GESTÃO E MONITORAMENTO DE REDES DE COMPUTADORES

CONCEITOS INICIAIS DE GERÊNCIA DE REDES

Autor: Me. Paulo Sérgio Pádua de Lacerda

Revisor: Rafael de Jesus Rehm

INICIAR

Introdução

A proposta principal desta unidade é definir conceitos, padrões e critérios fundamentais relacionados ao gerenciamento de redes de computadores. Além disso, falaremos sobre a importância da gerência de redes para o departamento de Tecnologia da Informação (TI) de empresas e organizações.

No atual cenário digital, com o crescimento do volume de ofertas de serviços on-line por meio da internet, a responsabilidade do departamento de TI em relação ao provimento de disponibilidade de serviços e aplicações de infraestrutura tem aumentado cada vez mais.

Assim, entender como funcionam as métricas e os *frameworks* utilizados na gerência de redes de computadores é indispensável ao profissional que atua na área.

Em suma, a partir deste material, você poderá identificar e compreender os fundamentos principais da gerência de redes de computadores.

O Porquê da Gerência de Redes

Neste tópico, abordaremos alguns assuntos relativos aos fundamentos da gerência de redes. Além disso, faremos um mapeamento histórico da gerência de redes de computadores ao longo das últimas décadas.

O fato é que, desde 1970, com o surgimento das primeiras redes de computadores, houve um crescimento explosivo da área. Com a chegada da internet, essa evolução cresceu exponencialmente. Originalmente, a rede de computadores foi criada pela necessidade de comunicação e transferência de arquivos entre máquinas (computadores), mas, ao longo do tempo, essa necessidade evoluiu, principalmente quando as redes de computadores foram incorporadas aos negócios das empresas.

Para Comer (2015), a partir do momento em que a rede passou a fazer parte da infraestrutura de empresas, transformando-se em algo essencial às organizações, todos os aspectos dos negócios corporativos, incluindo publicidade, produção, transporte, planejamento, faturamento, contabilidade, entre outros, migraram suas comunicações e transações para o mundo digital.

Assim, podemos exemplificar por meio de serviços de instituições financeiras.

Hoje, quase todos os serviços disponibilizados por bancos podem ser realizados através de redes de computadores, a exemplo de transações, consultas, aberturas de contas, entre outros. O aumento dos serviços *on-line* é devido ao crescimento da internet.

A internet tornou-se fundamental na vida do ser humano. Assim, na era digital, houve uma mudança não só em relação a como os serviços são prestados pelas empresas, mas também no tocante à forma de trabalho dos profissionais das mais diversas áreas. Atualmente, médicos podem monitorar pacientes a distância e empresas podem realizar reuniões *on-line* . Da mesma maneira, as análises de diagnóstico de doenças são mais precisas e rápidas, comidas podem ser solicitadas por meio de aplicativos em celulares, encontros entre pessoas são realizados via internet, grupos estabelecem comunicação por e-mail e *chats* eletrônicos para fins pessoais e profissionais, empresas fecham novos negócios *on-line* etc. A Figura 1.1 ilustra essa mudança de comportamento ocasionada pelo uso de dispositivos eletrônicos conectados à internet.

Figura 1.1 - Usuários conectados à internet
Fonte: Pressahotkey / Freepik.

Então, podemos dizer que esses serviços dependem de uma rede de

computadores confiável e disponível em sua totalidade, ou seja, 24 horas por dia, o tempo todo. Uma vez que a rede passa a ser um elemento indispensável às organizações, ela não pode parar.

Porém, as redes de computadores são complexas. Desde sua criação, estão associadas a uma evolução constante e dinâmica, pois existem muitas tecnologias, e cada uma tem suas próprias características. Assim, podemos entender que, mesmo neste cenário complexo e heterogêneo de tecnologia, a rede de computadores é transparente para o usuário, já que, na visão deste, é um sistema único.

Essa complexidade da rede de computadores também advém da evolução constante das necessidades de clientes e parceiros das empresas. Nesse sentido, as organizações têm buscado facilitar a comunicação e o relacionamento com seus clientes e parceiros.

Diante desse cenário complexo e associado a uma variedade de serviços disponíveis, a tarefa de monitorar e gerenciar redes torna-se fundamental. Logo, podemos dizer que a gerência de redes é o processo de monitoramento e controle de uma rede de dados, por meio da garantia da maximização de serviços e do aumento da eficiência e produtividade, com objetivo de melhorar a qualidade dos serviços prestados. Nesse sentido, temos também a atividade fundamental de gerência de elementos físicos de interconexão de rede, como roteadores, por exemplo, e lógicos, tais como os protocolos que proveem uma infinidade de serviços on-line.

Em suma, a gerência de redes deve:

- realizar o controle da rede de computadores;
- tornar possível a gerência da complexidade da rede;
- permitir a otimização dos serviços de comunicação;
- otimizar o uso dos recursos disponíveis na rede;
- reduzir o tempo de indisponibilidade de uma rede;
- auxiliar na gerência do controle de gastos.

Porém, esses objetivos estão inseridos em um cenário complexo, em que diversos desafios são impostos constantemente aos administradores de

redes. Sendo assim, vejamos a Figura 1.2 a seguir, por meio da qual é possível visualizar um cenário de redes de computadores composto por diversos elementos, tais como roteadores, servidores e *hosts* (KUROSE; ROSS, 2013):

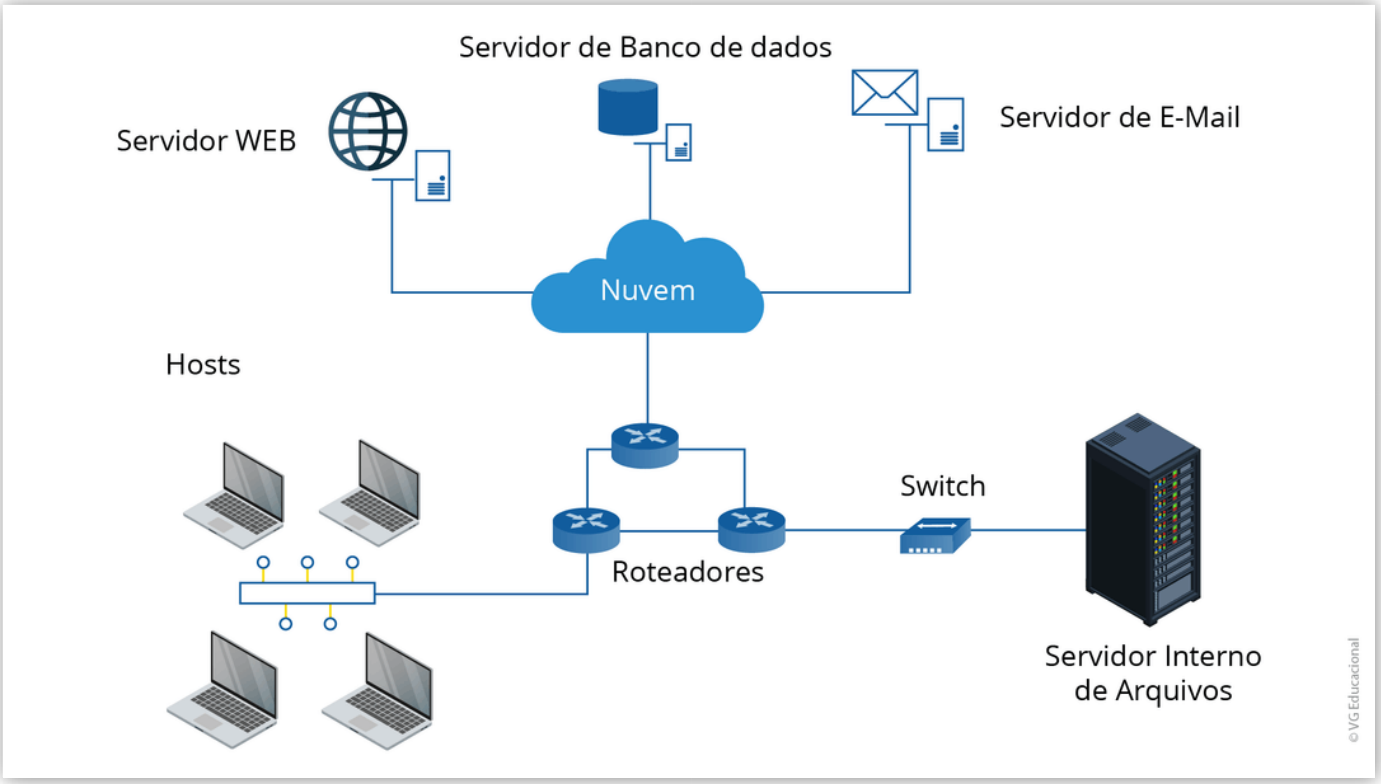


Figura 1.2 - Cenário de uma rede de computadores
Fonte: Elaborada pelo autor.

Nesse cenário, como dito anteriormente, diversos desafios são impostos ao administrador, por exemplo:

- Detecção de falha: placas de redes podem falhar e causar danos no envio de pacotes e interferir negativamente na comunicação de dados entre dois dispositivos roteadores, *hosts* ou servidores.
- Gerência do hospedeiro: a gerência de redes permite que o administrador de rede verifique um hospedeiro a fim de analisar seu comportamento na rede (por exemplo, verificar se todos os hospedeiros estão ativos na rede).
- Monitoramento de tráfego: o tráfego de redes pode ser monitorado por administradores por meio de ferramentas de monitoramento, com a finalidade, por exemplo, de evitar o congestionamento de *links* de comunicação.
- Alteração das tabelas de roteamento: a alternância constante de

rotas pode ser indicativo de uma má configuração em dispositivos como roteadores, por exemplo, gerando inconsistência na rede.

- Monitoramento de Acordos de Nível de Serviços (*Service Level Agreements* - SLAs): SLAs são contratos que definem parâmetros específicos de medida e níveis aceitáveis de desempenho do provedor de rede, incluindo disponibilidade de serviço (interrupção de serviços), latência, vazão etc.
- Detecção de invasão: por meio da gerência de redes, um administrador de rede pode ser notificado sobre um provável ataque externo à sua rede de computadores.

No mundo de redes de computadores, há diversos órgãos internacionais que determinam normas e padrões a serem seguidos com o intuito de padronizar e melhorar as práticas operacionais dentro de cada área. A International Organization for Standardization (ISO) é um dos principais órgãos mundiais que determinam regras a serem aplicadas à área de redes de computadores.

A ISO desenvolveu um modelo de gerenciamento de rede que posiciona cenários apresentados em um quadro mais estruturado (KUROSE; ROSS, 2013). Esse modelo é subdividido em cinco áreas de gerenciamento de rede: gerência de desempenho, gerência de falhas, gerência de configuração, gerência de contabilização e gerência de segurança.

Essas gerências têm a responsabilidade de:

- Gerenciamento de desempenho: tem a função de quantificar, medir, informar, analisar e controlar o desempenho de diferentes dispositivos de rede. Esse controle é feito para analisar características da rede, como, por exemplo, vazão, uso, interrupções etc.
- Gerenciamento de falhas: tem a função de registrar e detectar condições de falhas da rede, reagindo a elas. A fronteira entre a gerência de falhas e a gerência de desempenho é muito tênue, porém, podemos dizer que a gerência de falhas está associada à análise de falhas ao longo do tempo (falhas ocasionais e desempenho de tráfego). Já a gerência de desempenho está associada a falhas imediatas e ao tratamento imediato dessas falhas.

- Gerenciamento de configuração: nessa gerência, o administrador de rede pode ter uma visão geral dos equipamentos passíveis de gerenciamento, bem como de suas configurações de hardware e software.
- Gerenciamento de contabilização: está associada a atividades como controle de acesso de usuários, quotas de utilização, alocação de acessos privilegiados, cobrança por utilização etc.
- Gerenciamento de segurança: tem o objetivo de garantir e controlar a segurança de acesso aos recursos da rede definidos por meio de uma política. Componentes como a distribuição de chaves criptográficas e de autoridades certificadoras e o uso de *firewall* estão relacionados a essa gerência.

Agora que você já conheceu as necessidades da gerência de rede, os tipos de gerência e os problemas relacionados à rede que podem ser monitorados, analisados e corrigidos com o uso de gerência de rede, vamos descrever alguns aspectos importantes ao longo da história que determinaram o crescimento dessa área, hoje tão fundamental às empresas.

Panorama Histórico da Gerência de Redes

Nesta seção, vamos falar sobre o aspecto histórico da evolução da gerência de redes, pontuando os fatores relevantes de cada época e construindo uma cronologia até os tempos atuais.

Vamos começar pela década de 1970, em que tudo teve início. Nessa época, principalmente no começo, foram criadas as primeiras redes de computadores, com servidores centralizados, os chamados *mainframes* . Esses servidores eram ligados a terminais de computação, denominados de “terminais burros”, pois todo o processamento era realizado diretamente nos servidores *mainframes* . Não havia gerência de redes, e a taxa de transmissão nos *links* era baixa.

Reflita

Antes do desenvolvimento da comutação de pacotes, entre 1961 e 1972, o mundo de tecnologia tinha como rede dominante a rede de telefonia. Lembre-se de que a telefonia adota outro tipo de comutação, a comutação por circuito. Na comutação por circuito, a informação é transmitida da origem ao seu destino. Por exemplo, a voz é transmitida a uma taxa de velocidade constante entre a origem e o destino.

Fonte: Caruso (1990).

Ao mesmo tempo, surgiram as primeiras redes comutadas por pacotes, como a francesa TAYMNET e TRANSPAC, a ALOHAnet, utilizada entre ilhas no Havaí, e a TELENET, baseada na ArpaNet. Porém, em 1973, surgiu a rede Ethernet, desenvolvida por Robert Metcalfe e David Boggs, seu assistente, e consolidada por meio de uma publicação do artigo “Distributed Packet-Switching For Local Computer Networks”.

Já na década de 1980, surgiram os computadores pessoais, e a Ethernet tornou-se um padrão para as redes locais. Essa rede possuía características de comutação por pacotes, com uso da topologia em estrela. “O interessante é que o protocolo Ethernet de Metcalfe e Boggs foi motivado pela necessidade de conectar vários computadores pessoais, impressoras e discos compartilhados” (PERKINS, 1994 *apud* KUROSE; ROSS, 2013, p. 46). Ou seja, é

precursora do modelo de rede utilizado na era digital.

A década de 1980 foi muito importante para o aumento de máquinas interligadas. Para se ter uma ideia, no fim dessa década, mais de cem mil máquinas estavam interconectadas. Na década de 1970, eram apenas duzentas (KUROSE; ROSS, 2003). Todavia, a motivação para o desenvolvimento das redes era sempre a mesma: aumentar o número de redes interconectadas e, consequentemente, de computadores, sem a preocupação da gerência. Vale registrar que, naquela época, já existiam redes que conectavam partes diferentes dos Estados Unidos, como a BITNET (processamento de e-mails e transferência de arquivos entre as universidades do nordeste americano), contudo, o grande esforço era tentar criar uma rede que pudesse agregar todas as universidades norte-americanas.

A NSFET, rede de 56 kbps de velocidade, foi criada em meados da década de 1980, tendo como finalidade prover acesso a grandes centros de computação patrocinados pela *The National Science Foundation* (NSF), com *backbone* (link principal) aumentado em 1,5 Mbits/s e servindo como *backbone* primário para a interligação de redes regionais (CASTELLS, 2003).

A explosão da rede mundial aconteceu no início dos anos 1990, por meio de vários eventos, tais como: a extinção da ArpaNet e das restrições comerciais de uso da NSFNET; o carregamento da internet por provedores de serviços; e, principalmente, o surgimento da *World Wide Web* , criada por Tim Berners-Lee no Centro Europeu de Física Nuclear (CERN), fato que permitiu que a internet chegasse aos lares e às empresas ao redor do mundo, mediante um protocolo de transferência de hipertexto (HTTP) de páginas escritas pela linguagem *HyperText Markup Language* (HTML), acessadas a partir de um navegador de páginas (browser). A Figura 1.3 ilustra o uso de um navegador com as iniciais do endereço eletrônico, marco importante para o que é a navegação hoje em dia.

Figura 1.3 - Navegador com protocolo e serviço WWW
Fonte: Freepik.

A partir desse momento, o mundo passou a viver uma revolução de novas aplicações de busca (como Google e Bing) e de serviços eletrônicos (como Amazon e eBay). Além disso, surgiram redes sociais como o Facebook e outros serviços on-line de e-mail e de compartilhamento de arquivos de extensão mp3 (um bom exemplo é o Napster). Nessa época, já havia um volume alto de informações e, por essa razão, alguns ativos passaram a ter importância dentro da rede (como os servidores, por exemplo), sendo, então, monitorados, bem como alguns métricas relacionadas a *links* (vazão).

Com o novo milênio, outros fatores começaram a contribuir para o melhoramento da gerência de computadores. O maior deles, sem dúvidas, é a explosão da internet como a grande rede mundial. Podemos incluir também a velocidade dos elementos de interconexão de redes (roteadores), os serviços como teleconferência, a comunicação em tempo real, a exigência de uma banda maior de dados, o aumento da velocidade de transmissão, o barateamento das fibras como *link* de *backbone* , a onipresença das redes wi-fi, o processamento em nuvem, as redes sociais, o aumento da adesão dos usuários à rede, enfim, tudo isso passou a exigir uma melhor qualidade do sinal, uma melhor vazão, uma melhor disponibilidade, balanceamento de

carga etc.

Na atualidade, a internet figura como a grande rede mundial. Da mesma maneira, as empresas são as maiores fornecedoras de serviços. Por essas razões, a rede torna-se um ativo crítico para as organizações e, portanto, é necessário um bom planejamento da gerência. Na próxima seção, vamos apresentar como podemos gerenciar as redes de computadores e quais variáveis controlar.

praticar

Vamos Praticar

Uma rede de computadores possui diversos elementos, tais como *hosts* , servidores, roteadores, *hubs* , placas de rede, conectores etc., com a finalidade de transmitir e receber informações entre origem e destino. Supondo uma falha de comunicação entre dois computadores provocada por um defeito na placa de rede, assinale a alternativa correta com relação à gerência da rede responsável por essa falha.

- **a)** Gerência de configuração.
- **b)** Gerência de falhas.
- **c)** Gerência de segurança.
- **d)** Gerência de desempenho.
- **e)** Gerência de contabilização.

Métricas de Gerenciamento de Redes

Agora que você já foi apresentado aos princípios básicos de gerência de redes, neste tópico vamos falar sobre o conceito de métricas e quais são utilizadas no gerenciamento de redes de um servidor *web* , de elementos de rede como roteadores e *switches* , *links* de rede Ethernet e sistema, como sistemas multimídia, que precisam de tratamento diferenciado na rede.

Hoje, pelo fato de a rede de computadores ser um elemento crítico dentro de uma empresa, as redes de computadores precisam de mecanismos de medição. Esses mecanismos de medição são ferramentas de apoio ao administrador de rede, principalmente no que diz respeito às tomadas de decisão relativas a ações como validação, pré-implantação e análise de desempenho. Os mecanismos de análise geram resultados, e esses resultados são chamados de métricas. As métricas podem ser associadas a diversos fatores, tais como vazão, indisponibilidade e perda de pacotes, e a elementos de redes, por exemplo, roteadores, placas de rede, hosts, servidores e sistemas multimídia.

Métricas Relacionadas a Quality of Service (QoS)

Quando falamos em redes de computadores, a transferência do dado, da origem ao destino, através de um meio de comunicação (cabo, *wireless* , fibra etc.), é chamada de fluxo. Um fluxo contém pacotes de dados. Em uma rede orientada à conexão, todos os pacotes são transferidos seguindo o mesmo caminho, entretanto, em uma rede não orientada à conexão, os pacotes de dados seguem por rotas diferentes.

Sendo assim, cada fluxo de dados em uma rede não orientada à conexão, a exemplo da Ethernet, base da internet, pode necessitar de parâmetros diferentes, incluindo largura de banda, atraso, flutuação e perda de dados. Esses parâmetros associados determinam a qualidade de serviços (QoS) que cada fluxo exige (TANENBAUM; WETHERALL, 2011).

saiba mais

Saiba mais

A Tecnologia da Informação (TI), por meio da gerência de rede, passou de uma estrutura de suporte ao negócio para o papel estratégico e fundamental de modelo de negócio, pois a rede é agora um elemento crítico para as empresas, portanto, decidir quais métricas utilizar faz parte do planejamento da gerência. Nesse sentido, o administrador de rede precisa entender o papel da TI. Para aprofundar esse entendimento, leia o capítulo 1 do livro "Gerenciamento de serviços de TI na prática: uma abordagem com base na ITIL", dos autores Ivan Luizio Magalhães e Walfrido Brito Pinheiro.

ACESSAR

Aplicações multimídias são mais sensíveis a QoS, por exemplo, Skype, Zoom, jogos *on-line multiplayers* e *streams* de vídeo (Netflix). Para essas aplicações, alguns requisitos devem ser atendidos para que possam ser executadas com a qualidade esperada pelo usuário. Esses requisitos podem ser:

- Vazão (*throughput*): taxa de transferência medida em algum período de tempo, podendo ser medida em kbits/s, Mbits/s ou Gbits/s.
- Atraso ou latência (*delay*): teoricamente, o atraso é o tempo gasto pelo pacote desde sua origem até o destino. A unidade de medida é ms (milissegundos).
- Jitter: esse requisito pode ser definido pela variação do tempo de

atraso dos pacotes na entrega ou pela troca de ordem de chegada.

- Taxa de erros: esse requisito tem a unidade de média em percentual (%), pois faz referência à relação de pacotes perdidos que não chegaram ao destino e à quantidade de pacotes total enviados.
- Perda de pacotes: requisito relacionado à perda de pacotes de dados ou a pacotes corrompidos. A perda geralmente está relacionada aos elementos que foram descartados devido a fatores como: capacidade de armazenamento esgotada, estouro de memória, congestionamento da camada física etc.

Outras métricas podem ser aferidas em equipamentos de rede, a exemplo do roteador, que será o assunto abordado no próximo tópico desta unidade.

Métricas relacionadas ao roteador de rede

O roteador é o equipamento de rede que tem por finalidade ligar redes e encaminhar os pacotes (determina a melhor rota), ao longo da rede, até o destino. Assim, algumas métricas podem ser aferidas na contagem de saltos e no custo de rota (distância administrativa) (KUROSE; ROSS, 2013).

Com relação à métrica por contagem de salto (hop), a melhor distância entre dois pontos (A e B) na rede será aquela que apresentar o menor número de saltos.

A Figura 1.4 ilustra uma pequena rede, mostrando uma rota selecionada pela métrica por salto, em que a rota escolhida, ROTA A, utiliza três saltos em relação à outra rota, ROTA B, que utilizaria quatro saltos.

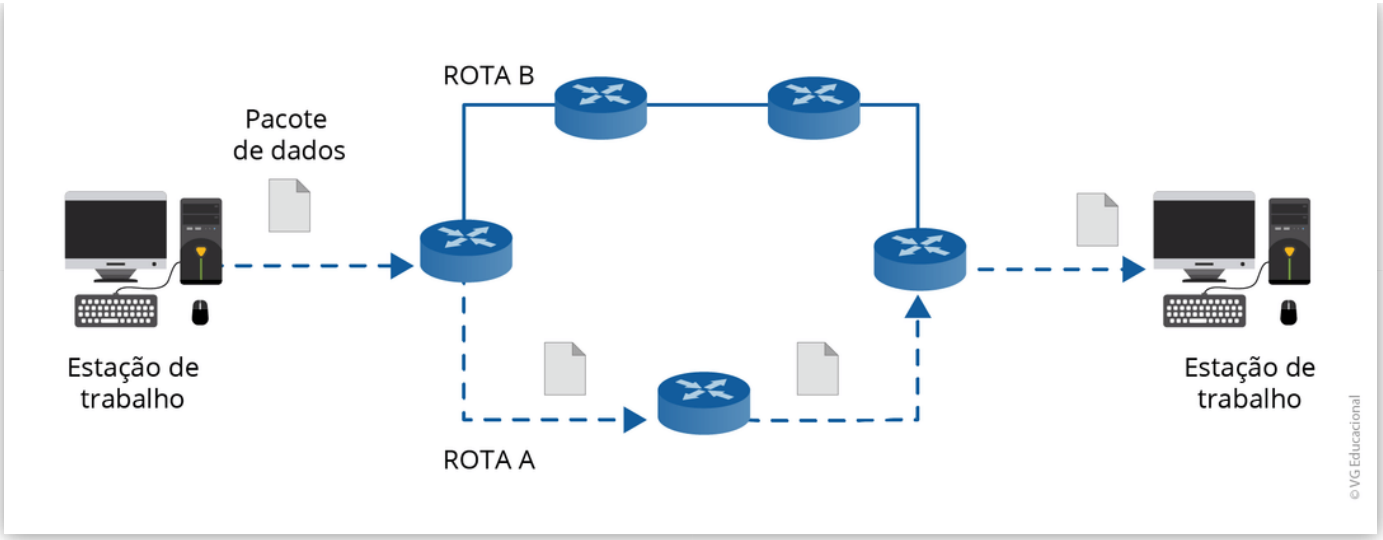


Figura 1.4 - Escolha da rota por salto
Fonte: Elaborada pelo autor.

Ao contrário da métrica por salto, a métrica por custo (distância administrativa) não leva em consideração o salto, mas, sim, o valor administrativo do link entre os equipamentos de rede, mais especificamente, o roteador. A melhor rota para o envio dos pacotes será a que apresentar o menor resultado no somatório dos custos administrativos. A Figura 1.5 traz a ilustração de uma rota com um custo administrativo total menor, pois a rota escolhida, ROTA B, tem o custo de 7 em relação à segunda rota, ROTA A, cujo valor total administrativo é 8.

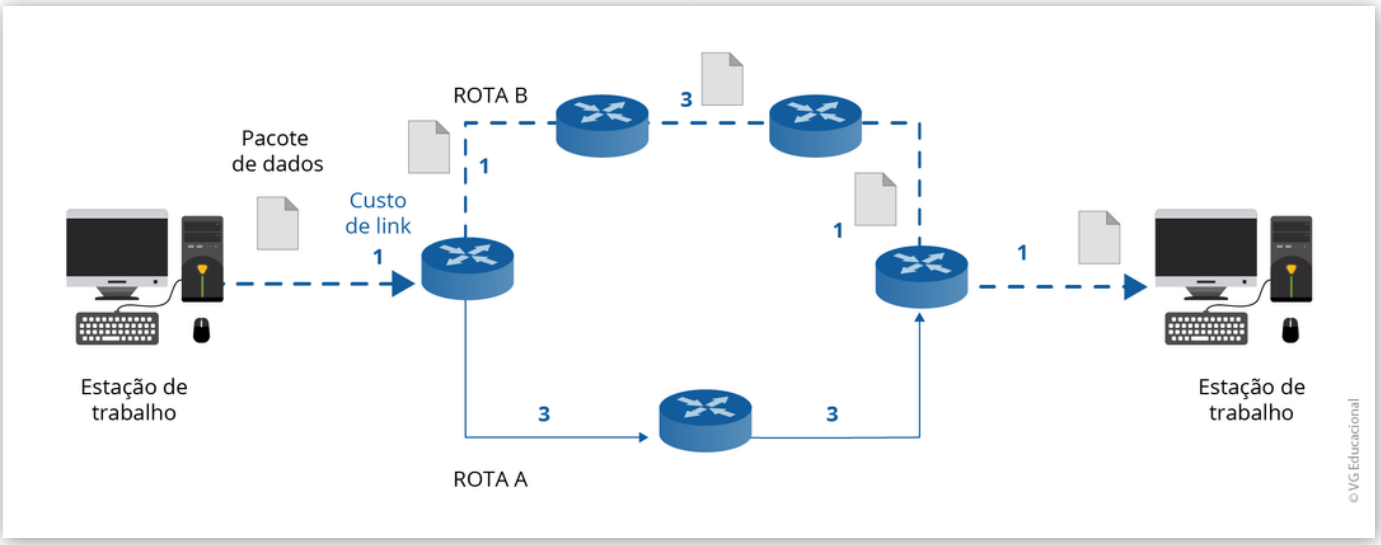


Figura 1.5 - Escolha da rota por custo
Fonte: Elaborada pelo autor.

Todavia, em uma rede de computadores, existem os equipamentos que são os provedores de serviços, os chamados servidores. No próximo tópico,

vamos explicar algumas métricas relativas ao servidor.

Métricas Relacionadas ao Servidor

Como exemplo de rede, a internet é a maior rede de computadores. Na verdade, ela é constituída de pequenas outras redes integradas e tem por finalidade interconectar diversos equipamentos de redes, a exemplo de *hosts* (notebooks, tablets, smartphones, computadores), além de outros equipamentos que fornecem serviços de rede utilizados pelos usuários, tais como páginas *web* , serviços de *download* , e-mails etc. Esses equipamentos são conhecidos como servidores de rede (KUROSE; ROSS, 2013).

Algumas métricas podem ser utilizadas para servidores de rede e auxiliam os administradores na gerência desses servidores. Porém, essas métricas têm de ser planejadas, pois a escolha vai depender do que o administrador de rede pretende gerenciar. Com relação ao servidor, dois problemas significativos são a disponibilidade dos serviços e a velocidade de resposta a uma requisição (tempo).

Com relação ao tempo de resposta (medido em milissegundos) a uma requisição, diversos fatores podem ser considerados um obstáculo que provoca lentidão de determinado sistema ou aplicativo, por exemplo, a lógica do aplicativo, a lentidão na consulta à base de dados, a limitação dos recursos de hardware (CPU e memória), o dimensionamento errado do servidor e *link* de acesso ao servidor com baixa largura de banda.

Já a disponibilidade de serviços é a capacidade de o servidor operar sem falhas durante um período (por exemplo, durante um ano). No entanto, algumas outras métricas estão relacionadas à confiabilidade do servidor. Elas são medidas estatisticamente por um histórico de observação (MAGALHÃES; PINHEIRO, 2007). Essas medidas são:

- Taxa de defeito (*failure rate*): número de defeitos durante um período de tempo.
- *Mean Time to Failure* (MTTF): tempo esperado até a primeira

ocorrência de defeito.

- *Mean Time to Repair* (MTTR): tempo médio para reparo do sistema.
- *Mean Time Between Failure* (MTBF): tempo médio entre os defeitos do sistema.

Agora que você já compreendeu quais métricas podemos utilizar como parâmetro para medir o desempenho de uma rede de computadores, o próximo passo é entender quais padrões de arquitetura de gerenciamento são utilizados na gerência de redes.

praticar

Vamos Praticar

Métricas são medidas utilizadas para analisar o desempenho de uma rede. Tendo em vista que a tecnologia Ethernet é a base da internet, é possível utilizar diversas métricas para aferir a qualidade de uma rede. Um tipo de métrica está relacionado aos pacotes enviados da origem até o destino. Nesse sentido, assinale a alternativa correta com relação à métrica associada a pacotes corrompidos e descartados por um roteador.

- **a)** Vazão.
- **b)** Taxa de erros.
- **c)** Perda de pacotes.
- **d)** Jitter.
- **e)** Taxa de falhas.

Padrões e Modelos de Gerenciamento

Padrões são estruturas desenvolvidas por entidades internacionais, a exemplo da International Organization for Standardization (ISO), que define modelos a serem seguidos e implementados em diversas áreas de TI, principalmente na área de redes de computadores. Nesta seção, vamos apresentar alguns conceitos relativos a padrões de gerenciamento, tais como o OSI e o *Transfer Control Protocol* (TCP) ou *Internet Protocol* (IP).

Com a evolução das redes de computadores no fim da década de 1980, as atividades empresariais foram incorporadas ao mundo digital, incluindo as tarefas de sistema de pagamento, inventário, suporte a cliente, transferência de fundos, aplicações com som, vídeo etc. Devido a isso, nessa mesma época, a ISO criou um framework de gerenciamento de redes com base no modelo *Open System Interconnection* (OSI).

Modelo OSI

Esse modelo de ambiente de gerenciamento OSI é constituído de ferramentas e serviços necessários para controlar e supervisionar atividades em rede e

objetos gerenciáveis associados a essa rede (KLERER, 1988).

O modelo garantiu cinco áreas de gerenciamento, definidas pela sigla FCAPS, são elas:

- Gerenciamento de falhas (*Fault*): é responsabilidade dessa gerência manter a continuidade da operação por meio de detecção, isolamento do problema, registro de ocorrência de falhas, reparo de ativos que falharam e teste de diagnóstico, a exemplo da monitoração de enlaces.
- Gerenciamento de configuração (*Configuration*): são de responsabilidade dessa gerência as seguintes atividades: coleta de dados sobre a topologia da rede, monitoramento de mudanças nas topologias física e lógica, configuração de avisos gerenciáveis e atualização dos ativos. Como exemplo, temos a atualização de sistemas operacionais de ativos (*firmware*).
- Gerenciamento de contabilização (*Account*): é responsabilidade dessa gerência o controle de uso dos recursos disponíveis, tais como: limite de banda, discos, telecomunicação etc. Podemos exemplificar como atividades dessa gerência os números de impressão e o uso de banda para *download* .
- Gerenciamento de desempenho (Performance): é responsabilidade dessa gerência a análise do desempenho da rede, por exemplo: visualizar congestionamentos, pontos críticos, entre outros. A medição da capacidade da rede ou da taxa de utilização de banda é uma atividade relacionada a essa gerência.
- Gerenciamento de segurança (*Security*): é responsabilidade dessa gerência a aplicação de políticas de procedimentos de segurança. Temos, como exemplo, a seguinte atividade: manter eventos de registros de logs de segurança, bem como o perfil de acesso à rede e as informações da empresa.

No modelo de gerência OSI, temos os protocolos *Common Management Information Service* (CMIS) e *Common Management Information Protocol* (CMIP). O protocolo CMIS tem a responsabilidade de definir os serviços de gerenciamento. Por sua vez, o protocolo CMIP tem a responsabilidade de

realizar os procedimentos voltados à transmissão de informações de gerenciamento, definindo a sintaxe para o serviço de gerenciamento do CMIS (KLERER, 1998). O *Remote Operations Service Element* (ROSE) é utilizado para a transferência de Protocol Data Unit (PDU). O modelo CMIP é complexo, gera *overhead* na rede e não é um padrão adotado pelo mercado, que costuma adotar o padrão TCP/IP.

Modelo TCP/IP

Como a internet se transformou na maior e mais importante rede de computadores do mundo, seu padrão de arquitetura, o modelo de camadas TCP/IP, foi adotado pelo mercado como o padrão principal de gerência de redes.

O modelo TCP/IP não sobrecarrega a rede e é simples de ser implementado, quando comparado ao modelo OSI. Ele implementa o protocolo de gerenciamento *Simple Network Management Protocol* (SNMP), introduzido pela *Internet Engineering Task Force* (IETF), na camada de aplicação. Os *Request for Comments* (RFCs) 1157, 1155, 1156 e 1213 fazem referência, respectivamente, ao protocolo SNMP, ao *Structure Management Information* (SMI), ao Management Information Base Version 1 (MIB-I) e ao *Management Information Base Version 2* (MIB-II).

Os componentes utilizados na gerência de rede TCP/IP são: o gerente; qualquer estação de trabalho com um software apropriado de gerência; os agentes; e os equipamentos de rede (ativos) gerenciáveis que fazem parte da rede (como roteadores, *switches* , *hubs* , servidor, modem, portas etc.) O protocolo SNMP utiliza a porta UDP, e quase todos os elementos de rede têm suporte a esse protocolo. A Figura 1.6 mostra o uso do modelo de gerência TCP/IP em forma de camadas.

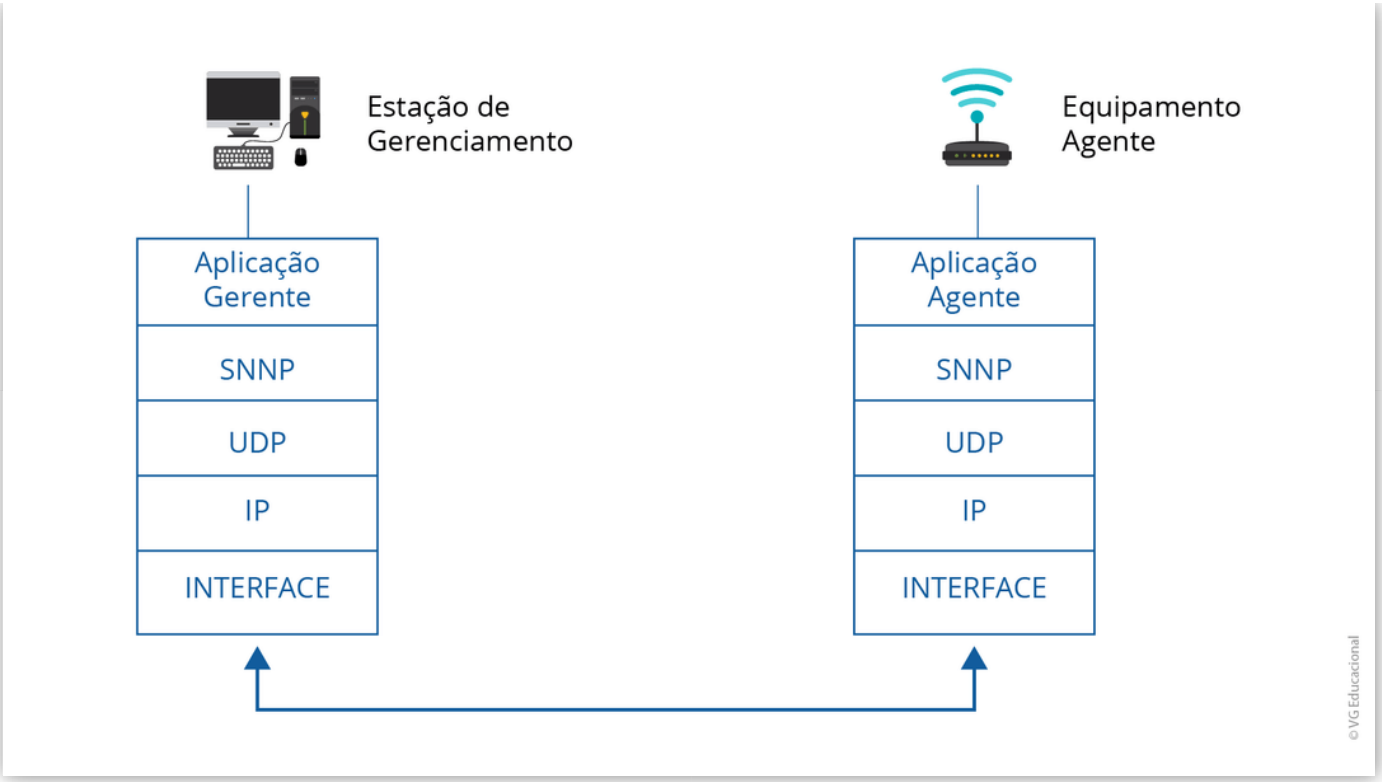


Figura 1.6 - Padrão TCP/IP
Fonte: Elaborada pelo autor.

Além dos padrões OSI e TCP/IP, existem outros padrões como o padrão *Telecommunication Network Management* (TNM) e o padrão de arquitetura, que utiliza o método *Discrete Multitone* (DMT) relacionado a linhas *Digital Subscriber Line* (DSL).

A competitividade existente entre as empresas na década de 1980, decorrente da evolução da rede de telecomunicações na implantação de equipamentos heterogêneos, tornou necessária a criação de um padrão de gerência que incluísse o modelo OSI/ISO. Todavia, em 1985, a instituição *International Telecommunications Union* (ITU) criou a Rede de Gerência de Telecomunicações (TNM). A TNM foi uma rede projetada para gerência, não estando associada à rede de telecomunicações que coletava e processava informações de gerência (RAMOS, 2000).

Já o DMT é um método que separa linhas DSL para que as faixas de frequências utilizáveis sejam divididas em 256 bandas de frequência (ou canais) de 4,3125 KHz cada. Desde 1994, o sistema DMT é o modelo previsto pelo ANSI e padronizado para o A(*Asymmetric*)-DSL conforme normas G.992.1 e G.992.2 do ITU-T [ITU992.1, ITU992.2].

Gerência de redes

123rf.co

Com a evolução da rede na década de 1980, a necessidade de monitoramento e controle faz com que a gerência de redes de computadores se torna em um setor, antes de suporte, agora crítico para a continuidade dos negócios, principalmente pelo surgimento e crescimento da Internet comercial.

Como visto, embora existam outros modelos e padrões, o protocolo SNMP é o mais utilizado atualmente. Ele será o assunto do próximo tópico da unidade.

Vamos Praticar

Usando uma ferramenta de análise de protocolo, faça um monitoramento do tráfego de sites navegados. Utilize a ferramenta Wireshark, de acordo com seu sistema operacional, faça a captura da placa de rede Ethernet ou Wireless e filtre o pacote pelo protocolo TCP e porta 80. Analise os tipos de protocolo. Vamos praticar.

Protocolo SNMP

Agora que você já conhece o protocolo de gerenciamento de redes adotado como padrão, o protocolo SNMP, vamos neste tópico detalhar um pouco mais suas características e os elementos relacionados ao padrão e à gerência TCP/IP.

O desenvolvimento do protocolo SNMP segue o mesmo padrão cronológico e histórico da pilha TCP/IP, do qual ele faz parte. Na pilha TCP/IP, o protocolo SNMP está situado na camada de aplicação e faz uso do protocolo UDP (*User Datagram Protocol*) da camada de transporte. Logo, esse protocolo é um protocolo padrão de internet para gerência de dispositivos IP (STALLINGS, 1999).

O protocolo SNMP possui outras versões com novas implementações, como o SNMPv2, por exemplo, que incluiu melhorias relacionadas à segurança e à confidencialidade das comunicações entre gerentes. Já a versão SNMPv3 implementou melhorias relacionadas à autenticação, ao controle de acesso e à privacidade. Todas as implementações possuem suporte no RFC 3584.

saiba mais

Saiba mais

O Request For Comments (RFC) reúne os melhores documentos técnicos a respeito de determinados padrões. O grupo internacional Internet Engineering Task Force (IETF) criou e mantém o RFC. Se você deseja conhecer mais sobre as especificações de protocolos, faça uma visita ao *site* do IETF, digite o RFC do protocolo desejado e obtenha mais conhecimentos sobre o padrão pesquisado.

ACESSAR

Conceitos Básicos do SNMP

O modelo de gerência de redes TCP/IP apresenta alguns elementos-chaves, por exemplo: estação de gerência, estação agente, base de informações gerenciais e protocolo de gerenciamento de redes. Vejamos detalhadamente a seguir cada um deles.

Estação de gerência: é o dispositivo, geralmente um computador, que possui um software capaz de ler e analisar as informações do protocolo SNMP.

Estação agente: são os dispositivos ou elementos de rede gerenciáveis que dão suporte ao protocolo SNMP. Roteador e servidor são exemplos de estação agente.

Base de informações gerenciais (conhecida pelo termo em inglês “MIB”): são os recursos de redes gerenciáveis tratados como objeto, pois cada objeto

possui informações variadas sobre o elemento gerenciável. O conjunto de objetos forma a MIB.

Uma MIB é definida por meio da estrutura de uma árvore que organiza todas as informações. Cada nó rotulado contém um identificador de objetos (OID) e uma pequena descrição textual. Um exemplo de MIB:

- directory(1);
- identificador de objetos: 1.3.6.1.1;
- descrição textual: {internet 1}.

Protocolo de gerenciamento de redes (NMS): responsável pelo link entre os agentes e a estação gerente. O conceito da arquitetura do protocolo SNMP é mostrado na Figura 1.7:

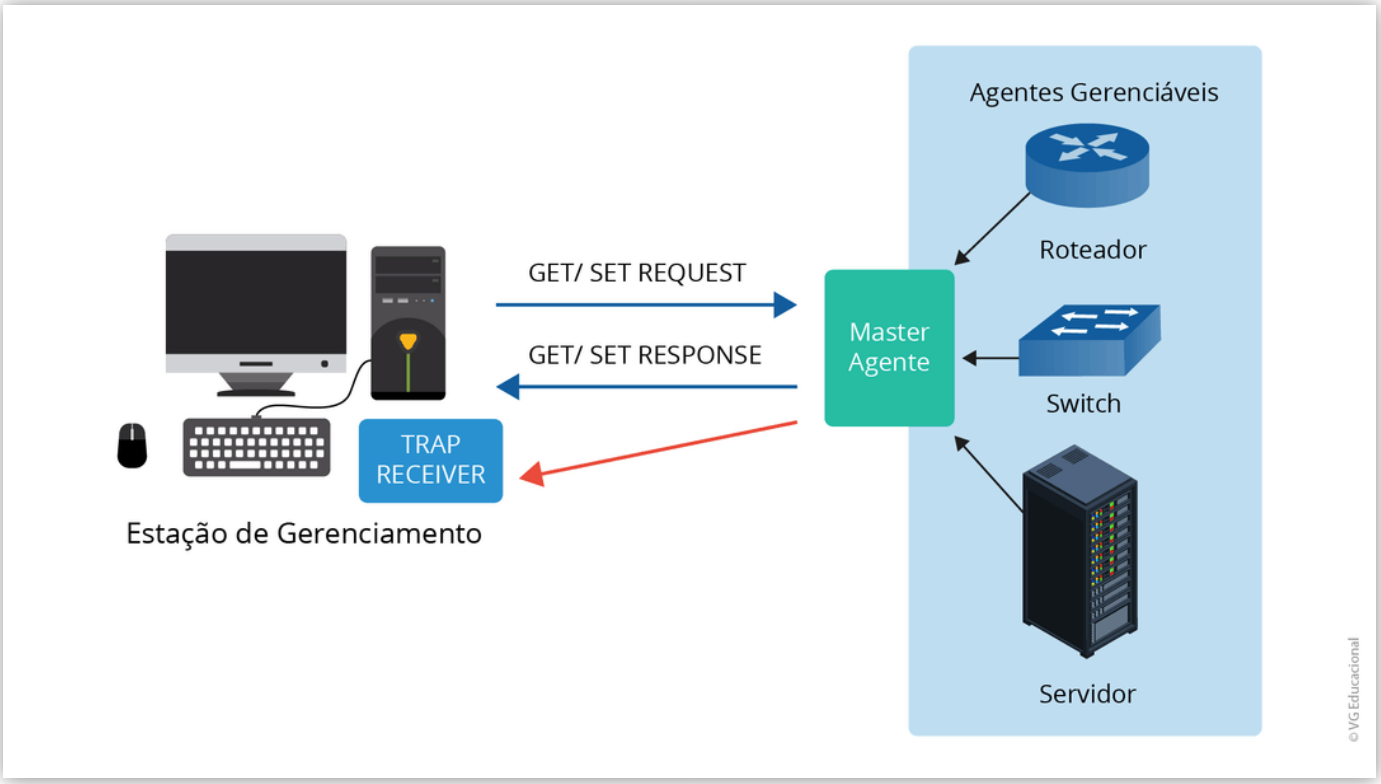


Figura 1.7 - Arquitetura do protocolo SNMP
Fonte: Elaborada pelo autor.

A Figura 1.7, além de apresentar a arquitetura do protocolo SNMP, ilustra a presença do agente master, que é o software que fica “rodando” no elemento de rede gerenciável e que recebe informações dos subagentes. Esses subagentes são os daemons responsáveis pelo monitoramento do elemento gerenciável de rede, e esses agentes enviam informações de monitoramento

da rede como estado de *link* e capacidade de espaço livre em um servidor entre diversos outros itens de gerenciamento. Alarmes podem ser gerados em certas ocasiões e repassados à estação gerente. Esses alarmes são conhecidos também como *traps* . Entretanto, o padrão SNMP teve um adicional muito importante, talvez o passo mais relevante no âmbito da gerência de redes do padrão TCP/IP, que foi a incorporação do protocolo de gerenciamento remoto (STALLINGS, 1999).

Remote *Network Management* **(RMON)**

O protocolo RMON permite obter informações sobre o gerenciamento de redes, de forma remota, por meio do MIBv2 ou MIB-III, especificado pelo RFC 2074, 2021. A concepção do uso do RMON é definida por inserir em redes locais (LAN) agentes monitores que têm a função de monitorar, capturar e analisar dados da rede (como estatística de tráfego, erros, número de pacotes entregues por segundo etc.). Esse monitor deve ser um por rede e ser um dispositivo isolado, ou pode ser uma função implementada no dispositivo de rede. Esse dispositivo pode ser uma estação de trabalho na rede denominada RMON probe e que envia os dados à estação de gerenciamento através das redes.

As configurações nas estações de trabalho são realizadas por meio da sintaxe de notificação abstrata ANS.1, sigla em inglês que significa Abstract Notation Syntaxe One. Desenvolvida por um projeto colaborativo entre a International Telecommunication Union Telecommunication Standardization Sector (ITU-T) e a International Electrotechnical Commission (ISSO/IEC), na década de 1980, tem a finalidade de criar uma sintaxe simples para a representação de dados. O Quadro 1.1 exemplifica alguns termos utilizados na sintaxe ANS.1 para representar os tipos de dados.

Tag	Tipo de dado	Detalhe
UNIVERSAL 1	BOOLEAN	*True* ou *false*
UNIVERSAL 2	INTEGER	Valores inteiros positivos e negativos, incluindo o zero
UNIVERSAL 6	OBJECT IDENTIFIER	Um conjunto de valores relacionados ao objeto gerenciável
UNIVERSAL 19	PrintableString	Caracteres imprimíveis

Quadro 1.1 - Tipos de dados
Fonte: Elaborado pelo autor.

A sintaxe ANS.1 é associada a diversos tipos de codificação e a conjuntos de regras básicas (BER) que descrevem métodos de representação para a codificação de dados de cada tipo ANS.1, com uma string de octetos. Esses conjuntos de regras definem uma ou mais formas de codificar qualquer valor ANS.1. O BER é baseado na estrutura *type-length-value* (TLV), em que: type indica o tipo ANS.1; *length* representa o tamanho atual da representação do valor; e value define o valor da ANS.1 como um tipo de *string* de octetos.

A partir das recomendações ANS.1, teve origem o conceito de identificadores de objetos (*Object Identifier Device* - OID), pois o OID é basicamente uma string de números que identifica os objetos hierarquicamente na rede de computadores para a gerência.

Object Identifier Device (OID)

Os elementos gerenciáveis na rede são identificados como um objeto. Assim,

qualquer elemento, como um indivíduo, um roteador ou uma tecnologia, por exemplo, pode ser identificado pelo seu OID.

Então, temos que um OID é um tipo de dados ASN.1, utilizado exclusivamente na definição ou identificação dos elementos como objetos. Os valores do tipo de dados do identificador de objeto podem então ser usados para nomear os objetos aos quais eles estão relacionados.

Há três instituições no mundo que fornecem o *Objejct Indentifier Device* , OID, são elas: a *Internet Assigned Numbers Authority* (IANA) que distribui OIDs gratuitamente sob a filial "Empresas Privadas", a *American National Standards Institute* (ANSI) que distribui OIDs sob a filial "Organizações dos EUA" e BSI que distribui OIDs sob a filial " *Uk Organizations* ".

reflita

Reflita

Na internet, o servidor *web* é um elemento fundamental. Você conseguiria descrever qual é o OID que representa um servidor *web* ?

Na representação de um OID, uma árvore hierárquica é construída por uma sequência de números inteiros não negativos. Em muitos casos, são referidos como arcos, definindo-se, então, uma hierarquia de objetos identificados. Os arcos são os números inteiros relativos a um objeto, por exemplo.

As autoridades de registro são as entidades de padronização existentes ao

redor do mundo, como a IEEE, a ISO, a W3C, entre outras. No nosso exemplo, vamos identificar segundo a ISO, que recebe o valor 1, ou seja, ISS(1). Posteriormente, vêm as autoridades subordinadas à ISO, como a *iso-identified-organization* (3). No próximo arco, é identificado o instituto IEEE (111), e essa sequência de três números "1" determina que o próximo arco está relacionado às entidades ligadas à IEEE. Nesse exemplo, a string OID ficaria 1.3.111, mas também, a partir de outros exemplos, {iso(1) org(3) dod(6) iana(1)} ou { 1 3 6 1} (IEEE, 2020).

O próximo exemplo está de acordo com a RFC 1157. É um exemplo de identificação mais amplo de uso do OID:

1 iso

1.3 org

1.3.6 dod

1.3.6.1 internet

1.3.6.1.1 directory

1.3.6.1.6 SNMPv2

1.3.6.1.6.1 snmpDomains

1.3.6.1.6.2 snmpProxys

1.3.6.1.6.3 snmpModules

1.3.6.1.7 mail

Inicialmente, a interpretação de objetos OID pode parecer complexa. Por essa razão, é necessário compreender os objetos por meio de uma leitura mais abrangente sobre o tema. Há diversos *sites* na rede mundial que o direciona através dos OId existentes, mas para melhor entendimento use as iniciais da Internet através do 1.3.6.1.???, por exemplo, na lista mostra uma referência autoritária e os demais arcos, números atribuídos pela Internet, encontrados

no RFC 1700.

1.3.6.1.1 - Directory

1.3.6.1.2 - Management (mgmt)

1.3.6.1.3 - Experimental

1.3.6.1.4 - Private

1.3.6.1.5 - Security

1.3.6.1.6 - SNMPv2

1.3.6.1.7 - mail

Lembre-se de que as referências são determinadas por RFC e encontradas facilmente na rede mundial. Para construir bons conhecimentos sobre o assunto, é necessário realizar uma leitura profunda dos RFCs.

praticar

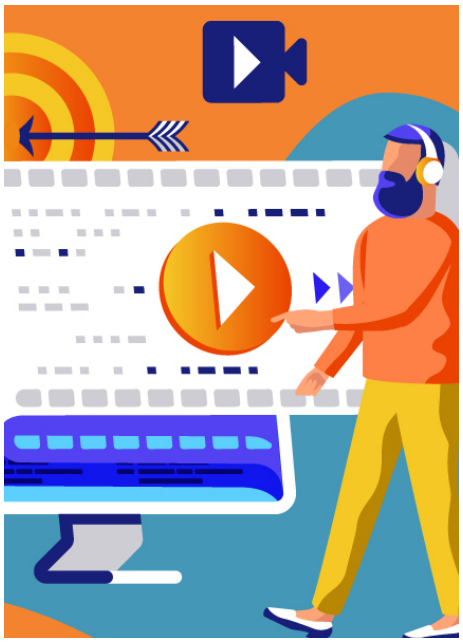
Vamos Praticar

Protocolos são utilizados em redes de comunicação de dados para diversos fins, a exemplo do gerenciamento. O protocolo SNMP é o protocolo padrão do modelo de gerência de redes TCP/IP. Esse protocolo, na sua arquitetura, é composto de alguns elementos, cada um com uma responsabilidade específica. Nesse sentido, assinale a alternativa que apresenta um elemento que armazena a aplicação de gerenciamento.

- **a)** NMS.

- **b)** TRAP.
- **c)** MIB.
- **d)** Agentes.
- **e)** Estação gerência.

Material Complementar



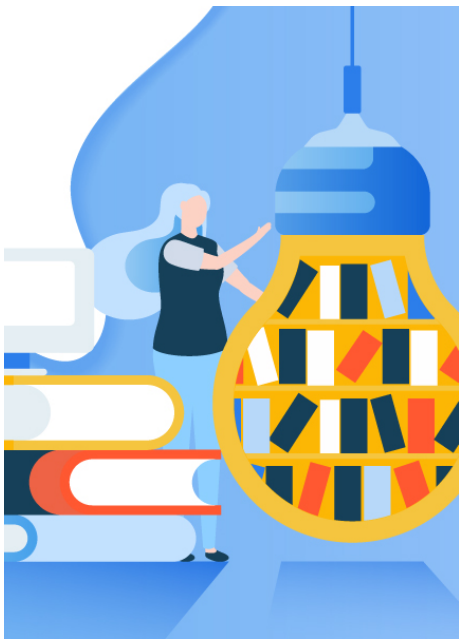
FILME

A Rede (*The Net*)

Ano: 1995

Comentário: Esse filme é uma das primeiras produções cinematográficas sobre invasões de hackers a empresas privadas. Vale muito a pena assistir, pois proporciona uma reflexão sobre o gerenciamento de redes de computadores e serve como um complemento à aprendizagem. Para conhecer mais sobre o filme, acesse o trailer a seguir.

TRAILER



LIVRO

Gerenciamento e segurança de redes

Editora: Senai/SP

Autor: Lindeberg Barros de Sousa

ISBN: 978-8583937654

Comentário: Esse livro descreve conceitos relacionados ao gerenciamento e à segurança de redes de computadores. O capítulo 1 retrata a necessidade do gerenciamento, bem como os tipos e exemplos de elementos gerenciáveis. É um excelente complemento para os estudos desta unidade!

conclusão

Conclusão

Ao longo desta unidade, estudamos os conceitos iniciais sobre gerenciamento de redes. Vimos também que os protocolos são referências essenciais ao entendimento do uso, por exemplo, das ferramentas de gerenciamento.

Foram abordados diversos tópicos sobre o protocolo mais adotado no mundo de redes de computadores, o protocolo SNMP. Falamos de suas versões, da linguagem sintaxe ANS.1, entre outros elementos. Nesta unidade, você teve a oportunidade de definir conceitos, padrões e critérios necessários à gerência em ambientes de TI, reconhecer a importância da gerência de redes para a administração de TI e analisar os principais conceitos relacionados aos protocolos de gerência de redes.

referências

Referências Bibliográficas

CARUSO, R. E. Network management: a tutorial overview. **IEEE Communications Magazine** , v. 28, n. 3, p. 20-25, 1990. Disponível em: https://ieeexplore.ieee.org/document/52887 . Acesso em: 7 maio 2020.

CASTELLS, M. **A galáxia da Internet:** reflexões sobre a Internet, os negócios, e a sociedade. . Rio de Janeiro, Jorge Zahar, 2003.

COMER, D. E. **Computer network and internet.** 6. ed. New Jersey, Pearson Education, 2015.

IEEE STANDARDS ASSOCIATION. **OID tutorial** . 2020. Disponível em: https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/oid.pdf . Acesso em: 9 abr. 2020.

KUROSE, J.; ROSS, E. K. W. **Redes de computadores e a internet** : uma abordagem top-down. 6. ed. São Paulo: Pearson Education, 2013.

KLERER, S. M. The OSI management architecture: an overview. **IEEE Network** , v. 2, n. 2, p. 20-29, 1988.

MAGALHÃES, I. L.; PINHEIRO, W. B. **Gerenciamento de serviços de TI na prática:** uma abordagem com base na ITIL. São Paulo: Novatec, 2007.

RAMOS, A. M. **Modelo para incorporar conhecimento baseado em experiências à arquitetura TMN** . 2000. Tese (Doutorado em Engenharia de Produção) - Universidade Federal de Santa Catarina, Florianópolis, 2000. Disponível em: https://pdfs.semanticscholar.org/b2c2/91c29f1e856803468af01593ce3e32b43055.pdf . Acesso em: 7 maio 2020.

STALLINGS, W. **SNMP, SNMPv2, SNMPv3, and RMON1 and 2. 3. ed** . Massachusetts: Addison-Wesley, 1999.

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores** . 5. ed. São Paulo: Pearson Education, 2011.