Unidade 3 - Webaula 9 - Camada de Aplicação - Básica

Olá! Tudo bem?

Seja bem-vindo(a) à Webaula 9 de **Redes de Computadores.**

INTRODUÇÃO

- Introdução à Webaula 9

TÓPICO 1

- Serviço de Diretório
- Atividade de Passagem

TÓPICO 2

- Transferência de Arquivos
- Atividade de Passagem

TÓPICO 3

- Correio Eletrônico
- Atividade de Passagem

TÓPICO 4

Gerenciamento de Redes

Atividade de Passagem

RESUMO

Resumo da Webaula 9

REFERÊNCIAS

Referências

Créditos

Introdução à Webaula 9

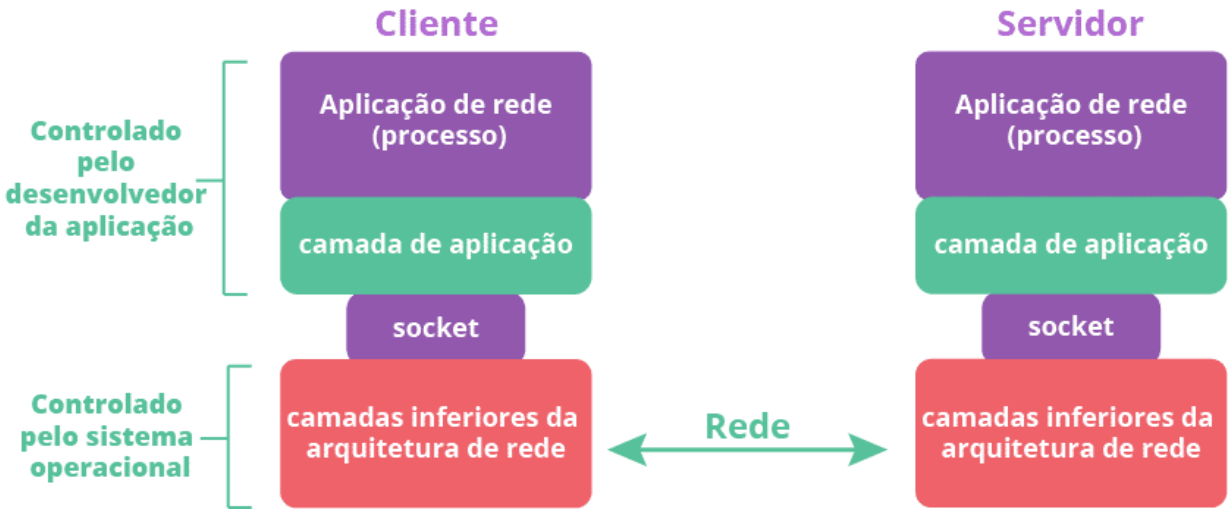
Olá!

Essencialmente, as aplicações de rede são a razão de ser das redes de computadores. É importante você perceber que as redes de computadores surgiram e continuam evoluindo para permitir que aplicativos de rede troquem dados entre si de forma cada vez mais eficiente. Aplicações de rede incluem desde as aplicações baseadas em texto, como o acesso remoto a computadores, correio eletrônico, transferência de arquivos, grupos de notícias, até as aplicações multimídia, como a navegação WWW (*World Wide Web*), telefonia IP, vídeo conferência e áudio e vídeo sob demanda.

Uma aplicação de rede é essencialmente distribuída entre um ou mais sistemas de computação. Em termos computacionais, a aplicação de rede é um processo sendo executado em um sistema operacional se comunicando com outro processo em outro sistema operacional usando um canal virtual chamado ***socket***, conforme estudamos na camada de transporte.

Processos em sistemas computacionais diferentes se comunicam através da troca de mensagens pela rede (Figura 1).

Figura 1 - Comunicação de Processos Entre Sistemas Computacionais



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

As aplicações de rede utilizam protocolos da camada de aplicação. Portanto, um protocolo da camada de aplicação é apenas uma parte das aplicações de rede. O protocolo da camada de aplicação define:

- os tipos de mensagens trocadas entre os processos;
- a sintaxe dos vários tipos de mensagens;
- a semântica (significado) dos vários campos das mensagens;
- as regras para determinar quando e como um processo envia ou responde mensagens.

A seguir serão abordados alguns tipos de aplicações de rede para internet consideradas as mais básicas: serviço de diretório, transferência de arquivos, correio eletrônico e gerenciamento de redes. Esses aplicativos de rede são importantes para que você compreenda como funcionam as funcionalidades mais básicas das redes de computadores.

CONTINUE

Serviço de Diretório

O **DNS** (*Domain Name System*), definido nas RFC 1034 e RFC 1035, é um esquema hierárquico de atribuição de nomes, baseado em domínios. Ele é principalmente usado para mapear nomes de equipamentos da internet em endereços IP. Observe que os equipamentos de rede são referenciados pelo seu endereço IP, mas nós memorizamos os nomes dos sites e não seus endereços.

Para mapear um nome de um equipamento da rede em um endereço IP, um programa aplicativo chama uma função de rede passando o nome do equipamento de destino como parâmetro. A função envia um pacote UDP para um servidor DNS, que procura o nome em sua base de dados e retorna o endereço IP encontrado para o aplicativo, o qual pode então estabelecer uma conexão com o equipamento de destino ou enviar pacotes UDP para ele.

A internet é dividida em centenas de domínios de primeiro nível, onde cada domínio cobre muitos equipamentos. Os domínios são particionados em subdomínios, que também são particionados, e assim sucessivamente (ALBITZ; LIU, 2001).

O órgão responsável por definir e controlar os domínios da internet é o **ICANN** (Internet Corporation for Assigned Names and Numbers – www.icann.org) através da **IANA** (Internet Assigned Numbers Authority – www.iana.org).

Os domínios de primeiro nível são divididos em dois tipos: genéricos (terminados com três ou mais letras) e de países (terminados com duas letras). Alguns dos domínios de primeiro nível genéricos (**GTLD** – *Generic Top Level Domain*) definidos pelo ICANN estão na Tabela 1.

Tabela 1 - Exemplos de Domínios de Primeiro Nível Genéricos

Terminação de Domínio Genérico	Descrição
.arpa	Infraestrutura técnica da internet
.com	Atividades comerciais
.edu	Instituições de ensino superior
.gov	Instituições governamentais (USA)
.int	Organizações governamentais
.org	Organizações não-governamentais
.xxx	Entretenimento adulto

Fonte: Elaborado pelo autor (2022).

Saiba Mais

Clique aqui e veja todos os domínios de primeiro nível genéricos.

O ICANN permite que se registrem novos domínios de primeiro nível (**New GTLD** – *New Generic Top Level Domain*) visando incrementar a inovação e as possibilidades comerciais de empresas no DNS. Alguns exemplos desses novos domínios, entre mais de 2000, estão na Tabela 2.

Tabela 2 - Exemplos de Novos Domínios de Primeiro Nível Genéricos

Terminação de Novo Domínio Genérico	Adquirente
.azure	Microsoft
.chrome	Google
.dhl	Deutsche Post
.hotels	Booking.com
.itau	Banco Itaú
.kindle	Amazon
.rio	Cidade do Rio de Janeiro
.space	Radix
.youtube	Google

Fonte: Elaborado pelo autor (2022).

Saiba Mais

Clique aqui e veja os novos domínios de primeiro nível genéricos.

Os domínios de primeiro nível de países (**CCTLD** – *Country Code Top Level Domain*) são definidos por duas letras ao final do nome de domínio e são administrados por órgãos gestores em cada um dos países. Alguns exemplos de domínios de países, entre mais de 300, estão na Tabela 3.

Tabela 3 - Exemplos de Domínios de Primeiro Nível de Países

Terminação de Domínio de País	País
.aq	Antártica
.br	Brasil
.ch	Suíça
.de	Alemanha
.jp	Japão
.tv	Arquipélago de Tuvalu
.us	Estados Unidos

Terminação de Domínio de País	País
.va	Cidade do Vaticano

Fonte: Elaborado pelo autor (2022).

Saiba Mais

Clique aqui e veja os domínios de primeiro nível de países.

Cada órgão gestor de domínios de país define a própria estrutura de nomes de domínio a partir do primeiro nível. No Brasil, o órgão responsável pela organização do domínio de país .br é o Comitê Gestor da Internet no Brasil – **CGI.br** (www.cgi.br).

No caso do **Comitê Gestor da Internet no Brasil**, através do **Núcleo de Informação e Coordenação** (www.nic.br), foram criadas categorias de nomes de domínios, cada qual com vários nomes de domínio de segundo nível. Alguns exemplos estão na Tabela 4.

Tabela 4 - Exemplos de Domínios de Segundo Nível do Brasil

Genéricos	
.com.br	Atividades comerciais
.emp.br	Pequenas e microempresas

Genéricos	
.net.br	Atividades comerciais

Pessoas Jurídicas	
.ind.br	Indústrias
.org.br	Entidades não governamentais
.srv.br	Empresas prestadoras de serviço

Profissionais Liberais	
.adv.br	Advogados
.eng.br	Engenheiros
.eti.br	Especialistas em tecnologia da informação

Cidades	
.curitiba.br	Curitiba - PR

Cidades	
.floripa.br	Florianópolis - SC
.sjc.br	São José dos Campos - SP

Fonte: Elaborado pelo autor (2022).

Saiba Mais

Clique aqui e veja as categorias de domínios de segundo nível do Brasil e clique aqui para ver a estatística do registro de cada um desses domínios brasileiros.

Cada domínio da internet tem seu nome definido pelo caminho ascendente entre ele e o nome de domínio de primeiro nível. Esses componentes do nome de domínio são separados por pontos. Por exemplo, um determinado *departamento* de uma *filial* de uma *empresa prestadora de serviços* do Brasil poderia ter seu nome de domínio dado pela nomenclatura hierárquica: *departamento.filial.empresa.srv.br.*

Para os nomes de domínio, não há distinção entre letras maiúsculas e minúsculas e é permitido o uso de vogais acentuadas e de cedilha. Porém um nome de domínio com estes caracteres especiais será equivalente ao nome com os correspondentes caracteres simples. Por exemplo, ao se registrar o nome de domínio *pão.açúcar.tur.br* será reservado o registro do nome de domínio *pao.acucar.tur.br* e eles serão equivalentes.

Na teoria, um único servidor de nomes poderia conter o banco de dados DNS inteiro, contendo todos os nomes de domínios, e responder a todas as consultas da internet. Além dos problemas inerentes ao excessivo tráfego que isto geraria, caso esse servidor viesse a ficar fora do ar, a internet inteira seria atingida.

Para contornar estas restrições, o DNS foi desenvolvido como sendo um grande banco de dados distribuído, onde os servidores locais de DNS passaram a conter apenas as informações de domínio dos equipamentos registradas localmente. Este processo é feito recursivamente e de forma hierárquica (KUROSE; ROSS, 2013).

YOUTUBE

Como funciona o DNS

Uploaded by FURBTUBE on 2022-12-14.

VISUALIZAR NO YOUTUBE >

Fonte: Elaboração própria (2022).

Arte/Diagramação: DME/FURB (2023).

Quando a função de rede para resolução de nomes tem uma consulta sobre um nome de domínio, ele a envia para um dos servidores de nomes locais. Se o domínio que estiver sendo procurado estiver sob a sua jurisdição de nomeação, será retornado o registro de recurso oficial.

Um **registro oficial** é aquele que é fornecido pela autoridade que gerencia o registro de nomeação e, portanto, está sempre correto. Os registros mantidos em cache, ao contrário dos registros oficiais, podem estar desatualizados. Se, no entanto, o domínio for remoto e localmente não houver informações disponíveis sobre ele, o servidor de nomes enviará uma mensagem de consulta para o servidor de nomes de primeiro nível respectivo fazendo perguntas sobre o domínio solicitado.

Dica

Utilizando a ferramenta gratuita da internet All-NetTools, procure obter o endereço IPv4 (A), IPv6 (AAAA) e de correio eletrônico (MX) de um nome de domínio que você conhece.

Com o objetivo de tornar o sistema de resolução de nomes mais seguro, reduzindo o risco de manipulação de dados e informações, criou-se o **DNSSEC** (*Domain Name Server Security Extensions*), definido na RFC 4033. Trata-se de um padrão que estende o protocolo DNS autenticando as informações trocadas pelo servidor de domínio, garantindo a integridade dos dados.

O DNSSEC soluciona alguns problemas encontrados na tecnologia DNS. Falsas informações DNS criam oportunidades para o roubo de informações ou a alteração de dados em transações eletrônicas. No protocolo DNS, um ataque em que a informação é corrompida torna-se extremamente difícil de ser detectado e, na prática, impossível de ser prevenido. O objetivo da extensão DNSSEC é validar os dados e garantir a origem das informações, impedindo este tipo de ataque.

CONTINUE

Atividade de Passagem

(ENADE) Uma empresa tem a sua sede em Natal e filiais em Brasília e Florianópolis. Em cada cidade, a empresa possui computadores que serão interligados. A seguir, encontram-se os requisitos que devem ser observados no projeto da rede.

Requisito A: em Natal, existem dois prédios. Para interligá-los, devem ser usados dispositivos que dividam o tráfego entre os prédios. Os dispositivos devem atuar na camada de enlace e a presença dos mesmos deve ser transparente às máquinas na rede.

Requisito B: em Brasília, há computadores em vários departamentos. Para interligar os departamentos, devem ser usados dispositivos que dividam o tráfego entre os departamentos e que possibilitem a comunicação simultânea entre esses departamentos.

Requisito C: as redes em Natal, Brasília e Florianópolis devem ser interligadas por dispositivos que dividam o tráfego e que possibilitem a interligação de redes com diferentes protocolos da camada física. Para decidir os destinos

dos dados, devem ser usados endereços de rede. Os dispositivos devem possibilitar que o tráfego seja filtrado.

Requisito D: a rede deve usar TCP/IP. O endereço da rede será da classe B privado e um dos bytes identificará o segmento da rede localizado em cada cidade. Em cada segmento, servidores distribuirão automaticamente os endereços IP entre as máquinas.

Requisito E: os nomes das máquinas serão traduzidos em endereços IP por servidores em cada cidade. Esses servidores estarão organizados em uma hierarquia. Cada servidor será responsável por um ou por vários subdomínios.

A seguir, encontram-se as decisões que foram tomadas para cada requisito. Indique quais das decisões que foram tomadas para cada requisito são corretas:

- [ ] usar hubs para atender ao requisito A
- [ ] usar switches para atender ao requisito B
- [ ] usar roteadores para atender ao requisito C
- [ ] usar o endereço de rede 164.41.0.0, a máscara 255.255.0.0 e servidores DHCP para atender ao requisito D

- [ ] configurar servidores Domain Name System (DNS) para atender ao requisito E

SUBMIT

CONTINUE

Transferência de Arquivos

O protocolo de aplicação utilizado especificamente para a transferência de arquivos entre sistemas computacionais é o **FTP** (*File Transfer Protocol*), definido na RFC 959.

O FTP usa duas conexões TCP em paralelo para transferência de arquivos (Figura 2):

(Clique nos cartões e acesse os conteúdos)

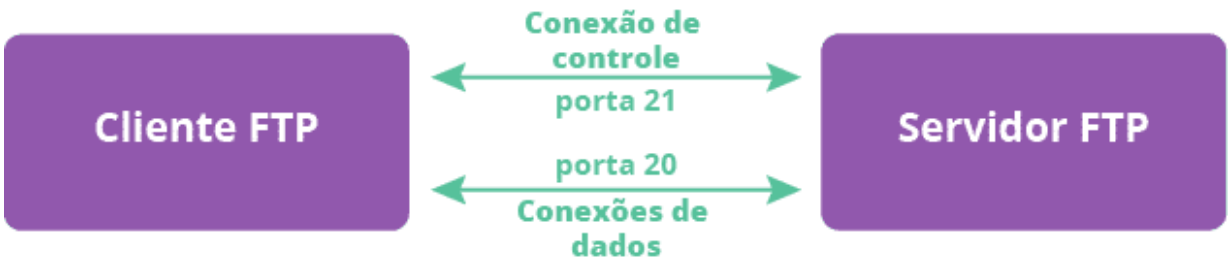
Conexão de Controle

Utilizada para enviar informações de controle entre os equipamentos, como identificação de usuário, senha de acesso, comandos para trocar de diretório e comandos para lidar com arquivos;

Utilizada para a transferência de

Conexão de Dados	arquivos, sendo que para cada arquivo a ser transferido é criada uma nova conexão de dados.

Figura 2 - Conexões TCP Utilizadas Pelo FTP



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

Quando um usuário inicia uma sessão FTP com um servidor remoto, o FTP primeiro cria uma conexão TCP de controle na porta 21 do servidor. Quando operando no **modo ativo**, sempre que o usuário na estação cliente pede pela transferência de um arquivo, o servidor FTP cria uma nova conexão TCP de dados a partir da porta 20 do servidor para uma porta indicada pelo cliente, envia ou recebe o arquivo e no final encerra a conexão. Para cada novo arquivo a ser transferido, uma nova conexão de dados é criada (KUROSE; ROSS, 2013).

Por outro lado, quando operando no **modo passivo**, sempre que o usuário na estação cliente pede pela transferência de um arquivo, o cliente FTP cria uma nova conexão TCP de dados para uma porta não bloqueada indicada pelo servidor, envia ou recebe o arquivo e no final encerra a conexão.

Os comandos do FTP, do cliente para o servidor, e as respostas, do servidor para o cliente, são enviadas pela conexão de controle em um formato texto legível.

O protocolo FTP foi o primeiro protocolo completo para permitir a transferência de arquivos entre equipamentos de rede. Apesar de ser eficiente, ele é bastante inseguro. Por isso, atualmente sugere-se que se use versões seguras desse protocolo chamadas FTPS (*File Transfer Protocol Secure*) definido na RFC 4217 ou SFTP (*Secure Shell File Transfer Protocol*) definido na RFC 4251, ou até mesmo se use outros mecanismos mais comuns para a transferência de arquivos, como o próprio HTTPS (*Hypertext Transfer Protocol Secure*).

CONTINUE

Atividade de Passagem

(ENADE) 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. Em relação ao protocolo FTP e a sua implementação, avalie as afirmações a seguir.

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 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:

- ◯ I.
- ◯ III.
- ◯ I e IV.
- ◯ II e III.
- ◯ II e IV.

SUBMIT

CONTINUE

Correio Eletrônico

O correio eletrônico é uma das aplicações mais importantes da internet, onde se podem enviar mensagens e lê-las quando for mais conveniente, sem ter que agendar um horário para se comunicar com outras pessoas.

Além da facilidade de criação e de envio, as mensagens eletrônicas permitem incluir referências a páginas internet, texto com formatação, imagens, som e até vídeo.

Um sistema de correio eletrônico (Figura 3) possui três componentes básicos (KUROSE; ROSS, 2013):

(Clique nas abas para acessar os conteúdos)

AGENTES DE USUÁRIO	SERVIDORES DE CORREIO ELETRÔN...	PROTOCOLOS

programas que oferecem um método baseado em comandos ou em interface gráfica e que permitem compor, receber e responder mensagens eletrônicas, bem como manipular caixas postais de correio eletrônico;

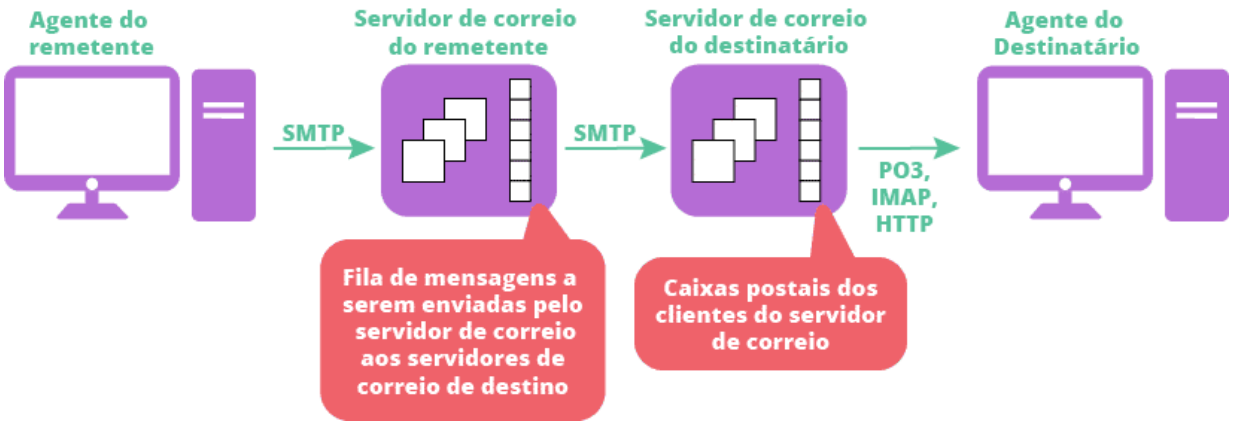
AGENTES DE USUÁRIO	SERVIDORES DE CORREIO ELETRÔN...	PROTOCOLOS

servidores que contêm as caixas postais dos seus usuários e encaminham as mensagens enviadas ao servidor de correio eletrônico dos destinatários de cada mensagem;

AGENTES DE USUÁRIO	SERVIDORES DE CORREIO ELETRÔN...	PROTOCOLOS

permitem a transferência confiável de mensagens até os servidores de correio eletrônico (SMTP - *Simple Mail Transfer Protocol*) e destes até os agentes de usuário (POP3 - *Post Office Protocol version 3*, IMAP - *Internet Mail Access Protocol*, HTTP - *Hypertext Transfer Protocol*).

Figura 3 - Funcionamento de um Sistema de Correio Eletrônico



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

1 Encaminhamento de Mensagens

Para o encaminhamento de mensagens foi criado o protocolo **SMTP** (*Simple Mail Transfer Protocol*), definido na RFC 2821, que transfere as mensagens eletrônicas desde o servidor de correio eletrônico do remetente até o servidor de correio eletrônico do destinatário.

O SMTP, um dos primeiros protocolos de aplicação que surgiram para a internet, só é capaz de transmitir mensagens que contêm caracteres ASCII de 7 bits. Como hoje se utiliza o código ASCII completo, além de dados binários de multimídia, é necessário codificar todas as mensagens para ASCII de 7 bits antes de transmitir a mensagem eletrônica através do protocolo SMTP e decodificá-la após o servidor de correio do destinatário recebê-la (KUROSE; ROSS, 2013).

Para que um servidor de correio eletrônico (cliente SMTP) envie uma mensagem da fila de mensagens para o servidor de correio eletrônico do destinatário (servidor SMTP), o primeiro cria uma conexão TCP com o segundo através da porta 25, eles trocam algumas mensagens de identificação indicando o endereço eletrônico do remetente e então se inicia o processo de envio de todas as mensagens para todos os destinatários do mesmo servidor de correio eletrônico de destino.

As mensagens eletrônicas consistem em um cabeçalho, uma linha em branco e o corpo da mensagem. Os principais campos de cabeçalho relacionados ao transporte de mensagens, definidos na RFC 822, estão na Tabela 5.

Tabela 5 - Principais Campos de Cabeçalho de Mensagens Eletrônicas

Cabeçalho	Significado

Cabeçalho	Significado
Bcc:	O(s) endereço(s) de correio eletrônico para cópias ocultas
Cc:	O(s) endereço(s) de correio eletrônico do(s) destinatário(s) secundário(s)
Date:	Data e hora local em que a mensagem foi criada
From:	O endereço de correio eletrônico que criou a mensagem
In-Reply-To:	O identificador da mensagem a que essa resposta será enviada
Message-id:	Identificador exclusivo da mensagem que pode ser utilizada posteriormente para referenciar esta mensagem eletrônica
Received:	A linha que é incluída por cada servidor de correio eletrônico durante o percurso até o destinatário
Reply-To:	O endereço eletrônico para onde as respostas devem ser enviadas
Sender:	O endereço de correio eletrônico do remetente
Subject:	Pequeno resumo da mensagem a ser apresentada em apenas uma linha (assunto da mensagem)
To:	O(s) endereço(s) de correio eletrônico do(s) destinatário(s)
Bcc:	O(s) endereço(s) de correio eletrônico para cópias ocultas

Cabeçalho	Significado
Cc:	O(s) endereço(s) de correio eletrônico do(s) destinatário(s) secundário(s)

Fonte: Elaboração própria (2022).

Para permitir a transferência de dados multimídia, criou-se uma extensão à estrutura do correio eletrônico denominada **MIME** (*Multipurpose Internet Mail Extensions*), definida na RFC 2045. A ideia básica do MIME é continuar a utilizar o mesmo formato das mensagens eletrônicas suportadas pelo SMTP, mas incluir uma estrutura no corpo da mensagem capaz de definir regras para mensagens não-ASCII.

No caso do correio eletrônico, para adicionar serviços criptográficos de segurança por meio do encapsulamento MIME de objetos cifrados e assinados digitalmente, utiliza-se o **S/MIME** (*Secure/Multipurpose Internet Mail Extensions*), descrito na RFC 2632.

O S/MIME oferece autenticação, integridade, sigilo e não repudiação, permitindo que todos os tipos de mensagens sejam protegidos. Foram criados novos cabeçalhos MIME para definir, por exemplo, o algoritmo de criptografia, o algoritmo de resumo de mensagem e a assinatura digital.

Reflita

Se assinar uma mensagem de correio eletrônico garante a integridade e a não repudiação de mensagens, por que é tão raro alguém utilizar este procedimento?

2 Consulta à Caixa Postal

Há duas formas básicas para acessar as mensagens de correio eletrônico armazenadas na caixa postal de um servidor de correio eletrônico: através de um agente de usuário (software de correio eletrônico) utilizando os protocolos POP3 (*Post Office Protocol version 3*) ou IMAP (*Internet Mail Access Protocol*); ou através de um navegador internet utilizando o protocolo HTTP (*Hypertext Transfer Protocol*).

O **POP3**, definido na RFC 1939, é um protocolo de acesso a caixas postais de servidores de correio eletrônico extremamente simples e, portanto, bastante limitado.

O POP3 é um protocolo utilizado para buscar as mensagens de um cliente de correio eletrônico no servidor que contém a sua caixa postal e movê-las para a estação cliente para que um agente de usuário possa visualizá-las e administrá-las apenas localmente (Figura 62). Este protocolo não provê nenhum meio para um usuário criar pastas no servidor e designar mensagens a estas pastas.

Figura 4 - Esquema de Funcionamento do POP3

Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

Como estas mensagens são armazenadas na estação do cliente, não é preciso manter uma conexão com o servidor de correio eletrônico durante a sua visualização e tratamento, mas, por outro lado, a

mobilidade do usuário entre diferentes estações clientes fica comprometida.

Quando um agente de usuário deseja obter as mensagens de correio eletrônico do servidor de correio eletrônico que contém a sua caixa postal através do POP3, ele faz uma conexão TCP utilizando a porta 110 com o servidor. Com a conexão TCP estabelecida, o POP3 passa por três fases:

(Clique nas abas para acessar os conteúdos)

AUTORIZAÇÃO | **TRANSAÇÃO** | **ATUALIZAÇÃO**

O usuário envia seu nome e senha para autenticação por parte do servidor (***user, pass***);

AUTORIZAÇÃO | **TRANSAÇÃO** | **ATUALIZAÇÃO**

O usuário pode obter estatísticas das mensagens presentes na sua caixa postal, recuperá-las e marcá-las para serem removidas (***stat, retr, dele***);

AUTORIZAÇÃO | **TRANSAÇÃO** | **ATUALIZAÇÃO**

É a conclusão da sessão POP3, quando o servidor remove as mensagens marcadas para remoção (***quit***).

O **IMAP**, definido na RFC 2060, é um protocolo de acesso a caixas postais de servidores de correio eletrônico muito mais elaborado que o POP3. Esse protocolo usa uma conexão TCP através da porta 143.

O IMAP permite que o usuário organize suas mensagens em pastas como é feito nos agentes de usuário, porém dentro do próprio servidor de caixa postal de correio eletrônico (sem mover as mensagens até a sua estação). Desta forma, o IMAP permite o acesso, através de um agente de usuário, ao conteúdo da sua caixa postal personalizada (com as pastas) de qualquer estação cliente desde qualquer ponto da internet (Figura 5).

Figura 5 - Esquema de Funcionamento do IMAP

Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

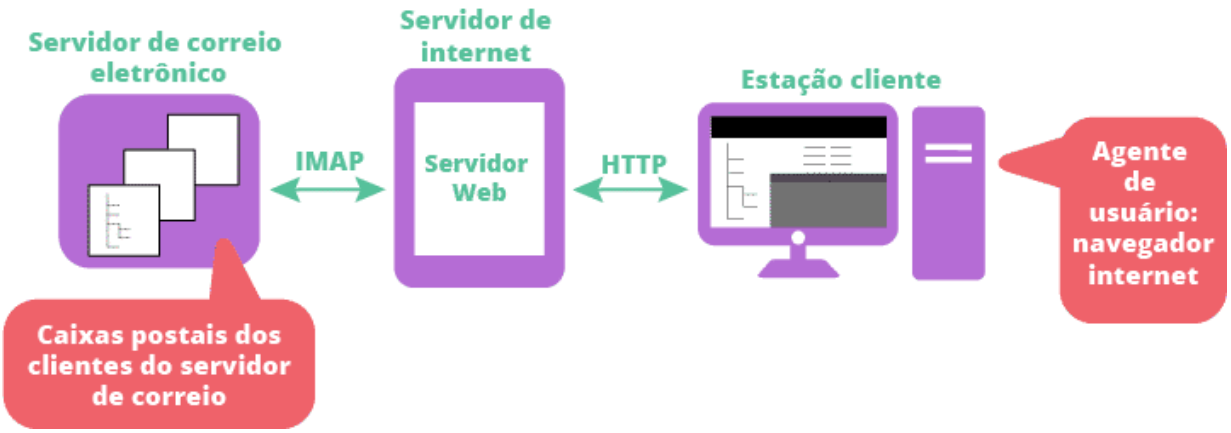
Outra possibilidade do IMAP é recuperar apenas partes de uma mensagem (seu cabeçalho, uma figura, um vídeo, etc.). Além disso, somente o conteúdo das mensagens que estiverem sendo visualizadas é

que é transferido até o agente do usuário. Essas características são úteis quando há uma conexão lenta entre o agente de usuário e o servidor de correio eletrônico.

Você já percebeu que cada vez menos se usa um software de gerenciamento de correio eletrônico? É que atualmente um número cada vez maior de usuários está acessando as suas mensagens de correio eletrônico através de um **navegador internet.** Neste caso, o agente de usuário é um navegador internet comum e o usuário se comunica com o servidor de correio eletrônico com sua caixa postal via **HTTP** (*Hypertext Transfer Protocol*).

Essa solução para o acesso ao correio eletrônico é extremamente conveniente quando o usuário está em trânsito, pois para enviar e receber mensagens basta que ele acesse um navegador internet a partir de um telefone móvel ou um computador (Figura 6).

Figura 6 - Funcionamento do Correio Via Navegador Internet



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

Nesta forma de acesso, como ocorre com o IMAP, o usuário pode organizar suas mensagens em pastas no servidor de correio eletrônico. Na verdade, muitas implementações de acesso à caixa postal de

correio eletrônico por um navegador internet utilizam um servidor IMAP para prover a funcionalidade de organização das mensagens em pastas, ou seja, o acesso às pastas e às mensagens é provido por scripts que rodam em um servidor HTTP e usam o IMAP para se comunicar com o servidor de correio eletrônico.

CONTINUE

Atividade de Passagem

(ENADE) Considere que a rede de uma empresa usará os protocolos TCP/IP para facilitar o acesso do público às informações dessa empresa a partir de máquinas conectadas à Internet. Considere ainda que, ao serem descritos os protocolos que serão usados na rede, alguns erros foram cometidos. Indique quais das descrições são verdadeiras:

- [ ] o Internet Protocol (IP) provê serviço não-orientado a conexão, e garante a entrega dos datagramas enviados. Além de garantir a entrega dos datagramas enviados, outra importante responsabilidade do IP é rotear os datagramas por meio de redes interligadas. O roteamento é feito usando-se endereços IP

- [ ] o Internet Control Message Protocol (ICMP) possibilita que mensagens de erro e de controle sejam trocadas entre máquinas. As mensagens ICMP são transferidas como dados em datagramas do IP

- [ ] o Transmission Control Protocol (TCP) provê um serviço orientado a conexão. Os dados são transferidos por meio de uma conexão em unidades conhecidas como segmentos. O TCP espera que a recepção dos segmentos transmitidos seja confirmada pelo destino e

retransmite segmentos cuja recepção não seja confirmada

- [ ] o User Datagram Protocol (UDP) provê um mecanismo para que aplicações possam comunicar-se usando datagramas. O UDP provê um protocolo de transporte orientado a conexão e não garante a entrega dos datagramas

- [ ] a emulação de terminal usará o protocolo TELNET, e a transferência de arquivos, o File Transfer Protocol (FTP). O correio eletrônico será provido pelo Simple Mail Transfer Protocol (SMTP) e as mensagens armazenadas nos servidores de correio eletrônico serão visualizadas nas máquinas dos usuários via Internet Mail Access Protocol (IMAP)

SUBMIT

CONTINUE

Gerenciamento de Redes

Observe a sua volta e perceba que as redes de computadores, tanto as públicas quanto as privadas, estão crescendo muito e cada vez se integrando mais, convergindo para uma enorme infraestrutura global. Como consequência deste crescimento, a possibilidade de gerenciar sistematicamente uma grande quantidade de sistemas de hardware e de software, componentes constituintes destas redes, tem tido cada vez mais importância.

Além de imprescindível, o segmento de sistemas de gerência de redes está evoluindo continuamente em função da disponibilidade de novas opções de tecnologias, as quais podem ser utilizadas tanto pelos provedores de serviços quanto pelas empresas de implementação de sistemas integrados de gerência (TANENBAUM; WETHERALL, 2011).

O ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) dividiu o gerenciamento de redes em áreas funcionais de gerenciamento permitindo desta forma identificar diferentes atividades características da gerência. Foram definidas cinco áreas funcionais básicas:

(Clique no + e acesse os conteúdos)

Gerência de Falhas

Permite a detecção, isolamento e correção de anomalias da rede e de seus equipamentos;

Gerência de Configuração

Permite o controle, a identificação e a coleta de dados de equipamentos e de conexões entre eles, assim como o planejamento, a instalação e a configuração dos equipamentos da rede de forma a garantir os serviços requeridos pelos seus clientes;

Gerência de Contabilização

Habilita o uso dos serviços da rede para medição e determinação de custos, provendo facilidades de definição de parâmetros de bilhetagem e de coleta de registros de cobrança do uso de uma rede;

Gerência de Desempenho

Permite a geração e a avaliação de relatórios de dados coletados de uma rede, com o objetivo de medir, analisar e controlar o seu desempenho, de acordo com requisitos de qualidade de serviço requeridos pelos usuários da rede e de seus equipamentos;

Gerência de Segurança

Permite prevenir e detectar o uso impróprio ou não autorizado de recursos de uma rede, assim como administrar a sua segurança.

O mundo ideal proposto pelas arquiteturas de gerenciamento de rede, em que todos os sistemas de uma planta heterogênea poderiam ser gerenciados de forma integrada, utilizando modelos de

informação padrões e abertos, não é necessariamente a realidade atual do mercado. Entre os motivos pelos quais isto ocorre, pode-se destacar (TANENBAUM; WETHERALL, 2011):

- o desinteresse por parte de fabricantes de equipamentos de transmissão de dados por razões de competitividade de mercado;
- a complexidade dos modelos de informação (MIB – *Management Information Base*), baseados em ASN.1 (*Abstract Syntax Notation One*);
- a impossibilidade de suportar modelos de informação de equipamentos e de serviços de forma dinâmica e incremental.

A incompatibilidade entre sistemas de gerência não é necessariamente consequência da utilização de diferentes protocolos, mas sim consequência da utilização de diferentes modelos de informação por parte das aplicações de gerenciamento destes sistemas, inviabilizando, portanto, a integração entre os de diferentes fornecedores. Ou seja, a implementação de um sistema padrão de gerência implica necessariamente na implementação de um modelo de informação bem especificado, padrão e disponível no mercado.

De uma maneira geral, a manutenção e as atualizações de aplicações de gerência são muito difíceis e caras de serem incorporadas no ambiente de gerenciamento de redes baseado na tecnologia atualmente consagrada para o modelo de referência TCP/IP, o **SNMP** (*Simple Network Management Protocol*), porque a sua natureza estática requer que todos os recursos e sistemas a serem gerenciados sejam previamente conhecidos pelos grupos de desenvolvimento dos sistemas de gerência de redes (MENDES, 2010).

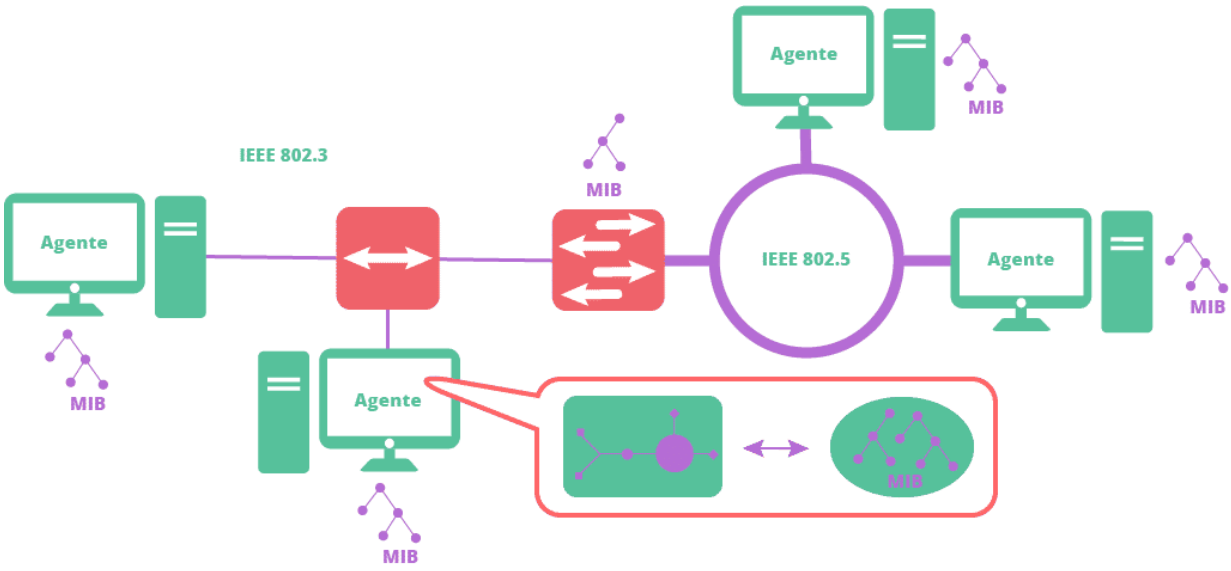
1 SNMP

A infraestrutura de gerenciamento especificada pela ISO para o modelo de referência OSI baseia-se em **informações de gerência** de recursos de rede modeladas como atributos de **objetos gerenciados**.

As informações de gerência de uma rede, assim como as regras pelas quais esta informação é apresentada e gerenciada, é referenciada como sendo a base de informações de gerência (**MIB** – *Management Information Base*).

Aplicações que gerenciam estas informações são denominadas **entidades de gerenciamento**. Uma entidade de gerenciamento pode assumir um dos seguintes dois papéis (Figura 7): **gerente** ou **agente**. Gerentes e agentes enviam e recebem requisições e notificações usando um **protocolo de gerência.**

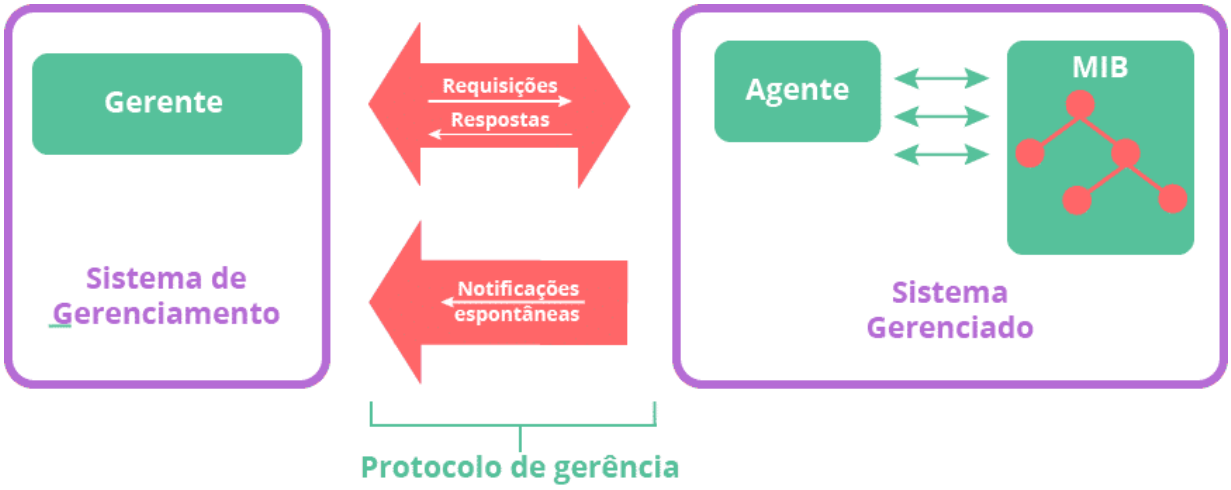
Figura 7 - Entidades de Gerenciamento



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

Uma aplicação de gerência no papel de gerente faz requisições de operações e recebe notificações, enquanto que no papel de agente processa operações, envia respostas e emite espontaneamente notificações. Estas formas de troca de informações entre as entidades de gerenciamento estão representadas na Figura 8.

Figura 8 - Comunicação Entre Entidades de Gerenciamento



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

A infraestrutura de gerenciamento especificada pela ISO foi utilizada para especificar o ambiente de gerência do modelo TCP/IP. Em 1990, com a publicação das RFC 1155 e RFC 1157 pelo IETF, definiu-se o protocolo de gerência SNMP (*Simple Network Management Protocol*), que foi aprimorado pelas RFC 1441 e RFC 1452 definindo o SNMPv2. Em 1999, a RFC 2570 definiu o SNMPv3, que incluiu funcionalidades de configuração remota e suporte a mecanismos de segurança (criptografia, autenticação e controle de acesso).

Para descrever e especificar as informações armazenadas em uma MIB SNMP adota-se uma abordagem orientada a objetos. O SNMP usa o **SMI** (*Structure of Management Information*), escrito

utilizando a notação **ASN.1** *(Abstract Syntax Notation One*), para definir tanto as classes quanto as sintaxes utilizadas pela MIB.

O SNMP é um protocolo sem conexão (usa o protocolo UDP para transporte). O modo como o SNMP é normalmente utilizado é aquele em que a estação de gerenciamento envia uma solicitação a um agente solicitando informações a ele ou forçando-o a atualizar seu estado de alguma forma. Em geral, o agente simplesmente responde com as informações solicitadas ou confirma que atualizou seu estado da forma solicitada. Os dados são enviados com base na sintaxe de transferência ASN.1 e de acordo com o formato especificado na MIB.

O SNMP define seis mensagens que podem ser usadas na comunicação entre as aplicações agente e a aplicação gerente, conforme apresentadas na Tabela 6.

Tabela 6 - Mensagens Entre Aplicações Gerente e Agente

Mensagem	Descrição
Get-request	Solicita o valor de uma ou de mais variáveis
Get-next-request	Solicita a variável seguinte à variável previamente solicitada
Get-bulk-request	Solicita uma tabela longa de dados
Set-request	Solicita a atualização de uma ou mais variáveis
Inform-request	Envio de mensagens entre aplicações gerente
SnmpV2-trap	Notificação espontânea enviada por uma aplicação agente

Fonte: Elaboração própria (2022).

2 MIB

Um objeto gerenciável é uma visão conceitual de um recurso que necessita ser monitorado e controlado para evitar falhas e degradação de desempenho em uma rede (TANENBAUM; WETHERALL, 2011).

Os objetos gerenciáveis com mesmas propriedades são instâncias de uma classe de objetos. A MIB é um repositório conceitual de instâncias de objetos gerenciáveis. Uma classe de objeto gerenciável é definida pelos:

Atributos

São elementos de dados e valores que caracterizam uma classe de objetos gerenciáveis;

Operações de gerência

São as operações que podem ser aplicadas às instâncias de objetos gerenciáveis;

Comportamento

É o que é apresentado por uma instância de objeto gerenciável baseado no recurso que ele representa;

são elementos de dados e valores que caracterizam uma classe de objetos gerenciáveis;

São as mensagens que instâncias de objetos gerenciáveis podem emitir espontaneamente.

A **MIB** (*Management Information Base*), ou modelo de informação de gerência, é o conjunto dos objetos gerenciados, que procura abranger todas as informações necessárias para a gerência da rede, possibilitando assim a automatização de grande parte das tarefas de gerência.

Na MIB, os objetos gerenciáveis são definidos através de uma hierarquia de registro, através da qual eles são identificados de uma maneira universal. Esta hierarquia é especificada segundo regras estabelecidas pela notação ASN.1 (Abstract Syntax Notation One), onde cada objeto é identificado por uma sequência de números, correspondente aos nós percorridos desde a raiz até o objeto em questão.

CONTINUE

Atividade de Passagem

(ENADE) Os aspectos funcionais para o gerenciamento de redes foram organizados pela ISO (International Organization for Standardization) em cinco áreas principais, compondo um modelo denominado FCAPS (acrônimo formado pelas iniciais em inglês de cada área funcional: Fault, Configuration, Accounting, Performance e Security). Considerando o modelo FCAPS, analise as afirmações que se seguem.

I. Na gerência de segurança são abordados aspectos relacionados ao acesso à rede e ao uso incorreto por parte de seus usuários.

II. A gerência de desempenho aborda a responsabilidade pela medição e disponibilização das informações sobre aspectos de desempenho dos serviços de rede. Esses dados são utilizados para a análise de tendências e para garantir que a rede opere em conformidade com a qualidade de serviço acordado com os usuários.

III. A gerência de contabilidade tem como objetivo permitir que o administrador de rede saiba quais dispositivos fazem parte da rede administrada e quais são suas configurações de hardware e software.

IV. Com a gerência de configuração, o administrador da rede especifica, registra e controla o acesso de usuários e dispositivos aos recursos da rede,

permitindo quotas de utilização, cobrança por utilização e alocação de acesso privilegiado a recursos.

V. O objetivo da gerência de falhas é registrar, detectar e reagir às condições de falha da rede.

É correto apenas o que se afirma em:

- I, II e V.
- I, III e IV.
- I, IV e V.
- II, III e IV.
- II, III e V.

SUBMIT

(ENADE) No projeto de uma rede de computadores, o gerente do sistema deve ser capaz de depurar problemas, controlar o roteamento e localizar

dispositivos que apresentam comportamento fora da especificação. Uma das ferramentas utilizadas para suportar essas ações é o protocolo de gerência de redes. Considerando a utilização do protocolo SNMP (Simple Network Management Protocol), versão 3, avalie as afirmações que se seguem.

I. A MIB (Management Information Base) padrão (mib-II) contém informações que permitem à aplicação gerente recuperar a tabela de rotas de um dispositivo IP, possibilitando a descoberta de erros de roteamento.

II. Para a investigação de defeitos em uma rede, através do SNMP, é necessário que todos os dispositivos gerenciados sejam desligados para iniciar seus contadores. Depois, esses dispositivos devem ser ligados simultaneamente.

III. Qualquer dispositivo gerenciado via SNMP pode fornecer dados sobre erros e tráfego de suas interfaces, permitindo o acompanhamento de problemas e o monitoramento de desempenho das mesmas.

IV. A MIB (Management Information Base) padrão (mib-II) possui entradas para a ativação de procedimentos de teste, tais como a medição do tempo de resposta de uma aplicação Cliente/Servidor.

- ◯ I.
- ◯ II.

- ◯ I e III.
- ◯ II e IV.
- ◯ III e IV.

SUBMIT

(ENADE) 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. Em relação aos protocolos de gerenciamento de rede, avalie as afirmações a seguir.

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 baseado 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:

- ◯ I e IV.
- ◯ II e III.
- ◯ II e IV.
- ◯ I, II e III.
- ◯ I, III e IV.

SUBMIT

(ENADE) 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 SNMP, avalie as afirmações 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:

- ◯ I.
- ◯ III.
- ◯ I e II.
- ◯ II e IV.

III e IV.

SUBMIT

CONTINUE

Resumo da Webaula 9

Como você viu nessa aula, uma das importantes aplicações que garante a funcionalidade da internet é o DNS. Através dele é que temos a organização dos nomes de domínio utilizados para referenciarmos os servidores espalhados ao redor do mundo, nomes estes geridos tanto de forma global quanto de forma local em cada um dos países.

Além dessa importante funcionalidade, apresentamos outros três tipos de aplicações disponíveis desde a criação da internet: a transmissão de arquivos, o correio eletrônico e o gerenciamento de rede.

Na próxima aula vocês conhecerá as duas aplicações suplementares e que hoje são as mais utilizadas na rede internet.

CONTINUE

Referências

O estudo das camadas do modelo de referência TCP/IP abordadas nesta parte do livro pode ser encontrado em:

ALBITZ, Paulo; LIU, Cricket. **DNS e BIND**. 4 ed. Rio de Janeiro: Editora Campus, 2001.

KUROSE, James F; ROSS, Keith W. **Redes de computadores e a internet**: uma abordagem top-down. 6 ed. São Paulo: Pearson Education do Brasil, 2013.

MENDES, Douglas R. **Redes de Computadores**: teoria e prática. São Paulo: Novatec, 2010.

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de computadores.** 5 ed. São Paulo: Pearson Prentice Hall, 2011.

As normas referenciadas nessa aula podem ser obtidas diretamente da página da internet dos respectivos organismos de padronização:

- **IANA:** www.iana.org
- **ICANN:** www.icann.org
- **IETF:** www.rfc-editor.org/rfc-index.html
- **ISO:** www.iso.org/standards-catalogue/browse-by-ics.html

- **ITU-T:** www.itu.int/pub/T-REC
- **W3C:** www.w3.org/standards

CONTINUE

Créditos

Reitora

Profª. Ma. Marcia Cristina Sardá Espindola

Vice-Reitor

Prof. Dr. Marcus Vinicius Marques de Moraes

Pró-Reitor de Ensino de Graduação, Ensino Médio e Profissionalizante

Prof. Dr. Romeu Hausmann

Pró-Reitor de Administração

Prof. Me. Jamis Antônio Piazza

Pró-Reitora de Pesquisa, Pós-Graduação, Extensão e Cultura

Profª. Drª. Michele Debiasi Alberton

Divisão de Modalidades de Ensino Chefia da Divisão

Profª. Drª. Clarissa Josgrilberg Pereira

Professores Autores

Prof. Me. Francisco Adell Péricas

Design Instrucional

Profª. Drª. Clarissa Josgrilberg Pereira

Prof. Dr. Maiko Rafael Spiess

Prof. Me. Francisco Adell Péricas

Marcia Luci da Costa

Me. Wilson Guilherme Lobe Junior

Revisão Textual

Me. Wilson Guilherme Lobe Junior

Laura Cristina Zorzo

Roteirização

Laura Cristina Zorzo

Produção de Mídia

Gerson Luís de Souza

Gustavo Bruch Féo

Equipe de Design Gráfico

Amanda Kannenberg

Camylle Sophia Teske

Laura Cristina Zorzo

Nicolle Sassella

Renan Diogo Depiné Fiamoncini

Diagramado por Camylle Sophia Teske em 13 de Fevereiro de 2023

CONTINUE