

NÃO PODE FALTAR

Imprimir

# GERÊNCIA DE DESEMPENHO, CONFIGURAÇÃO E CONTABILIZAÇÃO

0

Renato Cividini Matthiesen

Ver anotações

## O QUE É GERENCIAMENTO DE UMA REDE DE COMPUTADORES?

O gerenciamento de redes pode ser definido como o monitoramento, o teste, a configuração e o diagnóstico de componentes de rede para atender a um conjunto de exigências definidas por uma organização, as que se relacionam com a operação estável e eficiente da rede e que fornece a qualidade predefinida de serviços aos seus usuários. (FOROUZAN,2010)



Fonte: Shutterstock.

## Deseja ouvir este material?

Áudio disponível no material digital.

## PRATICAR PARA APRENDER

Caro aluno, esta seção apresentará a você conceitos, estratégias e ferramentas para o gerenciamento de sistemas de redes de computadores. Abordaremos, em um primeiro momento, as cinco áreas do gerenciamento de redes, as quais abarcam: configuração, falha, desempenho, segurança e contabilização. Em seguida, apresentaremos alguns comandos para análise e configurações de rede, seguidos dos padrões de gerenciamento de rede, dentre os quais se destaca o protocolo SNMP (*Simple Network Management Protocol*). Para dar sequência ao

aprendizado de gerenciamento de redes, mostraremos indicadores de gerência de desempenho, configuração, contabilização, disponibilidade de rede e QoS (*Quality of Services*). Esses indicadores são vistos através de ferramentas de gerenciamento de redes, muitas delas disponíveis através de comandos ou aplicativos dos sistemas operacionais Linux e Windows, sendo que algumas das ferramentas operam em ambos os ambientes e são de utilização livre. O *Microsoft Network Monitor* e o *Wireshark* são dois aplicativos que podem ser utilizados para análise e mensuração de alguns indicadores de gerenciamento de rede.

o

Ver anotações

Na segunda parte desta seção, trataremos de informações sobre comandos para reconhecimento, avaliação e configuração de sistemas de redes de computadores. O protocolo VLAN *Trunk Protocol* será apresentado como ferramenta para gerenciamento e customização de atividades em redes, e o protocolo SSH (*Secure Shell*), como ferramenta de conexão remota em sistemas de rede. Estas aplicações permitem que o administrador de um sistema de redes de computadores possa fazer a conexão remota com os sistemas e buscar a melhor administração da rede, independentemente de sua localização física.

Um determinado escritório de contabilidade possui uma rede de computadores instalada que suporta todas as atividades profissionais desenvolvida no ambiente interno para cerca de 30 estações de trabalho (desktops e notebooks) para as atividades profissionais de seus colaboradores. A topologia do escritório é apresentada na Figura 2.37 a seguir, na qual se pode perceber as distribuições dos computadores que realizam os trabalhos internamente.

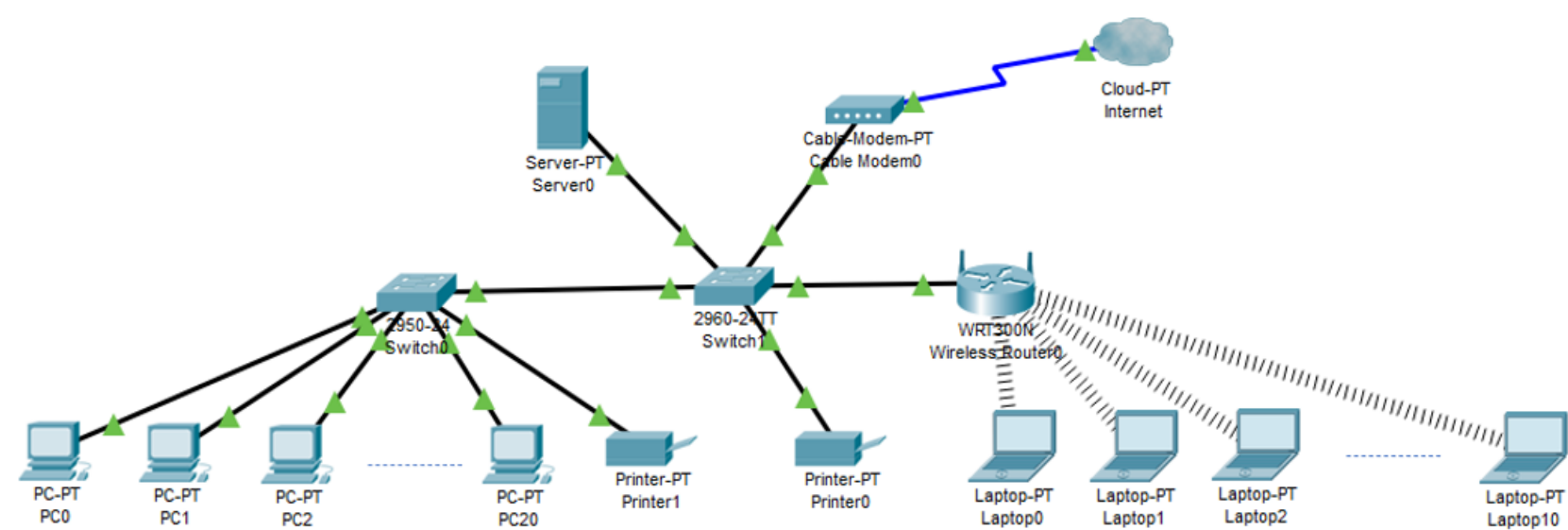
Neste escritório, a rede se tornou muito lenta em um determinado período do dia, quando todos os colaboradores estão atuando em suas atividades profissionais. O diretor da empresa solicitou que um profissional de tecnologia da informação pudesse apresentar uma análise sobre as atividades desenvolvidas na rede, pois entende que há colaboradores utilizando a infraestrutura de rede para fazer downloads de arquivos em formato de vídeo, atividade fora do escopo das atividades convencionais desenvolvidas no escritório. Neste primeiro momento, a consultoria deverá buscar uma solução, com a implantação de um sistema de

*sniffing*, para que se possa coletar os dados da rede. O sistema sugerido para implantação é o *Wireshark*, que tem interface simples e natureza de utilização livre. O *Microsoft Network Monitor* também pode ser utilizado para esta análise.

A consultoria ficou responsável por apresentar a topologia de rede descrita a seguir, utilizando-se da ferramenta *Packet Tracer* e adicionando à estrutura a representação do *sniffer*. Também foi solicitado que o relatório contenha pelo menos uma tela de dados capturados pelo monitoramento realizado pelo *Wireshark*.

Ver anotações

Figura 2.37 | Topologia de rede do escritório de contabilidade



Fonte: elaborada pelo autor.

A consultoria deve apresentar as informações de análise e orientações de utilização da ferramenta de monitoramento de rede através de um relatório chamado de **Relatório de projeto de redes: monitoramento de rede via *sniffing***.

Um sistema de redes de computadores necessita ser devidamente planejado, implantado e gerenciado. A simples implementação de infraestrutura, sistema operacional e aplicações distribuídas em rede não se faz suficiente para que a performance de todo este sistema seja eficaz. As tecnologias e as ferramentas de gerenciamento de redes são fundamentais para que o profissional de tecnologia da informação possa desenvolver uma rotina, na qual o monitoramento e os ajustes do sistema sejam aliados, a fim de que as empresas tenham suporte adequado para que seus sistemas distribuídos possam operar adequadamente.

CONCEITO-CHAVE

GERÊNCIA DE DESEMPENHO

Nesta terceira e última seção da unidade de Arquitetura e tecnologia de redes, conheceremos as áreas que formam o gerenciamento de redes e nos aprofundaremos na gerência de desempenho. Trabalharemos conceitos e aplicações da análise e configuração de redes e utilizaremos o protocolo VLAN *Trunk Protocol* como estratégia para gestão de redes e o SSH (*Secure Shell*) como ferramenta de gestão e acesso remoto em redes de computadores.

o  
Ver anotações

Forouzan (2010) define gerenciamento de redes como o monitoramento, o teste, a configuração e o diagnóstico de componentes de rede para atender a um conjunto de exigências definidas por uma organização. As exigências relacionam-se com a operação estável e eficiente da rede que fornece a qualidade predefinida de serviços aos seus usuários.

Ainda de acordo com o autor, o gerenciamento de redes abarca cinco áreas, conforme descritas a seguir:

- **Gerenciamento de configuração:** sistema utilizado para conhecimento sobre o estado de cada entidade da rede e sua relação com as outras entidades. Este gerenciamento pode ser um subsistema de reconfiguração ou de documentação. Na reconfiguração, há o ajuste dos componentes e das características da rede no que se refere ao hardware, ao software e às contas de usuários. Já na documentação há o registro das configurações da rede sobre o hardware, o software e as contas de usuário.
- **Gerenciamento de falhas:** relaciona-se à área do gerenciamento que trata das falhas de rede através de dois subsistemas: um reativo e outro proativo. No subsistema reativo, existe a detecção, o isolamento, a correção e o registro de falhas. No subsistema proativo, o sistema procura impedir a ocorrência de falhas.
- **Gerenciamento de desempenho:** esta área está relacionada ao gerenciamento de falhas e tenta monitorar e controlar a rede para garantir que ela seja executada de forma eficiente. Conforme sustenta Forouzan (2010), esta área busca quantificar o desempenho de uma rede de computadores usando quantidades mensuráveis, como: capacidade, *throughput* (vazão), tráfego e

tempo de resposta (latência). A capacidade da rede deve ser monitorada, porque as redes possuem capacidades de infraestrutura, hardware e software limitadas; o tráfego também necessita de monitoramento interno e externo, medido pelo número de pacotes transmitidos (no tráfego interno) e pela troca de pacotes (no tráfego externo); o *throughput* de um dispositivo (roteador, por exemplo) pode ser medido para analisar a performance da rede; e o tempo de resposta é medido durante a transmissão e obedece a parâmetros mínimos de retorno. Adicionalmente, o *Jitter*, que é uma medida de variação no atraso da transferência de dados e a perda de pacotes também influenciam no desempenho da rede.

o  
Ver anotações

- **Gerenciamento de segurança:** é a área responsável pelo controle de acesso à rede e considera uma política de rede predefinida pela empresa. Tem relação com os sistemas de segurança computacional e prevê a utilização de sistemas de proteção à rede para monitoramento de ameaças e ataques. Neste gerenciamento, são consideradas questões de ameaças, ataques e vulnerabilidade de sistemas e utilizam-se dispositivos, como firewall, *Intrusion Detection Systems* (IDS), *Intrusion Prevention Systems* (IPS), sistemas de monitoramento e captura de dados de rede, como os farejadores, ou *sniffers*, e sistemas de monitoramento em geral.
- **Gerenciamento de contabilização:** é a área relacionada à quantificação do acesso e à utilização de recursos de rede pelos usuários, departamentos ou divisões. Este gerenciamento é importante para que usuários não monopolizem recursos da rede, impedir que o sistema seja utilizado de forma ineficiente e para que os administradores da rede possam analisar sua utilização e desenvolver planos sobre o uso da rede, conforme sua demanda. Firewalls, IDS, IPS, sistemas farejadores e monitoramento auxiliam também nesta atividade.

**ASSIMILE**

Os princípios do gerenciamento de rede são definidos por Kurose e Ross (2013) através de três atividades:

- **Coleta de dados:** refere-se à coleta de dados da rede, realizada por um sistema de *sniffing*, por exemplo.



- **Análise e diagnóstico:** refere-se à organização dos dados coletados na rede para tomada de decisão de forma manual ou utilizando softwares específicos.
- **Controle:** refere-se a ações para a gestão da rede, a fim de cessar, mitigar ou minimizar os impactos de informações trafegadas na rede.

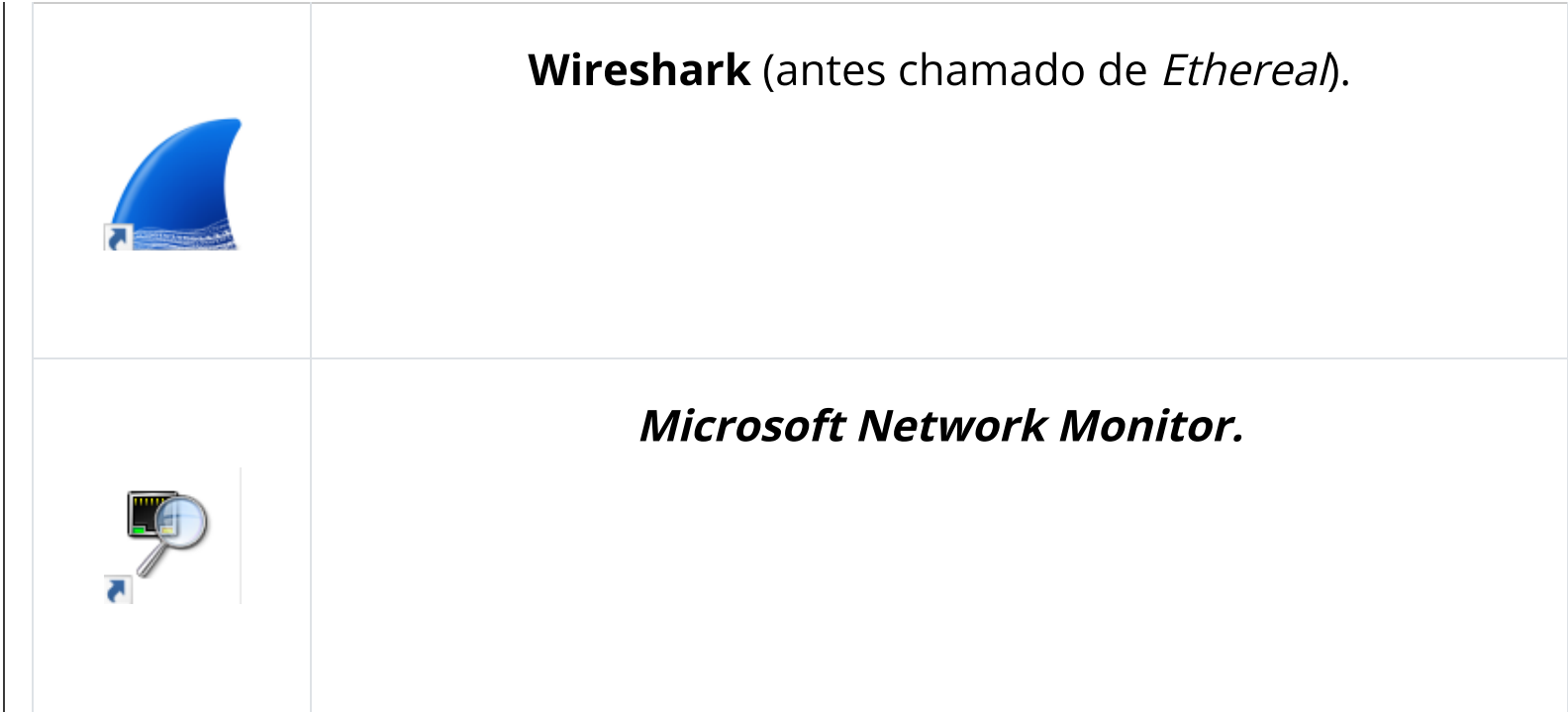
## ■ SNIFFER

Um sistema de *sniffing*, ou uma aplicação *sniffer*, é um aplicativo de software que busca realizar a análise e interceptação do registro de dados de um sistema de redes de computadores. São aplicativos que auxiliam os administradores de rede na análise do tráfego da rede e na checagem da sua performance mediante os parâmetros de operação estabelecidos. Estas ferramentas permitem também controlar o tráfego de um dispositivo de rede e capturar dados das transmissões nela realizadas. Os aplicativos que realizam estas atividades são chamados de farejadores e executam um algoritmo que captura fluxos de dados especificados pelos gestores de sistemas da empresa em sua configuração através de e-mail, login, texto e históricos de acesso à internet, por exemplo. A Figura 2.38 apresenta um exemplo de tela de uma ferramenta *sniffing*, o *Wireshark*.

Estas ferramentas representam, por um lado, um aliado ao gestor de redes de computadores, pois analisam e geram relatórios de análise da rede, porém também podem representar um ponto de atenção, porque representam uma ferramenta que impacta a vulnerabilidade de sistemas e trazem questões contra a segurança da rede.

### EXEMPLIFICANDO

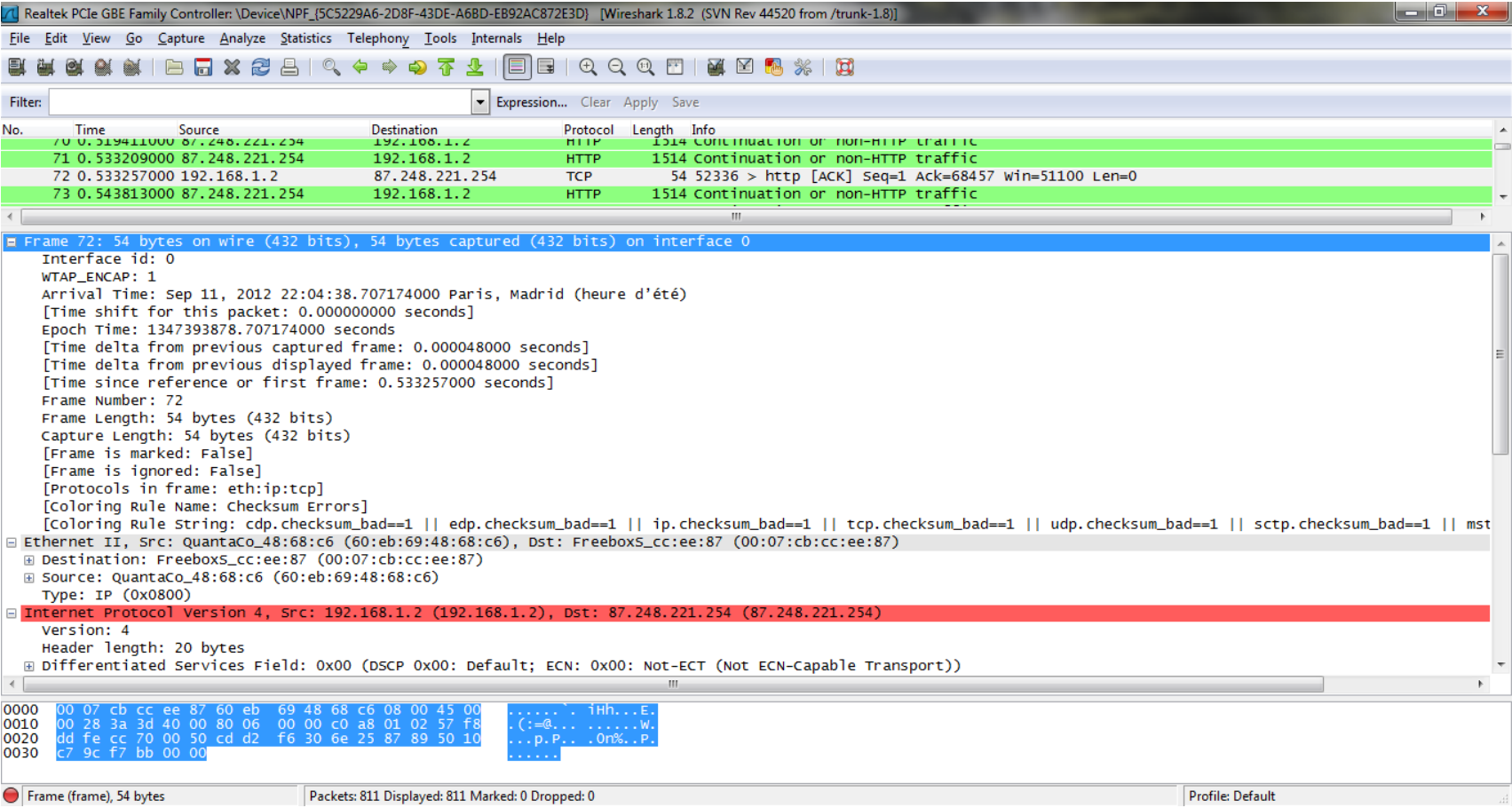
Alguns programas estão disponíveis para download e implantação de aplicativos de *sniffing* de forma livre. A seguir, apresenta-se dois exemplos de aplicativos que podem ser utilizados para análise e captura de dados da rede.



Ver anotações

A Figura 2.38 demonstra uma tela inicial da interface gráfica da ferramenta *Wireshark*. A ferramenta permite que se filtrem informações clicando nas interfaces ou informando-as.

Figura 2.38 | Tela de informações do *Wireshark*



Fonte: Wikimedia Commons.

▮ PADRÕES DE GERENCIAMENTO DE REDE

De acordo com Kurose e Ross (2013), os padrões de gerenciamento de rede começaram a amadurecer no final da década de 1980, sendo que o CMISE (*Common Management Service Element*), ou Elemento de Serviço de Gerenciamento Comum, e o CMIP (*Common Management Information Protocol*), ou Protocolo de Informação de Gerenciamento Comum, formavam o ISO CMISE/CMIP e o SNMP (*Simple Network Management Protocol*), ou Protocolo

Simples de Gerenciamento de Rede, e emergiram como os dois padrões mais importantes. O SMNP se tornou a estrutura de gerenciamento de rede mais usada e disseminada no mundo. Importante salientar que estes padrões de gerenciamento de redes são utilizados pelos profissionais de tecnologia da informação para análise de dados e tomada de decisões gerenciais, com o objetivo de manter uma infraestrutura de rede que garanta o QoS (*Quality of Services*), ou qualidade de serviços da rede.

o  
Ver anotações

### ■ SNMP (*SIMPLE NETWORK MANAGEMENT PROTOCOL*)

É um protocolo utilizado para realizar monitoramento de dispositivos e serviços de rede, que pode ser usado por dispositivos de diferentes arquiteturas e sistemas operacionais.

Defendido por Kurose e Ross (2013), ao contrário do que o nome possa sugerir, o gerenciamento de rede na internet é muito mais do que apenas um protocolo para transportar dados de gerenciamento entre uma entidade gerenciadora e seus agentes.

O SNMP é formado por quatro componentes básicos:

- **Agentes** ou **Dispositivo gerenciado**: são os nós (*host* ou roteador, impressora, etc.) gerenciados na rede de computadores.
- **Agente de Gerenciamento de rede**: são as estações de gerenciamento na rede.
- **MIB (*Management Information Base*)**: são as informações de gerenciamento da rede reunidas em um banco de dados com informações de configuração e status dos dispositivos gerenciáveis da rede.
- **SNMP**: é o protocolo propriamente dito de gerenciamento de rede instalado em dispositivos gerenciáveis da rede (computador, impressoras, câmeras IP, *switches*).

### ■ CMISE (*COMMON MANAGEMENT SERVICE ELEMENT*)

É formado por dois protocolos, o CMIS (*Common Management Information Service*), que define como os serviços serão oferecidos às aplicações de rede, e o CMIP (*Common Management Information Protocol*), que é um protocolo de



gerenciamento de referência, no qual as trocas das informações seguem a mesma estrutura entre o gerente e o agente nos processos de gerenciamento.

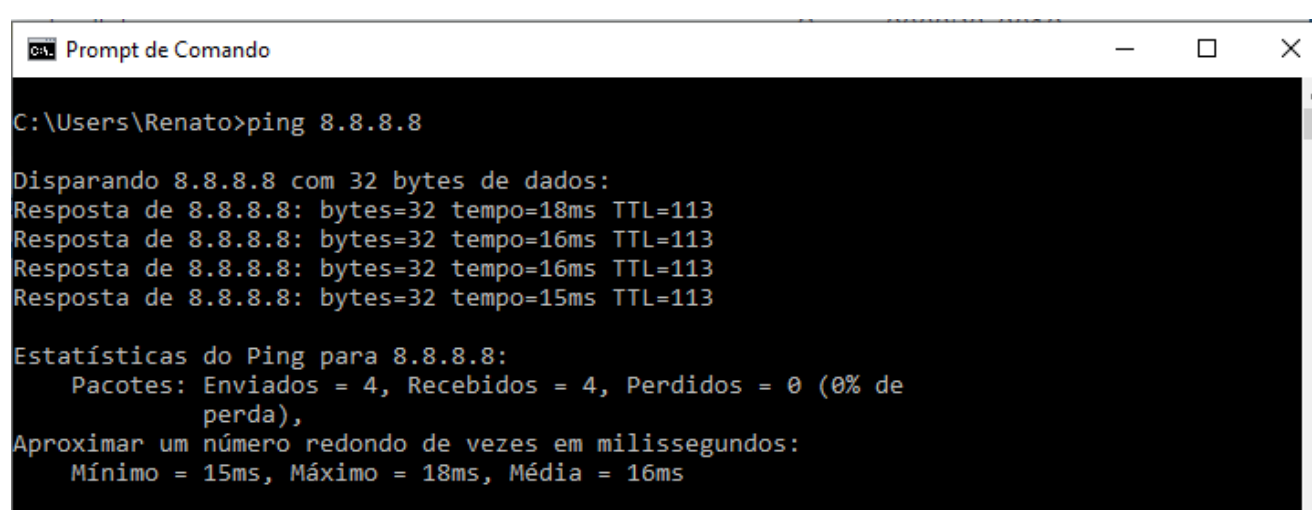
## COMANDOS PARA ANÁLISE E CONFIGURAÇÕES DE REDE

A análise e a configuração de redes de computadores fazem uso de comandos em *prompt* de comando nos sistemas operacionais Microsoft Windows e de distribuições Linux, para que pacotes de software sejam implementados no sistema e possam ser utilizados pelo administrador da rede para gerir os *host* e dispositivos de rede em geral e, assim, configurar hardware e software e gerenciar o tráfego na rede. A seguir, serão apresentados alguns comandos básicos de gestão de redes.

### PING

O comando **ping** é usado para testar a capacidade de um host de rede de se comunicar com outro. Ele retorna dados referente a um teste simples de conexão de rede e à qualidade de entrega de pacotes. A Figura 2.39 apresenta a saída do comando ping utilizado junto ao endereço IP (8.8.8.8) de um servidor do Google. Podem ser observadas informações sobre a conexão, como tempo de resposta e TTL (*Time To Live*) da mensagem, uma estatística de pacotes enviados como pacotes perdidos e a latência da rede, com mínimo, máximo e média.

Figura 2.39 | Exemplo de utilização do comando ping



```
C:\Users\Renato>ping 8.8.8.8

Disparando 8.8.8.8 com 32 bytes de dados:
Resposta de 8.8.8.8: bytes=32 tempo=18ms TTL=113
Resposta de 8.8.8.8: bytes=32 tempo=16ms TTL=113
Resposta de 8.8.8.8: bytes=32 tempo=16ms TTL=113
Resposta de 8.8.8.8: bytes=32 tempo=15ms TTL=113

Estatísticas do Ping para 8.8.8.8:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 15ms, Máximo = 18ms, Média = 16ms
```

Fonte: captura de tela do *prompt* de comando do sistema elaborada pelo autor.

### TRACERT

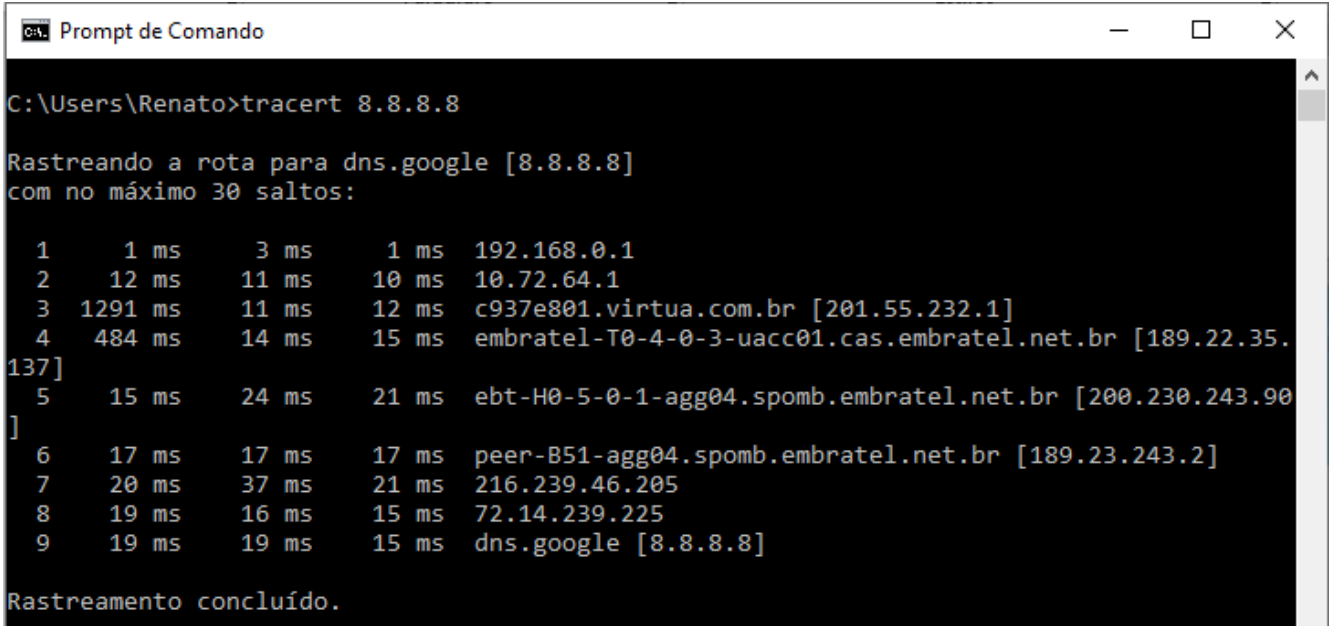
O comando **tracert** é semelhante ao ping, mas com a função adicional de enviar solicitações de eco do ICMP (*Internet Control Message Protocol*) e do TTL (*Time to Live*) da solicitação, para que se verifique a lista de roteadores pelos quais os

pacotes estão passando em cada salto. Este comando apresenta o caminho de um pacote percorrido na rede. Em distribuições Linux, utilize o comando **traceroute** para esta finalidade. A Figura 2.40 apresenta a saída do comando `tracert` utilizado junto ao endereço IP de um servidor do Google.

0

Ver anotações

Figura 2.40 | Exemplo de utilização do comando `tracert`

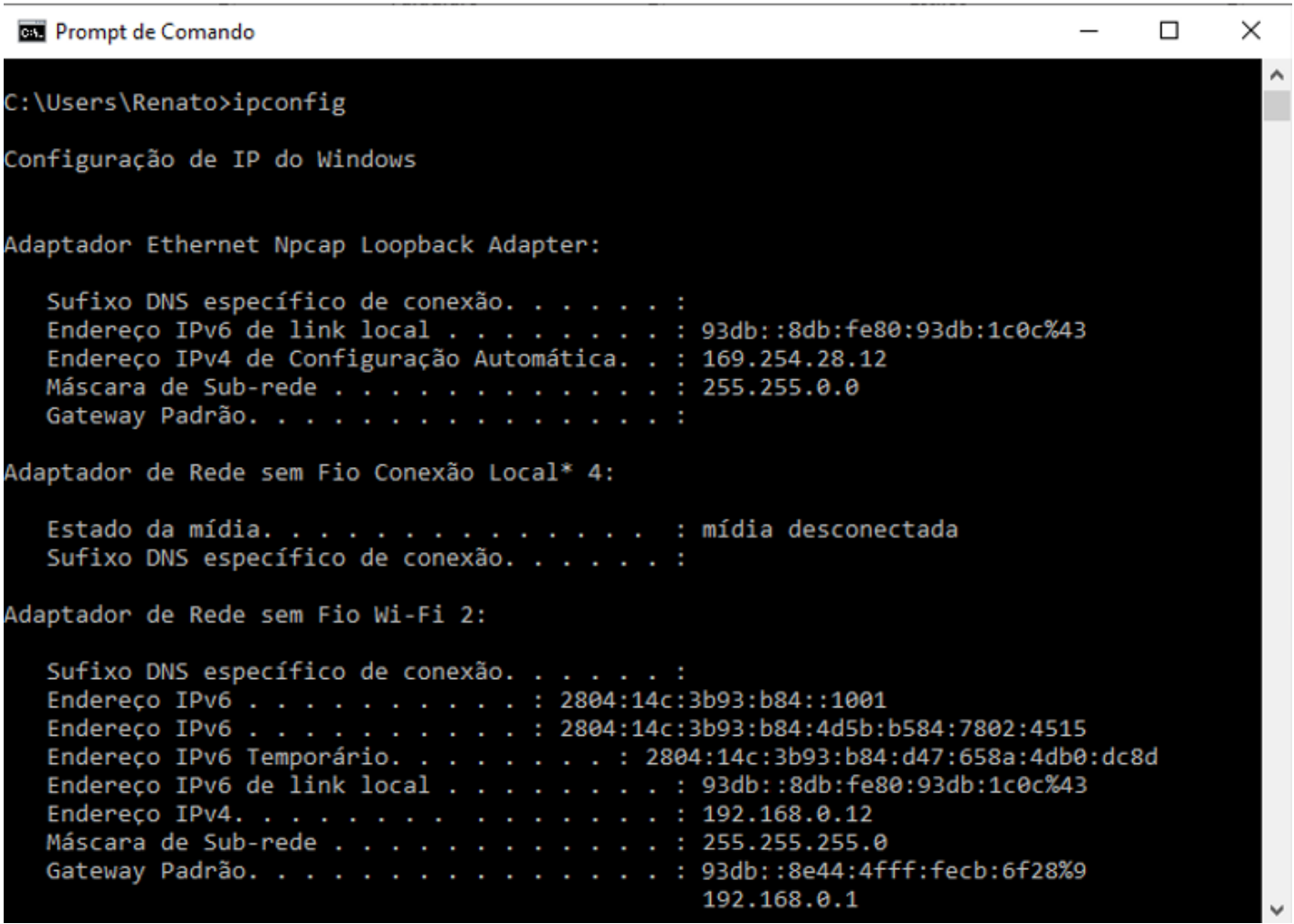


Fonte: captura de tela do prompt de comando do sistema operacional elaborada pelo autor.

■ IPCONFIG

O comando **ipconfig** exibe informações básicas de configuração do endereço IP do host. Pode-se utilizar a opção **ipconfig /all** para verificar informações detalhadas. Em distribuições Linux, utilize o comando `ifconfig` para realizar a operação realizada pelo `ipconfig` em sistemas Windows. A Figura 2.41 apresenta a saída do comando `ipconfig` utilizado no computador local. Veja que há um volume importante de informações de endereçamento do *host*, com o endereço IPv6, o endereço IPv4 de configuração automática, considerando que há um servidor de endereços no sistema (DHCP – *Dynamic Host Configuration Protocol*), a máscara de rede e o gateway padrão da rede, onde o host está se conectando localmente.

Figura 2.41 | Exemplo de utilização do comando `ipconfig`



Ver anotações 0

Fonte: captura de tela do *prompt* de comando do sistema operacional elaborada pelo autor.

HOSTNAME

O comando **hostname** retorna o nome do dispositivo (computador) local. A Figura 2.42 apresenta um exemplo de saída do comando **hostname** com o devido nome do *host* local.

Figura 2.42 | Exemplo de utilização do comando **hostname**



Fonte: captura de tela do *prompt* de comando do sistema operacional elaborada pelo autor.

NETSTAT

O comando **netstat** apresenta uma estatística da rede. Este comando possui várias funções, sendo que o comando **netstat -e** mostra um resumo das estatísticas da rede. A Figura 2.43 apresenta a saída do comando **netstat -e** com informações da rede. Veja que é apresentado um relatório com bytes recebidos e enviados, pacotes unicast, pacotes não unicast, descartados e erros. Com essas informações, o gestor pode reconhecer a performance da rede.

Figura 2.43 | Exemplo de utilização do comando **netstat**

Prompt de Comando

Estatísticas de interface

	Recebido	Enviado
Bytes	2519575000	404847110
Pacotes unicast	2174880	1366130
Pacotes não unicast	72440	31610
Descartados	0	0
Erros	0	0
Prot. desconhecidos	0	0

Fonte: captura de tela do *prompt* de comando do sistema operacional elaborada pelo autor.

■ NSLOOKUP

O comando **nslookup** apresenta um diagnóstico de problemas de resolução de nomes DNS (*Domain Name System*) apresentando o endereço IP do servidor DNS padrão do dispositivo. Conhecendo o nome do servidor DNS, pode-se digitar os nomes de *hosts*. Ele faz uma consulta de nomes de servidores de DNS na internet. A Figura 2.44 apresenta a saída do comando nslookup 8.8.8.8.

Figura 2.44 | Exemplo de utilização do comando netstat

Prompt de Comando

C:\Users\Renato>nslookup 8.8.8.8

Servidor: Unknown

Address: 2804:14d:1:0:181:213:132:2

Nome: dns.google

Address: 8.8.8.8

Fonte: captura de tela do *prompt* de comando do sistema operacional elaborada pelo autor.

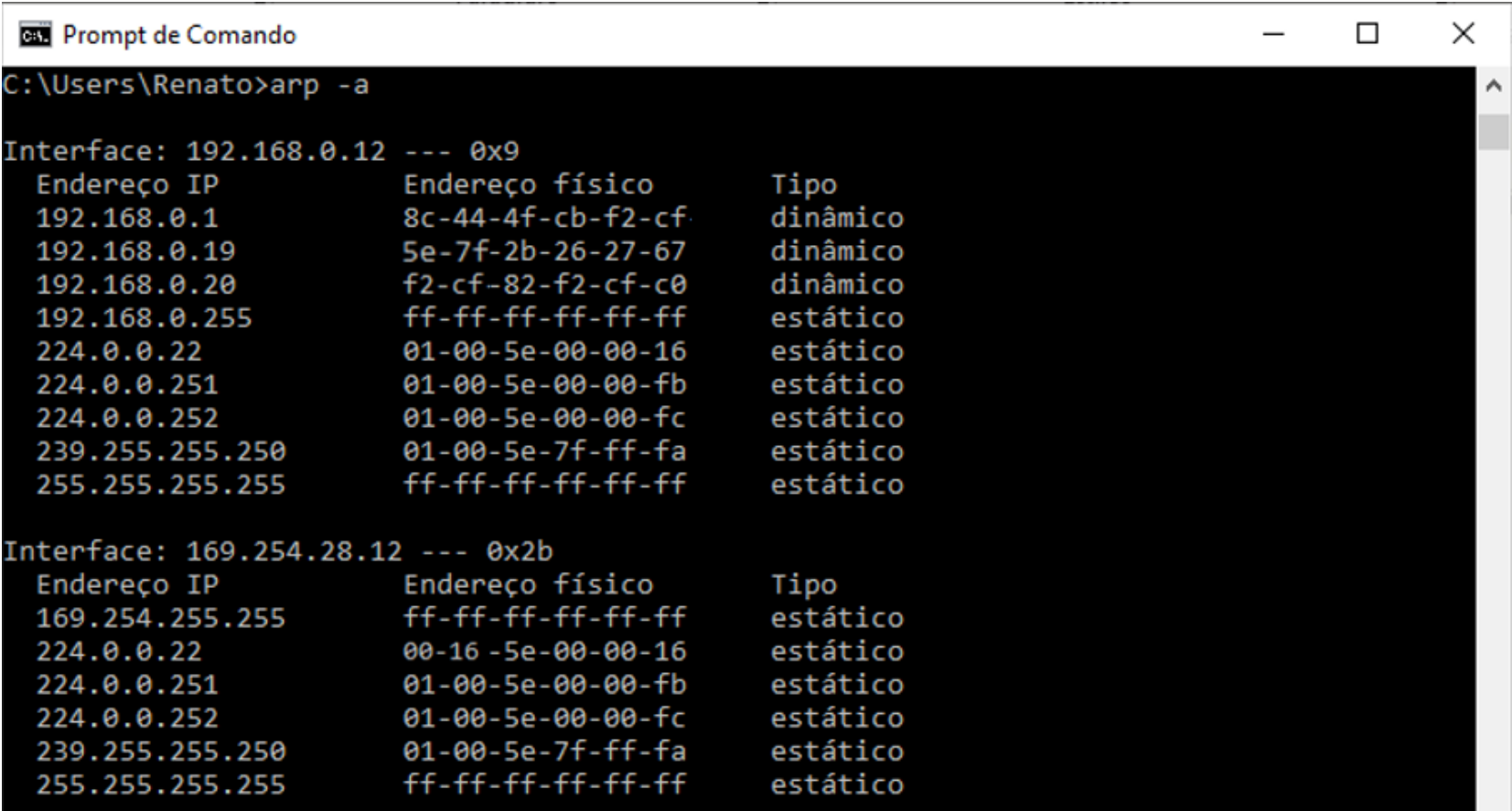
■ ARP

O comando **arp** corresponde a um protocolo de resolução de endereços através do mapeamento de endereços IP junto ao endereço MAC (*Media Access Control*). A Figura 2.45 apresenta a saída do comando arp com o mapeamento dos endereços lógicos (IP) e físicos (MAC) de um dispositivo.

Figura 2.45 | Exemplo de utilização do comando arp

0  
Ver anotações



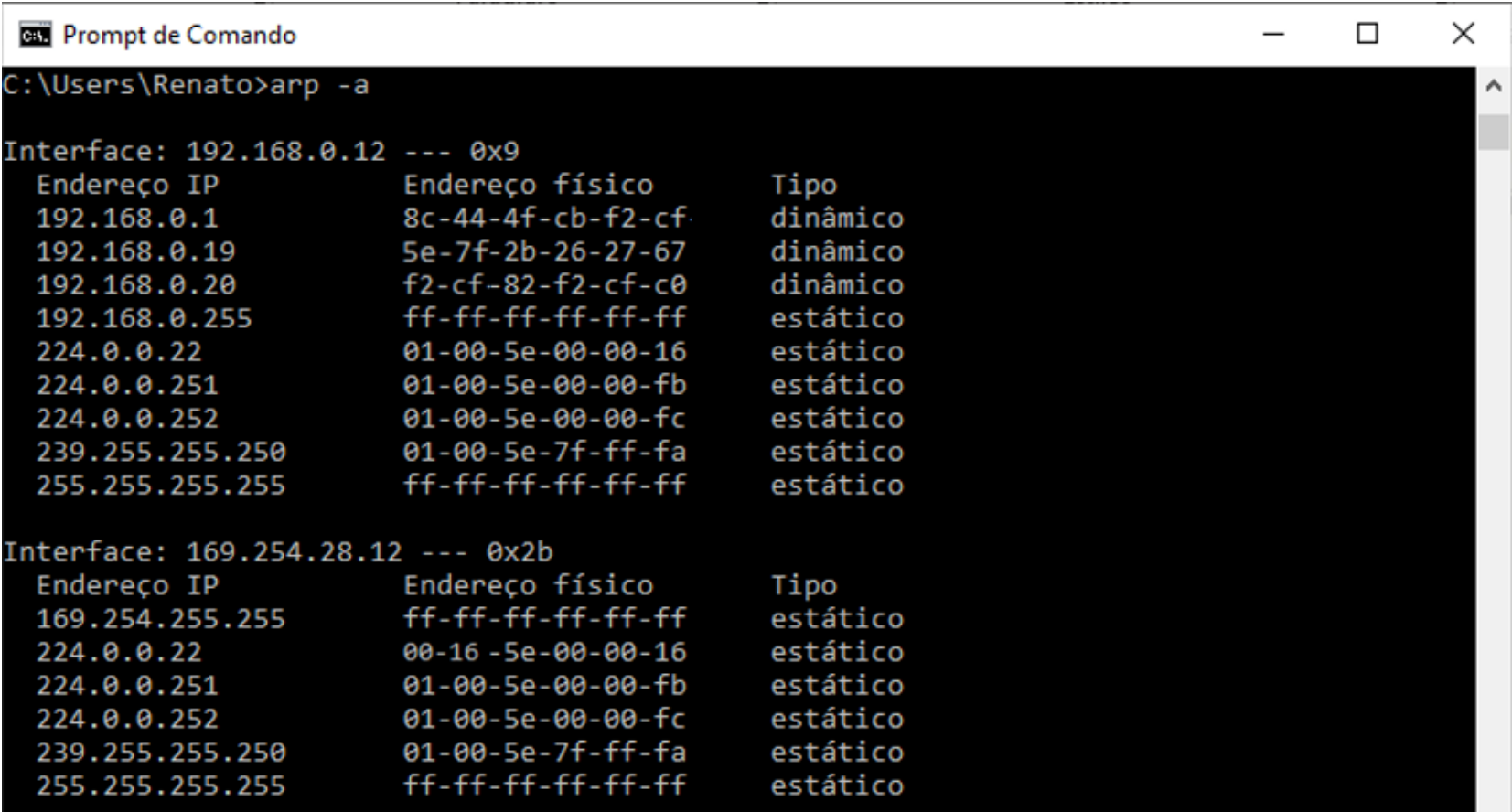


Fonte: captura de tela do *prompt* de comando do sistema operacional elaborada pelo autor.

ROUTE

O comando **route** exibe as tabelas de roteamento do dispositivo e permite observar informações de direcionamento de pacotes de uma sub-rede para outra. A Figura 2.46 apresenta a saída parcial de um comando **route print**, atributo que imprime as tabelas de roteamento local.

Figura 2.46 | Exemplo de utilização do comando route



Fonte: captura de tela do *prompt* de comando do sistema operacional elaborada pelo autor.

Ver anotações 0



Aqui, apresentamos alguns comandos básicos para análise e configuração de dados de rede, porém ainda há diversos outros comandos e sistemas operacionais que podem ser utilizados na configuração e gestão de redes de computadores.

INDICADORES DE GERÊNCIA DE DESEMPENHO, CONFIGURAÇÃO, CONTABILIZAÇÃO E QOS (QUALITY OF SERVICES)

Conforme define Comer (2016), as principais medidas de desempenho de uma rede de computadores são: **latência** ou atraso, **throughput**, vazão, capacidade ou taxa de transferência e **jitter** ou variação da latência. Outros indicadores também são importantes, como **perda de pacotes e disponibilidade**.

LATÊNCIA OU ATRASO

A primeira propriedade das redes que pode ser medida quantitativamente é latência ou atraso. A **latência** especifica quanto tempo leva para os dados viajarem através da rede de um computador para outro, medida em frações de segundo. Ela pode ser também considerada como o intervalo de tempo durante a emissão e a confirmação de recebimento de um pacote na rede. Há diversos fatores que impactam na latência de uma rede. O Quadro 2.9 apresentado a seguir mostra os tipos de atraso em uma rede de computadores.

Quadro 2.9 | Tipos de atraso

Tipo de atraso	Definição
Propagação	Tempo necessário para deslocamento no meio físico da rede.
Acesso	Tempo necessário para obtenção de acesso ao meio físico (cabo de rede, por exemplo).
Comutação	Tempo necessário para processamento do encaminhamento de um pacote na rede.
Enfileiramento	Tempo necessário que um pacote gasta na memória de um comutador de rede ou um roteador da rede esperando a transmissão.

0  
Ver anotações

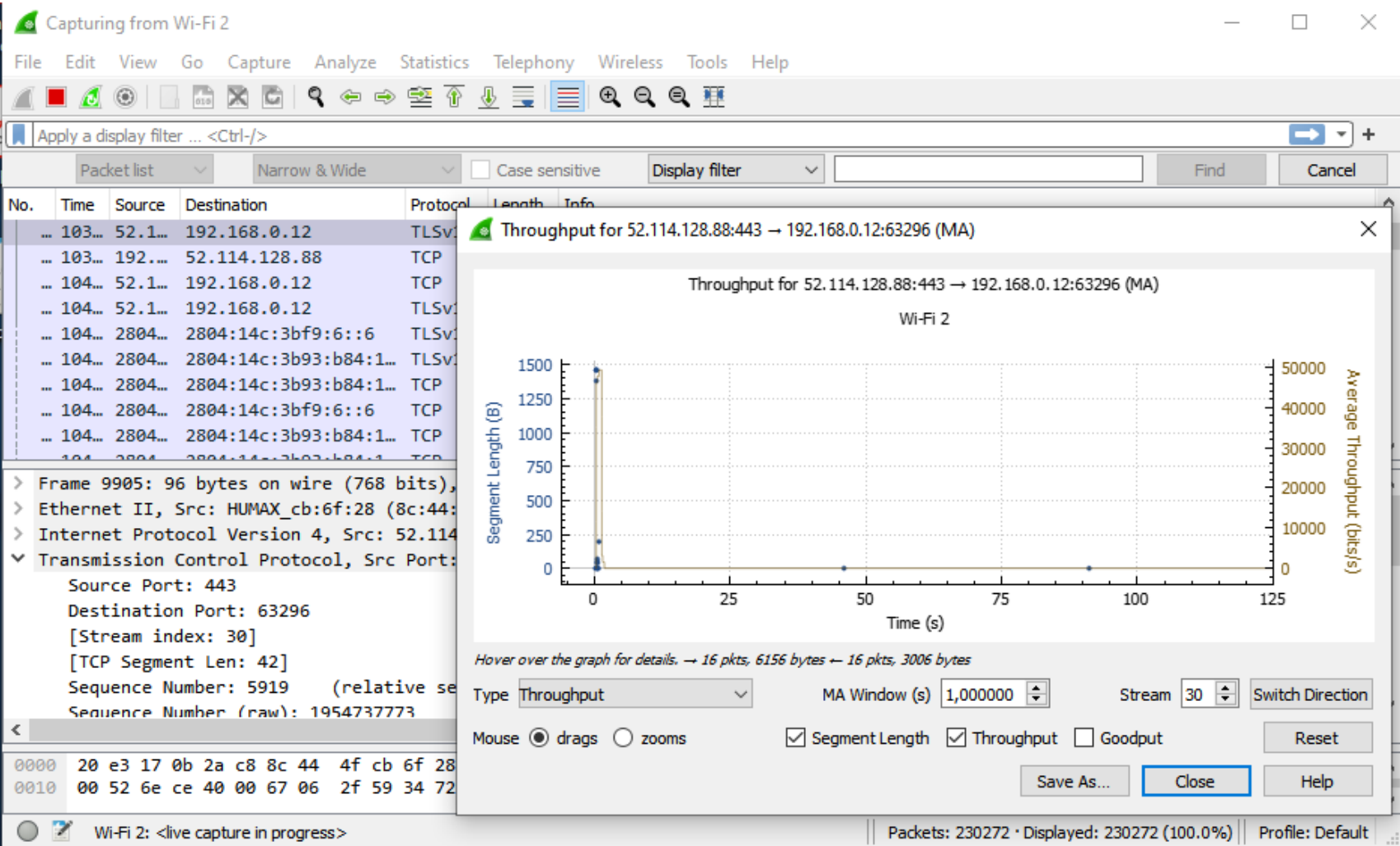
Tipo de atraso	Definição
Servidor	Tempo necessário para um servidor da rede enviar uma resposta a uma requisição de um <i>host</i> na rede.

Fonte: adaptado de Comer (2016, p. 412).

THROUGHPUT

Comer (2016) define a taxa de transferência ou **throughput** como uma medida da velocidade na qual os dados podem ser enviados através da rede, em bits por segundo (bit/s). Os fatores que influenciam no *throughput* da rede são: topologia da rede, número de usuários da rede e taxa de interfaces de rede. A Figura 2.47 apresenta um exemplo de mensuração de *throughput* de rede realizado através da ferramenta *Wireshark*.

Figura 2.47 | *Throughput* em uma rede medida pela aplicação *Wireshark*



Fonte: captura de tela da ferramenta *Wireshark* elaborada pelo autor.

ASSIMILE

A maioria das redes de comunicação de dados oferece uma taxa de transferência de mais de 1 Mbit/s, e as redes de maior velocidade operam mais rápido do que 1 Gbit/s. Casos especiais surgem quando uma rede tem

Ver anotações

uma taxa de transferência inferior a 1 kbit/s.

## ■ JITTER

O **jitter** é uma medida de variação no atraso da transferência de dados. Ela se tornou importante mediante as novas tecnologias de comunicação baseadas em streaming, com a transferência de voz e vídeos em tempo real via internet. Duas redes podem ter o mesmo atraso médio, mas diferentes valores de *jitter*. Por exemplo, se todos os pacotes que percorrem uma determinada rede têm o mesmo atraso X de um pacote e Y de outro pacote, a rede não tem *jitter*. Porém, se os pacotes alternam entre atrasos diferentes (com um atraso X de um pacote diferente de um atraso Y de outro pacote), a rede tem a mesma média de atraso, mas tem um *jitter* diferente.

Como um exemplo de importância da análise de *jitter*, considere que as transmissões de voz ou vídeo via internet devem utilizar um protocolo que compensa o *jitter*. Como o uso de protocolos em tempo real é mais econômico do que a construção de uma rede isócrona (onde há envio de mensagens ininterruptamente com intervalos conhecidos e fixos), as empresas de telefonia estão atenuando os requisitos rigorosos de redes isócronas.

### REFLITA

Conforme afirma Comer (2016), medir o desempenho da rede pode ser surpreendentemente difícil por quatro motivos:

- As rotas podem ser assimétricas.
- As condições podem mudar rapidamente.
- A própria medição pode afetar o desempenho.
- O tráfego é em rajadas.

Ao contrário do tráfego telefônico de voz, o tráfego de dados ocorre em rajadas.

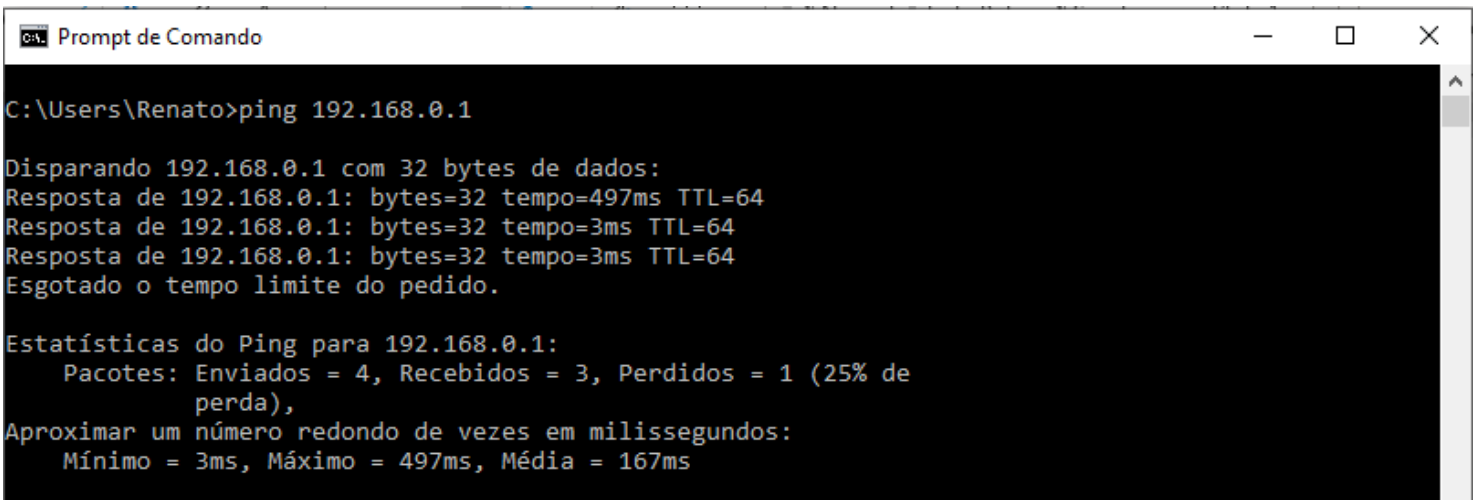
O desempenho de uma rede de computadores é considerado estável dentro do que se chama de redes convergentes, nas quais redes de dados e redes de telefonia estão operando através de linhas de distribuição de

dados unificada?

PERDA DE PACOTES

A perda de pacotes na rede refere-se à situação em que se encaminham informações pela rede, porém estas não respondem com a totalidade da sua entrega. Pode ocorrer devido à capacidade de armazenamento de pacotes nos roteadores, considerando que estes possuem capacidade de memória limitada. É possível verificar a resposta de perda de 25% dos pacotes enviados através do comando ping 192.168.0.1 no teste de rede apresentado na Figura 2.48.

Figura 2.48 | Perda de pacotes na rede



Fonte: captura de tela do *prompt* de comando do sistema operacional elaborada pelo autor.

EXEMPLIFICANDO

Redes padrão Ethernet (802.3) são baseadas em conexões realizadas através de enlaces físicos por cabos. Os cabos metálicos de par trançado UTP (*Unshield Twisted Pair*) é o tipo mais comum em redes locais e possuem comprimento limitado (100 metros), para garantir a qualidade do sinal eletromagnético. A instalação adequada dos cabos dentro dos limites de comprimento estabelecidos, assim como os graus de curvatura que são submetidos, influenciam na perda de pacotes em uma rede.

Outra medida importante para prevenir a perda de pacotes é a escolha adequada do padrão de rede Wi-Fi (802.11), que possui diversas especificações, com diferentes faixas de frequência e cobertura. Por exemplo, uma rede 802.11ac trabalha na faixa de frequência de 5,8 GHz, velocidade de até 1,3 Gbps e possui menor distância de operação e menor capacidade de transpassar obstáculos, o que pode ocasionar perda de

o  
Ver anotações

pacotes na rede. Outro padrão recente é o 802.11ad, com frequência de 60 GHz, que possui maior dificuldade para transpassar obstáculos devido à alta frequência.

## ■ DISPONIBILIDADE

Como sustenta Comer (2016), as redes de computadores são compostas por diversos equipamentos, como nodos, computadores, servidores, cabeamentos, entre outros, e todos esses dispositivos podem sofrer algum tipo de falha. A **disponibilidade** de uma rede é a capacidade que seus equipamentos possuem de manterem-se em operação de forma ininterrupta dentro de um determinado período de tempo.

Alguns conceitos referentes à disponibilidade de uma rede de computadores são:

- **Mean Time Between Failures (MTBF):** ou tempo médio entre falhas, é uma previsão por modelo estatístico/matemático do tempo médio entre as falhas. É útil para prever as manutenções necessárias dentro de um sistema de redes de computadores. Para o cálculo, utiliza-se a fórmula:

$$\text{MTBF} = \sum (\text{FINAL} - \text{INICIAL}) / \text{NÚMERO DE FALHAS}$$

- **Mean Time to Repair (MTTR):** ou tempo médio para reparos, é uma previsão por modelo estatístico/matemático do tempo médio para se realizar o reparo da rede após a ocorrência de uma falha. Para o cálculo, utiliza-se a fórmula:

$$\text{MTTR} = \text{TEMPO DE PARADA POR FALHA} / \text{NÚMERO DE FALHAS}$$

- **Mean Time to Failure (MTTF):** ou tempo médio para falha, é o tempo de vida de uma rede que compreende os períodos alternados de operação de falhas. Este termo é utilizado para efetuar o cálculo de disponibilidade de uma rede de computadores por meio da função de frequência com que as falhas ocorrem e do tempo necessário para reparo, definido pela fórmula:

$$D = \text{MTTF} / (\text{MTTF} + \text{MTTR})$$

Por exemplo: considere que um sistema de rede de computadores possui um MTTF de 8.760 horas de operação no ano (referente a um sistema que opera 365 dias por 24 horas) e um MTTR de 288 horas anual (com sistema off-line 12 dias por ano). Nesse caso:



$$D = \text{MTTF} / (\text{MTTF} + \text{MTTR})$$

$$D = 8760 / (8760 + 288)$$

$$D = 96,816$$

A disponibilidade da rede é de 96,82% ao ano.

## ■ QOS (QUALITY OF SERVICE)

Comer (2016) define que o objetivo da medição de redes é o provisionamento da rede: projetar uma rede para fornecer um nível específico de serviço e, em termos gerais, isto é conhecido como Qualidade de Serviço, ou **Quality of Service (QoS)**. Ela pode ser vista como o conjunto de regras, mecanismos e tecnologias que objetivam a utilização eficaz do sistema. Como vimos anteriormente, os fatores que influenciam na performance da rede são a latência, o *jitter*, a perda de pacotes e a largura de banda disponível. O QoS busca garantir ao usuário ou gestor da rede de computadores controle adequado sobre sua estrutura de rede. Uma aplicação de utilização de QoS é determinar quais dispositivos da rede e quais serviços de rede precisam de prioridade na conexão.

O atendimento às necessidades de performance dos sistemas de redes de computadores, a QoS, utiliza-se de dois modelos conceituais:

- **IntServ:** utiliza o fluxo dos dados por meio do protocolo no caminho que a mensagem deve percorrer e garante o envio e recebimento de mensagens fim a fim.
- **DiffServ:** utiliza uma marcação no pacote transmitido pela rede para classificá-lo e efetuar os tratamentos necessários de forma independente para os pacotes.

De acordo com Comer (2016), o IETF (*Internet Engineering Task Force*) criou uma série de tecnologias e protocolos relacionados à QoS. Os três mais significativos são: RSVP/COPS (*Resource ReSerVation Protocol / Common Open Policies Services*), DiffServ e MPLS (*Multiprotocol Label Switching*).

- **RSVP/COPS:** modelo baseado no IntServ, no qual o IETF desenvolveu dois protocolos para fornecer QoS: o protocolo de reserva de recursos (RSVP) e os serviços abertos de políticas comuns (COPS). O RSVP é uma versão de QoS, em

que a reserva de recursos é necessária para cada sessão TCP ou UDP. O COPS é um protocolo usado conjuntamente com o RSVP para especificar e aplicar políticas.

- **DiffServ:** uma vez abandonados os IntServ, o IETF criou os serviços diferenciados (*DiffServ, ou Differentiated Services*) para definir um mecanismo de QoS que define como as classes podem ser especificadas para o cabeçalho IPv4 ou IPv6, para especificar a classe de um datagrama.
- **MPLS:** é um mecanismo de comunicação orientado à conexão construído em cima do IP. Para usar o MPLS, um gerente configura caminhos de encaminhamento através de um conjunto de roteadores com o MPLS habilitado.

A análise da performance da rede que considera a qualidade dos serviços, a disponibilidade da rede, a capacidade de processamento e o armazenamento é determinada pelo termo *Service Level Agreement* (SLA), ou seja, um acordo de nível de serviço definido e medido constantemente.

## ■ INTRODUÇÃO AO VLAN *TRUNK* PROTOCOL

O VLAN *Trunk Protocol* (VTP) é um protocolo de camada 2 (inter-rede), desenvolvido pela Cisco e utilizado para configuração de *Virtual Local Area Network* (VLAN), com o objetivo de facilitar a administração dos sistemas. Este protocolo define uma estrutura do tipo cliente-servidor, na qual as alterações são feitas necessariamente no servidor e replicadas aos clientes da rede. Importante apontar que esta técnica é utilizada por administradores de redes para melhorar o controle do sistema.

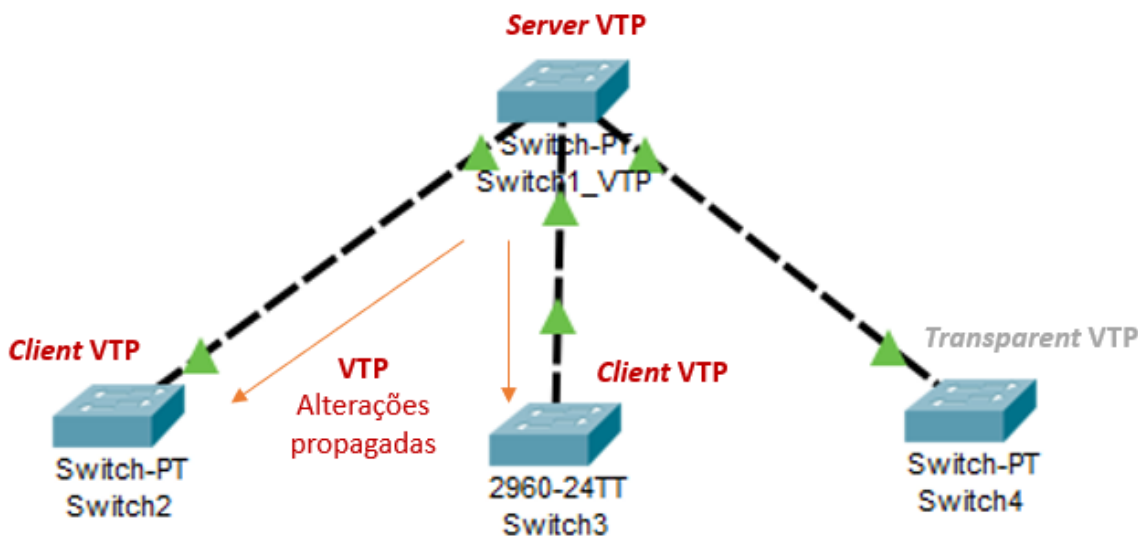
### ASSIMILE

Uma VLAN é uma forma de criar sub-redes virtuais em uma estrutura de rede local implementada em switches, onde cada interface de rede (*host*) pode se comportar como uma VLAN e definir seu próprio domínio de *broadcast*.

Com a utilização do VLAN *Trunk Protocol*, o trabalho de configuração de redes locais virtuais é reduzido, pois o gestor da rede configurará apenas um *switch*, que será o responsável pela função de distribuir e sincronizar as informações para os outros *switches* da rede. Esta tecnologia oferece redução de atividades de configuração e reconfiguração e minimização de erros através da centralização das configurações em um switch chamado de VLAN *Trunk Protocol* Server. Na VLAN, nos switches que fazem parte de uma rede com VLAN, as tabelas de roteamento são atualizadas, isso porque as VLANs são criadas na interface de rede do *switch*. A estrutura de uma rede configurada com o VLAN *Trunk Protocol* é:

- **Server VTP**: dispositivo responsável por criar, deletar, renomear e definir o domínio e as configuração das VLANs.
- **Client VTP**: dispositivos que compõem a VLAN, porém não podem configurá-la.
- **Transparent VPT**: *switch* com VLANs configuradas manualmente, que não participa do VTP.

A Figura 2.49 mostra uma estrutura formada pelo VLAN *Trunk Protocol* (VTP).



Fonte: elaborada pelo autor.

REFLITA

Caso um administrador de redes tenha desejo de implementar redes locais virtuais, ele deverá fazer a configuração manualmente em cada *switch* da rede. Isto é simples em uma rede com dois ou três *switches*, porém se torna inviável em uma rede maior, com uma estrutura mais complexa e suscetível a erros de configuração.

O VTP pode ser a tecnologia adequada para gestão de redes com múltiplos switches?

## ■ ACESSO REMOTO – SERVIDOR SSH

O protocolo de rede SSH (*Secure Socket Shell* ou *Secure Shell*) permite que se faça comunicação com segurança (criptografada) entre um *host* cliente e um servidor de rede, permitindo fazer o gerenciamento de dados e informações deste servidor de forma remota (em local físico diferente de sua localização). Através do SSH, um usuário ou gestor da rede pode fazer *login* em outro computador da rede e executar comandos como se estivesse diretamente operando um sistema servidor local. A interface é realizada através de um Shell remoto, que executa os comandos digitados e faz a ponte entre a máquina do usuário e o servidor remoto

Os comandos de interação são realizados através de um terminal, chamado de *Shell*, responsável pela interpretação dos comandos do usuário junto ao sistema operacional de rede. Trata-se de um serviço que possui um protocolo que estabelece a administração remota de um servidor. É baseado em interação via texto, porém sua utilização é simples, através de um conjunto de recursos que permitem desde a transferência de arquivos entre cliente e servidor até a instalação e configuração de serviços de gerenciamento de redes de forma remota.

O SSH é originalmente desenvolvido para sistemas operacionais, UNIX, adaptados em distribuições baseadas em Linux. No entanto, também é possível utilizá-lo em sistemas operacionais baseados em plataforma Windows com aplicativos adicionais e a partir da sua versão 10 sem utilização de aplicações complementares.

O comando SSH segue a seguinte estrutura:

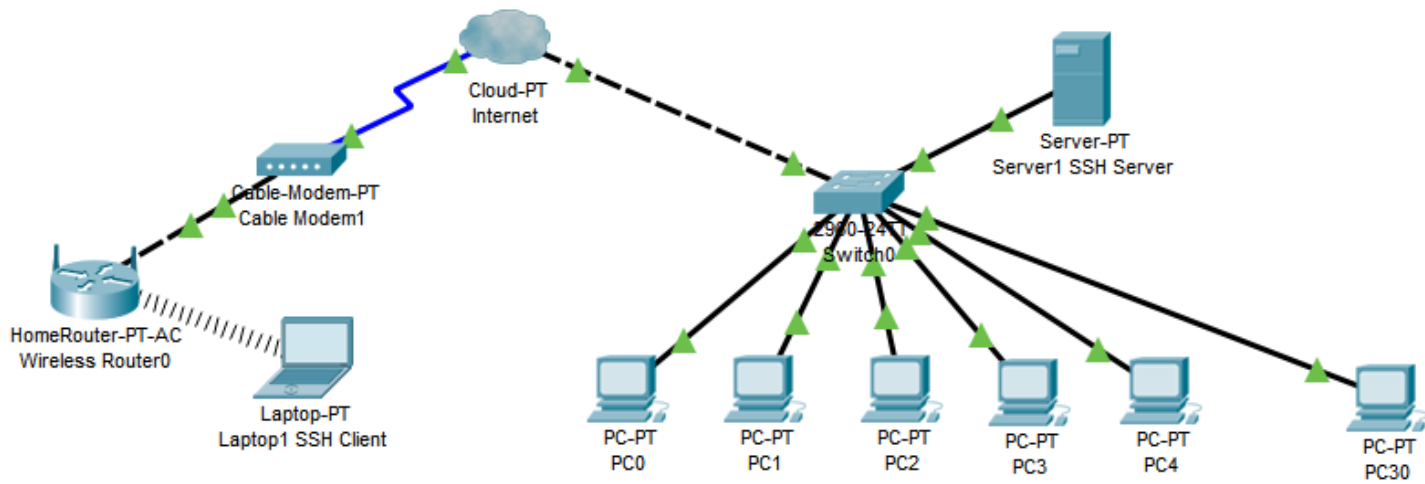
### ■ SSH *USER@HOST*

- **ssh**: indica o uso do comando para abertura de conexão remota criptografada.
- **user**: exemplificado como a conta à qual se deseja conectar remotamente (necessário ter direitos de administrador (Windows) e *root* (Linux)).
- **host**: indica o computador que se deseja acessar, identificado através do endereço IP ou nome de domínio.

Após a digitação do comando para inicialização dos serviços de SSH, será necessário informar nome de usuário e senha de acesso à conta, definidos no servidor SSH em um sistema operacional de rede. A Figura 2.50 apresenta um exemplo de conexão de SSH realizada pelo *Laptop-1 SSH Client* com um *SSH Server* em uma localização física diferente.

Ver anotações

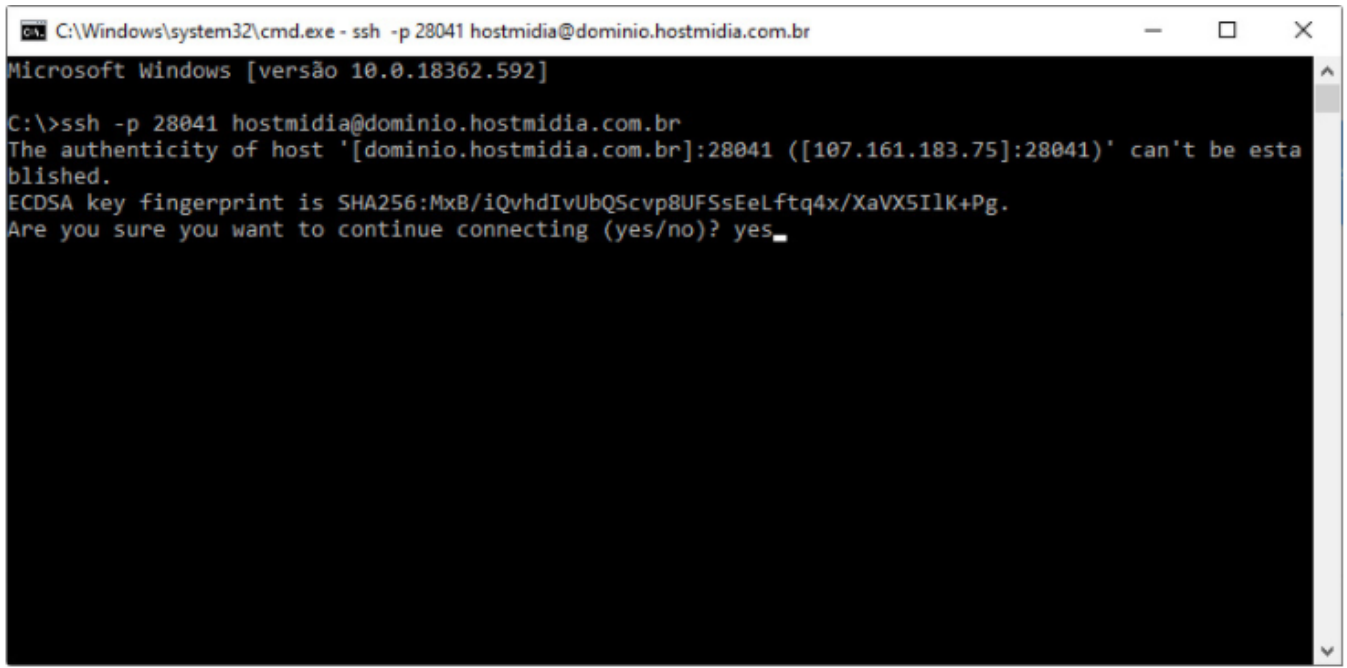
Figura 2.50 | SSH Conexão remota com SSH



Fonte: elaborada pelo autor.

A seguir, a Figura 2.51 apresenta um exemplo de utilização de cliente SSH para acesso remoto a um servidor determinado.

Figura 2.51 | SSH Cliente no Windows 10



Fonte: Hostmidia.

EXEMPLIFICANDO

Para habilitar a ferramenta SSH no Windows, siga os seguintes passos:

- 1. Abra as configurações do Windows.
- 2. Acesse Aplicativos.



3. Clique em “Aplicativos e Recursos”.
4. Clique em “Recursos Opcionais”.
5. Selecione o OpenSSH, caso não apareça.
6. Clique em “Adicionar um recurso”; Localize “Cliente OpenSSH”, caso deseje instalar o cliente ou “Servidor OpenSSH” para o servidor e clique em Instalar.

Para utilizar o SSH, é necessário que se tenha acesso à internet e privilégios de administrador. Se for distribuição Linux, deverá ter acesso como *root* (administrador). Os dados de acesso como conta do usuário, senha e porta do servidor também são necessários para que se realize uma conexão SSH.

Para melhor compreender a instalação e execução do Open SSH no Windows 10, você pode visitar o site da Microsoft com as devidas orientações e a página *OpenSSH*.

Outras ferramentas para implementação de SSH:

- **PuTTY: cliente SSH para a plataforma Windows e Unix (Linux).**
- **SmarTTY: um cliente SSH.**
- **XShell: clientes SSH versátil.**

Esta unidade buscou trazer conceitos importantes sobre o gerenciamento de redes de computadores e a aplicação de comandos e ferramentas para verificação, análise e gerenciamento de redes, observando informações de configuração de dispositivos da rede e o seu tráfego. Estas ferramentas são importantes para que o profissional de tecnologia da informação possa conceber e operar sistemas de redes de computadores, porém com naturalidade, visto que não abarca todo o conhecimento necessário para uma gestão completa de redes. Neste cenário, bibliografias complementares e ferramentas foram sugeridas para que você possa se aprofundar na área de redes de computadores e se tornar um profissional de excelência.

A utilização de comandos e aplicativos para configuração e gestão de redes de computadores não se restringe aos exemplos dados e pode ser conhecida com maiores detalhes em literaturas específicas de cada plataforma operacional.

Para configurações de sistemas Windows, pode ser consultado o livro *Configuração do Windows Server 2008: infraestrutura de rede*, de T. Northrup e J. C. Mackin, disponível na biblioteca virtual.

Para configurações de sistemas Linux, pode ser consultado o livro *Manual completo do Linux: guia do administrador*, de Eve Nemeth, Garth Snyder e Trent R. Hein, disponível na biblioteca virtual.

Para configurações de sistemas Linux, pode ser consultado o livro *Dominando o Linux: Red Hat e Fedora*, de Bill Ball e Hoyt Duff, disponível na biblioteca virtual.

Para conhecimento de projeto de interconexão de redes, pode ser verificado o livro *Projeto de Interconexão de redes: Cisco Internetwork Design – CID*, de Matthew Birkner, disponível na biblioteca virtual.

Considerando a segurança dos sistemas nas áreas onde tem Wi-Fi, a escolha do equipamento com recursos providos e configuráveis é importante. Sugerimos a leitura do texto *Porque você precisa se preocupar com o gerenciamento do Wi-Fi na sua empresa*, da página Olhar Digital (2017).

#### PESQUISE MAIS

Para contribuir com a compreensão e o uso de ferramentas de gerenciamento de redes, é sugerida a leitura das informações do texto *Conheça as Principais Ferramentas de Gerenciamento de Redes de Mercado*, de Marcelo Brenzink do Nascimento.

Para realizar análise de performance e gerenciamento de redes, é importante a utilização de ferramentas de software. Fica a sugestão para conhecer as seguintes ferramentas:

#### 1. **Wireshark**

0

Ver anotações

- 2. **Capsa.**
- 3. **Microsoft Network Monitor.**
- 4. **SLAView.**
- 5. **Zenoss.**
- 6. **Cisco Prime Network Analysis.**

0  
Ver anotações

FAÇA VALER A PENA

Questão 1

Forouzan (2010) define **gerenciamento de redes** como o monitoramento, o teste, a configuração e o diagnóstico de componentes de rede para atender a um conjunto de exigências definidas por uma organização. As exigências relacionam-se com a operação estável e eficiente da rede que fornece a qualidade predefinida de serviços aos seus usuários. Este gerenciamento relaciona-se a cinco áreas: configuração, falhas, desempenho, segurança e contabilização.

Assinale a alternativa que corresponde à área de gerenciamento de redes que monitora e controla a rede para garantir que ela esteja rodando de forma eficiente. Esta área avalia variáveis mensuráveis, como: capacidade, chamada de *throughput* ou vazão, tráfego e tempo de resposta.

- a. Gerenciamento de configuração.
- b. Gerenciamento de falhas.
- c. Gerenciamento de desempenho.
- d. Gerenciamento de segurança.
- e. Gerenciamento de contabilização.

Questão 2

A análise e a configuração de redes de computadores fazem uso de comandos em *prompt* de comando nos sistemas operacionais Microsoft Windows e de distribuições Linux, para que pacotes de software sejam implementados no sistema e possam ser utilizados pelo administrador da rede para gerir os host e dispositivos de rede em geral e, assim, configurar hardware e software e gerenciar o tráfego na rede. Um dos comandos de gestão de redes emite o rastreamento de

rota para um determinado endereço de IP (*Internet Protocol*), conforme apresentado na figura a seguir.



Fonte: elaborada pelo autor.

Assinale a alternativa que apresenta o comando para saída de dados com o rastreamento da rota para o servidor dns.google, conforme a figura apresentada:

- a. `ping 8.8.8.8.`
- b. `tracert 8.8.8.8.`
- c. `Ipconfig /all.`
- d. `hostname 8.8.8.8.`
- e. `netstat -e.`

Questão 3

O gerenciamento de uma rede de computadores toma como parâmetro alguns indicadores quantitativos de performance na rede. Conforme define Comer (2016), as principais medidas de desempenho de uma rede de computadores são:

**latência, throughput e jitter**, porém outros fatores também são quantificados e utilizados para medir a performance da rede.

Avalie as assertivas apresentadas a seguir e sua relação com a performance de uma rede de computadores:

- I. A perda de pacotes na rede refere-se a não entrega de dados durante a transmissão na rede e pode ocorrer devido à capacidade de armazenamento de pacotes nos roteadores, considerando que estes possuem capacidade de

Ver anotações

memória limitada.

II. A latência é uma medida de variação no atraso da transferência de dados. Esta medida se tornou importante mediante as novas tecnologias de comunicação baseadas em *streaming*, com a transferência de voz e vídeos em tempo real via internet. Duas redes podem ter o mesmo atraso médio, mas diferentes valores de *jitter*. Por exemplo, se todos os pacotes que percorrem uma determinada rede têm o mesmo atraso, X e Y, a rede não tem *jitter*. Porém, se os pacotes alternam entre atrasos diferentes (com X diferente de Y), a rede tem a mesma média de atraso, mas tem um *jitter* diferente.

III. Taxa de transferência ou *throughput* é uma medida da velocidade por meio da qual os dados podem ser enviados através da rede, em bits por segundo (bit/s). Os fatores que influenciam no *throughput* da rede são: topologia da rede, número de usuários da rede e taxa de interfaces de rede.

IV. O *jitter* especifica quanto tempo leva para os dados viajarem através da rede de um computador para outro; ela é medida em frações de segundo. A latência pode ser também considerada como o intervalo de tempo durante a emissão e confirmação de recebimento de um pacote na rede.

Sobre indicadores de desempenho de redes de computadores, é correto o que se encontra nas assertivas:

a. I, II, III e IV.

b. II, III e IV, apenas.

c. I, III e IV, apenas.

d. I e III, apenas.

e. II e III, apenas.

## REFERÊNCIAS

BALL, B.; DUFF, H. **Dominando o Linux**: Red Hat e Fedora. São Paulo: Pearson Makron Books, 2004.

BIRKNER, M. H. **Projeto de interconexão de redes**: Cisco Internetwork Design – CID. São Paulo: Pearson Education do Brasil, 2003.

Ver anotações



CAPSA. Disponível em: <http://www.colasoft.com/capsa-free/>. Acesso em: 19 abr. 2020.

CISCO PRIME NETWORK ANALYSIS. Disponível em: [https://www.cisco.com/c/pt\\_br/support/cloud-systems-management/prime-network-analysis-module-software/products-user-guide-list.html](https://www.cisco.com/c/pt_br/support/cloud-systems-management/prime-network-analysis-module-software/products-user-guide-list.html). Acesso em: 15 nov. 2020.

COMER, D. E. **Redes de Computadores e Internet**. 6. ed. Porto Alegre, RS: Bookman, 2016.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. ed. Porto Alegre, RS: AMGH, 2010.

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

MICROSOFT NETWORK MONITOR. Disponível em: <https://www.microsoft.com/en-us/download/details.aspx?id=4865>. Acesso em: 16 nov. 2020.

NASCIMENTO, M. B. Conheça as principais ferramentas de gerenciamento de redes de mercado. **DLTEC**, 2019. Disponível em: <http://www.dltec.com.br/blog/redes/conheca-as-principais-ferramentas-de-gerenciamento-de-redes-de-mercado/>. Acesso em: 31 jan. 2021.

NEMETH, E.; SNYDER, G.; HEIN, T. R. **Manual completo do Linux**: guia do administrador. São Paulo: Pearson Makron Books, 2004.

NORTHROP, T.; MACKIN, J. C. **Configuração do Windows Server 2008**: infraestrutura de rede. Porto Alegre, RS: Bookman, 2013.

NUNES, S. E. **Redes de Computadores**. Londrina, PR: Editora e Distribuidora Educacional S. A., 2017.

OLHAR DIGITAL. Por que você precisa se preocupar com o gerenciamento do Wi-Fi na sua empresa?. **Olhar Digital**, 2017. Disponível em: <https://bit.ly/3rC0jCu>. Acesso em: 31 jan. 2021.

PAKET, C. **Construindo redes Cisco de acesso remoto**. São Paulo: Pearson Education do Brasil, 2003.

SLAVIEW. Disponível em: <https://www.telcomanager.com/slaview-monitoramento-de-performance/>. Acesso em: 15 nov. 2020.

WIRESHARK. Disponível em:

<https://www.wireshark.org/download.html><https://www.wireshark.org/download.html>.

Acesso em: 16 nov. 2020.

ZENOSS. Disponível em: <https://community.zenoss.com/home>. Acesso em: 14 nov. 2020.

0  
Ver anotações