmos de chave assimétrica utilizam chaves diferentes para a o processo de encriptação e o processo de descriptografia. Uma das chaves, conhecida como chave pública, pode ser distribuída, enquanto a chave privada deve ser mantida em segredo. Os algoritmos tendem a ser mais lentos que os de criptografia de chave simétrica.*

**Parte B.**

*De acordo com a figura do enunciado, sabemos que o certificado foi emitido por VeriSign Class 3 Secure Server CA - G3, tendo sido emitido para www.bancoenade.com.br ou www2.bancobrasil.com.br. O algoritmo de hash foi SHA1 e foi utilizado o algoritmo de criptografia pública RSA, com chave pública de 2048 bits.*

**Parte C.**

*Utiliza-se o algoritmo SHA1 para gerar uma assinatura digital da mensagem. O hash da mensagem é então codificado utilizando a chave privada do emissor, utilizando-se o algoritmo RSA. Posteriormente, a assinatura pode ser validada pela chave de criptografia pública do emissor.*

Disponível em <<http://download.inep.gov.br/educacao_superior/enade/padrao_resposta/2014/padrao_resposta_tecnologia_redes_computadores.pdf>>. Acesso em 18 set. 2017.

**3. Indicações bibliográficas**

* FAIRCLOTH, J. *Penetration tester's open source toolkit.* Cambridge: Syngress, 2016.
* FOROUZAN, A.B. *Comunicação de dados e redes de computadores*. São Paulo: McGraw-Hill, 2008.
* KATZ, J. *Digital signatures.* Heidelberg: Springer, 2010.
* Kościelny, C.; KURKOWSKI, M.; SREBRNY, M. *Modern cryptography primer: theoretical foundations and practical applications*. Heidelberg: Springer, 2013.
* TANENBAUM, A. S.; WHETHERALL, D. J. *Redes de computadores.* São Paulo: Pearson Prentice Hall, 2011.

**Questão 5**

**Questão 5.[[5]](#footnote-5)**

Um empreendedor na área de redes de computadores tem um bom faturamento com as mensalidades que seus vizinhos de condomínio pagam para ter acesso à Internet. Seu *link* de banda larga residencial compartilhado é de 356 Mbps, contratado junto a uma grande prestadora desse serviço. Com seus conhecimentos técnicos ele provê, informalmente, acesso aos seus "assinantes". Um antigo professor o alertou que seu negócio deve ser legalizado com base na Resolução da Anatel Nº 614, de 28 de maio de 2013, que regulamenta a modalidade de Serviço de Comunicação Multimídia (SCM).

Em relação às providências que o empreendedor deve tomar para legalizar seu negócio, avalie as afirmativas a seguir.

1. O empreendedor deve elaborar um projeto de redes de computadores definindo a faixa de frequências, o tipo de equipamento e a tecnologia a ser empregada, utilizando sempre equipamentos certificados pela Anatel.
2. O empreendedor deve requerer a licença SCM junto ao seu provedor para a realização da transmissão e distribuição do sinal de internet, independente do meio que será utilizado.
3. O empreendedor deve tornar disponíveis ao assinante informações sobre as características e especificações técnicas dos terminais, necessárias à conexão deles à sua rede.
4. O empreendedor deve contratar uma equipe técnica com profissionais experientes no ramo de redes de computadores, TCP/IP e acesso à internet, além de cadastrar-se junto ao CREA do seu Estado.
5. O empreendedor deve manter o seu link de banda larga residencial pré-existente para compartilhar acesso entre seus assinantes.

É correto apenas o que se afirma em

1. I, II e V.
2. I, III e IV.
3. I, IV e V.
4. II, III e V.
5. II, III e IV.
6. **Introdução teórica**

**Resolução Anatel Nº 614 - Regulamento do Serviço De Comunicação Multimídia**

A Resolução Nº 614 (Anatel, 2013), de 28 de maio de 2013,

*aprova o Regulamento do Serviço de Comunicação Multimídia e altera os Anexos I e III do Regulamento de Cobrança de Preço Público pelo Direito de Exploração de Serviços de Telecomunicações e pelo Direito de Exploração de Satélite.*

Artigos e trechos de anexos dessa resolução, necessários para a resolução da questão, serão apresentados na análise das afirmativas.

1. **Análise das afirmativas**

I – Afirmativa correta.

JUSTIFICATIVA. A Resolução Anatel Nº 614 (Anatel, 2013), Anexo II (DO PROJETO TÉCNICO), artigo 1º, diz que

*o Projeto Técnico, elaborado pela pretendente, deve conter pelo menos as seguintes informações:*

*a) descrição do serviço a ser prestado contemplando as aplicações previstas;*

*b) radiofrequências pretendidas, quando for o caso;*

*c) pontos de interconexão previstos;*

*d) capacidade pretendida do sistema em termos de número de canais e largura de banda ou taxa de transmissão;*

*e) localização dos principais pontos de presença, no formato Município/UF; e,*

*f) diagrama ilustrativo do sistema com a descrição das funções executadas por cada elemento do diagrama.*

O artigo 47 da referida resolução afirma o que segue.

*Sem prejuízo do disposto na legislação aplicável, as Prestadoras de SCM têm a obrigação de:*

*(…)*

*IV - utilizar somente equipamentos cuja certificação seja expedida ou aceita pela Anatel;*

II – Afirmativa incorreta.

JUSTIFICATIVA. O Artigo 21, do Capítulo V (DA INSTALAÇÃO E LICENCIAMENTO DO SISTEMA), da Resolução Anatel Nº 614 (Anatel, 2013), diz que

*antes de iniciar o funcionamento de uma Estação em caráter comercial, a Prestadora deve obter na Anatel a Licença para Funcionamento de Estação, salvo hipótese de dispensa de licenciamento prevista em regulamentação específica.*

Logo, a licença deve ser solicitada à Anatel e não ao provedor de acesso.

III – Afirmativa correta.

JUSTIFICATIVA. No TÍTULO V (DAS REGRAS DE PRESTAÇÃO DO SCM), CAPÍTULO I (DAS DISPOSIÇÕES GERAIS), artigo 63, da Resolução Anatel Nº 614 (Anatel, 2013), temos o que segue.

*§ 3º As prestadoras de SCM devem, em seus Planos de Serviços e em todos os demais documentos relacionados às ofertas, informar a(s) velocidade(s) máxima(s), tanto de download quanto de upload, de maneira clara, adequada e de fácil visualização, bem como as demais condições de uso, como franquias, eventuais reduções desta(s) velocidade(s) e valores a serem cobrados pelo tráfego excedente.*

IV – Afirmativa correta.

JUSTIFICATIVA. No Anexo I (DOCUMENTAÇÃO NECESSÁRIA AO REQUERIMENTO DE AUTORIZAÇÃO) da Resolução Anatel Nº 614 (Anatel, 2013), artigo 1º, item II, é listada a documentação para prestação de serviço de provedor de internet, no que se refere à qualificação técnica, conforme segue.

*a) Registro e quitação da pretendente no Conselho Regional de Engenharia, Arquitetura e Agronomia do local de sua sede, conforme Lei nº 5.194, de 24 de dezembro de 1966.*

*b) Declaração do representante legal da pretendente ou atestado emitido por pessoas jurídicas de direito público ou privado, comprovando a aptidão para o desempenho da atividade pertinente, bem como a existência de pessoal técnico adequado e disponível para a realização do objeto da autorização.*

O artigo 2º da referida resolução diz que

*o Projeto técnico deve ser acompanhado de Anotação de Responsabilidade Técnica, relativa ao projeto, devidamente assinada por profissional habilitado pelo Conselho Regional de Engenharia, Arquitetura e Agronomia que possua competências para se responsabilizar por atividades técnicas na área de telecomunicações.*

V – Afirmativa incorreta.

JUSTIFICATIVA. O artigo 42, do Capítulo III (DOS DIREITOS E OBRIGAÇÕES DA PRESTADORA), da Resolução Anatel Nº 614 (Anatel, 2013), diz que

*quando uma Prestadora contratar a utilização de recursos integrantes da rede de outra Prestadora de SCM ou de Prestadoras de qualquer outro serviço de telecomunicação de interesse coletivo para a constituição de sua própria rede, caracterizar-se-á a situação de exploração industrial.*

Logo, o empreendedor não pode redistribuir a banda larga que ele contrata da operadora.

Alternativa correta: B.

1. **Indicação bibliográfica**

* ANATEL. Resolução Nº 614, de 28 de maio de 2013. *Regulamento do Serviço de Comunicação Multimídia.* Disponível em <http://www.anatel.gov.br/legislacao/ resolucoes/2013/465-resolucao-614#art50>. Acesso em 22 set. 2017.

**Questão 6**

**Questão 6.**[[6]](#footnote-6)

A função da auditoria de sistemas é promover adequação, revisão e recomendações para o aprimoramento dos controles internos em qualquer um dos sistemas de informação da empresa, bem como avaliar a utilização dos recursos humanos, materiais e tecnológicos envolvidos no processamento desses sistemas.

Com base nessas informações, avalie as informações a seguir.

1. A auditoria de sistemas permite detectar, de forma automática, o uso dos recursos e dos fluxos de informação em uma empresa, embora não identifique qual informação é crítica para o cumprimento da missão e objetivos empresariais.
2. As ferramentas de auditoria classificadas como generalistas apresentam softwares com a capacidade de processar, analisar e simular amostras e apontar possíveis duplicidades.
3. As ferramentas de auditoria classificadas como de utilidade geral apresentam softwares próprios para a execução de funções muito comuns de processamento, como sortear arquivos, concatenar, sumarizar e gerar relatórios.

É correto o que se afirma em

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. I, apenas. | 1. III, apenas. | 1. I e II, apenas. | 1. II e III, apenas. | 1. I, II e III. |

1. **Análise da questão**

**Auditoria de sistemas**

Está explícito na questão que o assunto tratado é a auditoria de sistemas. Sabe-se a auditoria de sistemas de informática é uma atividade cuja missão é o gerenciamento do risco operacional envolvido nas tecnologias (técnicas) e nos sistemas de informação empregados em uma organização.

A auditoria de sistemas de informação tem como objetivo a garantia da integridade dos dados manipulados pelos sistemas de informação da empresa. Isso é feito por meio do estabelecimento de procedimentos que são documentados e que devem ser usados no planejamento e na utilização dos recursos computacionais da empresa.

A auditoria de sistemas acompanha os controles, o desenvolvimento de sistemas, os procedimentos de TI, a ampliação de infraestrutura, as operações, o desempenho e a segurança que envolvem o processamento de informações críticas para a tomada de decisão.

Além desses aspectos, a questão aborda a classificação das ferramentas passíveis de serem usadas em uma auditoria de sistemas de informação. Essas ferramentas podem ser classificadas em generalistas, especializadas ou de utilidade geral.

1. **Análise das afirmativas**

I - Afirmativa incorreta.

JUSTIFICATIVA. A auditoria de sistemas identifica as informações que são críticas para as tomadas de decisão e que envolvem vários aspectos da organização, abrangendo a missão e os objetivos empresariais.

II - Afirmativa correta.

JUSTIFICATIVA. De acordo com Teruel (2020), as ferramentas generalistas de auditoria são softwares que podem processar, simular, analisar amostras, gerar dados estatísticos, sumarizar informações, apontar duplicidade e realizar outras funções que o auditor desejar.

III - Afirmativa correta.

JUSTIFICATIVA. De acordo com Teruel (2020),

*as ferramentas de utilidade geral são softwares utilitários utilizados para executar algumas funções muito comuns de processamento, como sortear arquivos, sumarizar, concatenar, gerar relatórios etc. Esses programas não foram desenvolvidos para executar trabalhos de auditoria, portanto, não tem recursos tais como verificação de totais de controles, ou gravação das trilhas de auditoria. A grande vantagem desse tipo de ferramenta é que elas podem ser utilizadas como “quebra-galho” na ausência de outros recursos.*

Alternativa correta: D.

1. **Indicações bibliográficas**

* DUTRA, E. C. *Auditoria de sistemas de informação: introdução, controles organizacionais e operacionais.* Disponível em <https://jus.com.br/artigos/56084/auditoria-de- sistemas-de-informacao-introducao-controles-organizacionais-e-operacionais>. Acesso em 17 fev. 2020.
* IMONIANA, J. O. *Auditoria de sistemas de informação.* São Paulo: Atlas, 2016.
* LYRA, M. R. *Segurança e auditoria em sistemas de informação.* São Paulo: Ciência Moderna, 2017.
* RIBEIRO, G. F. *Auditoria de sistemas de informação – Conheça mais sobre o assunto*. Disponível em <https://www.profissionaisti.com.br/2012/04/auditoria-de-sistemas- de-informacao-conheca-mais-sobre-o-assunto/>. Acesso em 17 fev. 2020.
* TERUEL, E. C. *Principais ferramentas utilizadas na auditoria de sistemas e suas características.* Disponível em <http://www.portal.cps.sp.gov.br/pos-graduacao/ workshop-de-pos-graduacao-e-pesquisa/anais/2010/trabalhos/gestao-e-desenvolvimento -de-tecnologias-da-informacao-aplicadas/trabalhos-completos/teruel-evandro-carlos.pdf>. Acesso em 17 fev. 2020.

**Questão 7**

**Questão 7.**[[7]](#footnote-7)

Leia o texto a seguir.

*Um erro comum que se observa nas abordagens da Internet das Coisas (Internet of things – IoT) é o desenvolvimento de um produto sem uma visão clara de geração de valor. É comum os desenvolvedores não terem a clareza do real valor a ser gerado aos usuários finais, concebendo um produto sem o seu valor agregado.*

*Nesse sentido, para abertura de negócios inovadores, é essencial compreender o surgimento de novos negócios baseados em IoT e como essa revolução criará oportunidades.*

Disponível em <http://www.convergenciadigital.com.br>. Acesso em 27 jul. 2017 (com adaptações)

Com base nesse contexto, avalie as afirmativas.

1. Para que a IoT possa gerar valor aos negócios, é necessário considerar questões relacionadas a problemas da interoperabilidade de plataformas.
2. O IoT permite uma independência da infraestrutura de telecomunicação e os seus projetos exigem o uso de novas tecnologias, como as impressoras 3D.
3. A tríade composta pela criação de novos mercados digitais, gestão de risco e melhorias de eficiência é a chave para a transformação de modelos de negócios atuais a partir da revolução da IoT.

É correto o que se afirma em

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. I, apenas. | 1. II, apenas. | 1. I e III, apenas. | 1. II e III, apenas. | 1. I, II e III. |

1. **Análise da questão**

**Internet das Coisas *(Internet of things – IoT)***

Desde a década de 1980, temos observado dois fenômenos nas áreas da computação e da eletrônica:

* o aumento do poder computacional;
* a diminuição dos custos de produção.

A produção de equipamentos eletrônicos se tornou cada vez mais barata, ao mesmo tempo em que as possibilidades de aumento na complexidade desses equipamentos se tornaram cada vez maiores.

Outro fenômeno que também verificamos refere-se à explosão, em popularidade, da Internet, vinda da disseminação do uso das redes de computadores.

O efeito integrado de todos esses fenômenos foi o surgimento da possibilidade de fazermos equipamentos eletrônicos que apresentam, além de elevado grau de complexidade computacional (incluindo a utilização da inteligência artificial), a possibilidade de comunicação autônoma em uma rede de computadores. Esse é o mundo da Internet das Coisas, ou IoT (Internet of Things). Contudo, ainda que exista ampla disponibilidade de produção de dispositivos inteligentes e interconectados, não podemos esquecer a dimensão comercial envolvida nos projetos desses produtos.

Nesse contexto, a questão em análise busca determinar se o estudante tem a percepção da agregação de valor que a IoT pode proporcionar aos produtos e aos serviços oferecidos por uma empresa. As afirmativas tratam, também, da dependência existente entre a IoT e a infraestrutura disponível.

Para responder à questão, é importante que o aluno tenha conhecimentos sobre a IoT e sobre como ela pode agregar valor aos produtos e aos serviços oferecidos. Trata-se de um diferencial de sucesso para uma empresa.

1. **Análise das afirmativas**

I - Afirmativa correta.

JUSTIFICATIVA. Toda a cadeia de desenvolvimento de IoT é suportada pelo hardware,pela rede, pela infraestrutura, pelas plataformas e pelos sistemas integrados. Dessa forma, para que a IoT possa agregar valor aos negócios, é preciso considerarmos questões que viabilizem a interoperabilidade completa em vários níveis, desde o estabelecimento de protocolos e dispositivos até as tarefas que envolvem instâncias do topo da hierarquia institucional.

II - Afirmativa incorreta.

JUSTIFICATIVA. Uma solução de negócios fundamentada em IoT pode ser baseada na infraestrutura de telecomunicações existente na empresa. Isso não requer, necessariamente, o uso de impressoras 3D.

III - Afirmativa correta.

JUSTIFICATIVA. Segundo Cossini (2020),

*a tríade composta pela criação de novos mercados digitais, gestão de risco e melhorias de eficiência é a chave para a transformação dos modelos de negócio atuais a partir da revolução que a Internet das Coisas vem trazendo para o bem-estar das pessoas ao redor do planeta. As empresas devem inovar por meio de novas parcerias e uso intensivo de inovadoras tecnologias para levarem produtos e serviços que melhor atendam os novos consumidores digitais e aqueles que, não tão novos, já estão inseridos na economia digital por meio de seus smartphones ou dispositivos inteligentes.*

Alternativa correta: C.

1. **Indicações bibliográficas**

* BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL – BNDES. *Internet das coisas – Um plano de ação para o Brasil.* Disponível em <http://www.mctic.gov.br/mctic/export/sites/institucional/tecnologia/SEPOD/politicasDigitais/arquivos/arquivos\_estudo\_iot/fase-4-3.pdf>. Acesso em 18 fev. 2020.
* BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL – BNDES. *Internet das coisas: estimando impactos na economia.* Disponível em <https://www. bndes.gov.br/wps/portal/site/home/conhecimento/noticias/noticia/internet-coisas-iot>. Acesso em 18 fev. 2020.
* COELHO, P. *Internet das Coisas – Introdução prática.* Lisboa: FCA, 2017.
* COSSINI, R. *A Internet das Coisas pode mudar a economia?* Disponível em <https://computerworld.com.br/2016/04/19/internet-das-coisas-pode-mudar-economia/>. Acesso em 18 fev. 2020.
* FURTADO, F.; PEIXOTO, E.; PEREIRA, D. *Roadmap de Educação para IoT - Internet of Things.* Disponível em <https://www.cesar.org.br/index.php/2017/12/12/r oadmap-de-educacao-para-iot%E2%80%8A-%E2%80%8Ainternet-of-things/>. Acesso em 18 fev. 2020.
* MAGRANI, E. *A Internet das Coisas.* Rio de Janeiro, FGV. 2018.
* SINCLAIR, B. *IoT: Como usar a "Internet das Coisas" para alavancar seus negócios.* São Paulo: Autêntica Business, 2018.

**Questões 8 e 9**

**Questão 8.**[[8]](#footnote-8)

Durante o projeto da rede de uma empresa, muitas vezes é necessário limitar o domínio de broadcast, dividindo a rede em diversas LANs (Local Area Networks). Uma forma flexível de se realizar esse particionamento é por meio do uso de VLANs (virtual LANS). Nesse caso, diversas redes lógicas são criadas em um mesmo switch físico, o qual segrega o tráfego entre elas.

No que se refere às VLANs, avalie as afirmativas.

1. O padrão IEEE 802.1Q especifica como pode ser estabelecido o trunking, isto é, a ligação ponto a ponto entre dois switches que compartilham mais de uma VLAN.
2. A interligação entre duas VLANs pode ser realizada sem a necessidade de um equipamento da camada de rede, uma vez que elas compartilham o mesmo switch.
3. É possível criar uma VLAN em função dos endereços MAC de seus membros, ou seja, um equipamento fará parte da VLAN independentemente da porta do switch onde ele seja conectado.
4. Equipamentos ligados em uma mesma VLAN, em switches diferentes que estejam ligados entre si, fazem parte de diferentes domínios de broadcast.

É correto apenas o que se afirma em

A. I e II.

B. I e III.

C. III e IV.

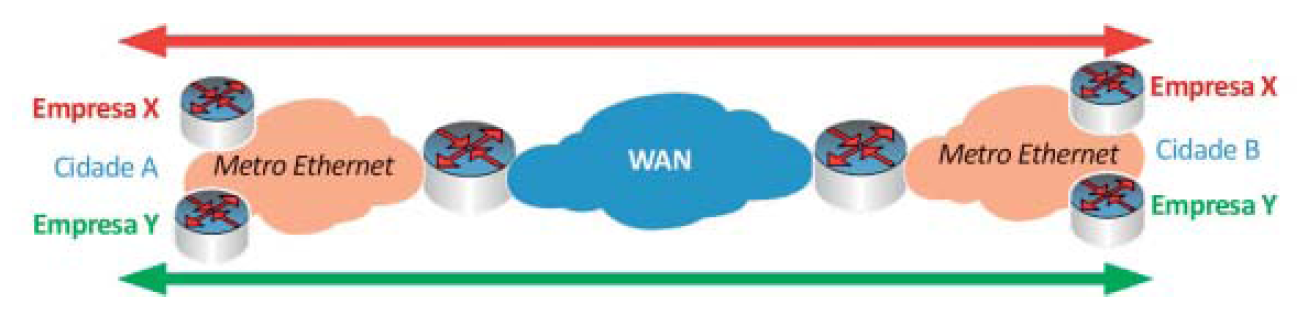
D. I, II e IV.

E. II, III e IV.

**Questão 9.**[[9]](#footnote-9)

Um provedor de serviços de rede interliga as cidades A e B por meio de uma rede WAN de longa distância, e, em cada uma das cidades, o provedor opera uma rede Metro Ethernet para prover serviços a seus clientes.

As empresas X e Y contrataram o provedor de serviços corporativos e possuem escritórios fisicamente presentes em cada uma das cidades mencionadas, conforme mostra a figura a seguir.



Cada empresa possui várias VLANs (Virtual Local Area Networks) configuradas internamente e os dados dessas VLANs devem trafegar da cidade A para a cidade B, passando pelas redes Metro Ethernet e WAN do provedor, de forma segura e independente.

Nessa situação, os protocolos que devem ser configurados pelo provedor na rede Metro Ethernet e na rede WAN para ocorrer o tráfego dos dados das VLANs das empresas entre cidades diferentes são

A. IEEE 802.1ad (QinQ) na rede Metro Ethernet e IEEE 802.1Q na rede WAN.

B. IEEE 802.1Q na rede Metro Ethernet e VPLS(Virtual Private Lan Services) na rede WAN.

C. VPLS (Virtual Private Lan Services) na rede Metro Ethernet e IEEE 802.1Q na rede WAN.

D. IEEE 802.1ad (QinQ) na rede Metro Ethernet e VPLS(Virtual Private Lan Services) na rede WAN.

E. VPLS (Virtual Private Lan Services) na rede Metro Ethernet e IEEE 802.1ad (QinQ) na rede WAN.

1. **Análise da questão**

**Construção de redes de computadores**

As questões abordam temas especialmente ligados à camada de enlace e englobam diferentes aspectos na construção de redes de computadores. No nível interno de uma organização, pode existir um problema de isolamento do tráfego: uma rede com um único comutador (*switch*) teria um único domínio de broadcast. A utilização de Virtual LANs permite a construção de "redes virtuais", cada uma com o seu domínio de broadcast. Assim, é possível criar várias redes lógicas dentro de um único equipamento físico (KUROSE e ROSS, 2014).

Contudo, há outro aspecto envolvido na construção de redes, que é praticamente o oposto do problema da construção de VLANs: trata-se do problema da interligação de redes geograficamente dispersas. Empresas que têm filiais e escritórios em diferentes locais enfrentam esse problema, visto que operam com uma série de redes LANs separadas, mas que deveriam, idealmente, estar interligadas.

A interligação demanda a superação de diversos desafios e isso depende de vários fatores, especialmente do tamanho da empresa e da forma como ela pretende adquirir essa interligação. Provedores de serviços corporativos podem oferecer diferentes tipos de alternativas. Para a construção de MANs (Metropolitan Area Networks), que são redes que ocupam áreas de tamanho geográfico de uma cidade, uma das possibilidades é a Metro Ethernet. Nesse caso, o provedor de serviço deve pensar em como lidar com as VLANs criadas pelos clientes nas suas redes e em como garantir a interligação dessas VLANs (lembrando que o provedor vai trabalhar não apenas com várias VLANs de um mesmo cliente, mas, potencialmente, com VLANs de clientes diferentes). O padrão IEEE 802.1ad foi criado com a finalidade de viabilizar o empilhamento de VLANs e sua integração.

Outro aspecto abordado por uma das questões é a criação de VPNs (*Virtual Private Networks* ou redes privadas virtuais). Uma VPN comporta-se como se fosse uma grande rede LAN, mesmo sendo composta de redes geograficamente distantes (KUROSE e ROSS, 2014). Nesse sentido, devemos lembrar que é possível utilizar a tecnologia VPLS (*Virtual Private Lan Services*) para criar uma VPN na camada de enlace de dados (JUNIPER, 2020).

1. **Análise das afirmativas e alternativas**

**Questão 8.**

I - Afirmativa correta.

JUSTIFICATIVA. A utilização de VLANs permite que se criem redes LANs virtuais, ou lógicas, mesmo quando utilizamos um único comutador (*switch*) físico. Essas redes virtuais comportam-se como uma rede LAN real, tendo domínios de broadcast diferentes, configuráveis pelo administrador de redes. Além disso, em redes (reais), pode ser necessário o uso de diversos comutadores (*switches*), que devem ser interconectados. Nessas situações, pode ser necessário que determinada VLAN se "espalhe" por diversos comutadores diferentes. Por exemplo, portas em comutadores físicos distintos podem pertencer a uma mesma VLAN. Para que isso seja possível, precisamos interconectar os diversos comutadores por meio do processo de entroncamento de VLANs (*trunking*), o que é especificado no padrão IEEE 802.1Q.

II - Afirmativa incorreta.

JUSTIFICATIVA. A interligação de VLANs é similar à interligação de LANs, sendo necessária a utilização de um roteador (que atua na camada de rede). Contudo, é possível que um mesmo dispositivo físico apresente as funcionalidades de roteador e de comutador (também chamado de *switch*).

III - Afirmativa correta.

JUSTIFICATIVA. Existem diversas formas de configuração de VLANs, como por tipos de portas, de grupos de endereços MAC ou de protocolos.

IV - Afirmativa incorreta.

JUSTIFICATIVA. Equipamentos em uma mesma VLAN estão no mesmo domínio de broadcast.

Alternativa correta: B.

**Questão 9.**

A - Alternativa incorreta.

JUSTIFICATIVA. O protocolo que deve ser configurado na rede WAN é o VPLS, não o IEEE 802.1Q, uma vez que este último está relacionado à criação das VLANs, e não à WAN.

B - Alternativa incorreta.

JUSTIFICATIVA. O protocolo a ser configurado para a rede Metro Ethernet deve ser o IEEE 802.1ad, pois é ele que possibilita o empilhamento de VLANs. Contudo, devemos ter em mente que o padrão IEEE 802.1ad foi posteriormente incorporado ao padrão IEEE 802.1Q-2011.

C - Alternativa incorreta.

JUSTIFICATIVA. É o protocolo VPLS deve ser configurado na rede WAN, e não o protocolo IEEE 802.1Q.

D - Alternativa correta.

JUSTIFICATIVA. O protocolo IEEE 802.1ad permite o empilhamento de VLANs na rede Metro Ethernet. O protocolo VPLS é utilizado na rede WAN.

E - Alternativa incorreta.

JUSTIFICATIVA. A resposta correta corresponde justamente à situação inversa da apresentada. Devemos observar que o empilhamento de VLANs precisa ser configurado na rede Metro Ethernet.

1. **Indicações bibliográficas**

* KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a Internet: uma abordagem top-down.* 6. ed. São Paulo: Pearson Education do Brasil, 2014.
* JUNIPER, *Network Configuration Example Virtual Private LAN Services*. Sunnyvale: Juniper Networks, 2017. Disponível em <https://www.juniper.net/documentation/ en\_US/release-independent/nce/information-products/pathway-pages/nce/feature-guide-virtual-private-lan-service.pdf>. Acesso em 07 abr. 2020.
* TANENBAUM, A. S.; WETHERALL, J. *Redes de computadores*. 5. ed. São Paulo: Pearson Education do Brasil, 2011.

**Questão 10**

**Questão 10.**[[10]](#footnote-10)

Leia o texto a seguir.

*A virtualização, tecnologia que provê uma abstração dos recursos físicos e lógicos, permite que instâncias de um sistema operacional sejam executadas em hardware virtual, suportadas por um hipervisor que gerencia o acesso aos recursos do hardware físico.*

STALLINGS, W.; BROWN, L. Segurança de computadores: princípios e práticas. 2. ed. Rio de Janeiro: Elsevier, 2014 (com adaptações).

Considerando que, para a elaboração e a implantação de projetos lógicos e físicos, a virtualização é considerada na manutenção, administração, segurança e gerenciamento de serviços de redes de computadores em um datacenter, avalie as afirmativas a seguir.

1. A virtualização faz com que um único recurso de hardware suporte várias instâncias simultâneas de sistemas, ou que vários recursos de hardware suportem uma instância única de sistema.
2. Na virtualização, um drive de disco pode ser particionado e apresentado como vários drives de disco para um sistema computacional.
3. Na virtualização, vários drives de disco podem ser concatenados e apresentados como um único drive de disco para um sistema computacional.

É correto o que se afirma em

1. I, apenas.
2. III, apenas.
3. I e II, apenas.
4. II e III, apenas.
5. I, II e III.
6. **Análise da questão**

**Virtualização e uso de máquinas virtuais**

A questão aborda o tema da virtualização e o uso de máquinas virtuais.

A ideia de virtualização é antiga, sendo que um dos artigos fundamentais relativo a esse tema, de Popek e Goldberg (1974), foi publicado ainda na década de 1970. Nesse artigo, são definidos dois tipos de abordagens para a virtualização:

* a abordagem em que o hipervisor executa diretamente no hardware;
* a abordagem em que o hipervisor executa sobre um sistema operacional convencional.

Na primeira abordagem, em que o hipervisor executa diretamente no hardware, ele desempenha papel similar ao de um sistema operacional convencional. Contudo, seus principais objetivos são criar uma camada de abstração para o hardware e permitir a execução das diversas máquinas virtuais. Esse tipo de hipervisor também é chamado de nativo, tipo 1 ou *bare metal*.

Na segunda abordagem, em que o hipervisor executa sobre um sistema operacional convencional, ele é instalado de forma similar a um programa, ainda que, nesse processo, diversos drivers especiais também devam ser instalados para que o sistema operacional nativo seja capaz de interagir com o hipervisor e apresentar performance aceitável. Em tais casos, as máquinas virtuais são executadas de uma forma similar a um programa convencional (TANENBAUM e BOS, 2016). É o que acontece com diversos programas populares de virtualização, como o Oracle VirtualBox, por exemplo.

É importante termos em mente a flexibilidade oferecida pela virtualização: em uma mesma máquina física, diversas máquinas virtuais podem ser executadas simultaneamente. Elas podem executar sistemas operacionais diferentes e ter configurações completamente distintas umas das outras. Isso faz com que uma mesma máquina física possa executar programas feitos para sistemas operacionais completamente diferentes.

A execução de máquinas virtuais apresenta tanto oportunidades quanto desafios com relação à questão da segurança. Podemos pensar que a execução de todo o sistema operacional em um ambiente virtual poderia ser mais segura do que sua execução em um hardware real, já que o comprometimento da máquina virtual não implica o comprometimento da máquina física.

Contudo, programas quase sempre apresentam vulnerabilidades, sejam eles sistemas operacionais ou hipervisores. Assim, aplicações mal intencionadas poderiam tentar quebrar o isolamento do hipervisor e ter acesso ao hardware real ou ao sistema operacional hospedeiro.

É importante adicionarmos que, com o tempo, outras formas de virtualização foram surgindo. Por exemplo, alguns sistemas operacionais podem oferecer um recurso de virtualização semelhante aos recursos descritos anteriormente, mas com grau de isolamento intermediário entre as diversas entidades virtualizadas.

1. **Análise das afirmativas**

I - Afirmativa correta.

JUSTIFICATIVA. Pelo uso da virtualização, é possível executar, em máquinas virtuais, sistemas operacionais convidados. Por exemplo, um computador que rode nativamente o sistema operacional Windows pode executar máquinas virtuais rodando outros sistemas operacionais como convidados, como o GNU Linux, por exemplo.

II - Afirmativa correta.

JUSTIFICATIVA. Um exemplo que ilustra a situação da afirmativa é aquela na qual criamos vários arquivos no disco da máquina real, sendo que cada um desses arquivos funciona como um disco em separado para a máquina virtual. Para o sistema operacional convidado (que executa na máquina virtual), esses arquivos funcionam como discos reais. Contudo, na realidade, temos apenas um único disco "simulando" vários discos em separado. Além disso, para cada uma das máquinas virtuais e para o sistema operacional convidado, esses discos podem ser particionados e formatados de forma independente.

III - Afirmativa correta.

JUSTIFICATIVA. Essa situação, que se refere à situação inversa da afirmativa anterior e corresponde à utilização de um disco lógico, também chamado de *logical disk* (ou vdisk), o qual pode ser composto de mais de um disco real.

Alternativa correta: E.

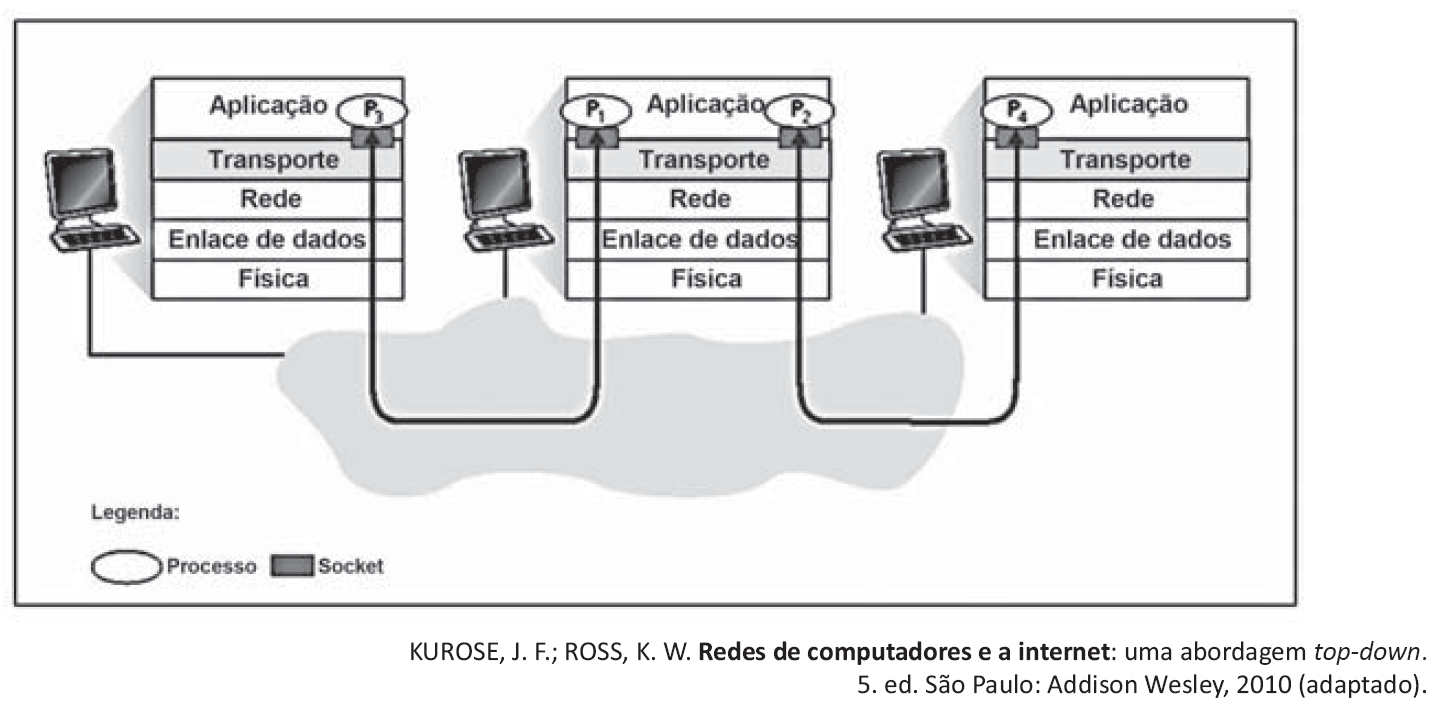
1. **Indicações bibliográficas**

* POPEK, G. J.; GOLDBERG, R. P. *Formal requirements for virtualizable third generation architectures.* Communications of the ACM, New York, v.17, n.7, p.412-421, 1974.
* SILBERSCHATZ, A.; GALVIN, P. B.; GAGNE. G. *Fundamentos de sistemas operacionais*. 4. ed. Rio de Janeiro: LTC, 2015.
* STALLINGS, W.; BROWN, L. *Segurança de computadores: princípios e práticas*. 2. ed. Rio de Janeiro: Elsevier, 2014.
* TANENBAUM, A. S.; BOS, H. *Sistemas operacionais modernos*. 4. ed. São Paulo: Pearson Education do Brasil, 2016.

**Questão 11**

**Questão 11.**[[11]](#footnote-11)

Em uma rede de computadores baseada na arquitetura TCP/IP, a camada de transporte fornece o serviço de comunicação fim a fim entre os processos de aplicações executadas em cada um dos hospedeiros. Do ponto de vista das aplicações, a comunicação lógica fim a fim significa que tudo se passa como se os hospedeiros que rodam os pares de processos estivessem conectados diretamente. A figura a seguir mostra o recorte de uma rede com três hospedeiros e quatro processos. Observe a existência de uma comunicação lógica entre os processos P1 e P3 e entre os processos P2 e P4.



KUROSE, J. F.; ROSS, K. W. Redes de computadores e a internet: uma abordagem top-down. 5. ed. São Paulo: Addison Wesley, 2010 (com adaptações).

Com base na figura apresentada, assinale a opção correta.

1. O processo P3 se conecta a P1 por meio de um número de porta UDP, que é um identificador exclusivo entre 0 e 1023.
2. No hospedeiro do meio, o serviço de multiplexação/demultiplexação fornecido pela camada de transporte garante a entrega dos dados ao processo de aplicação apropriado.
3. O endereço IP de destino contido no cabeçalho do protocolo TCP identifica o hospedeiro para o qual o segmento está sendo enviado e garante a comunicação fim a fim.
4. O protocolo de camada de transporte usado na comunicação entre os pares de processos é o TCP, que utiliza uma apresentação de três vias para estabelecer a comunicação fim a fim.
5. No protocolo de camada de transporte utilizado na comunicação entre os processos P2 e P4, cada segmento de dados enviado entre esses dois processos obterá uma confirmação de recebimento.
6. **Análise da questão**

**Protocolos TCP e UDP**

A questão aborda o uso dos protocolos TCP e UDP em um cenário bastante simplificado. Um dos pontos explorados pela questão refere-se aos processos de multiplexação e de demultiplexação. Para compreendermos esses conceitos, podemos imaginar um cenário no qual um computador está executando diversos processos simultaneamente. Suponha que mais de um processo está conectado a outros processos, execute em outros computadores e se comunique via uma rede que utiliza os protocolos TCP/IP. O sistema operacional, por meio dos seus serviços de rede, especificamente da implementação da pilha de protocolos TCP/IP, deve fazer com que cada processo "veja" apenas a sua comunicação, separando os diversos fluxos de dados dos processos executando em paralelo.

A pilha de protocolos TCP/IP, também chamados de protocolos internet, utiliza uma estratégia na qual identificamos cada máquina, ou, mais precisamente, cada interface de rede), por meio de um endereço IP. Mas, além do endereço IP, um processo pode utilizar uma ou mais portas. A associação do endereço IP e da porta permite que vários processos executando em um mesmo computador se comuniquem com outros processos paralelamente.

A ligação entre os processos executando em diferentes máquinas é feita com a ajuda de sockets (traduções possíveis para esse termo seriam “tomada” ou “encaixe”, mas, normalmente, utilizamos o vocábulo em inglês). Do ponto de vista do processo, a comunicação é feita pelo envio das informações para o socket, sendo que os demais cuidados são feitos pela pilha de protocolos TCP/IP (KUROSE e ROSS, 2014). Na criação do socket, usamos o endereço IP da máquina que desejamos contactar e a porta associada a determinado serviço ou processo. De forma simplificada, podemos pensar que uma porta é um número de 16 bits utilizado de forma a selecionar o processo ao qual queremos nos conectar. Reforçamos que precisamos de duas informações: o endereço IP e o número da porta.

A ideia de porta permite que, em uma mesma máquina executando vários processos diferentes e simultâneos, possam ser estabelecidos fluxos de comunicação individuais para cada um dos processos. Além disso, todos esses processos vão utilizar a mesma interface de rede e o mesmo endereço IP (associado a essa interface). Assim, por exemplo, em um mesmo computador, podem ser executados simultaneamente um servidor web na porta 80 e um servidor de ftp na porta 21. Os dois processos têm seus fluxos de dados individuais e separados, pois trabalham em portas diferentes. No entanto, o endereço IP é o mesmo.

Adicionalmente, é interessante termos em mente que tanto o protocolo UDP quanto o protocolo TCP oferecem um mecanismo de porta (ambos são protocolos da camada de transporte). No caso do protocolo UDP, contudo, a comunicação é feita sem o estabelecimento de conexão, mas utilizando *sockets*. Vale notar que o protocolo TCP exige o estabelecimento de uma conexão entre os processos e também usa sockets para a comunicação.

1. **Análise das alternativas**

A - Alternativa incorreta.

JUSTIFICATIVA. Para que o processo P3 se conecte ao processo P1, precisamos utilizar a combinação de um endereço IP e de uma porta. O valor da porta é especificado por um número de 16 bits. Logo, há 65.536 possibilidades. Assim, o número das portas varia de 0 até 65.535. No entanto, devemos lembrar que as portas mais baixas (de 0 até 1023) são reservadas.

B - Alternativa correta.

JUSTIFICATIVA. Os processos de multiplexação e de demultiplexação permitem que a camada de transporte seja capaz de "coletar" e "distribuir" as diversas informações enviadas aos diversos processos ou recebidas pelos diversos processos que executam simultaneamente em um sistema operacional. Por exemplo, dois programas que executam em uma mesma máquina podem enviar para um servidor na rede ou receber dados de um servidor na rede, sendo que a camada de transporte tem de ser capaz de separar essas informações e entregá-las ao processo correspondente.

C - Alternativa incorreta.

JUSTIFICATIVA. Ainda que o enunciado afirme que a rede utilizada é baseada na arquitetura TCP/IP, não é possível saber se a aplicação usa o protocolo TCP ou o protocolo UDP para a camada de transporte. Caso seja empregado o protocolo UDP, não podemos garantir a entrega dos pacotes. Adicionalmente, mesmo no caso TCP, seriam necessárias outras informações, como a porta do destino.

D - Alternativa incorreta.

JUSTIFICATIVA. Não podemos garantir, pelo contexto do enunciado, que o protocolo da camada de transporte utilizado seja o TCP. Outra possibilidade é o uso do protocolo UDP e, também, da camada de transporte.

E - Alternativa incorreta.

JUSTIFICATIVA. Não sabemos se o protocolo utilizado é o TCP ou o UDP. Se fosse o protocolo UDP, não haveria garantia da entrega de pacotes.

1. **Indicações bibliográficas**

* KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a Internet: uma abordagem top-down*. 6. ed. São Paulo: Pearson Education do Brasil, 2014.
* SILBERSCHATZ, A.; GALVIN, P. B.; GAGNE. G. *Fundamentos de sistemas operacionais*. 4. ed. Rio de Janeiro: LTC, 2015.
* TANENBAUM, A. S.; BOS, H. *Sistemas operacionais modernos*. 4. ed. São Paulo: Pearson Education do Brasil, 2016.
* TANENBAUM, A. S.; WETHERALL, J. *Redes de computadores*. 5. ed. São Paulo: Pearson Education do Brasil, 2011.

**Questão 12**

**Questão 12.**[[12]](#footnote-12)

O protocolo IPv6 foi desenvolvido para substituir o IPv4, tendo sua implementação ocasionado várias mudanças importantes, como a capacidade de endereçamento expandida, o cabeçalho aprimorado de 40 bytes e a rotulação de fluxo e prioridade.

Considerando essas informações, avalie as afirmativas a seguir, relativas à descrição dos campos de cabeçalho IPv6.

1. Em "endereço de origem" e "endereço de destino", cada campo possui 64 bits, tendo sido expandidos os 32 bits usados no IPv4.
2. Em se tratando do cabeçalho IPv6, insere-se o valor 32 no campo "versão" de 4 bits que é usado para identificar a versão do protocolo IP.
3. O campo "próximo cabeçalho" identifica o protocolo ao qual os dados presentes no datagrama serão entregues, por exemplo, TCP ou UDP.
4. No IPv6, o campo "classe de tráfego" de 8 bits é semelhante ao campo "tipo de serviço" do IPv4, ambos utilizados para diferenciar os tipos de pacotes IP.
5. O valor do campo "limite de saltos" é decrementado em um para cada roteador que repassa o pacote; caso a contagem do limite de salto chegue a zero, o pacote será descartado.

É correto apenas o que se afirma em

A. II e IV.

B. I, II e III.

C. I, III e V.

D. III, IV e V.

E. I, II, IV e V.

1. **Análise da questão**

**Protocolo IP**

O IP é um protocolo da camada de rede fundamental para a construção da Internet e das diversas redes baseadas na pilha de protocolos TCP/IP. Podemos dizer que a versão IPv4 é uma das mais populares. No entanto, tal versão apresenta um problema: a limitação com relação ao seu espaço de endereçamento.

O endereço IP é um número de 32 bits, o que impõe uma restrição ao número máximo de endereços possíveis de aproximadamente 4 bilhões. Em virtude do crescimento de uso e a popularização da Internet, esse número se tornou claramente insuficiente. Com as finalidades de ampliar o espaço de endereçamento disponível e de melhorar diversos aspectos do protocolo, foi criada uma nova versão, o padrão IPv6, que dispõe de um espaço de endereçamento muito maior, além de oferecer as funcionalidades de rotulação de fluxo e de prioridade (KUROSE e ROSS, 2014).

1. **Análise das afirmativas**

I - Afirmativa incorreta.

JUSTIFICATIVA. No IPv6, os campos "endereço de origem" e "endereço de destino" têm 128 bits de tamanho, e não 64 bits, como indicado no texto da afirmativa.

II - Afirmativa incorreta.

JUSTIFICATIVA. O valor a ser inserido é o número 6 (na forma decimal) ou 0110 (na forma binária), e não 32, como indicado no texto da afirmativa.

III - Afirmativa correta.

JUSTIFICATIVA. Esse campo é normalmente utilizado para indicar qual é protocolo a ser utilizado pela camada de transporte, ou seja, se é o protocolo TCP ou o protocolo UDP.

IV - Afirmativa correta.

JUSTIFICATIVA. O campo "classe de tráfego" (em inglês, "traffic class") tem duas funções:

* classificação dos pacotes (via o campo "differentiated services");
* identificação de congestionamento.

V - Afirmativa correta.

JUSTIFICATIVA. O objetivo desse campo é limitar a durabilidade dos dados em circulação em uma rede, evitando que pacotes muito antigos (e que provavelmente se tornaram inúteis) fiquem circulando indefinidamente e congestionando a rede de modo desnecessário.

Alternativa correta: D.

1. **Indicações bibliográficas**

* KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a Internet: uma abordagem top-down*. 6. ed. São Paulo: Pearson Education do Brasil, 2014.
* SILBERSCHATZ, A.; GALVIN, P. B.; GAGNE. G. *Fundamentos de sistemas operacionais*. 4. ed. Rio de Janeiro: LTC, 2015.
* TANENBAUM, A. S.; BOS, H. *Sistemas operacionais modernos*. 4. ed. São Paulo: Pearson Education do Brasil, 2016.
* TANENBAUM, A. S.; WETHERALL, J. *Redes de computadores*. 5. ed. São Paulo: Pearson Education do Brasil, 2011.

**Questão 13**

**Questão 13.[[13]](#footnote-13)**

Em uma rede local de uma instituição bancária, foi implantado um sistema gerenciador de banco de dados (SGDB), tendo o administrador efetuado um comando GRANT para a realização das configurações de acesso ao SGDB na rede.

Com o objetivo de realizar autenticação por aplicações para acesso ao banco de dados, de forma segura, devem ser enviados ao servidor

1. o IP do servidor e a senha.
2. a senha e o endereço MAC.
3. o IP do servidor e o endereço MAC.
4. o IP do servidor, o nome físico do banco e a senha.
5. o IP do cliente, o nome físico do banco, a senha e o endereço MAC.
6. **Análise da questão**

**Sistemas gerenciadores de banco de dados (SGBDs)**

Existem diversos tipos de sistemas gerenciadores de banco de dados (SGBDs) no mercado. O tamanho e a complexidade desses sistemas dependem muito do tipo de aplicação a que se destinam.

Alguns sistemas de gerenciamento de banco de dados são extremamente pequenos, como é o caso da pequena biblioteca SQLite em C. Ela é, em geral, integrada à aplicação e pode ser utilizada de diversas formas, como, por exemplo, para armazenar informações de configurações dos usuários de um programa.

Existem também sistemas de gerenciamento de banco de dados grandes e complexos, projetados para atender a milhares de solicitações de muitos usuários simultaneamente, como o Oracle, o Microsoft SQL Server e o Postgres, entre outros. Nesses casos, os SGBDs utilizam tipicamente uma arquitetura cliente-servidor.

Sistemas criados com tais SGBDs normalmente são compostos por um software cliente que se conecta diretamente ao SGBD ou a um servidor de aplicação (e esse último se conecta ao SGBD). Nesse tipo de cenário, é bastante comum que vários clientes diferentes se conectem simultaneamente a um SGBD, enviando consultas e recebendo resultados.

Nos casos da utilização da arquitetura cliente-servidor, a questão da segurança é fundamental. Para garantir um mínimo de segurança na utilização da base de dados, o administrador do SGDB (o DBA, em geral) deve criar um usuário no banco de dados. Esse usuário tem um perfil associado, de forma similar a um usuário de um sistema operacional, com limitações de acordo com as necessidades da aplicação. Normalmente, definimos uma senha para garantir um mínimo de segurança: assim, evitamos que qualquer pessoa com acesso à rede seja capaz de fazer consultas no banco de dados.

Adicionalmente, é possível que uma mesma máquina física tenha várias instâncias de banco de dados diferentes. Ainda que o SGDB seja o mesmo, as instâncias individuais podem pertencer a projetos diferentes, com diferentes nomes (associados na sua criação). A chamada "string de conexão" é o conjunto de informações necessárias para que uma aplicação seja capaz de se conectar a uma instância, o que envolve várias informações, como o nome do banco de dados, o endereço IP do servidor, o nome do usuário e uma senha.

1. **Análise das alternativas**

A - Alternativa incorreta.

JUSTIFICATIVA. A aplicação deve indicar o nome da instância na qual vai ser feita a conexão.

B - Alternativa incorreta.

JUSTIFICATIVA. Existem várias formas de se conectar a uma base de dados e nem todas elas utilizam o protocolo TCP/IP. Contudo, os casos mais comuns envolvem a identificação do endereço IP do servidor, o nome da base de dados, o nome de usuário e uma senha. A identificação do endereço MAC associado ao endereço IP do servidor é um serviço feito pelos protocolos da rede.

C - Alternativa incorreta.

JUSTIFICATIVA. Os protocolos da rede são responsáveis por identificar o endereço MAC associado ao endereço IP do servidor (quando necessário). Além disso, devemos prover informações como o nome da instância do banco de dados, o usuário e uma senha.

D - Alternativa correta.

JUSTIFICATIVA. O endereço IP é utilizado para identificar a máquina na rede que está com o SGDB instalado. O nome do banco identifica a instância específica à qual se quer conectar. Além disso, normalmente é necessário que um usuário e uma senha também sejam fornecidos, garantindo um mínimo de segurança para a base de dados.

E - Alternativa incorreta.

JUSTIFICATIVA. Na conexão, deve ser indicado o endereço IP do servidor ao qual se deseja conectar. Além disso, a identificação do endereço MAC associado ao endereço IP do servidor é uma tarefa da rede.

1. **Indicações bibliográficas**

* KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a Internet: uma abordagem top-down*. 6. ed. São Paulo: Pearson Education do Brasil, 2014.
* SILBERSCHATZ, A.; GALVIN, P. B.; GAGNE. G. *Fundamentos de sistemas operacionais*. 4. ed. Rio de Janeiro: LTC, 2015.
* SILBERSCHATZ, A.; KORTH, H. F.; SUDARSHAN, S. *Sistema de banco de dados*. 5. ed. Rio de Janeiro: Elsevier, 2006.
* TANENBAUM, A. S.; BOS, H. *Sistemas operacionais modernos*. 4. ed. São Paulo: Pearson Education do Brasil, 2016.
* TANENBAUM, A. S.; WETHERALL, J. *Redes de computadores*. 5. ed. São Paulo: Pearson Education do Brasil, 2011.

**ÍNDICE REMISSIVO**

|  |  |
| --- | --- |
| **Questão 1** | Redes sem fio e protocolos de acesso múltiplo. |
| **Questão 2** | Sistemas operacionais. Sistemas operacionais de redes. Arquitetura de sistemas operacionais. |
| **Questão 3** | Qualidade de serviço (QoS). IntServ. DiffServ. |
| **Questão 4** | Criptografia simétrica. Criptografia assimétrica. Assinatura digital. |
| **Questão 5** | Resolução Anatel Nº 614 - Regulamento do Serviço De Comunicação Multimídia. |
| **Questão 6** | Governança corporativa e auditoria. Segurança e auditoria nos sistemas de informação. Classificação das ferramentas de auditoria. |
| **Questão 7** | Tecnologias emergentes. IoT. Inovação. |
| **Questão 8** | Construção de redes de computadores. |
| **Questão 9** | Construção de redes de computadores. |
| **Questão 10** | Virtualização e uso de máquinas virtuais. |
| **Questão 11** | Protocolos TCP e UDP. |
| **Questão 12** | Protocolo IP. |
| **Questão 13** | Sistemas gerenciadores de banco de dados (SGBDs). |

1. Questão 12 – Enade 2014. [↑](#footnote-ref-1)
2. Questão 20 – Enade 2014. [↑](#footnote-ref-2)
3. Questão 35 – Enade 2014. [↑](#footnote-ref-3)
4. Questão Discursiva 5 – Enade 2014. [↑](#footnote-ref-4)
5. Questão 31 - Enade 2014. [↑](#footnote-ref-5)
6. Questão 26 – Enade 2017. [↑](#footnote-ref-6)
7. Questão 33 – Enade 2017. [↑](#footnote-ref-7)
8. Questão 9 – Enade 2017 (com adaptações). [↑](#footnote-ref-8)
9. Questão 25 – Enade 2017. [↑](#footnote-ref-9)
10. Questão 10 – Enade 2017. [↑](#footnote-ref-10)
11. Questão 11 – Enade 2017. [↑](#footnote-ref-11)
12. Questão 13 – Enade 2017. [↑](#footnote-ref-12)
13. Questão 16 – Enade 2017. [↑](#footnote-ref-13)