UNIP
EDUCAÇÃO, POR SUA ESCOLHA

# ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

MATERIAL INSTRUCIONAL ESPECÍFICO

**TOMO 17**

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

# ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

MATERIAL INSTRUCIONAL ESPECÍFICO

**TOMO 17**

**Christiane Mazur Doi**

Doutora em Engenharia Metalúrgica e de Materiais, Mestra em Ciências - Tecnologia Nuclear, Especialista em Cálculo e Matemática Aplicada, Especialista em Estatística Aplicada e Ciência de Dados, Especialista em Língua Portuguesa e Literatura, Especialista em Recursos Gramaticais para Revisão Textual, Engenheira Química e Licenciada em Matemática, com Aperfeiçoamento em Estatística e MBA em Engenharia Econômica. Professora titular 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.

## Questão 1

### Questão 1.[1]

Leia o texto a seguir.

*O protocolo FTP trabalha na camada de aplicação do modelo OSI e possibilita que um usuário em um computador transfira, renomeie ou remova arquivos remotos. A implementação do protocolo FTP ocorre por meio de um programa, conhecido como servidor de FTP, sendo o programa ProFTPD um exemplo de sua utilização.*

SOARES, L. F. G.; LEMOS, G.; COLCHER, S. Redes de computadores: das LANS, MANS e WANS às redes ATM. Rio de Janeiro: Campus, 1995 (com adaptações).

A figura abaixo apresenta a análise de tráfego, por meio de um sniffer, de uma comunicação FTP entre a origem 192.168.56.1 e o destino 192.168.56.10, portanto, dentro de uma LAN.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.00000000 | 192.168.56.1 | 192.168.56.10 | TCP | 66 | 59362 > ftp [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=1 SACK_PERM=1 |
| 2 | 0.00029800 | 192.168.56.10 | 192.168.56.1 | TCP | 66 | ftp > 59362 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=32 |
| 3 | 0.00036400 | 192.168.56.1 | 192.168.56.10 | TCP | 54 | 59362 > ftp [ACK] Seq=1 Ack=1 Win=8192 Len=0 |
| 4 | 28.0395680 | 192.168.56.10 | 192.168.56.1 | FTP | 113 | Response: 220 ProFTPD 1.3.2c Server (Debian) [::ffff:192.168.56.10] |
| 5 | 28.0886880 | 192.168.56.1 | 192.168.56.10 | TCP | 54 | 59362 > ftp [ACK] Seq=1 Ack=60 Win=8133 Len=0 |
| 6 | 30.7887280 | 192.168.56.1 | 192.168.56.10 | FTP | 70 | Request: USER estudante |
| 7 | 30.7894960 | 192.168.56.10 | 192.168.56.1 | TCP | 54 | ftp > 59362 [ACK] Seq=60 Ack=17 Win=5856 Len=0 |
| 8 | 30.7909180 | 192.168.56.10 | 192.168.56.1 | FTP | 91 | Response: 331 Password required for estudante |
| 9 | 30.8399650 | 192.168.56.1 | 192.168.56.10 | TCP | 54 | 59362 > ftp [ACK] Seq=17 Ack=97 Win=8096 Len=0 |
| 10 | 32.9814520 | 192.168.56.1 | 192.168.56.10 | FTP | 70 | Request: PASS estudante |
| 11 | 33.0174140 | 192.168.56.10 | 192.168.56.1 | FTP | 84 | Response: 230 User estudante logged in |
| 12 | 33.0687510 | 192.168.56.1 | 192.168.56.10 | TCP | 54 | 59362 > ftp [ACK] Seq=33 Ack=127 Win=8066 Len=0 |
| 13 | 34.9035540 | 192.168.56.1 | 192.168.56.10 | FTP | 81 | Request: PORT 192,168,56,1,231,227 |
| 14 | 34.9041520 | 192.168.56.10 | 192.168.56.1 | FTP | 83 | Response: 200 PORT command successful |
| 15 | 34.9069720 | 192.168.56.1 | 192.168.56.10 | FTP | 60 | Request: NLST |
| 16 | 34.9078030 | 192.168.56.10 | 192.168.56.1 | FTP | 108 | Response: 150 Opening ASCII mode data connection for file list |
| 17 | 34.9182760 | 192.168.56.10 | 192.168.56.1 | FTP | 77 | Response: 226 Transfer complete |
| 18 | 34.9183200 | 192.168.56.1 | 192.168.56.10 | TCP | 54 | 59362 > ftp [ACK] Seq=66 Ack=233 Win=7960 Len=0 |

Em relação ao protocolo FTP e a sua implementação, avalie as afirmativas.

I. Não há a necessidade de estabelecimento do handshake de três vias por se tratar de uma conexão TCP.

II. Trata-se de um protocolo inseguro, pois não oferece criptografia, sendo recomendado a utilização de um protocolo mais seguro, como SFTP (Secure File Transfer Protocol).

III. A operação do FTP baseia-se no estabelecimento de duas conexões entre o cliente e o servidor, em que a primeira é a conexão de controle, usada para transferência de comandos, e a outra é uma conexão de transferência de dados.

IV. O protocolo FTP permite somente um modo de transferência, o modo binário.

É correto apenas o que se afirma em

A. I.

B. III.

C. I e IV.

D. II e III.

E. II e IV.

[1]Questão 11 – Enade 2014.

# 1. Introdução teórica

## 1.1. Protocolo FTP

Um dos primeiros objetivos da construção de redes de computadores foi a possibilidade de trocar (enviar e receber) uma grande quantidade de arquivos entre diferentes máquinas remotas. Por exemplo, alguns centros de pesquisa poderiam querer que pesquisadores de diferentes partes de um país (e até mesmo do mundo) pudessem enviar e receber arquivos de diferentes formatos em suas pesquisas. Para que isso fosse possível, era necessário desenvolver um protocolo que especificasse como sistemas distintos poderiam se comunicar em uma rede de computadores e trocar arquivos entre si.

Nesse sentido, outro problema que o protocolo deveria ajudar a superar é a diferença entre os diversos sistemas operacionais e as suas formas de armazenar arquivos. Em especial durante as décadas de 1970, 1980 e 1990, havia considerável quantidade de plataformas computacionais diferentes, frequentemente incompatíveis entre si e com modos de operação completamente diferentes.

Assim, o protocolo FTP foi criado para resolver esses problemas e prover uma forma simples, eficaz e eficiente de realização de trocas de arquivos em uma rede.

Ainda que o modelo de arquitetura do FTP seja cliente/servidor, ele apresenta algumas características peculiares. Por exemplo, nele, existem duas conexões simultâneas feitas por cada cliente: uma delas é a conexão de controle e a outra é a conexão de dados. Ainda que a especificação original do protocolo FTP seja anterior ao TCP, ele foi posteriormente reformulado para trabalhar com a pilha de protocolos TCP/IP.

Na figura 1, temos um exemplo de funcionamento do FTP, com um cliente conectando-se a um servidor.

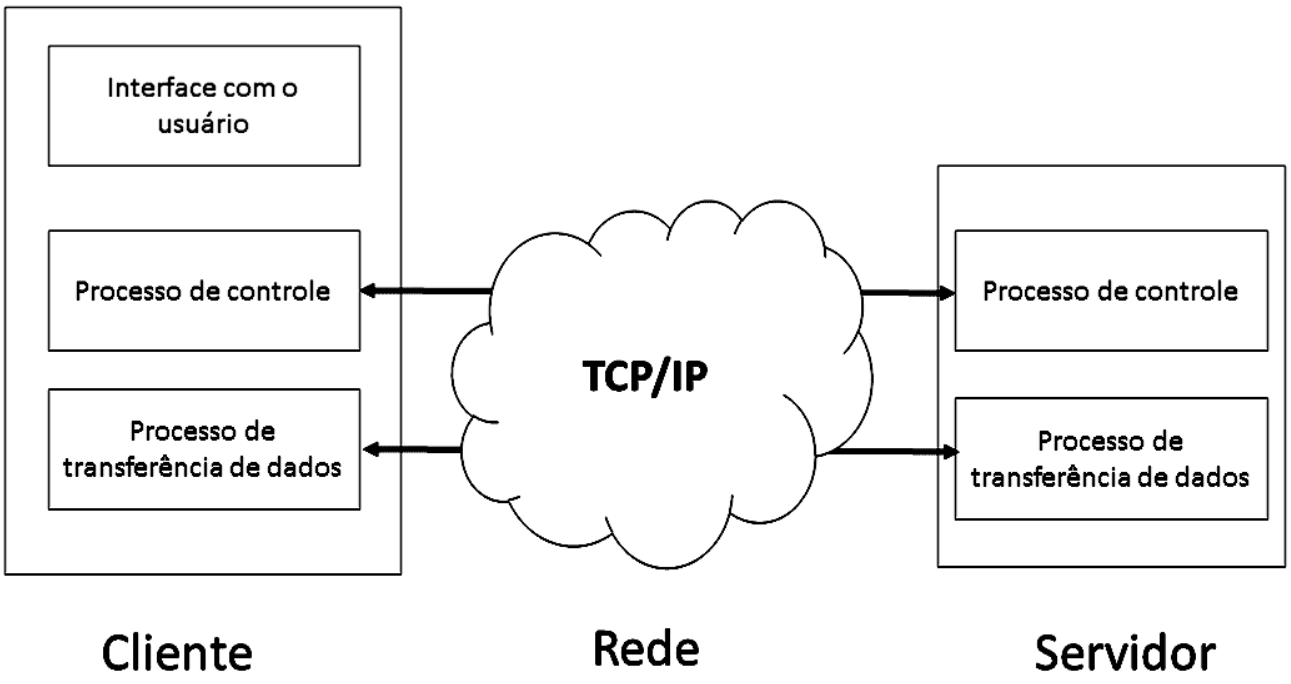



**Figura 1.** Protocolo FTP.
FOROUZAN, 2008 (com adaptações).

A conexão de controle serve para o envio dos comandos entre o cliente e o servidor. Um ponto interessante é que os comandos do protocolo FTP (que envolvem operações típicas de manipulação de arquivos, como, por exemplo, a navegação entre diretórios, a especificação de qual arquivo deve ser transferido e a remoção de arquivos) são padronizados e são os mesmos para diferentes sistemas operacionais e para diferentes plataformas computacionais. Dessa forma, o protocolo facilita a troca de arquivos entre usuários de sistemas distintos, que não precisam ter que aprenter uma série de novos comandos apenas para trocar arquivos. Os comandos são enviados para o servidor no formato textual padrão (ASCII), normalmente na porta 21, no lado do servidor.

A finalidade da conexão de dados é efetuar a troca de dados, ou seja, enviar ou receber os arquivos especificados pelos comandos da conexão de controle.

Lembremos, novamente, que a arquitetura do protocolo FTP é do tipo servidor e, dessa forma, estamos sempre falando de um cliente FTP se conectando em um servidor. As conexões devem ser feitas em portas e, por termos duas conexões, são necessárias duas portas diferentes. No caso da conexão de dados, é comum a utilização da porta 20 do lado do servidor, mas isso pode mudar dependendo do modo de operação.

Vale destacar que um servidor é uma máquina dedicada para fornecer serviços para diversos clientes e, por isso, é comum a utilização de portas baixas. No cliente, o cenário é um pouco diferente, sendo que na maioria das vezes o processo da máquina do cliente é

executado por um usuário que não possui permissões administrativas. Nesse cenário, devem ser utilizadas as portas mais altas, normalmente superiores a 1023.

O protocolo FTP possui dois modos de operação: passivo e ativo. No modo ativo, o cliente deve informar ao servidor, além das informações usuais de qual arquivo deve ser transferido, um número correspondente à porta (na máquina que está executando o cliente) que vai ser utilizada para a transferência dos dados. Posteriormente, o servidor vai iniciar a transferência de dados e se conectar nessa porta. No lado do servidor, a porta é normalmente a número 20. O problema dessa abordagem é que, se existir um firewall entre o cliente e o servidor (uma situação frequente na atualidade), o servidor pode não ser capaz de conectar no cliente, pois é bastante comum um firewall estar configurado para bloquear conexões externas. Nesse caso, a transferência de arquivos torna-se impossível. Para contornar tal problema, foi criado um segundo modo de operação, o modo passivo.

Diferentemente do modo ativo, no modo passivo as duas conexões (a conexão de controle e a conexão de dados) são iniciadas pelo cliente. O programa cliente de FTP continua conectando-se na porta 21 para a conexão de controle, mas recebe do servidor a informação sobre qual porta será utilizada para a conexão de dados, que normalmente é uma porta elevada. O cliente conecta-se nessa outra porta e inicia a transferência de dados. Como ambas as conexões foram iniciadas pelo cliente, não existe o problema da conexão "reversa" vinda do servidor para o cliente, o que contorna o problema da configuração do firewall.

Ainda que o protocolo FTP possuísse originalmente alguma forma limitada de segurança (como a possibilidade da configuração de um usuário e uma senha para a conexão no servidor), muitos aspectos foram negligenciados. Por exemplo, no início (e, na realidade, por quase toda a vida do protocolo), o tráfego de informações era feito sem o uso de nenhuma forma de criptografia. Dessa maneira, é possível e relativamente fácil que um terceiro obtenha informações trocadas durante a comunicação entre o cliente e o servidor.

Com o tempo, algumas medidas de segurança foram sendo incorporadas ao protocolo FTP, o que melhorou as suas características e tornou-o um pouco mais seguro. Contudo, comparado a outros protocolos mais novos, cujos projetos já incorporam aspectos de segurança desde o seu início (como é o caso, por exemplo, do protocolo SSH File Transfer Protocol), o FTP é bastante inseguro.

Apesar dos problemas com relação à segurança, é notável como esse protocolo foi bastante utilizado ao longo de várias décadas e continua sendo utilizado, ainda que proporcionalmente muito menos do que foi no passado. Alguns dos motivos dessa durabilidade tão grande (o que é pouco usual na área de tecnologia) são a sua simplicidade e a sua ampla

disponibilidade nos mais diferentes tipos de máquinas. Há uma enorme quantidade de programas cliente e servidores executando nas mais diferentes plataformas de sistemas operacionais. Até mesmo dispositivos como impressoras e outros equipamentos embarcados já tiveram pequenos servidores de FTP instalados para permitir a troca de arquivos entre dispositivos distintos.

### 1.2. Handshake triplo

No momento em que duas máquinas se reconhecem, elas estão prontas para iniciar a comunicação. O nome desse início de comunicação é handshake. Quando três pacotes iniciais são trocados para estabelecer uma conexão, ocorre um handshake triplo.

## 2. Análise das afirmativas

I – Afirmativa incorreta.
JUSTIFICATIVA. O handshake triplo ainda é necessário, pois as máquinas precisam sincronizar os seus números de sequência.

II – Afirmativa correta.
JUSTIFICATIVA. O protocolo FTP padrão não apresenta nenhuma forma de segurança na transmissão de arquivos; ele prevê apenas um login com usuário e senha.

III – Afirmativa correta.
JUSTIFICATIVA. Duas conexões são sempre necessárias, contudo, existem dois modos de operação, passivo e ativo, que diferem no sentido de qual lado, servidor ou cliente, é iniciada a conexão de transferência de dados.

IV – Afirmativa incorreta.
JUSTIFICATIVA. O protocolo prevê a transferência no modo binário, ASCII e EBCDIC.

Alternativa correta: D.

## 3. Indicações bibliográficas


- FOROUZAN, A. B. *Comunicação de dados e redes de computadores*. São Paulo: McGraw-Hill, 2008.
- KOZIEROK, C. M. *The TCP/IP Guide v.3.0.* Tcpguide.com. 2005. Disponível em <http://www.tcpipguide.com/free/t_FTPOverviewHistoryandStandards.htm>. Acesso em 11 jul. 2025.
- RFC 114. BHUSHAN, A. *A File Transfer Protocol*. RFC 114, abr. 1971.
- TANENBAUM, A. S.; WHETHERALL, D. J. *Redes de computadores.* São Paulo: Pearson Prentice Hall, 2011.
- TORRES, G. *Redes de computadores.* Rio de Janeiro: Novaterra, 2013.

## Questões 2, 3 e 4

### Questão 2.[2]

Leia o texto a seguir.

*A solução de gerência padronizada mais usada no mundo chama-se Internet-Standard Network Management Framework. Essa solução é mais conhecida como Gerência SNMP (Simple Network Management Protocol). Esse modelo descreve não apenas o protocolo de gerenciamento, mas também um conjunto de regras que são usadas para definir as informações que podem ser utilizadas.*

Rose, T. M. *The Simple Book: An Introduction to Network Management*. 2. ed. Prentice-Hall, 1996 (com adaptações).

Em relação aos protocolos de gerenciamento de rede, avalie as afirmativas.

I. O SNMP atua na camada 7 do modelo OSI.

II. Apenas o SNMPv1 usa a noção de comunidades para estabelecer um grau de confiança entre os agentes e os gerentes, o SNMPv2 e o SNMPv3 utilizam um subsistema de segurança que fornece serviços de autenticação e privacidade baseados no usuário.

III. O SNMPv2 fornece gerenciamento de rede centralizado e distribuído incluindo aprimoramentos na sua estrutura e gerenciamento.

IV. O SNMPv3 foi criado para solucionar as questões de segurança das versões anteriores, fornecendo acesso seguro às informações de gerenciamento por meio de autenticação e criptografia de pacotes.

É correto apenas o que se afirma em

A. I e IV.

B. II e III.

C. II e IV.

D. I, II e III.

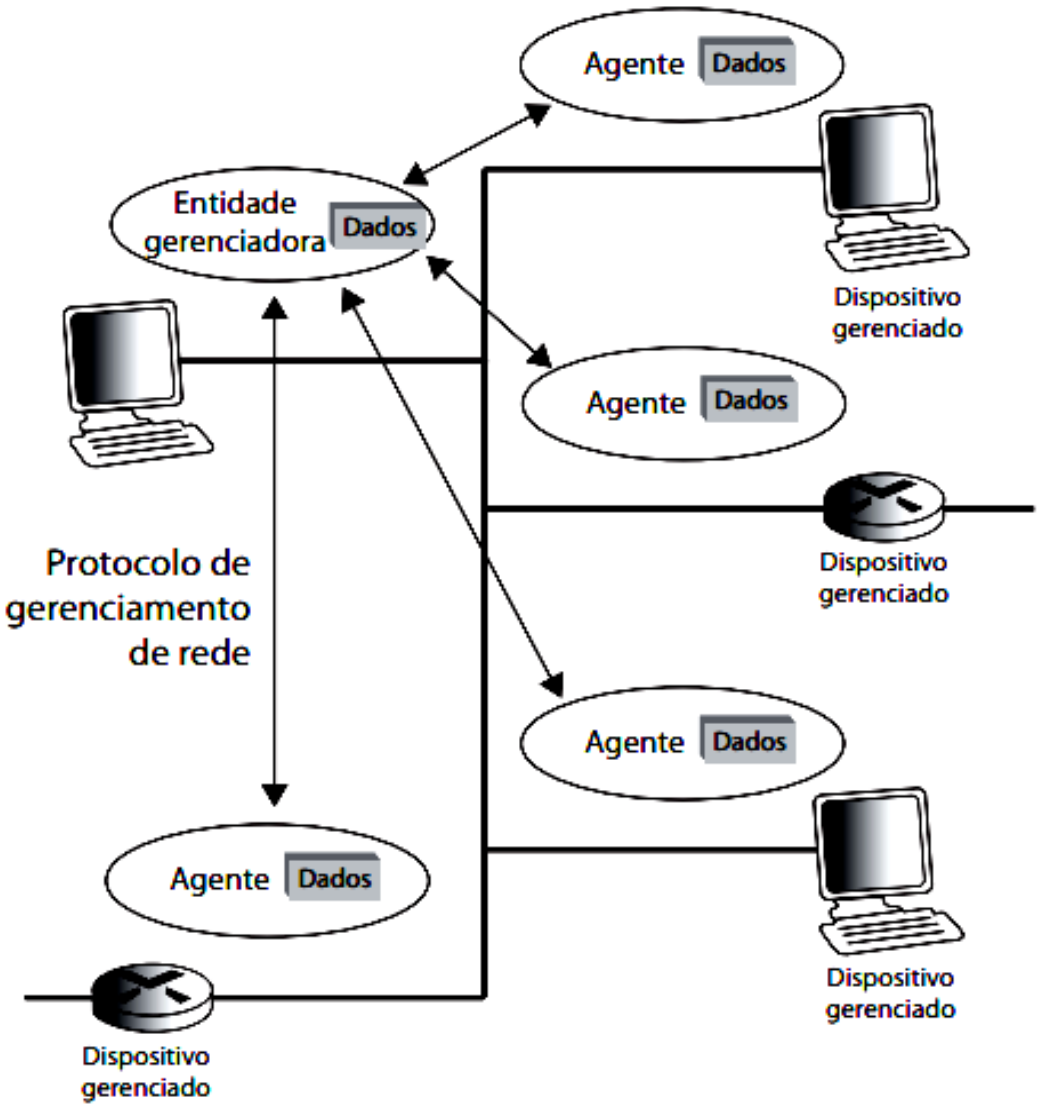
E. I, III e IV.

### Questão 3.[3]

O gerenciamento de redes inclui o fornecimento, integração e coordenação de hardware, software e elementos humanos para monitorar, testar, configurar, consultar, analisar e controlar a rede. Além disso, disponibiliza recursos para atender aos requisitos de desempenho, qualidade de serviço e operação em tempo real, dentro de um custo aceitável pela empresa. A figura a seguir ilustra um ambiente de Gerenciamento de Redes.

[2]Questão 19 – Enade 2014.

[3]Questão 22 – Enade 2014.




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).

Considerando a utilização do protocolo SNMP (Simple Network Management Protocol) no gerenciamento de redes, avalie as asserções e a relação proposta entre elas.

I. O SNMP é o protocolo mais usado para transmitir informações e comandos entre a entidade gerenciadora e os agentes que os executam em nome da entidade, dentro de um dispositivo de rede gerenciado.

PORQUE

II. Os agentes coletam informações por meio de objetos gerenciados que, juntos, formam um banco virtual de informações, conhecido como MIB (Management Information Base).

Acerca dessas asserções, assinale a opção correta.

A. As asserções I e II são proposições verdadeiras, e a asserção II justifica a I.

B. As asserções I e II são proposições verdadeiras, e a asserção II não justifica a I.

C. A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.

D. A asserção I é uma proposição falsa, e a II é uma proposição verdadeira.

E. As asserções I e II são proposições falsas.

**Questão 4.**[4]

A gestão de elementos de redes baseada na pilha de protocolos TCP/IP tem como seu principal protocolo de gerenciamento o SNMP (Simple Network Management Protocol). Acerca do protocolo SMTP, avalie as afirmativas a seguir.

I. É baseado numa estrutura de comunicação requisição/resposta, não suportando outro tipo de comunicação.

II. É implementado por diversas aplicações, como PING e TRACERT, nas quais o comando é emitido pelo dispositivo cliente.

III. Permite o monitoramento de elementos de rede, como roteadores e switches, podendo ser utilizado para servidores e estações de trabalho, desde que se tenha o suporte ao SNMP instalado.

IV. Gerencia elementos em qualquer rede IP alcançável e permite o encaminhamento de pacotes de uma rede para outra.

É correto apenas o que se afirma em

A. I. B. III. C. I e II. D. II e IV. E. III e IV.

## 1. Introdução teórica

### 1.1. Protocolo SNMP

Redes de computadores são ambientes complexos, em que dispositivos de diferentes tipos e com diferentes finalidades interagem. O papel do administrador de redes é gerenciar essa estrutura complexa, garantindo o seu bom funcionamento.

Com a finalidade de facilitar o gerenciamento de redes de computadores que utilizam o protocolo TCP/IP, foi criado o Protocolo de Gerenciamento de Redes Simples (SNMP). Não devemos confundir o protocolo SNMP com o protocolo SMTP (Simple Mail Transfer Protocol), desenvolvido com intenção distinta (transmissão de correio eletrônico).

[4]Questão 23 – Enade 2014.

O protocolo SNMP foi ciado para auxiliar no gerenciamento da rede, permitindo que sejam coletadas informações dos dispositivos nela conectados. Além da coleta das informações, o protocolo também possibilita o controle de equipamentos por meio do envio de comandos.

Do ponto de vista arquitetural, o protocolo SNMP é composto por gerentes e agentes. A estação gerenciadora (ou gerente) é normalmente uma máquina que o administrador utiliza para a monitoração e para o controle da rede, enquanto os agentes são os equipamentos gerenciados. Tipicamente, os agentes podem ser os diversos roteadores e switches, além de outros computadores.

É interessante observar que, na arquitetura do protocolo SNMP, ocorre uma espécie de "inversão de papéis": o gerente atua como um cliente dos agentes, que fornecem dados como um servidor. Cada agente apresenta um banco de dados com as informações de gerenciamento, chamado de MIB, ou Management Information Base, que vai fornecer informações para o seu gerenciamento.

Segundo Forouzan (2008), além do MIB, o protocolo SNMP também utiliza outro protocolo auxiliar, o SMI (Structure of Management Information), que

> *define as regras para o estabelecimento de nomes a objetos, estabelece tipos de objeto (inclusive abrangência e comprimento) e mostra como codificar objetos e valores.*

No entanto, no mesmo texto afirma-se que o MIB

> *cria um conjunto de objetos com nomes, tipos e relações entre si para uma entidade a ser gerenciada" (FOROUZAN, 2008).*

Dessa forma, podemos dizer que o SNMP utiliza os protocolos auxiliares MIB e SMI.

O protocolo UDP (User Datagram Protocolo) é utilizado para a comunicação entre o(s) gerente(s) e os agentes. A decisão de utilizar o protocolo UDP em vez do protocolo TCP (Transmission Control Protocol) é proposital: o monitoramento da rede deve ocorrer mesmo quando essa rede se encontra com problemas (especialmente nesses casos) e deve ter o menor custo de transmissão possível. Por não oferecer garantia de entrega, o protocolo UDP não impõe sobrecarga adicional à rede. O protocolo IP é utilizado para transmitir os pacotes SNMP ao seu destino.

O protocolo SNMP passou por diferentes versões, sendo que a sua versão inicial, denominada SNMPv1, foi definida na RFC 1157, em 1990. Essa primeira versão oferecia

poucos recursos de segurança. Versões posteriores (SNMPv2 e SNMPv3) adicionaram mais funcionalidades de segurança e novos recursos de gerenciamento.

## 1.2. Comandos PING e TRACERT

Os comandos PING e TRACERT são utilizados para o diagnóstico de problemas de rede na maioria dos sistemas operacionais.

O programa PING utiliza o protocolo ICPM (Internet Control Message Protocol) para enviar pacotes pela rede e mede o tempo de ida e volta desses pacotes, sendo útil para identificar o funcionamento básico da comunicação.

O programa TRACERT funciona de forma um pouco diferente, apresentando a rota seguida pelos pacotes e o tempo associado aos trechos dessa rota. Diferentes implementações podem utilizar o protocolo UDP ou ICMP, dependendo do sistema operacional utilizado.

## 1.3. Modelo OSI

A organização ISO (International Standartization Organization), em conjunto com outras entidades, criou o modelo OSI (Open System Interconnection) em parte como uma tentativa de padronizar os equipamentos e os protocolos de rede, em uma época em que era muito comum o uso de padrões proprietários (final da década de 1970). Contudo, por uma série de razões, algumas de natureza técnicas e outras de natureza comercial, o modelo OSI acabou sendo mais um referencial idealizado do que um padrão utilizado de forma prática.

Vale notar que a pilha de protocolos TCP/IP antecede o modelo OSI, sendo mais simples e tornando-se muito mais popular, o que pode ter contribuído para o uso mais teórico do modelo OSI.

A figura 1 apresenta, de forma sumária, a organização em 7 camadas definidas pelo modelo OSI.


**Figura 1.** Modelo OSI.
Disponível em <https://pplware.sapo.pt/tutoriais/networking/redes-sabe-o-que-e-o-modelo-osi/>. Acesso 31 mai. 2017 (com adaptações).

## 2. Análise das questões e das afirmativas

### Questão 2

I – Afirmativa correta.

JUSTIFICATIVA. O protocolo SNMP atua na camada de aplicação (camada 7) do modelo OSI, que é um modelo conceitual de um sistema de telecomunicações.

II – Afirmativa incorreta.

JUSTIFICATIVA. Apenas o SNMPv3 apresenta um subsistema sofisticado de segurança, adicionando elementos como autenticação forte e comunicação privada entre as entidades gerenciadas.

III e IV – Afirmativas corretas.
JUSTIFICATIVA. O SNMPv2 é uma evolução do SNMPv1, com a incorporação de algumas novas funcionalidades e melhorias de segurança do protocolo. Vale notar que mudanças de fato relevantes no aspecto da segurança foram apenas adicionadas na versão SNMPv3.
Alternativa correta: E.

**Questão 3**

Ambas as asserções (I e II) estão corretas, contudo, a asserção II não é a causa da asserção I. O MIB não é a justificativa da existência do SNMP; é apenas um recurso utilizado pelo MIB para armazenar as informações de gerenciamento.

Alternativa correta: B.

**Questão 4**

I – Afirmativa incorreta.
JUSTIFICATIVA. O protocolo SNMP permite que o agente envie também notificações para o gerente.

II – Afirmativa incorreta.
JUSTIFICATIVA. O protocolo SNMP é baseado em diversos outros protocolos, como os protocolos SMI, MIB, UDP e IP. O programa PING e o programa TRACERT não estão relacionados ao protocolo SNMP. Contudo, é possível obter informações similares aos resultados dos comandos PING e TRACERT pela utilização do protocolo SNMP (às vezes, chamado de "SNMP ping"). É importante ter em mente que o PING "tradicional" é baseado em outro protocolo, o protocolo ICMP (Internet Control Message Protocol), e não no protocolo SNMP.

III – Afirmativa correta.
JUSTIFICATIVA. O protocolo SNMP pode ser utilizado para monitorar diferentes tipos de equipamentos. Os agentes devem apresentar um programa que funcione como um servidor, acessado pelo gerente por meio da porta UDP.

IV – Afirmativa correta.

JUSTIFICATIVA. O protocolo funciona desde que o equipamento monitorado apresente suporte ao protocolo SNMP e que haja uma rede IP capaz de transportar os pacotes entre os agentes e o(s) gerente(s).

Alternativa correta: E.

## 3. Indicações bibliográficas


- FOROUZAN, A. B. *Comunicação de dados e redes de computadores*. São Paulo: McGraw-Hill, 2008.
- MAURO, D.; SCHMIDT, K. *Essential SNMP: help for system and network administrators.* 2. ed. Sebastopol: O´Reilly, 2005.
- TANENBAUM, A. S.; WHETHERALL, D. J. *Redes de computadores.* São Paulo: Pearson Prentice Hall, 2011.
- TORRES, G. *Redes de computadores.* Rio de Janeiro: Novaterra, 2013.

## Questão 5

**Questão 5.**[5]

Em um cenário de administração de Servidores de Redes, um administrador realiza a publicação de um site no servidor web com a funcionalidade de vhost (virtual host) no arquivo de configuração do sistema operacional. Em seguida, ele cria o diretório e armazena nesse local todo o conteúdo necessário para o correto funcionamento do site. Após essas ações, no entanto, o administrador percebe que o site não está funcionando, mesmo após o reinício do daemon do serviço do servidor web.

Considerando que o servidor de DNS (Domain Name System) está configurado corretamente, o procedimento pendente a ser realizado pelo administrador para o correto funcionamento do site é

A. habilitar a funcionalidade de DNS do vhost do site.
B. iniciar o daemon do serviço web em modo seguro.
C. verificar as permissões dos arquivos declarados no vhost.
D. habilitar a porta 80 para atender o vhost no arquivo de configuração.
E. adicionar a entrada NS no servidor de DNS apontando para o endereço do vhost do site.

# 1. Introdução teórica

## 1.1. Virtual hosting

Com a popularização da Internet, pequenas empresas e até mesmo indivíduos passaram a ter sites, visando à divulgação de produtos e de serviços ou visando ao divertimento e ao entretenimento. Isso levou a uma explosão no número de sites e nos serviços de hospedagem, especialmente os de baixo custo.

Inicialmente, um servidor web era tratado da mesma forma que servidores tradicionais: uma máquina (física) rodava um único servidor web, que hospedava um único site. Essa estratégia tem a vantagem de ser simples, mas é bastante cara, especialmente se o site em questão não tiver grande volume de tráfego. Para sites com poucos acessos, a dedicação exclusiva de uma máquina é um desperdício de poder computacional.

Uma possível abordagem para contornar esse problema é colocar vários sites em um mesmo domínio, separando os nomes dos sites na url, como, por exemplo,

[5]Questão 21 – Enade 2014.

<www.exemplo.com/site1> e <www.exemplo.com/site2>. Essa abordagem é pouco elegante e passa a impressão de que o site1 e o site2 fazem parte de uma mesma entidade, sendo que, na realidade, pode ser que sejam duas pessoas (ou empresas) completamente diferentes.

Uma segunda abordagem possível está em se configurar várias instâncias de um servidor web (como o Apache) funcionando em diferentes portas em uma mesma máquina física. Essa abordagem é um pouco melhor do que a anterior, mas ainda apresenta alguns problemas. Em primeiro lugar, a máquina tem de rodar duas instâncias completas e separadas de um servidor web ao mesmo tempo, o que implica grande custo computacional. Em segundo lugar, os diversos sites vão operar em portas diferentes da porta- padrão (a porta 80), algo que o cliente pode não querer que aconteça (por questões de simplicidade ou por questões técnicas).

Uma outra possível abordagem está em se utilizar diferentes endereços IPs em uma mesma máquina para cada site. O problema dessa abordagem é que o número de IPs de 32 bits é escasso e há demanda e custos bastante elevados. Assim, essa abordagem não é mais aconselhada.

Finalmente, uma abordagem bastante comum utilizada por diversos servidores web é a chamada Name-based Virtual Host. Nesse caso, uma mesma instância de um servidor web (por exemplo, o servidor Apache), em um mesmo computador e com apenas um endereço IP, é capaz de fornecer diversos sites diferentes. Nessa situação, o hostname contido no cabeçalho do protocolo HTTP é utilizado pelo servidor web para identificar qual é o site correto.

A principal vantagem da utilização do Name-based Virtual Host é a transparência para o cliente, o não desperdício de endereços IP e a otimização do processo de utilização do servidor. No entanto, deve-se ter em mente que se um site passar a ter grande volume de acessos, isso pode afetar a performance dos outros sites hospedados na mesma máquina e na mesma instância. Por essa razão, normalmente, os provedores desse tipo de serviço costumam impor limitações no tráfego e no acesso ao site e procuram compartilhar os custos de forma equilibrada.

## 1.2. DNS (Domain Name Server)

As máquinas presentes em uma rede que utiliza o protocolo TCP/IP devem ter, ao menos, um endereço numérico, chamado de endereço IP, para a sua identificação.

O protocolo IPv4 especifica que o endereço IP deve ter 32 bits, mas, devido à grande expansão da Internet após o final da década de 1990, esse tamanho tornou-se muito restritivo.

Então, foi criado o IPv6, que passou a ter 128 bits, o que aumentou consideravelmente a quantidade total de endereços disponíveis. Contudo, a implantação do IPv6 vem ocorrendo de forma gradual e ainda não está totalmente completa.

A ideia de duas máquinas comunicarem-se por meio de endereços IP é bastante conveniente para os computadores, mas não necessariamente para seres humanos. Por exemplo, para acessar o site da Unip <www.unip.br> pelo endereço IP (v4, de 32 bits), o número 200.196.224.129 deve ser digitado. Obviamente, navegar por sites utilizando números grandes é bastante inconveniente para a maioria dos usuários, sendo muito mais simples utilizar o nome <www.unip.br>. No entanto, as máquinas continuam utilizando o endereço IP para a comunicação. Logo, é necessário que exista alguma tecnologia para "traduzir" o nome do endereço (no caso <www.unip.br>) para o endereço IP, ou seja, o número 200.196.224.129.

O serviço de DNS (Domain Name Server) faz precisamente essa "tradução". Dessa forma, ao digitarmos a URL de um site no navegador, o servidor de DNS procura o endereço IP correspondente ao site <www.unip.br> e retorna essa informação para o computador cliente, que utiliza o endereço IP para a comunicação. Para o usuário, essa é uma operação transparente: ele apenas deve saber a URL do site <www.unip.br> e o computador vai automaticamente solicitar o endereço IP para o servidor de DNS.

## 2. Análise das alternativas

A – Alternativa incorreta.
JUSTIFICATIVA. O DNS (Domain Name Server) e o virtual host são duas tecnologias diferentes. O DNS não é configurado no vhost do site.

B – Alternativa incorreta.
JUSTIFICATIVA. O problema indicado no enunciado não está relacionado à forma de execução do processo em si, mas, provavelmente, ao fato de que o processo não está conseguindo acessar os arquivos do site.

C – Alternativa correta.
JUSTIFICATIVA. O servidor web não está sendo capaz de acessar algum arquivo do site por alguma das razões a seguir:

- existem problemas de permissões de acesso;

- algum arquivo necessário não foi criado, por esquecimento;
- há nome errado ou local errado de arquivo.

D – Alternativa incorreta.
JUSTIFICATIVA. Normalmente, a porta 80 é a porta padrão dos servidores web e é mantida aberta para programas como o Apache (que vão escutar, nessa porta, atendendo às requisições).

E – Alternativa incorreta.
JUSTIFICATIVA. O problema do enunciado não está em delegar parte do domínio para outros servidores DNS, mas sim em possibilitar que um mesmo IP forneça diversos sites diferentes.

## 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.
- FUNDAÇÃO APACHE. *Apache vrtual host documentation*, versão 2.2. Disponível em <http://httpd.apache.org/docs/2.2/vhosts/>. Acesso em 16 mar. 2017.
- TANENBAUM, A. S.; WHETHERALL, D. J. *Redes de computadores.* São Paulo: Pearson Prentice Hall, 2011.

## Questão 6

**Questão 6.**[6]

Leia o texto a seguir.

*A partir de agora, o Brasil possui uma legislação ampla, o Marco Civil da Internet, que estabelece não apenas a atuação do poder público e o intuito do uso da Internet no Brasil, como também indica, de forma expressa, obrigações e direitos, identifica termos técnicos, agentes, procedimentos relacionados ao uso e armazenamento de dados, assim como sanções em caso de infrações.*

Disponível em <http://www.administradores.com.br>. Acesso em 28 jul. 2014 (com adaptações).

Em relação ao Marco Civil da Internet, avalie as asserções e a relação proposta entre elas.

I. Os provedores de aplicação não podem retirar conteúdos disponibilizados por terceiros sem determinação judicial, exceto nos casos de nudez ou de atos sexuais de caráter privado.

PORQUE

II. De acordo com o Marco Civil da Internet, a fim de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações somente será responsabilizado por danos decorrentes de conteúdo com nudez ou atos sexuais de caráter privado se, após ordem judicial, ou da notificação em caso de material sexual, não tomar as medidas necessárias para tornar indisponível o conteúdo em questão.

A respeito dessas asserções, assinale a opção correta.

A. As asserções I e II são proposições verdadeiras, e a asserção II justifica a I.
B. As asserções I e II são proposições verdadeiras, e a asserção II não justifica a I.
C. A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.
D. A asserção I é uma proposição falsa, e a II é uma proposição verdadeira.
E. As asserções I e II são proposições falsas.

## 1. Introdução teórica

### Marco Civil da Internet

O artigo primeiro do Capítulo I da Lei Nº 12.965/2014 estabelece os princípios do Marco Civil da Internet, conforme segue.

> *Esta lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.*

[6]Questão 26 – Enade 2014.

No Capítulo III da mesma lei, na seção III, aborda-se a questão da responsabilidade por danos decorrentes de conteúdo gerado por terceiros, segundo trecho reproduzido abaixo.

> *Art. 21. O provedor de aplicações de Internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.*
> *Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.*
> *BRASIL. Lei Nº 12.965, de 23 de abril de 2014.*

## 2. Análise das asserções

I – Asserção verdadeira.

JUSTIFICATIVA. É importante que a lei estabeleça um limite entre a liberdade de expressão e a preservação da privacidade. Não se deve encarar a publicação de material de conteúdo sexual privado da mesma forma com que se encara a publicação de uma notícia ou de uma opinião política.

II – Asserção verdadeira.

JUSTIFICATIVA. É importante que o provedor também tenha limites e obrigações com relação ao material, para garantir a liberdade de expressão dos usuários e o funcionamento do Estado de Direito, cujo objetivo é o de garantir a todo cidadão o máximo de liberdade, limitado apenas pela certeza de que essa liberdade não infrinja nem coíba a liberdade de quaisquer outros cidadãos.

Relação entre as asserções. Conforme justificado acima, tanto a asserção I quanto a asserção II são proposições verdadeiras. Além disso, a segunda asserção justifica a primeira.

Alternativa correta: A.

## 3. Indicações bibliográficas


- BRASIL. *Lei Nº 12.965, de 23 de abril de 2014*. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 21 jan. 2025.
- DE JESUS, D.; MILAGRE, J. A. *Marco Civil da Internet – comentários à Lei Nº 12.965/14*. São Paulo: Saraiva, 2014.

## Questões 7 e 8

**Questão 7.**[7]

Virtualização não é uma tecnologia nova e está presente desde o tempo dos primeiros sistemas de grande porte. Recentemente, o termo tornou-se onipresente em infraestrutura de TI, representando qualquer tipo de método de ofuscação, em que um processo de TI é removido do seu ambiente operacional físico, tornando-se virtual. Por isso, a virtualização pode ser aplicada a quase todas as partes de uma infraestrutura de TI.

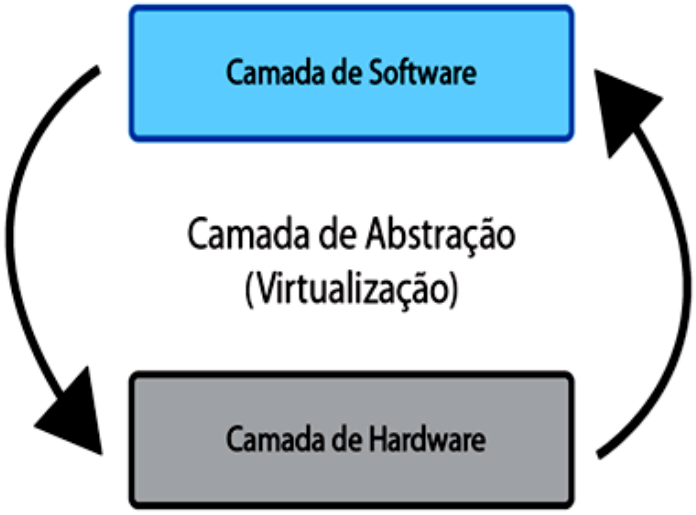
Sobre as diversas formas de virtualização de infraestrutura de TI é correto afirmar que

A. a virtualização de switches implica em um controle direto das interfaces de rede de um equipamento hospedeiro por suas máquinas virtuais.
B. as Redes Locais Virtuais (VLANs) não podem ser consideradas exemplos de virtualização de rede, pois não permitem independência no acesso à rede.
C. o uso de servidores de terminais, um exemplo de virtualização de desktops, torna complexa a entrega de novas estações de trabalho e sua respectiva administração.
D. a virtualização de armazenamento trata da técnica na qual os discos de dados são abstraídos do sistema operacional que os utiliza, não importando onde estejam fisicamente instalados.
E. os valores maiores de manutenção e um tempo maior de indisponibilidade são custos associados à virtualização de servidores, e são mais elevados quando comparados ao modelo de servidores físicos.

**Questão 8.**[8]

Quando o artigo *Time Sharing Processing in Large Fast Computers* foi publicado na Conferência Internacional de Processamento de Informação, realizada em Nova York, no ano de 1959, surgiu a ideia da virtualização. No trabalho apresentado, o foco era o uso da multiprogramação em tempo compartilhado, assim estabelecendo um novo conceito na utilização dos computadores de grande porte. A figura a seguir apresenta o posicionamento da camada de abstração (virtualização).

[7]Questão 27 – Enade 2014.
[8]Questão 28 – Enade 2014.




VERAS, M. *Virtualização de servidores*. Rio de Janeiro: RNP, 2011 (com adaptações).

Em relação aos conceitos e características de virtualização e o seu uso como tecnologia emergente atualmente nas empresas, avalie as afirmativas.

I. A virtualização pode ser utilizada para algumas finalidades, tais como: implementar a consolidação de servidores, reduzir custos, prover alta disponibilidade, implementar uma solução para recuperação de desastres e simplificar testes no desenvolvimento de softwares.

II. Os serviços de data centers oferecem segurança, economia e produtividade para empresas que precisam de infraestrutura atualizada para seus servidores. A virtualização é a tecnologia central de um data center.

III. A camada de virtualização de servidores mais conhecida é o Hipervisor ou Monitor de Máquina Virtual (Virtual Machine Monitor).

IV. São exemplos de tipos de virtualização: virtualização completa, paravirtualização e virtualização incompleta.

É correto apenas o que se afirma em

A. I e II.

B. II e IV.

C. III e IV.

D. I, II e III.

E. I, III e IV.

## 1. Introdução teórica

### Virtualização de servidores

Atualmente, computadores têm enorme capacidade de processamento. Essa capacidade é muito superior ao consumo típico de uma única aplicação. Além disso, as máquinas atuais dispõem de extraordinária capacidade de entrada e saída de dados. No processo de entrada e de saída de dados em uma máquina, é possível que ela fique ociosa por muito tempo. Isso significa que uma mesma máquina poderia ser utilizada para duas ou mais aplicações simultaneamente e, dessa forma, ela apresentaria uso mais eficiente.

Isso não é uma novidade no mundo da computação. Desde a década de 1970, sistemas multiusuários e multitarefas tornaram-se comuns, com o objetivo de aproveitar a capacidade de processamento das máquinas, porque tais sistemas operacionais ainda não tinham "virtualizado" a máquina, como é usual nas tecnologias atuais. Cada usuário utilizava o sistema de forma independente e os diversos recursos das máquinas (processamento, armazenamento e comunicação) eram compartilhados entre os usuários; somente o sistema operacional era único para todos os usuários do sistema. Em alguns sistemas pioneiros, podia existir uma forma rudimentar de máquina virtual.

Um dos grandes objetivos no desenvolvimento de um sistema operacional é o de isolar os processos em execução e o de isolar usuários entre si. Cada usuário deve ser capaz de utilizar o sistema e influenciar ao mínimo os demais usuários do sistema (a menos que isso seja desejado, como no caso de comunicação). Cada processo deve executar de forma independente dos demais (também se excetuando os casos em que há essa comunicação deliberada).

No caso limite, o objetivo passa a rodar mais de um sistema operacional em uma mesma máquina, ao mesmo tempo. E mais do que apenas abstrair somente o acesso ao hardware, passa-se a querer abstrair completamente o seu funcionamento e oferecer a possibilidade de simulação em um ou mais hardwares virtuais. Dessa forma, é possível criar "máquinas virtuais", definidas por software. Essa é a ideia básica da virtualização.

A virtualização oferece uma série de vantagens. As várias máquinas virtuais, rodando em uma máquina real, podem rodar diferentes sistemas operacionais. Elas têm configurações específicas para cada aplicação e podem levar a um processo de atualização e migração rápido e eficiente dos recursos de informática previamente instalados e/ou em uso em dada empresa.

Contudo, existe um custo computacional associado a esse tipo de solução, uma vez que uma série de operações que eram feitas por um hardware dedicado agora são feitas por uma camada de software.

Na figura 1, é possível ver o cenário convencional, com aplicações executando diretamente em um servidor. Os diversos aplicativos rodam no sistema operacional diretamente instalado na máquina real.

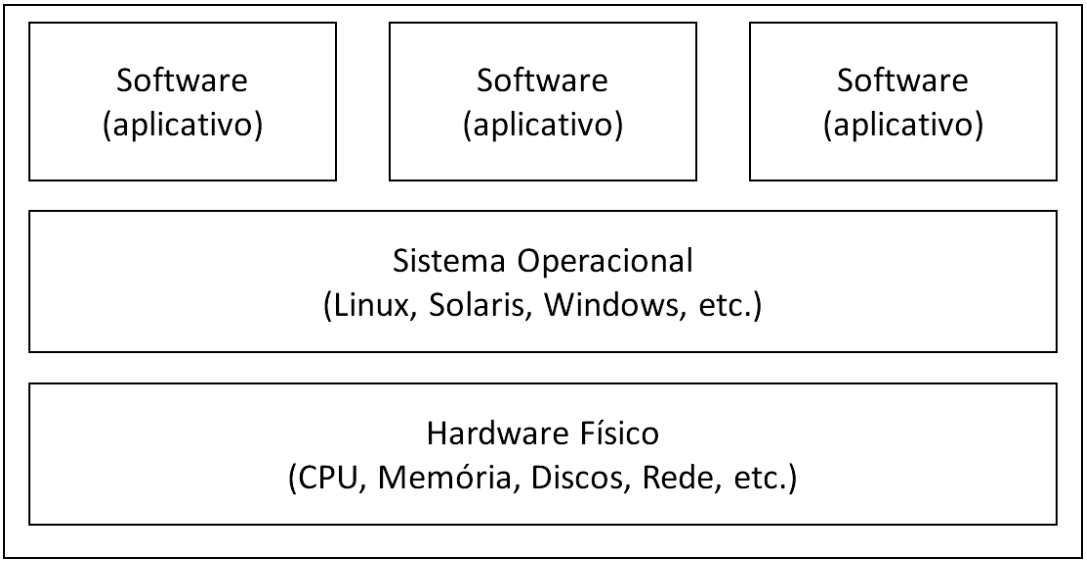



**Figura 1.** Arquitetura tradicional.
Adaptado de MARSHALL, REYNOLDS e MCCROY (2006).

Uma outra possibilidade é a ilustrada na figura 2.

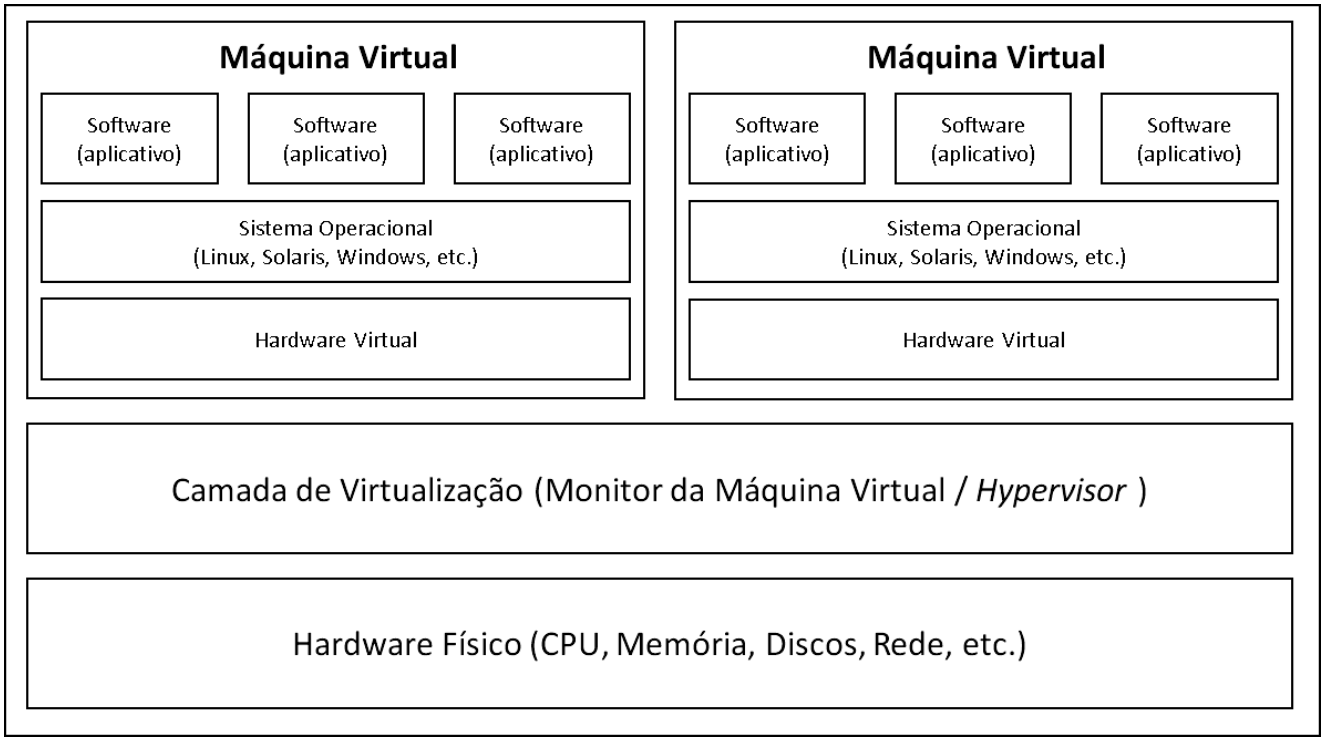



**Figura 2.** Um tipo de arquitetura virtualizada.
MARSHALL, REYNOLDS e MCCROY, 2006 (com adaptações).

No caso da figura 2, um conjunto de máquinas virtuais executa em um hardware real. Cada máquina virtual pode executar um sistema operacional diferente e ter um conjunto de configurações específicas. Além disso, cada aplicativo que executa dentro de cada uma das máquinas virtuais está completamente isolado dos aplicativos que rodam nas demais máquinas virtuais. A "máquina real" executa um hypervisor, uma espécie de sistema operacional mínimo, especialmente projetado para executar máquinas virtuais. Essa é a principal estrutura utilizada em servidores de empresas que vendem serviços de virtualização.

Finalmente, na figura 3, apresenta-se outra possibilidade: um sistema operacional que executa no hardware real e que tem instalado um software de virtualização (como alguns produtos para desktop da VMWare ou o VirtualBox da Oracle, entre outros). Esse software, por sua vez, "virtualiza" a máquina real e torna-a capaz de executar diversas máquinas virtuais, cada uma com um sistema operacional potencialmente diferente. Essa abordagem é bastante comum em desktops e workstations, em função da sua praticidade.

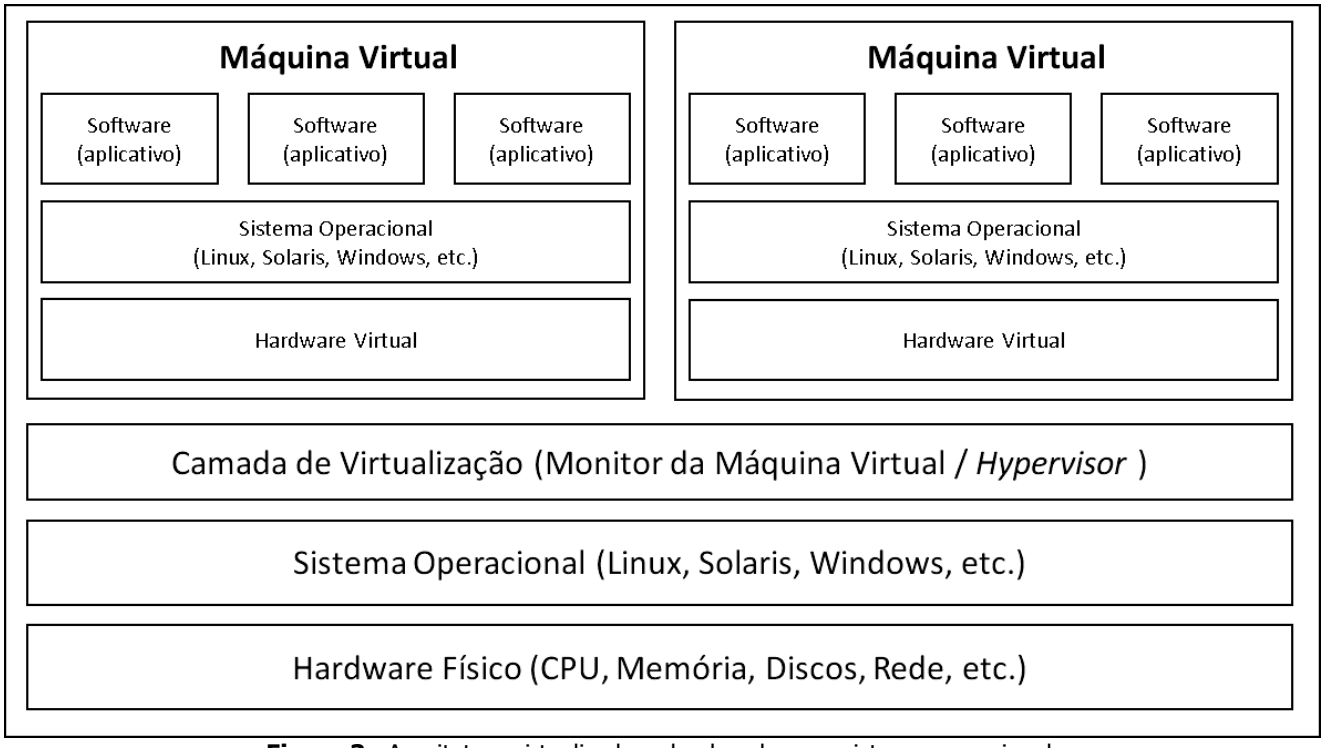



**Figura 3.** Arquitetura virtualizada rodando sobre um sistema operacional.
MARSHALL, REYNOLDS e MCCROY, 2006 (com adaptações).

A configuração da figura 3 impõe um custo computacional mais elevado do que o da configuração da figura 2, que tende a ser mais eficiente, e, por isso, é bastante utilizada em servidores.

## 2. Análise das alternativas e afirmativas

### Questão 7

A – Alternativa incorreta.
JUSTIFICATIVA. A camada de virtualização deve isolar o controle direto da placa de rede das máquinas virtuais.

B – Alternativa incorreta.
JUSTIFICATIVA. VLANs são exemplos de virtualização, pois criam uma estrutura de redes lógicas virtuais independentes e rodam em uma mesma rede física.

C – Alternativa incorreta.
JUSTIFICATIVA. O uso de servidores de terminais simplifica e barateia a entrega de novas estações de trabalho para os funcionários em uma empresa, uma vez que a TI pode inclusive entregar máquinas mais simples e baratas para os funcionários, enquanto os servidores de terminais centralizam a configuração mais complexa.

D – Alternativa correta.
JUSTIFICATIVA. A virtualização de armazenamento possibilita que o sistema operacional trabalhe com diferentes dispositivos em diferentes localizações de forma transparente.

E – Alternativa incorreta.
JUSTIFICATIVA. A virtualização de servidores tem justamente o papel de reduzir o custo de manutenção e diminuir o tempo de indisponibilidade, uma vez que várias máquinas virtuais rodam sob um mesmo servidor físico.

### Questão 8

I – Afirmativa correta.
JUSTIFICATIVA. A utilização de máquinas virtuais é perfeita para o processo de consolidação, pois as aplicações que rodam nas máquinas virtuais não reconhecem que se trata de uma máquina virtual, e não real. Isso significa que mesmo aplicações antigas que foram desenvolvidas pensando em uma máquina real podem ser virtualizadas. Além disso, máquinas

virtuais podem ser rapidamente movidas de um ambiente para outro, quando comparadas a outras máquinas reais.

II – Afirmativa correta.
JUSTIFICATIVA. A virtualização permite que um data center ofereça um serviço de qualidade a um preço mais acessível a uma grande quantidade de empresas, especialmente se avaliarmos o custo que essas empresas teriam se tivessem de construir um data center de qualidade comparável aos data centers comerciais.

III – Afirmativa correta.
JUSTIFICATIVA. Para grandes data centers que querem fornecer serviços de virtualização para elevado número de empresas, a tecnologia de hypervisor é a mais comum e adequada na atualidade.

IV – Afirmativa incorreta.
JUSTIFICATIVA. Se considerarmos como virtualização apenas a completa abstração do hardware e do sistema operacional da máquina virtual, não poderemos considerar a paravirtualização ou a virtualização incompleta como exemplos reais de virtualização.

Alternativa correta: D.

## 3. Indicação bibliográfica


- MARSHALL, D.; REYNOLDS, W. A.; MCCROY, D. *Advanced server virtualization: VMware and Microsoft Platforms in the virtual data center*. Boca Raton: Auerbach Publications, 2006.

## Questões 9 e 10

**Questão 9.**[9]

No mercado atual, é crescente a necessidade de preocupação com o uso racional de recursos naturais, descarte de lixo eletrônico, eficiência energética e outras temáticas ligadas ao conceito de sustentabilidade. As empresas de construção civil passaram a construir edifícios inteligentes que possuem melhor planejamento do consumo energético destinado a iluminação, elevadores, entre outros. No que se refere ao projeto de redes de dados nesses edifícios, não é diferente. Com o crescimento do conceito de TI Verde, torna-se essencial o uso de tecnologias que atendam essa nova necessidade. Uma delas envolve a consolidação de servidores (blades) de forma a reduzir o espaço físico nos racks de data centers, consequentemente reduzindo o consumo elétrico e o nível de calor produzido, o que implica diretamente na redução de consumo energético de aparelhos de ar condicionado e uma série de outros benefícios correlatos, além de possibilitar o gerenciamento centralizado, maior flexibilização de distribuição de recursos (CPU, memória e disco) e provisionamento de serviços.

Nesse sentido, o que fundamentalmente tem permitido essa consolidação de servidores e a redução do consumo energético é

A. a TI Verde.
B. a Virtualização.
C. a Governança de TI.
D. a Sustentabilidade Digital.
E. a BYOD ou Consumerização.

**Questão 10.**[10]

As empresas que utilizam as tecnologias da informação estão cada vez mais compromissadas com as questões de sustentabilidade e meio ambiente. As tecnologias convergentes visam, entre as diversas vantagens, a proporcionar economia nos custos, possibilitando às empresas praticarem um preço final competitivo, preservando o meio ambiente e mantendo o negócio sustentável.

Nesse contexto, avalie as asserções a seguir e a relação proposta entre elas.

[9]Questão 18 – Enade 2014.
[10]Questão 24 – Enade 2014.

I. A tecnologia de VoIP é utilizada para substituir redes telefônicas convencionais portando o tráfego de voz para as redes de dados e proporcionando economia nos custos de telefonia da empresa.

PORQUE

II. Sustentabilidade é a habilidade em manter alguma condição, ou seja, possibilitar que um processo exista e permaneça.

A respeito dessas asserções, assinale a opção correta.

A. As asserções I e II são proposições verdadeiras, e a asserção II justifica a I.
B. As asserções I e II são proposições verdadeiras, e a asserção II não justifica a I.
C. A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.
D. A asserção I é uma proposição falsa, e a II é uma proposição verdadeira.
E. As asserções I e II são falsas.

## 1. Introdução teórica

### Sustentabilidade e TI Verde

As empresas atuais necessitam manter uma imagem pública aceitável e positiva. A consciência ecológica da população tem crescido desde o final da década de 1980 e a maneira como a empresa aborda esse tema pode contribuir de forma positiva para essa imagem.

Os produtos e serviços relacionados à Tecnologia da Informação (TI) têm impacto ambiental significativo, especialmente no que tange ao consumo de energia elétrica, necessária tanto para manter o funcionamento dos servidores nos data centers quanto para prover a refrigeração das máquinas, sendo, portanto, um dos principais custos de manutenção.

Segundo a International Federation of Global & Green ICT (2007), Green-ICT é um conjunto de tecnologias que possibilita a conservação do ambiente e a mitigação crescente dos impactos das áreas de TI e de comunicação nas mudanças climáticas globais.

A questão da TI Verde relaciona-se a dois aspectos: se, por um lado, as empresas querem ter uma imagem positiva, por outro, elas querem reduzir seus custos de operação. Nesse sentido, ações de TI Verde são úteis, uma vez que podem implicar aumento de eficiência e redução do desperdício. Embora haja custos iniciais para a implantação de um sistema de TI Verde, ele gera benefícios à imagem da empresa, o que faz com que o investimento nesse setor seja uma tendência.

O movimento ecológico que ocorreu nas últimas décadas no mundo atingiu vários elementos das cadeias produtivas industriais. Por exemplo, estima-se que a indústria de tecnologia da informação e comunicação (Information and Communications Technology - ICT) seja responsável por 2 a 3% da pegada de carbono do mundo. Vale notar que os esforços que visem a efetivamente minimizar ou a até eliminar essa pegada (isso é, tornar a TI neutra em carbono) são iniciativas de sustentabilidade digital.

## 2. Análise das alternativas e das asserções

### Questão 9

A – Alternativa incorreta.
JUSTIFICATIVA. A TI Verde propõe a redução do consumo energético, mas não aborda a questão da consolidação de servidores.

B – Alternativa correta.
JUSTIFICATIVA. A virtualização é fundamental para permitir que um único servidor físico possa rodar vários servidores virtuais, o que elimina a necessidade de uso de muitas máquinas (processo de consolidação). Isso também pode auxiliar na redução do consumo energético, uma vez que há diminuição de máquinas físicas.

C – Alternativa incorreta.
JUSTIFICATIVA. A governança de TI está relacionada a aspectos gerenciais e não ocasiona, ao menos diretamente, a consolidação de servidores e a redução de consumo energético.

D – Alternativa incorreta.
JUSTIFICATIVA. A sustentabilidade digital é importante e ajuda a impulsionar a redução do consumo energético, mas ela não permitiu a consolidação de servidores.

E – Alternativa incorreta.
JUSTIFICATIVA. A utilização de dispositivos particulares de funcionários e alunos, como é o caso de empresas que adotam a filosofia BYOD (Bring Your Own Device), não está diretamente relacionada à redução do consumo energético ou à consolidação.

**Questão 10**

I – Asserção verdadeira.
JUSTIFICATIVA. A tecnologia VoIP pode reduzir bastante os custos com telefonia, especialmente se considerarmos soluções livres como o Asterisk, que permitem a configuração de um servidor VoIP em uma plataforma open-source.

II – Asserção verdadeira.
JUSTIFICATIVA. O termo sustentabilidade está ligado a uma condição que pode ser mantida por um período prolongado. A ideia oposta corresponde às situações em que um sistema, físico ou econômico, não pode se manter por tempo longo, tanto devido à ausência de recursos físicos, como combustíveis e água, quanto à escassez de recursos financeiros.

Embora ambas as duas asserções sejam verdadeiras, a II não justifica a I, pois essas proposições não apresentam relação de causalidade.

Alternativa correta: B.

# ÍNDICE REMISSIVO

| | |
|---|---|
| **Questão 1** | Protocolo FTP (File Transfer Protocol). Transmissão de arquivos. Handskake triplo. |
| **Questão 2** | Protocolo de Gerenciamento de Redes Simples (SNMP). Gerenciamento de redes. |
| **Questão 3** | Protocolo de Gerenciamento de Redes Simples (SNMP). Gerenciamento de redes. |
| **Questão 4** | Protocolo de Gerenciamento de Redes Simples (SNMP). Gerenciamento de redes. |
| **Questão 5** | Virtual hosting. DNS (Domain Name Server). |
| **Questão 6** | Legislação. Marco Civil da Internet. Cidadania. |
| **Questão 7** | Virtualização. Máquinas virtuais. TI Verde. |
| **Questão 8** | Virtualização. Máquinas virtuais. |
| **Questão 9** | Sustentabilidade. TI Verde. |
| **Questão 10** | Sustentabilidade. TI Verde. Tecnologias VoIP. |