

## Unidade 1

### Fundamentos de Redes de Computadores

#### Aula 1

Introdução à Comunicação de Dados

#### Introdução à comunicação de dados



##### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

#### Ponto de Partida

Olá, estudante!

O histórico das redes de computadores é um campo fascinante que nos leva a uma jornada através das inovações tecnológicas que moldaram nosso mundo digital. Tudo começou com a ARPANET na década de 1960, uma rede experimental criada pelo Departamento de Defesa dos EUA, a qual serviu como base para o desenvolvimento da Internet. À medida que as décadas avançaram, as redes de computadores evoluíram de estruturas centralizadas para descentralizadas e, finalmente, para a internet global que conhecemos hoje, interconectando bilhões de dispositivos em todo o mundo.

As redes de computadores e a internet se tornaram uma parte inextricável de nossas vidas, permitindo a troca instantânea de informações, comunicação, comércio eletrônico e muito mais. É uma rede global de redes, na qual cada dispositivo é um ponto de acesso à vasta rede digital.

Além de possibilitar a comunicação e o compartilhamento de informações, a internet também desempenha um papel fundamental no desenvolvimento de aplicativos e serviços inovadores, desde as redes sociais até a computação em nuvem.

Os conceitos de ISP (provedor de serviços de internet) e backbone são fundamentais para entender como a Internet funciona. ISPs são empresas que conectam usuários e empresas à internet, fornecendo acesso e serviços. Eles usam uma infraestrutura de alta capacidade conhecida como “backbone” para interconectar regiões geográficas e rotear o tráfego de dados em escala global. Estudar esses conceitos é crucial para compreender a arquitetura da internet e sua importância na conectividade moderna. Recomenda-se explorar recursos como livros, cursos online e documentários para aprofundar seus conhecimentos sobre esses tópicos e como eles moldaram nossa sociedade digital.

Imagine que você é um pesquisador em redes de computadores e tem sido encarregado de criar uma apresentação que explique a evolução das redes de computadores, desde o seu surgimento até os dias atuais. Vamos abordar três tópicos essenciais: o histórico das redes de computadores, o funcionamento das redes de computadores e da internet e o papel desempenhado pelos ISPs e backbones na conectividade global.

Vamos entender como a história de rede e da internet começou e como ela impacta nossa vida atual. Participe dessa trilha conosco; excelentes estudos!

## Vamos Começar!

### Histórico das redes de computadores

- **Década de 1961 a 1972**

Segundo Kurose (2006), os primeiros estudos relacionados à redes de computadores ocorreram no início da década de 1960. A década marcou o início da evolução das redes de computadores.

Posteriores ao período pós-Segunda Guerra Mundial, os primeiros estudos relacionados à transmissão de dados foram efetuados. Os fatos históricos beneficiaram a ciência da computação, pois havia interesses dos envolvidos nos conflitos pós-guerra para a interceptação e decodificação dos códigos de comunicação dos países em conflitos.

- **Década de 1972 a 1980**

De acordo com Kurose (2006), durante a década de 1972 a 1980, houve avanços em redes de computadores. Ocorreu a expansão da ARPANET e o surgimento de novas tecnologias e protocolos.

- **Década de 1980 a 1990**

Este período de evolução das redes de computadores marca o crescimento da internet, o desenvolvimento de protocolos-chave e a disseminação de computadores pessoais (Kurose, 2006).

- **Década de 1990 a 2000**

Na década de 1990 a 2000, a evolução das redes de computadores avançou com a internet na popularização da web e no surgimento de novas tecnologias de rede.

- **Anos 2000 a 2023**

Segundo Kurose (2006), o período de 2000 a 2023 testemunhou o crescimento da internet, a popularização das redes sociais, a proliferação de dispositivos móveis e a expansão das tecnologias de comunicação. Surge a disponibilização de serviços como: vídeo *on demand*, VoIP, jogos online, streaming de músicas, entre outros. Além disso, dispositivos utilizados no nosso cotidiano passaram a se conectar à rede mundial, tais como os carros, celulares, televisores, entre diversos outros.

## O que são redes de computadores?

Segundo Tanenbaum, Feamster e Wetherall (2021), redes de computadores apontam para equipamentos de computação e comunicação interconectados, os quais trocam dados e compartilham recursos tecnológicos. Os dispositivos conectados em rede usam uma forma de norma, conhecida como protocolo de comunicação, para transmitir informações por meio de tecnologias físicas ou meios sem fio. As redes de computadores superam as distâncias geográficas e possibilitam que informações sejam compartilhadas entre equipamentos, pessoas, empresas e organizações no mundo inteiro. Elas disponibilizam informação em nível local ou global, e são úteis para a prestação de diversos serviços para as pessoas, empresas e governos. Recursos como mandar e-mails, assistir vídeos, receber mídias pelo celular ou outros serviços só são possíveis através de uma rede de comunicação.

Podemos fazer a analogia de que as redes de computadores são como ruas para as informações que trafegam. Imagine que você tem várias casas (computadores) e precisa que elas se comuniquem entre si, assim como você e outras pessoas precisam se encontrar. Pense nas redes como ruas que ligam essas casas. Cada casa (computador) está em um local diferente, e as ruas (redes) permitem que essas casas se conectem, como as rodovias ligando cidades. Imagine que essas casas (computadores) precisam compartilhar coisas, como eletricidade. As

redes de computadores são como os meios para que essas casas compartilhem informações, assim como as ruas permitem que as cidades compartilhem recursos (infraestrutura).

Em redes de computadores, os “protocolos” são como regras de trânsito. Eles permitem que a comunicação entre computadores seja organizada e segura, assim como as regras de trânsito mantêm o tráfego seguro nas ruas. Cada casa (computador) na rede tem um “endereço IP”, que é como um número de telefone. É esse endereço que permite aos computadores se encontrarem e compartilharem informações, de modo semelhante a como usamos números de telefone para ligar para os amigos.

Os “roteadores” são como semáforos e placas de trânsito orientando o caminho. Eles ajudam a direcionar o tráfego de informações para que chegue ao destino correto. Os “firewalls” são como guardas de trânsito ouseguranças de residenciais. Eles controlam quem pode entrar nas redes e quem deve ficar de fora, garantindo que apenas os fluxos de informações seguros entrem na rede.

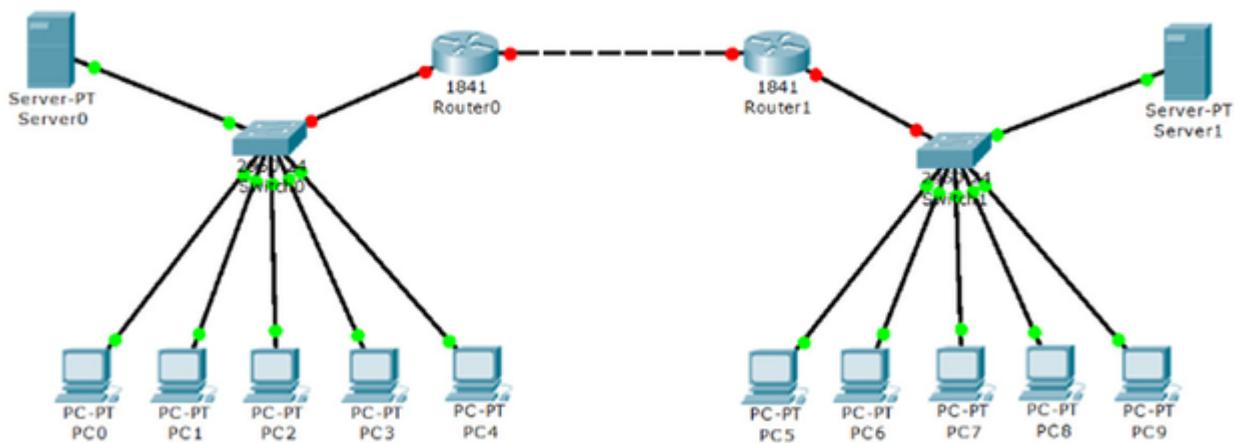


Figura 1 | Exemplo de uma pequena rede no software Cisco Packet Tracer. Fonte: elaborada pelo autor.

Tanenbaum, Feamster e Wetherall (2021) explicam que as redes de computadores são como um sistema de estradas para informações e dados, permitindo que os equipamentos de infraestrutura e dispositivos se comuniquem, compartilhem e acessem informações. Podemos pensar, assim, que são como as ruas, que conectam lugares e permitem o movimento de pessoas e recursos. É um sistema essencial para a comunicação em nosso mundo digital, e que nos fornece acesso à internet, redes sociais, mensagens instantâneas, e-mail, streaming de mídia, trabalho remoto, videoconferência, GPS e navegação, compras online, bancos online, aprendizado online, redes domésticas, redes de celular, redes sociais profissionais, controle de dispositivos inteligentes, etc.

**Siga em Frente...**

**ISP (provedor de serviços de internet)**

Você já se questionou sobre como a internet chega a sua residência? Os provedores de serviços de internet, ou ISPs, são eles que proveem nosso acesso à internet. ISP (da sigla em inglês *Internet Service Provider*) se refere a uma organização que oferece serviços para permitir que as pessoas acessem e utilizem a internet. Os ISPs podem ser de empresas privadas, comunitárias, comerciais ou organizações filantrópicas. De acordo com Oliveira, Lummertz e Souza (2019), eles oferecem serviços de acesso à internet, hospedagem web, trânsito de internet, serviços de e-mail, servidores proxy, registros de nomes de domínio, etc. Sem um ISP, você não poderá usar a internet e realizar atividades, como jogar online, usar mídias sociais, fazer compras online, entre outras.

Podemos fazer a seguinte analogia: imagine que você quer ler um livro e comparece a uma biblioteca para buscá-lo. Pense que a Internet é uma enorme biblioteca cheia de informações. O ISP é como a rua que leva até lá. Ele faz a conexão entre você e a Internet.

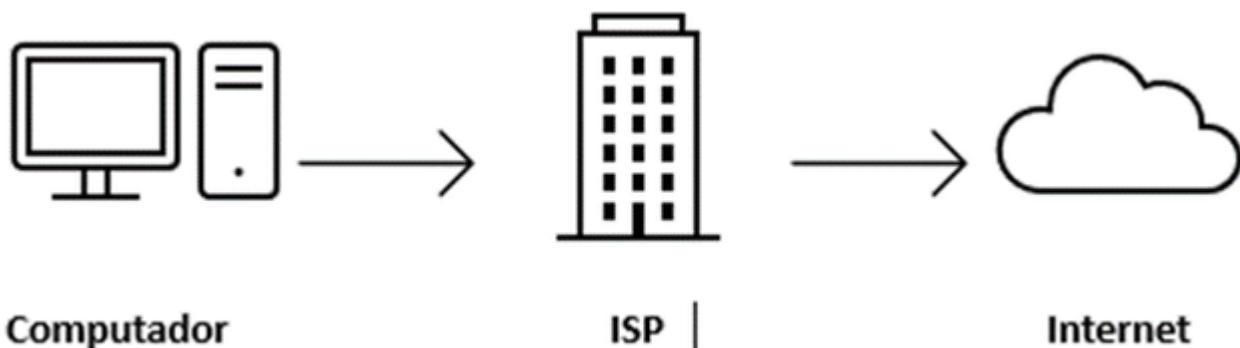


Figura 2 | Funcionamento ISP. Fonte: elaborada pelo autor.

O ISP realiza a conexão à internet; para isso você precisa de um contrato com um ISP. É como ter uma assinatura de biblioteca que permite que você entre e pegue livros emprestados. Temos que considerar o endereço IP; cada dispositivo que se conecta à internet tem um número especial chamado “Endereço IP”. Isso é como o número do seu cartão de biblioteca, que ajuda a identificar quem você é e de onde está acessando. O ISP tem sua própria “biblioteca” de informações, chamada de servidor. Quando você busca por algo na Internet, o ISP ajuda a encontrar o que você busca, assim como um bibliotecário que ajuda a encontrar o livro certo.

Contamos também com encaminhamento de dados; quando você solicita uma página da web ou envia um e-mail, o ISP pega as informações e as envia através de suas “ruas” (cabos e servidores) até o ponto de destino. Isso é como o bibliotecário pegando o livro que você pediu e trazendo-o até você. No retorno de dados, quando a página ou o e-mail que você solicitou é encontrado, o ISP o traz de volta para você. É como o bibliotecário entregando o livro. Ponto importante é a segurança: o ISP também atua como um segurança para garantir que apenas informações seguras entrem e saiam da sua “biblioteca” (seu equipamento). Ele ajuda a manter os dados protegidos, assim como um segurança mantém a biblioteca segura.

## O backbone

Vamos continuar a pensar na internet como uma grande rede de vias urbanas; você está em sua casa, enquanto o site ou serviço que deseja acessar está em outro local. O “backbone” é como uma rodovia que liga todas as cidades da internet. Permite que dados trafeguem rapidamente entre diferentes partes da rede. Backbone significa “espinha dorsal” em inglês; trata-se de um importante sistema que fornece o suporte central para que múltiplas redes se conectem e comuniquem entre si.

Uma analogia que podemos fazer é o sobre o funcionamento do backbone, operando com conexão entre redes locais: cada cidade (ou rede local) tem suas próprias ruas (ou cabos) que se conectam a essa rodovia. As redes locais podem ser em escolas, empresas ou nossa residência. Contamos com o encaminhamento de informações, quando você envia uma solicitação para um site ou serviço, como clicar em um link; seus dados viajam pela “rua” até chegar à “rodovia” (o backbone). Isso é como andar de carro e dirigir até a rodovia para ir a outra cidade. O backbone é como uma rodovia expressa, permitindo que as informações trafeguem em alta velocidade entre diferentes partes da internet.

Por isso, acessamos sites de todo o mundo em segundos. Grandes empresas e provedores de serviços de internet têm acesso direto ao backbone; são como as cidades grandes que têm várias entradas na rodovia. Isso permite que eles ofereçam conexões rápidas e confiáveis. O backbone é construído de forma estruturada e precisa, com rotas alternativas. Isso significa que, mesmo que uma parte da rodovia tenha problemas (como obras na estrada), os dados ainda podem seguir o fluxo por outra rota para chegar ao destino correto.

CONEXÃO | JULHO/23

Capacidade agregada 3,43 Tb/s

Capacidade internacional 600 Gb/s

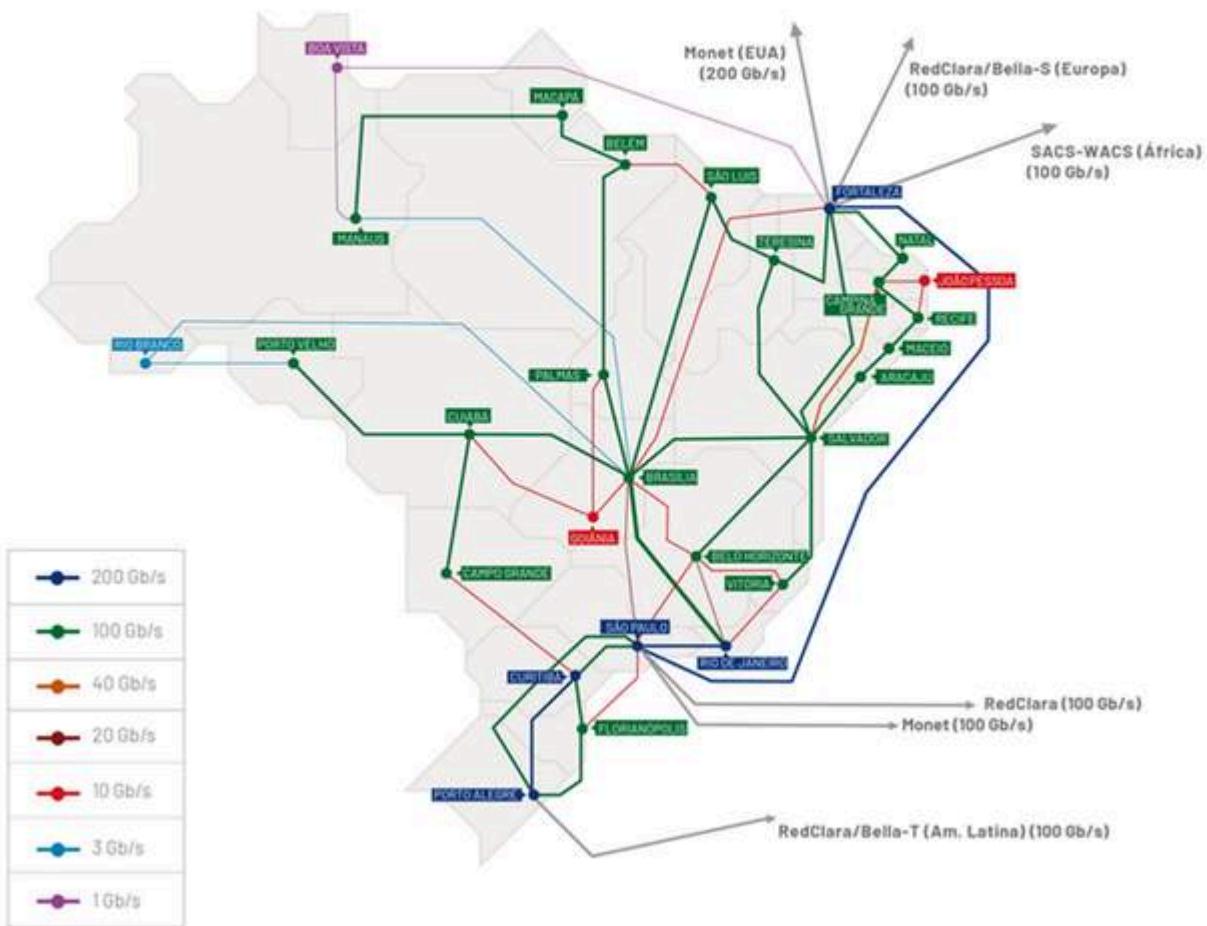


Figura 3 | Backbone: estrutura do Brasil. Fonte: RNP [s.d.].

O backbone é a parte da infraestrutura da rede de computadores que interconecta diferentes redes e fornece uma rota para a troca de informações. Sem o backbone, a internet não funcionaria tão eficientemente, e é por isso que ele é uma parte fundamental da experiência online.

Segundo Nunes (2017), o desenvolvimento do backbone envolve avaliar e compreender como todos os elementos da rede que se conectam (de roteadores, switches e servidores a desktops, laptops e impressoras) e como podem ser executados da forma mais eficiente possível. O cabeamento de backbone deve ter a largura de banda mais alta de qualquer cabeamento em sua rede, uma vez que os backbones são usados para unir switches e roteadores, conectando LANs departamentais ou sub-redes em redes em todo o edifício ou campus. Pontos a considerar na criação de backbone em uma rede:

- Mapa rede.

- Layout do cabeamento.
- Todos os dispositivos que serão conectados na rede.
- Estrutura de endereçamento IP.
- Estrutura e processos de segurança da estrutura de rede.

## Vamos Exercitar?

Temos que entender a origem e desenvolvimento das tecnologias de redes de computadores, com o objetivo de explorar a evolução das redes desde o seu início até os dias atuais. Destacando os pontos abaixo, reflita e exercite sobre eles:

### Histórico das redes de computadores:

- Destaque os principais marcos históricos, começando com a criação da ARPANET na década de 1960 como precursor da internet.
- Mencione o desenvolvimento de protocolos de comunicação, como o TCP/IP, que são fundamentais para a interconectividade global.
- Destaque a transição de redes centralizadas para descentralizadas, permitindo o crescimento exponencial da internet.

### Redes de computadores e a internet:

- Explique o funcionamento das redes de computadores, por meio da qual dispositivos estão interconectados, compartilhando informações e serviços.
- Introduza os conceitos de protocolos, roteamento e camadas OSI para mostrar como os dados são transmitidos.
- Ilustre como a internet é a interconexão de redes em escala global, permitindo a comunicação instantânea e o acesso a recursos em todo o mundo.

### Conceitos de ISP e backbone:

- Descreva o papel dos ISPs (provedores de serviços de internet) como intermediários que conectam os usuários à internet.
- Explique que os backbones são redes de alta capacidade que interligam ISPs e regiões geográficas, permitindo o tráfego de dados em larga escala.
- A relevância dos ISPs e backbones na infraestrutura global de comunicação é de extrema importância.

## Saiba mais

A evolução das redes de comunicação de dados ao longo do tempo, desde os primórdios da ARPANET até as modernas redes globais, compreende a interconexão de dispositivos e sistemas, possibilitando a troca de informações e serviços em escala global por meio da infraestrutura da internet. ISPs são provedores de serviços de internet que conectam usuários à rede mundial, enquanto backbones são as “espinhas dorsais” de alta capacidade que interligam diferentes partes da rede, permitindo o tráfego de dados em larga escala. A seguir, indicamos mais conteúdos para complementar seu conhecimento nesta área:

- **O menino da internet: a história de Aaron Swartz** (The Internet's Own Boy: The Story of Aaron Swartz). Direção: Brian Knappenberger. Produção: Brian Knappenberger. Estados Unidos: Participant Media, 2014. 1 DVD (105 min.). Narra a história do jovem Aaron Swartz (1986-2013), um jovem programador, escritor e ativista norte-americano que acreditava na mudança radical do mundo através da internet e da computação. Um prodígio da internet que contribuiu significativamente para a evolução das redes de computadores e da Internet.
- **NIC.br (Núcleo de Informação e Coordenação do Ponto BR)** – o [NIC.br](http://NIC.br) é um órgão importante para informações relacionadas à internet no Brasil. Eles oferecem relatórios, estatísticas e informações sobre o desenvolvimento da internet no país.
- **Download: a verdadeira história da internet**. Direção: John Heilemann. Produção: Discovery Channel. Estados Unidos: Discovery Channel, 2008. 1 DVD (180 min.). É uma série de documentários com quatro episódios, que se propõe a mostrar o contexto histórico da web, desde sua criação no início dos anos 1990, passando pela icônica Guerra dos Navegadores, pela bolha ponto.com no início dos anos 2000 e, finalmente, o surgimento da web 2.0.

## Referências

KUROSE, J. F. **Redes de computadores e a internet: uma abordagem top-down**. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

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

OLIVEIRA, D. B.; LUMMERTZ, R. S.; SOUZA, D. C. **Qualidade e desempenho de redes**. Porto Alegre: Sagah, 2019.

RNP. **Rede Ipê**. Conexão atual. [s.d.]. Disponível em: <https://www.rnp.br/sistema-rnp/rede-ipê>. Acesso em: 14 de outubro de 2023.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Aula 2

Meios de transmissão

### Meios de transmissão



#### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

### Ponto de Partida

Olá, estudante!

Nesta aula, vamos abordar os sinais analógicos, que têm como característica representações contínuas e variáveis no tempo, enquanto sinais digitais são representados por valores discretos, geralmente 0 (zero) e 1 (um). Os sinais analógicos usam uma gama contínua de valores, como uma onda, enquanto sinais digitais usam estados binários para representar informações, tornando-os mais robustos e fáceis de processar em dispositivos eletrônicos.

Para os sinais propagarem, são necessários os meios de transmissão, os quais podem ser meios de transmissão guiados. Exemplos destes são cabos físicos utilizados para transmitir sinais em redes de computadores; eles incluem cabo de par trançado, cabo coaxial e fibra óptica, que são ideais para redes locais (LANs) devido à sua confiabilidade e alta velocidade de transmissão de dados.

Há também os meios de transmissão não guiados, conhecidos como sem fio, que usam ondas eletromagnéticas para transmitir dados sem a necessidade de cabos físicos. Exemplos incluem redes Wi-Fi, bluetooth, redes celulares (4G e 5G) e satélites. Eles permitem mobilidade e flexibilidade, sendo amplamente utilizados em redes móveis e comunicações sem fio em todo o mundo.

Pensando em montar uma pequena rede de alto desempenho e com mobilidade, quais tecnologias de meio de transmissão podemos utilizar? Reflita sobre como os aspectos de sinais e meios de transmissão podem influenciar nossa rotina.

Siga firme nos estudos e terá ótimos resultados! Bons estudos!

## Vamos Começar!

### Tipos de sinais

#### Sinal analógico

Segundo Tanenbaum, Feamster e Wetherall (2021), os sinais analógicos são ondas eletromagnéticas que assumem infinitos valores ao longo do tempo. Este sinal é representado por uma onda senoidal com as seguintes características:

- **Amplitude:** representa intensidade mais alta dos sinais elétricos (volts).
- **Frequência:** medida em hertz, define a quantidade de ciclos em um intervalo de tempo.
- **Fase:** define o formato da onda senoidal e pode ser medida em graus ou radianos.

Kurose (2006) explica que o emprego do sinal analógico em redes de computadores é incomum na maioria das redes modernas, uma vez que elas operam principalmente com sinais digitais. No entanto, o sinal analógico foi historicamente usado em tecnologias mais antigas, como modems de discagem (Dial-up) e redes de televisão a cabo.

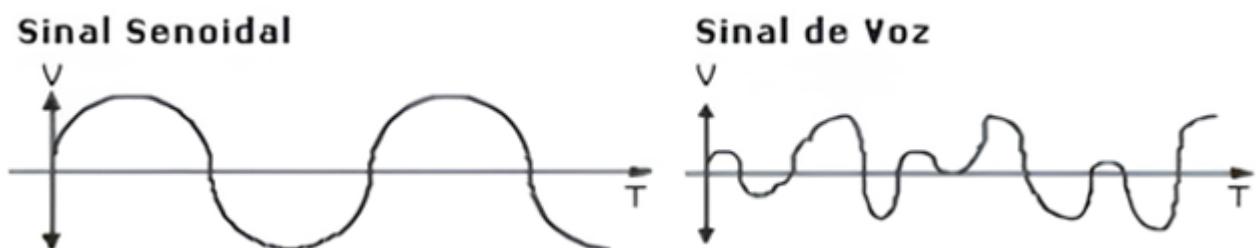


Figura 1 | Exemplo de sinal analógico. Fonte: Nunes (2017, p. 45).

Devido às limitações de velocidade, confiabilidade e qualidade de sinal, as redes de computadores modernas utilizam principalmente sinais digitais. A tecnologia de transmissão analógica foi largamente substituída por comunicações digitais mais eficazes, como Ethernet, fibra óptica e tecnologias de banda larga, que oferecem velocidades de transmissão mais rápidas e maior robustez contra interferências.

## Sinal digital

O funcionamento do sinal digital em redes de computadores é o método predominante de comunicação nas redes modernas. Ele envolve a representação de dados em forma de bits, de modo que cada bit é uma unidade digital que pode ter um de dois valores: 0 (zero) ou 1 (um). Isso é conhecido como forma binária. A representação dos seus valores é dada como discreta ao longo do tempo e amplitude. Uma vez que torna possível reduzir a taxa de oscilação, esse fenômeno é responsável pela performance da qualidade de serviço. Quando ocorre uma transmissão de dados, há um processo de codificação (digitalização) desse sinal. Suas vantagens são que:

- Os sinais digitais não sofrem degradação dos serviços por interferência ou ruídos.
- Pode-se transmitir maior quantidade de informações.

Tanenbaum, Feamster e Wetherall (2021) explicam que o funcionamento desses sinais, em uma transmissão efetuada por internet cabeadas (operadoras comuns) com intenção de acessar um site a partir de um dispositivo, é efetuado no seguinte modelo:

- I. Os modems fornecidos pelas operadoras fazem a adequação do sinal digital com o meio disponibilizado por elas.
- II. O modem recebe os sinais emitidos pelo computador (desktop, notebooks, tablets e smartphones) e coloca no meio de transmissão fornecido pela operadora (processo conhecido como modulação).
- III. Ao chegar ao destino, é efetuado o processo inverso. Os modos de transmissão dos sinais nas redes de comunicação de dados podem variar conforme o sentido pelo qual ocorrem as trocas de mensagens, o número de bits enviados simultaneamente e a sincronização entre computador e servidor.

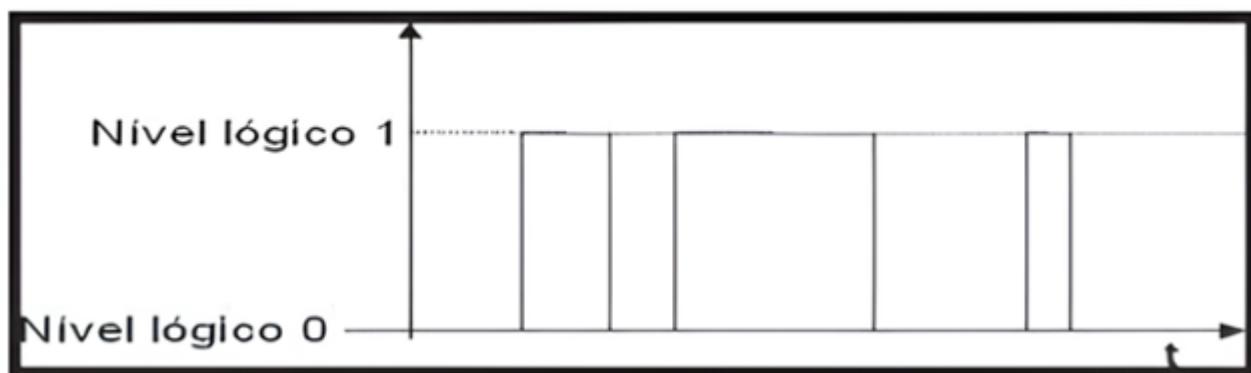


Figura 2 | Exemplo de sinal digital. Fonte: Nunes (2017, p. 53).

O benefício do sinal digital é sua capacidade de transmitir dados de forma precisa, eficiente e resistente a interferências. Além disso, a representação binária (0s e 1s) é facilmente interpretada por dispositivos eletrônicos, tornando-a ideal para a comunicação em redes de

computadores. Como resultado, o sinal digital é amplamente utilizado em todas as formas de redes de computadores, desde redes locais (LANs) até a internet.

**Siga em Frente...**

## Modos de transmissão

### Os meios de transmissão guiados

Tanenbaum, Feamster e Wetherall (2021) definem que, para que os sinais possam ser transmitidos, os meios de transmissão guiados, também conhecidos como meios de cabeamento, são os meios físicos pelos quais os sinais são transmitidos em redes de computadores. Existem diversos tipos de meios de transmissão guiados com características e aplicações distintas.

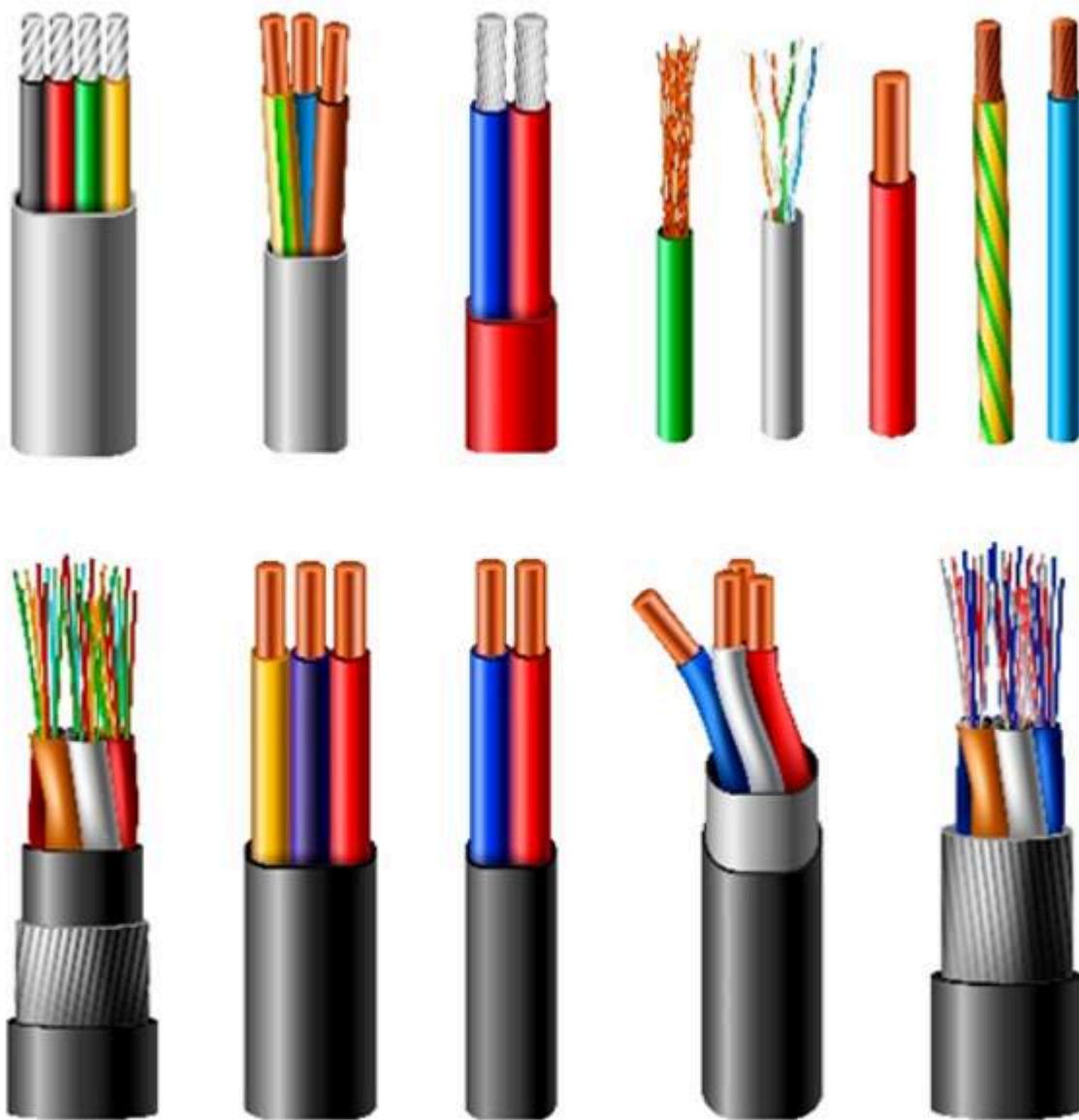


Figura 3 | Exemplo de transmissão guiada. Fonte: Freepik.

Alguns dos meios de cabeamento mais comuns incluem:

- **Cabo de par trançado (*twisted pair*)**: nesta modalidade, os fios são enrolados de forma helicoidal, pela qual ocorre menos interferência, uma vez que as ondas formadas em volta dos fios se cancelam. Esses fios dão suporte a sinais analógicos e digitais nas suas transmissões e são divididos em CAT 5, 5e, 6 e 7. Elas se diferenciam pela largura de banda suportada ou pela presença ou não de blindagem, oferecendo diferentes níveis de desempenho e velocidade de transmissão. Este é o meio de transmissão mais comum em redes locais (LANs).

- **Cabo coaxial (*coaxial cable*):** o cabo coaxial é usado em algumas redes e em sistemas de televisão a cabo. Ele é composto por um núcleo de cobre revestido por um condutor metálico, isolado por uma camada dielétrica e, finalmente, protegido por uma camada externa. Possibilita ligar redes com distância maiores e com maior velocidade que o par trançado; também recebe menos ruídos. São dois tipos utilizados na comunicação de dados: coaxial 10Base2 para taxas de transmissão de 10 Mbps e segmentos de até 185m e o cabo 10Base5, para redes de banda larga e alcance de até 500m.
- **Fibra óptica (*optical fiber*):** a fibra óptica é amplamente utilizada em redes de alta velocidade e comunicações de longa distância. Ela consiste em filamentos de vidro ou plástico que transmitem dados na forma de luz. A fibra óptica é conhecida por sua alta largura de banda e imunidade a interferências eletromagnéticas. Ao receber as informações, o sinal óptico é transformado em sinal elétrico. Nesse tipo de transmissão, é possível alcançar velocidade de até 10 terabytes por segundo.

Cada tipo de cabo tem suas próprias características, vantagens e desvantagens, e a escolha do meio de transmissão depende das necessidades específicas da rede e do ambiente em que será implantado. As redes modernas muitas vezes usam combinações de diferentes meios de transmissão, dependendo dos requisitos de conectividade e desempenho.

## Os meios de transmissão não guiados

De acordo com Tanenbaum, Feamster e Wetherall (2021), os meios de transmissão não guiados, ou seja, os meios sem fio, são usados em redes de computadores para transmitir sinais e dados sem a necessidade de cabos físicos.



Figura 4 | Exemplo de transmissão não guiada. Fonte: Freepik.

Esses meios de transmissão incluem:

- **Rádio:** o sinal do rádio é feito por torres de transmissão até o ponto de instalação das antenas receptoras. Apesar das distâncias alcançadas, o sinal recebe atenuação de vários obstáculos, como as construções, as árvores, além das interferências climáticas e, com isso, há perda na qualidade e às vezes até falha no sinal.
- **Micro-ondas:** neste tipo de transmissão, as ondas viajam em linha reta entre o emissor e o receptor; portanto, para fazer a ligação entre duas redes, faz-se necessário que haja visada

entre as antenas. Pode-se atingir uma distância de até 80 km com uma antena elevada 100m do solo, em uma geografia plana.

- **Wi-Fi (*Wireless Fidelity*):** as redes Wi-Fi utilizam ondas de rádio para transmitir dados sem fio. São amplamente usadas em redes locais (LANs) e em conexões à internet sem fio, permitindo que dispositivos se conectem a roteadores ou pontos de acesso sem a necessidade de cabos físicos.
- **Bluetooth:** é uma tecnologia de comunicação sem fio de curto alcance, frequentemente usada para conectar dispositivos como fones de ouvido, teclados, mouses e smartphones a outros dispositivos.
- **Redes celulares:** as redes celulares, como 4G e 5G, usam comunicações sem fio para conexões de dados móveis em dispositivos móveis, permitindo acesso à internet e comunicações de voz em telefones celulares e tablets.
- **Satélites:** a comunicação via satélite transmite sinais de rádio de longa distância. É usada em comunicações globais, como transmissões de TV via satélite e redes de satélites para comunicações de longa distância. Neste meio de transmissão, os sinais são enviados para os objetos que ficam estacionados acima da atmosfera terrestre, conhecidos como geoestacionários. São divididos em LEO (*Low Earth Orbit* – órbita terrestre baixa), MEO (*Medium Earth Orbit* – órbita terrestre média) e HEO (*Hight Earth Orbit* – órbita terrestre alta). Tais transmissões podem sofrer atrasos graças à distância entre emissor e receptor, além das interferências climáticas. Os meios escolhidos para a transmissão podem variar conforme disponibilidade de infraestrutura, geografia, distância entre os pontos, viabilidade financeira, entre outros propósitos.
- **Redes mesh sem fio:** consistem em dispositivos que se comunicam entre si de forma autônoma, formando uma rede de malha auto-organizada. Isso é usado em cenários como redes de sensores, redes de dispositivos IoT (internet das coisas) e redes de área urbana.
- **Infravermelho (IR):** embora menos comum atualmente, a tecnologia infravermelha foi usada para transmissão de dados entre dispositivos, como controles remotos de TV e comunicação ponto a ponto de curto alcance.
- **Zigbee:** é um padrão de comunicação sem fio de curto alcance amplamente utilizado em aplicações de automação residencial, como sistemas de iluminação inteligente e termostatos.
- **NFC (*Near Field Communication*):** é uma tecnologia de comunicação de curto alcance que permite a troca de informações entre dispositivos próximos, geralmente em um alcance de alguns centímetros. É usado em dispositivos móveis para pagamentos, transferência de dados e outras aplicações.

Segundo Nunes (2017), os meios de transmissão não guiados através do espectro, em redes de computadores, funcionam aproveitando diferentes faixas de frequência no espectro eletromagnético para transmitir dados sem fio.

Cada tecnologia de comunicação sem fio utiliza uma faixa de frequência específica dentro do espectro eletromagnético. Por exemplo, redes Wi-Fi operam na faixa de frequência de 2,4 GHz ou 5 GHz, enquanto as redes celulares operam em faixas de frequência como 700 MHz, 1,8 GHz e 2,6 GHz. Esses meios de transmissão sem fio são fundamentais para a conectividade moderna, permitindo mobilidade, comunicação flexível e conectividade de dispositivos em uma variedade de cenários, desde redes locais até redes de longa distância.

## Vamos Exercitar?

Para montar uma rede de alto desempenho com mobilidade, considerando tanto a rede cabeada quanto a sem fio. Projete a infraestrutura de rede cabeada com base nas necessidades de alta velocidade e confiabilidade. Use cabeamento de alta qualidade, como cabos de par trançado CAT6 ou fibra ótica.

Para a rede sem fio, instale roteadores e pontos de acesso estrategicamente para cobrir eficazmente a área desejada.

Implemente medidas de segurança sólidas em ambas as redes. Para a rede cabeada, utilize firewalls, VLANs e sistemas de detecção de intrusão. Para a rede sem fio, utilize criptografia e autenticação forte. Certifique-se de que os dispositivos móveis estejam atualizados com antivírus e software de segurança.

Configure políticas de controle de acesso para determinar quem pode se conectar à rede, tanto para a rede cabeada quanto para a sem fio. Mantenha um monitoramento constante de ambas as redes para identificar problemas em tempo real e realizar manutenção preventiva. Desenvolva políticas de uso da rede que estabeleçam diretrizes claras para o comportamento esperado dos usuários em ambas as redes.

Integrar redes cabeada e sem fio em uma rede de alto desempenho com mobilidade oferece o equilíbrio entre a confiabilidade da rede cabeada e a flexibilidade da rede sem fio, permitindo que dispositivos móveis se conectem de maneira eficaz e segura. Também podemos construir soluções das mais diferentes formas, com a mesma segurança e confiabilidade.

## Saiba mais

Os sinais analógicos e digitais influenciam nosso dia a dia; os meios de transmissão otimizam diariamente nossa produtividade. A seguir, algumas indicações para aprofundar seu conhecimento sobre o tema:

- Leitura do artigo de Cruz et al. (2023): [\*Proposta de ampliação da tecnologia de internet via satélite para as escolas da rede pública do município de Tabatinga/AM\*](#), da Revista de Gestão e Secretariado.
- Leitura do artigo de Oliveira et al. (2022): [\*Emprego dual – civil e militar – do 5G na defesa brasileira: uma proposta para o SISFRON, sob domínio do Exército\*](#), da Revista Ibérica de Sistemas e Tecnologias de Informação (RISTI).
- Leitura do artigo de Moura Júnior (2015): [\*Desafios em Infraestrutura de Tecnologia da Informação: Obras de Construção Civil e Movimentação de Datacenter\*](#), da GVcasos.
- Assista ao filme: **A Rede Social (The Social Network)**. Direção: David Fincher. Produção: Ceán Chaffin. Estados Unidos: Sony Pictures, 2010. 1 DVD (120 min.). Mark Zuckerberg, estudante de Harvard, decide trabalhar na ideia de uma rede de relacionamento dentro do campus. Seis anos e 500 milhões de amigos depois, ele se torna um jovem bilionário, um

dos homens mais poderosos do planeta. Todavia, o sucesso do Facebook lhe acarreta complicações na vida social e amorosa.

## Referências

CRUZ, B. C. R. *et al.* Proposta de ampliação da tecnologia de internet via satélite para as escolas da rede pública do município de Tabatinga, da /AM. **Revista de Gestão e Secretariado**, São Paulo, v. 14, n. 4, p. 6914-6935, 2023. Disponível em: <https://ojs.revistagesec.org.br/secretariado/article/view/2088>. Acesso em: 1 abr. 2024.

KUROSE, J. F. **Redes de computadores e a internet**: uma abordagem top-down. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

MOURA JÚNIOR, P. J. Desafios em Infraestrutura de Tecnologia da Informação: Obras de Construção Civil e Movimentação de Datacenter. **GVcasos**, v. 5, n. 2, 2015. Disponível em: <https://periodicos.fgv.br/gvcasos/article/view/56359>. Acesso em: 1 abr. 2024.

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

OLIVEIRA, R. C. F. *et al.* Emprego dual – civil e militar – do 5G na defesa brasileira: uma proposta para o SISFRON, sob domínio do Exército. **Revista Ibérica de Sistemas e Tecnologias de Informação (RISTI)**, ed. 49, 2022. Disponível em: [https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante\\_de\\_publicacao-1.pdf](https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-1.pdf). Acesso em: 1 abr. 2024.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Aula 3

Hardware e Cabeamento

### Hardware e cabeamento



**Este conteúdo é um vídeo!**

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

## Ponto de Partida

Olá, estudante!

Quanto a hardwares básicos em redes de computadores, podemos apontar que as placas de rede permitem a conexão a redes; modems traduzem sinais digitais em analógicos; *hubs* replicam dados para todas as portas; *switches* direcionam dados com eficiência.

Roteadores conectam redes e encaminham dados; bridges conectam segmentos de rede; *gateways* traduzem protocolos entre redes diferentes. Há também os modos de operação: *simplex* permite a comunicação unidirecional; *half-duplex* permite a comunicação bidirecional alternada; *full duplex* permite comunicação simultânea em ambas as direções.

Com o conhecimento nesses tópicos, vamos propor uma pequena rede ao final da aula. A ideia é criar uma rede local (LAN) de alto desempenho que conecte três computadores (dois notebooks e um desktop) usando uma rede sem fio (Wi-Fi) e um switch com suporte a Gigabit Ethernet.

Este exercício permitirá que você monte e experimente uma pequena rede de alto desempenho e compreenda as diferenças de desempenho entre conexões com e sem fio, bem como as vantagens do uso de dispositivos Gigabit Ethernet em redes locais. Além disso, você terá a oportunidade de explorar algumas medidas de segurança que podem ser aplicadas à rede.

Agora é mão na massa, e vamos montar nossa rede! Bons estudos!

## Vamos Começar!

## Hardwares básicos: placas de rede, modem, hub e switch

As redes de computadores são o núcleo da conectividade moderna, permitindo que equipamentos em todo o mundo se comuniquem, compartilhem informações e acessem recursos em tempo real. Para que essa conectividade seja possível, uma série de hardwares desempenha papéis essenciais no funcionamento das redes. Nesta aula, vamos conhecer alguns dos hardwares básicos que são fundamentais em qualquer ambiente de rede de computadores. A escolha dos dispositivos a serem utilizados depende das necessidades específicas da rede e do desempenho desejado. Vamos conhecer mais a fundo cada um deles.

## Placas de Rede

Kurose (2006) define que a placa de rede corresponde a um dispositivo de E/S (entrada/saída) que se conecta por meio de cabeamento aos dispositivos de rede (*hub*, roteador, *switch* ou *brigde*). O controlador de interface da rede (NIC – *Network Interface Controller*) pode estar ou não integrado à placa-mãe.



Figura 1 | Exemplo de placa de rede. Fonte: Adobe Stock.

A arquitetura do barramento das placas de rede pode ser na forma PCI, PCI Express, ISA e USB, ou seja, o formato de encaixe no slot da placa-mãe. A sua função lógica é efetuar o tratamento de endereçamentos, no envio e recebimento das mensagens.

## Modem

Segundo Nunes (2017), o modem tem a função de fazer a modulação e a demodulação das mensagens; também é conhecido como transceptor. Veja o Quadro 1 a seguir, apontando os tipos de modems disponíveis e as suas funções.

TIPO	FUNÇÃO
------	--------

Analógico	Transmissão por canal de voz
Cable Modem	Transmissão de TV a cabo
ADSL	Par de fios da linha de assinante
Canal E1, E3 e E4	Canais digitais de telecomunicações
Ópticos	Transmissão por fibras ópticas

Quadro 1 | Tipos e funções dos modems. Fonte: elaborado pelo autor.

Em sua forma analógica, os dados são transmitidos pelo canal de voz; por sua vez, em sua forma digital, é feita a codificação da banda base. Esse equipamento está entre os mais populares dos hardwares encontrados nas redes.



Figura 2 | Exemplo de modem DSL.. Fonte: Wikimedia Commons.

Com a maior oferta de prestadoras de serviços de internet, esse dispositivo é cada vez mais encontrado nos lares brasileiros. Atualmente, o mercado oferece modems do tipo residencial, com conexão cabeada, 4G/5G e fibra óptica, com a possibilidade de wi-fi integrado.

## Hub

Tanenbaum, Feamster e Wetherall (2021) explicam que um *hub* pode conter várias portas de entrada responsáveis por distribuir o sinal conexão na rede interna. O equipamento assume o comportamento de repetidor de sinal, pois a informação, ao chegar, é replicada para todas as portas.



Figura 3 | Exemplo de hub. Fonte: Wikimedia Commons.

Por ter o comportamento de repetidor em uma rede e por replicar uma informação para todos os equipamentos conectados a ele, deve-se evitar o cascamenteo, devido à redução de performance que o dispositivo apresenta.

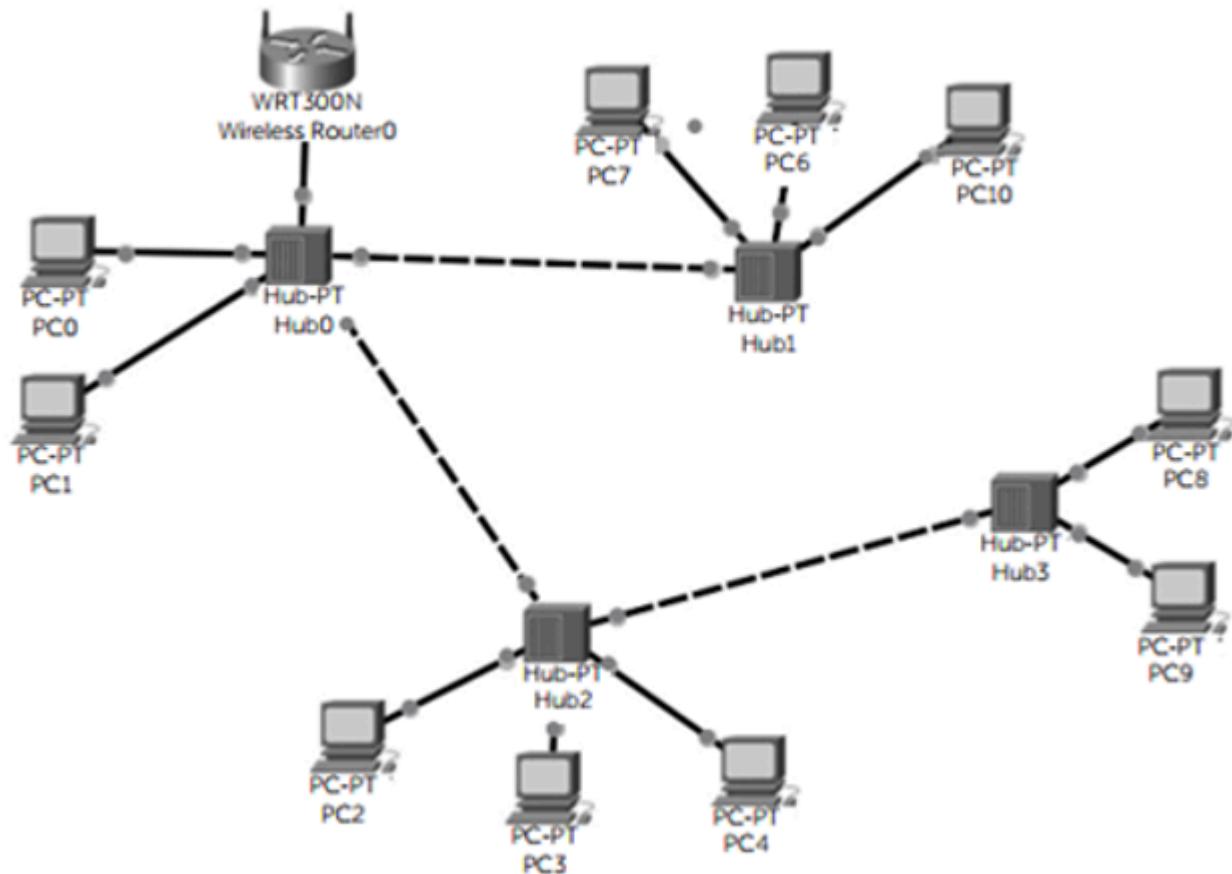


Figura 4 | Exemplo de cascamenteamento de hubs. Fonte: Nunes (2017, [s. p.])

De acordo com Tanenbaum, Feamster e Wetherall (2021), o cascamenteamento deve ser evitado principalmente com a utilização de *hubs*; entretanto, o ideal é evitá-lo com qualquer outro dispositivo, como roteador, *switch* ou bridge. Com o cascamenteamento, ao ser enviada uma mensagem, a cada processamento efetuado pelos equipamentos intermediários, o tempo para recebimento da informação pelo destinatário será maior.

O *hub* tem a função de prover a conexão entre os equipamentos de rede; porém, o excesso de mensagens que ele envia ao replicá-la para todos os equipamentos ocupa a largura de banda e gera o consequente aumento do consumo de processamento dos equipamentos intermediários.

## Switch

Este dispositivo é comumente encontrado em organizações, empresas e faculdades; ou seja, em redes que necessitam de grande quantidade de dispositivos. Segundo Tanenbaum, Feamster e Wetherall (2021), quando a informação chega a uma das interfaces de rede, o sistema do dispositivo lê o endereço destino do cabeçalho e envia para a interface correta. *Switches* normalmente possuem diversas portas de conexão.



Figura 5 | Exemplo de switch. Fonte: Wikimedia Commons.

A grande diferença do *hub* para o *switch* são os recursos disponíveis; no segundo, cada uma das portas possuem o seu controle de colisão; já o primeiro não tem essa tecnologia: envia a mensagem para todas as portas e no máximo tem velocidade de 1000Mbps (1GB). Os *switches* pode ser encontrado com velocidades que podem variar entre 100Mbps, 1000Mbps (1GB) e 10.000Mbps (10GB).

Oliveira, Lummertz e Souza (2019) explicam que o controle de colisão é utilizado por profissionais de redes de computadores para apontar aquelas mensagens que são replicadas para todos os equipamentos e não conseguem atravessar equipamentos como o roteador e o *switch*. Com esse recurso, se uma rede possuir um roteador em cada departamento, as mensagens replicadas para os equipamentos não serão enviadas para outros departamentos, pelo limite imposto pelos dispositivos, formando, assim, o controle de colisão.

## Siga em Frente...

## Roteador, bridges e *gateways*

### Roteador

Kurose (2006) define que os roteadores são equipamentos de redes que contêm microprocessadores, responsáveis pelo gerenciamento dos tráfegos de pacotes de dados. Entretanto, diferente do *hub*, ele tem a capacidade de analisar o endereçamento lógico (TCP/IP), evitando a colisão dos dados.

O roteador forma tabelas lógicas dos dispositivos disponíveis nas redes, entre eles, roteador, *switch*, computadores, dispositivos móveis, impressoras IP e câmeras IP. Para realizar esse processo, é utilizado um recurso de descoberta de equipamentos, efetuado por roteadores e *switches* por meio dos protocolos de comunicação, como:

- **ICMP:** realiza diagnóstico da rede, apresenta os erros no recebimento de pacotes e no informe de características da rede.
- **ARP:** efetua o mapeamento dos endereços físicos dos dispositivos de rede (MAC ADDRESS) por meio do endereço lógico.
- **RARP:** faz o inverso do ARP, associando um endereço lógico ao físico.

O roteador envia, em ciclos, um protocolo de atualização de “vizinhança” aos roteadores conhecidos. O envio da atualização é efetuado sucessivamente; assim, a tabela lógica de endereçamento dos dispositivos continua atualizada constantemente.



Figura 6 | Exemplo de roteador residencial. Fonte: Adobe Stock.

Segundo Kurose (2006), o roteador recebe a informação pela porta de entrada e repassa o pacote para o processador que efetua o roteamento. Esse processador realiza a análise do endereçamento de destino e encaminha a informação para a porta de saída, na verdade, apontando a interface de rede (placa de rede Ethernet).

## Bridges (pontes)

Para o administrador de redes que necessita conectar duas redes diferentes, um recurso possível é a utilização do dispositivo bridges (pontes), um tipo de equipamento que tem funções parecidas com o switch. Entretanto, as suas aplicações em uma infraestrutura são bem distintas, exemplo:

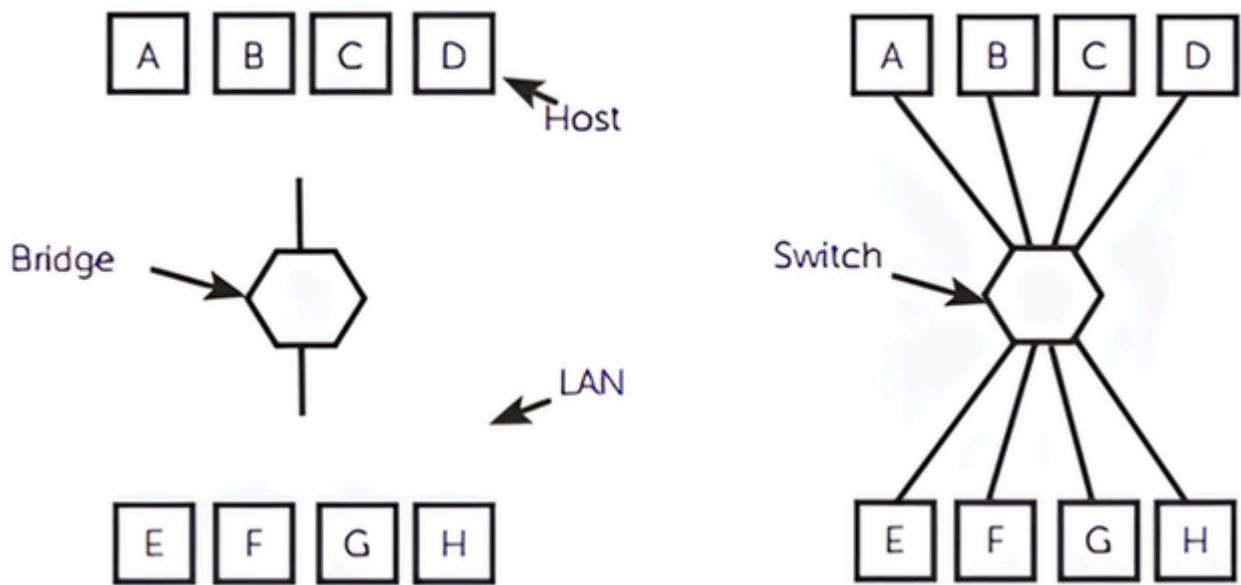


Figura 7 | Exemplo de bridge e switch. Fonte: Tanenbaum, Feamster e Wetherall (2021, p. 255).

De acordo com Tanenbaum, Feamster e Wetherall (2021), o *switch* é utilizado para conectar dispositivos da rede; a bridge é empregada para interligar duas redes (LAN). Porém, nada impede que o administrador utilize o switch para interligar duas redes, desde que os equipamentos estejam configurados e planejados corretamente. A vantagem de utilizar as bridges é que a sua configuração é mais fácil de realizar, necessitando apenas fazer o direcionamento do endereço das interfaces dos equipamentos das redes que serão conectados. Por sua vez, com o *switch*, o ganho no processamento das informações pode proporcionar melhor desempenho na comunicação entre os equipamentos de redes diferentes.

## Gateway

Um *gateway* é um dispositivo ou software que atua como uma interface entre duas redes distintas, permitindo a comunicação e a transferência de informações entre elas. O gateway atua como um ponto de entrada ou saída que traduz os protocolos de comunicação e regras utilizados em uma rede para que sejam compatíveis com a outra rede.

Tanenbaum, Feamster e Wetherall (2021) definem que o *gateway* pode ter funções específicas numa rede, dependendo do planejamento do administrador dela. Entre essas funções, estão:

- **Direcionamento:** todas as mensagens são enviadas para o nó da rede, que pode ser roteador ou *switch*.
- **Proxy:** uma lista de sites que os dispositivos da rede interna têm ou não permissão para acessar.

- **Firewall:** um dispositivo de segurança que verifica o conteúdo dos pacotes e efetua o bloqueio quando há ação nociva aos serviços disponíveis na rede. Pode ser software ou hardware.

Os *gateways* desempenham um papel fundamental em redes ao permitir que diferentes redes e equipamentos se comuniquem eficazmente, mesmo quando usam protocolos diferentes ou têm requisitos específicos de segurança. Eles atuam como portões de entrada ou saída que garantem a eficiência e a segurança da comunicação entre redes distintas.

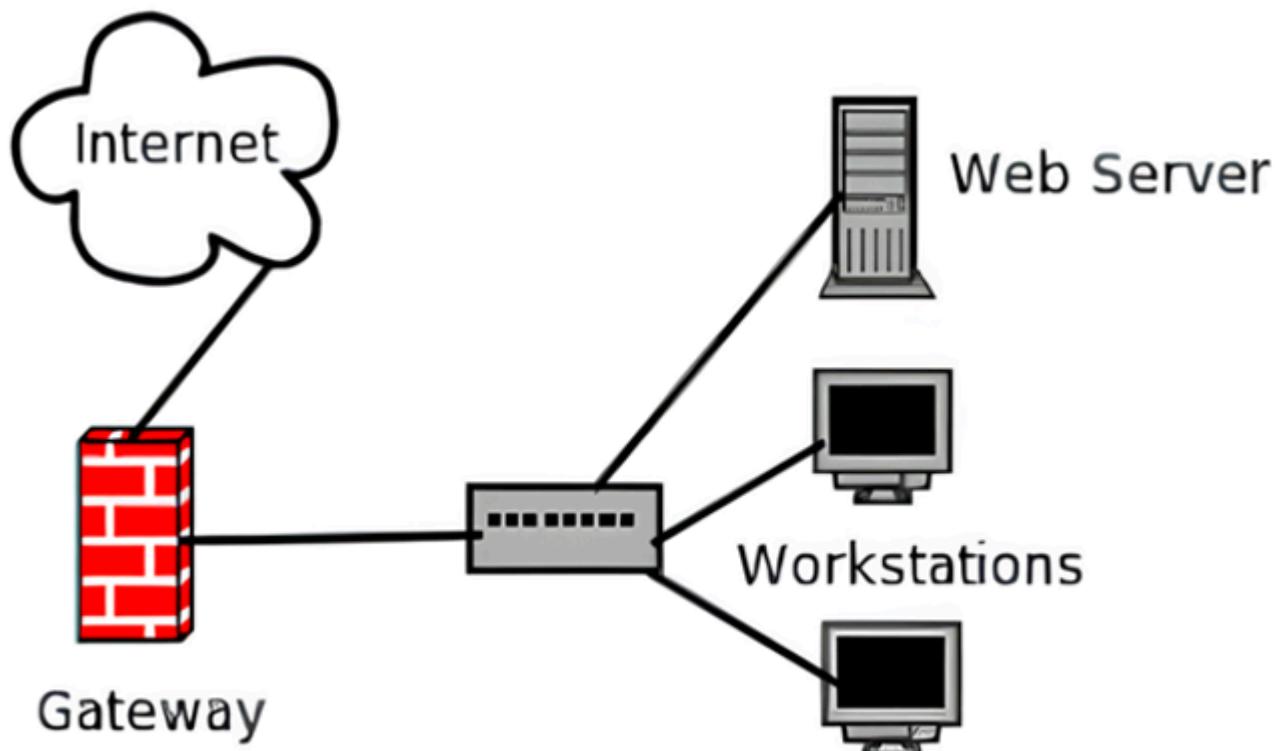


Figura 8 | Exemplo de gateway. Fonte: Polsonetti (2018, [s. p.]).

O conceito está ligado a um termo utilizado por profissionais de redes de computadores, que é “borda de rede”, o que explica o nome: é que o dispositivo fica após o roteador. O dispositivo já está conectado à internet (rede mundial e não interna).

## Modos de operação

Segundo Kurose (2006), há os seguintes modos de operação:

- **Simplex:** nele, a transmissão dos dados ocorre apenas em uma direção (unidirecional); ou seja, os dados fluem apenas do emissor para o receptor. Um exemplo é a comunicação de

TV ou rádio, na qual o receptor apenas recebe os dados transmitidos pelo emissor.

- **Half-duplex:** a comunicação dos dados pode ocorrer em ambas as direções, mas não simultaneamente. Os equipamentos alternam entre transmissão e recepção. Isso é comum em walkie-talkies, nos quais um usuário deve pressionar um botão para falar e soltá-lo para ouvir.
- **Full duplex:** a comunicação de dados é bidirecional, ocorre simultaneamente. Os equipamentos podem transmitir e receber dados ao mesmo tempo. É comum em redes Ethernet, telefonia e videoconferências.
- **Multiplexação:** é um conceito que permite a vários sinais compartilharem o mesmo meio de transmissão. Os modos de multiplexação, como a TDM (*Time-Division Multiplexing*) e a FDM (*Frequency-Division Multiplexing*), são frequentemente usados para otimizar o emprego de recursos de rede compartilhados.

A escolha entre os tipos de sinais e modos de transmissão depende das necessidades e requisitos específicos de uma rede de computadores, levando em consideração a confiabilidade, a eficiência e a capacidade de comunicação desejada. Em redes de computadores modernas, a transmissão digital em modo *full-duplex* é amplamente utilizada para garantir comunicação rápida e confiável.

## Vamos Exercitar?

Este passo a passo ajudará você a montar a sua rede (concepção teórica), verificar a conectividade e realizar testes de desempenho. Certifique-se de destacar detalhes como velocidades de transferência, conexões, etc. Tenha um checklist de todos os pontos a verificar na sua rede. Isso proporcionará uma experiência na montagem de uma rede de alto desempenho e a compreensão das implicações do hardware utilizado futuramente.

Para resolver nosso exercício de montar uma pequena rede de alto desempenho, podemos listar os itens a seguir:

- Dois notebooks com capacidade Wi-Fi.
- Um desktop com uma placa de rede Gigabit Ethernet.
- Um *switch* com suporte a Gigabit Ethernet.
- Cabos de rede Ethernet (CAT6 ou superior) para conectar os dispositivos ao *switch*.
- Roteador Wi-Fi.

Certifique-se de que todos os componentes necessários estão disponíveis: notebooks, desktop, *switch* Gigabit Ethernet, cabos Ethernet, roteador Wi-Fi e fonte de alimentação para o *switch*. Escolha um local adequado para montar a rede. Certifique-se de que haja espaço suficiente e acesso a tomadas elétricas para todos os dispositivos.

Conecte os cabos Ethernet aos computadores (notebooks e desktop) e ao *switch* Gigabit Ethernet. Conecte o roteador Wi-Fi à fonte de alimentação e configure-o de acordo com as instruções do fabricante.

Nos notebooks, acesse as configurações de rede sem fio e conecte-se à rede Wi-Fi criada pelo seu roteador. Se o desktop não estiver configurado para obter automaticamente um endereço IP, configure-o manualmente para se ajustar à rede.

Verifique se todos os dispositivos estão conectados corretamente. Os LEDs no switch devem indicar que os cabos estão ativos. Verifique se há conectividade à internet para os notebooks, se aplicável. Você deve ser capaz de acessar a internet em ambos.

Realize um teste de velocidade de transferência de dados entre os dispositivos. Tente transferir um arquivo grande de um notebook para o desktop e vice-versa. Anote as velocidades de transferência.

**Bônus:** explore outras configurações de rede, como configurações de firewall, configurações de QoS (qualidade de serviço) no *switch* e outras configurações avançadas.

## Saiba mais

Hardware, tipos de sinais e o cabeamento, fundamentais em redes de computadores, fornecem a base sobre a qual a conectividade, a comunicação e a colaboração são construídas. Investir em hardware de qualidade e cabeamento bem projetado é fundamental para garantir o sucesso e a confiabilidade de qualquer rede, independentemente de seu tamanho ou finalidade. A seguir, algumas indicações para aprofundar seu conhecimento sobre o tema:

- Leitura do artigo de Cirne (2019): [O processo de transição para a TV digital no Brasil: um olhar sobre o cenário de interesses e de entraves políticos](#), da Revista Compolítica.
- Leitura do artigo de Medeiros et al. (2014): [Uma análise de desempenho da rede metropolitana de telemedicina dos hospitais universitários da cidade de Natal-RN/Brasil](#), da revista HOLOS.
- Leitura do artigo de Silva et al. (2013): [Segurança e confiabilidade para ambiente SOHO](#), da revista HOLOS.
- Assista à série Mr. Robot. Direção: Sam Esmail. Produção: Sam Esmail. Estados Unidos: USA Network Inc., 2015. DVD (484 min.). Elliot (Rami Malek) é um jovem programador que trabalha como engenheiro de segurança virtual durante o dia, e como hacker vigilante durante a noite. Elliot se vê numa encruzilhada quando o líder (Christian Slater) de um misterioso grupo de hacker o recruta para destruir a firma que ele é pago para proteger. Motivado pelas suas crenças pessoais, ele luta para resistir à chance de destruir os CEOs da multinacional que ele acredita estarem controlando – e destruindo – o mundo.

## Referências

CIRNE, L. O processo de transição para a TV digital no Brasil: um olhar sobre o cenário de interesses e de entraves políticos. Revista Compolítica, Rio de Janeiro, v. 9, n. 1, 2019. Disponível

em: <https://revista.compolitica.org/index.php/revista/article/view/181>. Acesso em: 2 abr. 2024.

KUROSE, J. F. **Redes de computadores e a internet**: uma abordagem top-down. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

MEDEIROS, R. M. *et al.* Uma análise de desempenho da rede metropolitana de telemedicina dos hospitais universitários da cidade de Natal-RN/Brasil. **HOLOS**, Natal, v. 30, n. 4, 2014. Disponível em: <https://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/987>. Acesso em: 2 abr. 2024.

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

OLIVEIRA, D. B.; LUMMERTZ, R. S.; SOUZA, D. C. **Qualidade e desempenho de redes**. Porto Alegre: Sagah, 2019.

POLSONETTI, C. What are Industrial Network Gateways? **ARC Advisory Group**, 4 jan. 2018. Disponível em: <https://www.arcweb.com/blog/what-industrial-network-gateways>. Acesso em: 5 abr. 2024.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Aula 4

Topologias de Redes e Classificação de Redes

### Topologias de redes e classificação de redes



#### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

## Ponto de Partida

Olá, estudante!

As redes de computadores podem ser organizadas em diferentes topologias, como malha, estrela, barramento, anel e híbrida, cada uma com vantagens e desvantagens específicas. Além disso, as redes são classificadas com base em sua abrangência, como PAN, LAN, MAN, WAN e SAN, adequadas a diferentes necessidades de conectividade. As redes sem fio, como o Wi-Fi, oferecem mobilidade, mas podem ter alcance limitado e enfrentar questões de segurança. Esses conceitos básicos são fundamentais para iniciantes em redes de computadores.

Imagine que você é um administrador de rede em uma pequena empresa que está planejando atualizar sua infraestrutura de rede. A empresa atualmente possui uma rede de computadores com fios, mas está considerando a implementação de uma sem fio para fornecer mais mobilidade aos funcionários. Além disso, deseja melhorar a confiabilidade e a escalabilidade da rede. Você foi encarregado de avaliar as diferentes topologias de rede e ajudar a escolher a melhor opção.

### Requisitos do cliente:

A empresa tem os seguintes requisitos para sua nova rede:

- **Melhor mobilidade:** ela deseja que os funcionários tenham a capacidade de se mover livremente dentro do escritório e ainda permanecerem conectados à rede.
- **Confiança e redundância:** a empresa valoriza a confiabilidade e deseja uma rede que continue funcionando mesmo se ocorrerem falhas em alguns dispositivos ou conexões.
- **Facilidade de gerenciamento:** ela prefere uma rede de fácil gerenciamento que não demande muita manutenção.
- **Baixo custo:** como é pequena, a empresa deseja manter os custos sob controle.

Agora é mão na massa, e vamos montar a rede para este cliente! Bons estudos!

## Vamos Começar!

## Topologias de redes de computadores

Segundo Kurose (2006), a topologia de uma rede pode ser dada como uma representação geométrica da relação dos links entre os equipamentos. Estão divididas em:

- **Malha:** nesta topologia, cada um dos equipamentos da rede possui uma conexão dedicada com os demais da rede. A transferência de informações ocorre entre dois equipamentos.

Veja a representação desta topologia a seguir (Figura 1):

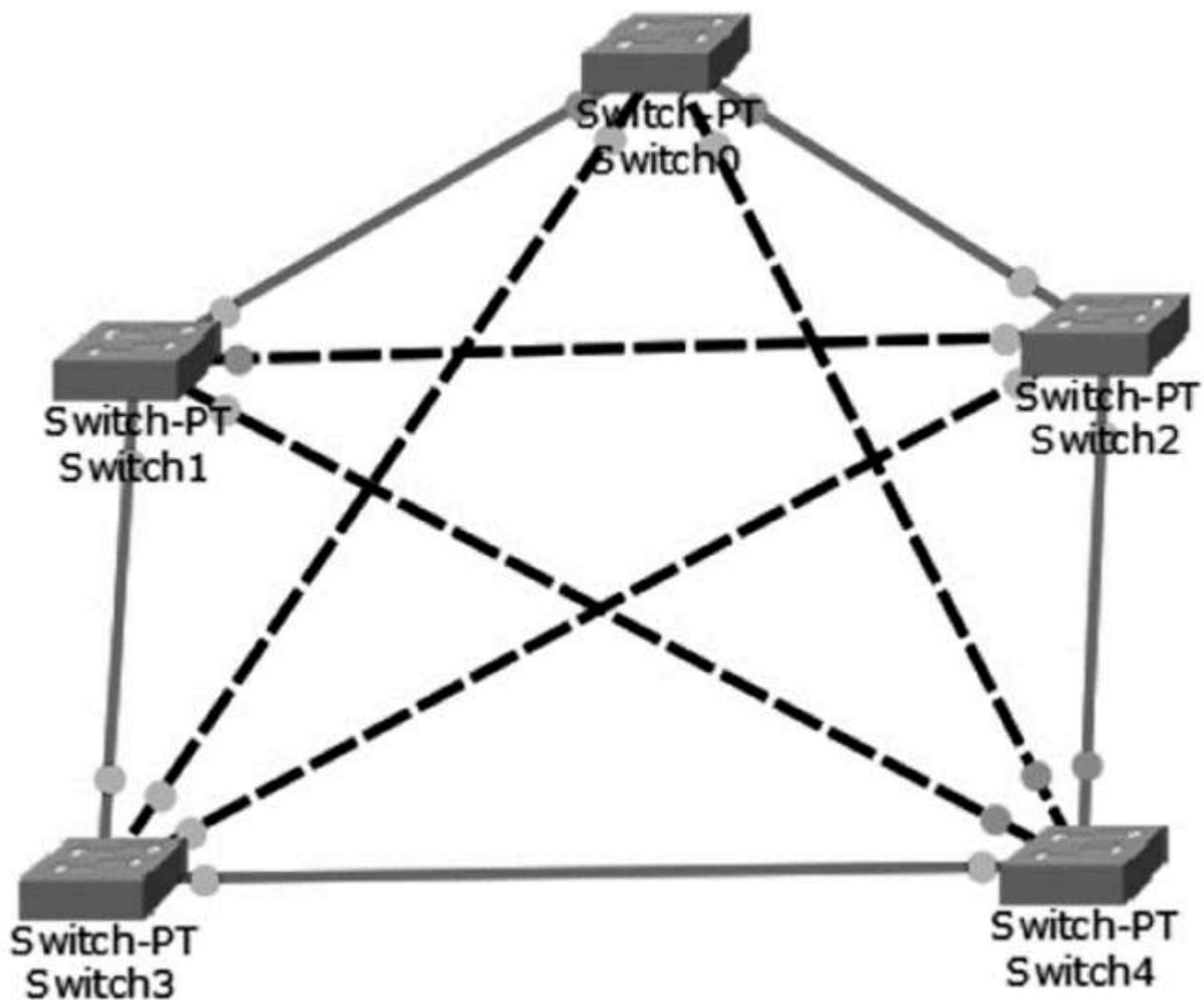


Figura 1 | Exemplo de topologia em malha. Fonte: elaborada pelo autor.

Souza *et al.* (2021) explicam que uma rede necessita de links entre todos os *switches* da empresa, a fim de garantir a continuidade dos seus serviços na ocorrência de falha de um ou mais dos seus links. O administrador da rede sabe que pode contar com backup das conexões. Tem vantagens, como alta redundância, confiabilidade e escalabilidade. Caso um link falhe, a rede ainda permanece ativa. Entretanto, as desvantagens são a alta complexidade e custos de implementação, devido ao grande número de conexões diretas. Podemos utilizar em redes de data centers, onde a confiabilidade e a redundância são essenciais.

- **Estrela:** nesta topologia, cada dispositivo possui uma conexão ponto a ponto com um centralizador, podendo este ser um *hub*, roteador ou *switch*. Tem vantagens da simplicidade, facilidade de gerenciamento e falhas em um dispositivo não afetam outros. A desvantagem é a dependência do nó central (*hub* ou *switch*); uma falha nele paralisa a rede

toda. Podemos utilizar em redes domésticas e de escritórios, nas quais a simplicidade e a gerenciabilidade são importantes. Veja a Figura 2 a seguir.

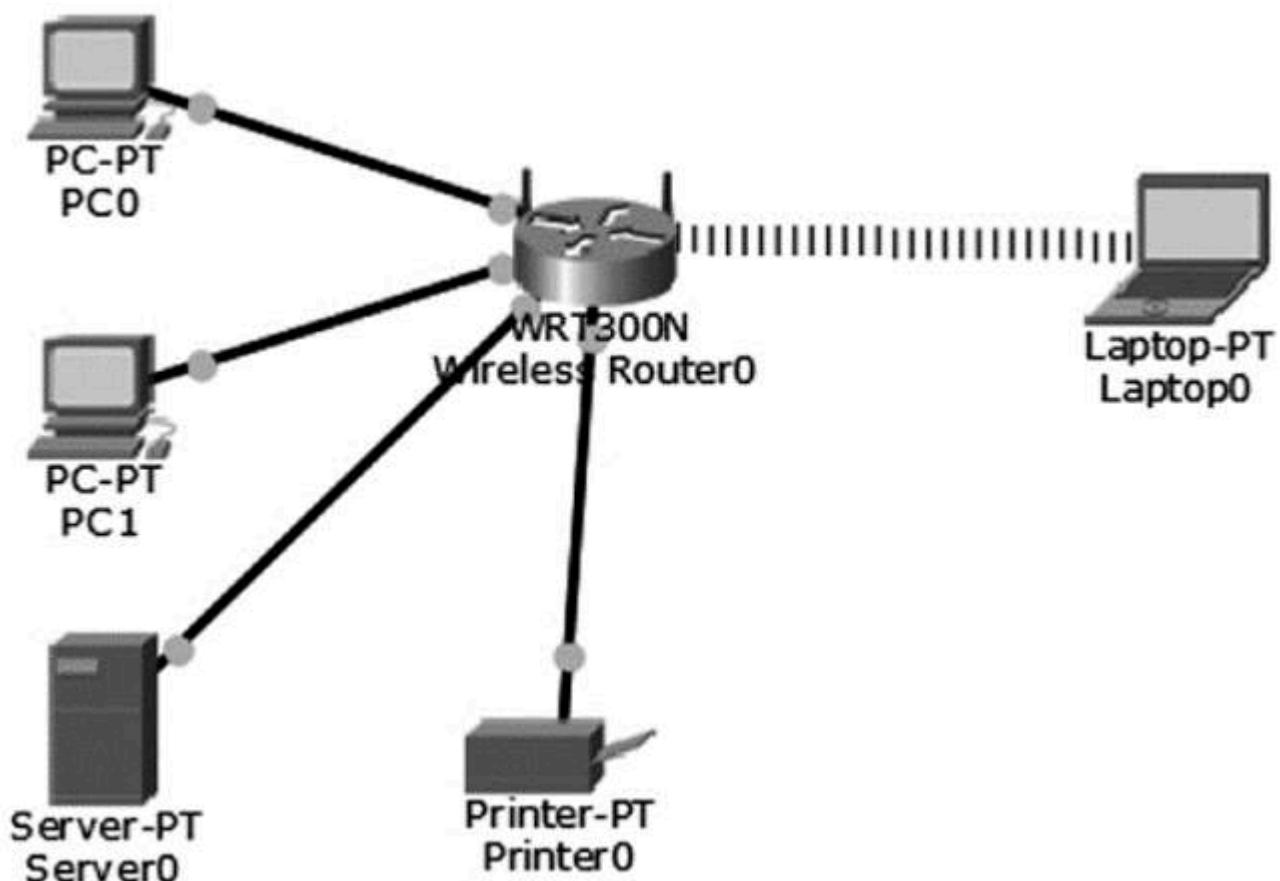


Figura 2 | Exemplo de rede estrela. Fonte: elaborada pelo autor.

Os dispositivos não estão diretamente ligados entre si, porém ainda assim é possível efetuar o compartilhamento de seus recursos.

- **Barramento:** esta topologia é considerada ponto a ponto, pois, para fazer a conexão ,é necessário um backbone (tronco central) para interligar os dispositivos. Suas vantagens são simplicidade, baixo custo e facilidade de instalação. As desvantagens são conflitos de colisão, limitações de distância e escalabilidade limitada. O uso é em redes Ethernet tradicionais (ex.: 10Base2) em ambientes pequenos. Veja na imagem abaixo.

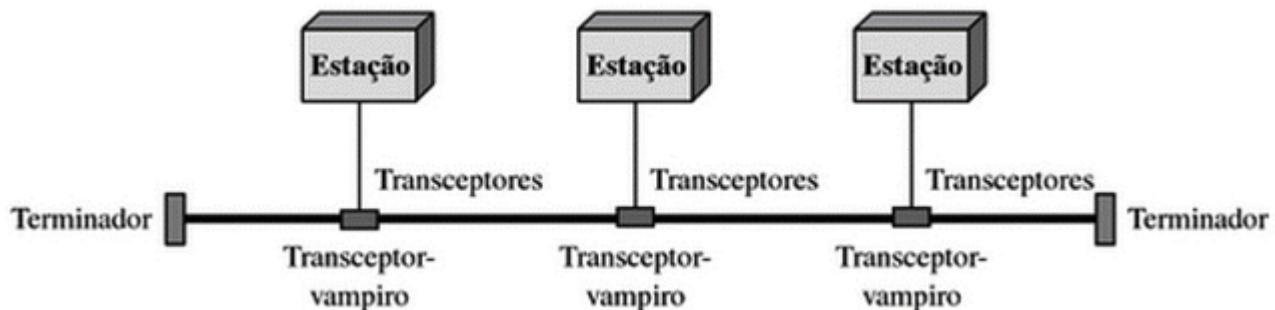


Figura 3 | Exemplo de topologia barramento. Fonte: Kurose (2006, p. 31).

Na maioria das casas onde há internet cabeada, as operadoras utilizam esse tipo de topologia. O backbone da rede é o cabo instalado nos postes nas ruas e as estações são os modems que estão diretamente ligados ao tronco principal.

- **Anel:** cada dispositivo possui uma conexão com o dispositivo ao lado, mais próximo, o sinal, quando enviado, percorre o anel até que o destino seja encontrado. As vantagens são eficiência em termos de largura de banda e desempenho previsível. As desvantagens são as falhas em um nó, que podem afetar a rede inteira, e a complexidade de implementação. É usado em redes *token ring* (menos comuns atualmente) e redes de fibra óptica. Veja uma representação da topologia em anel na Figura 4:

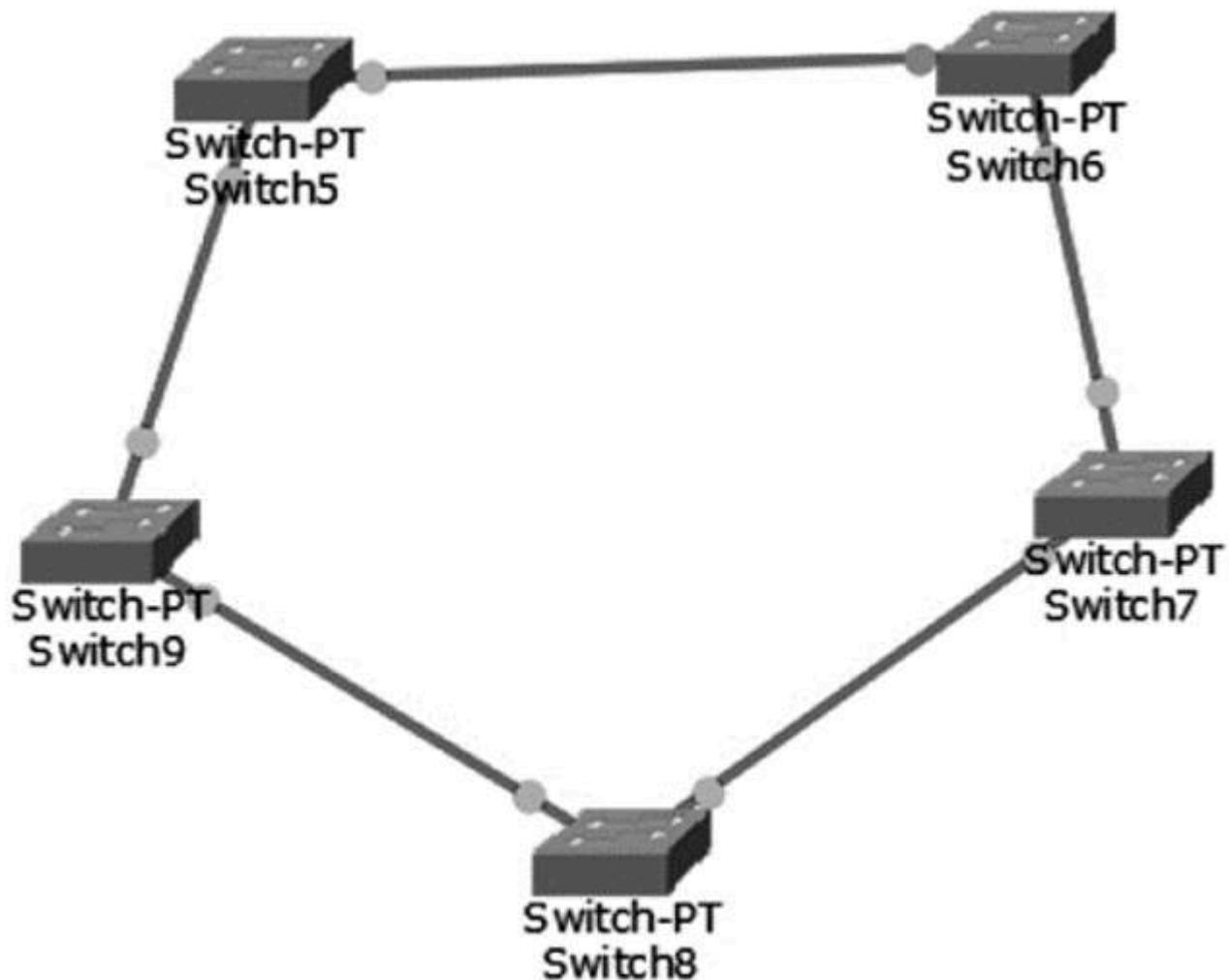


Figura 4 | Exemplo de topologia em anel. Fonte: elaborada pelo autor.

A topologia em anel é uma das mais fáceis de ser instalada e configurada em razão de possuir somente duas conexões em um nó na rede desta topologia.

- **Híbrida:** este tipo de formato de rede pode ser encontrado em muitas redes internas; podemos apontar as redes em estrela conectadas em um barramento (backbone). Podemos considerar a rede global como uma rede híbrida, uma vez que ela se forma da conexão de redes com as mais variadas tipologias. A vantagem desse tipo é que combina benefícios de diferentes topologias para atender a requisitos específicos. As desvantagens são complexidade e custos adicionais de implementação.

Podemos utilizar em redes de grande escala que exigem flexibilidade e redundância, como algumas redes de *campus* universitários.

Kurose (2006) defende que as aplicações das topologias podem variar conforme a disponibilidade de recursos e as necessidades de cada rede. Outro fator importante é que,

independentemente da topologia adotada pelo administrador de uma rede, todas elas apresentam algumas vantagens e desvantagens.

## Siga em Frente...

## Redes PAN, LAN, MAN, WAN e SAN

As redes de computadores podem ser classificadas quanto ao seu nível de abrangência, isto é, pelo alcance dos seus links e serviços. Segundo Forouzan (2006), as categorias estão divididas em PAN, LAN, MAN, WAN e SAN. Vejamos cada uma delas. Elas desempenham um papel fundamental em diferentes cenários de rede, desde comunicações pessoais até a conectividade em grande escala em nível mundial.

- **PAN (*personal area network – rede pessoal*):** uma PAN é uma rede de curto alcance destinada a dispositivos pessoais, como smartphones, laptops e tablets. Ela permite a conexão e a comunicação entre dispositivos pessoais próximos, geralmente em um raio de alguns metros. Um exemplo de seu uso é a conexão de dispositivos pessoais, como smartphones, fones de ouvido bluetooth e smartwatches, para transferência de dados e áudio em curtas distâncias. Por exemplo, você pode conectar seu smartphone ao seu fone de ouvido bluetooth para ouvir música.
- **LAN (*local area network – rede local*):** uma LAN é uma rede de área local que abrange uma área geográfica limitada, como um escritório, casa ou *campus*. Ela permite a conexão de dispositivos locais para compartilhar recursos e informações. Uma LAN é comumente usada em escritórios e empresas para permitir que computadores compartilhem impressoras, servidores de arquivos e acessem a internet em uma área local. Por exemplo, uma LAN de escritório permite que funcionários compartilhem documentos e recursos de rede. São projetadas para o compartilhamento de recursos computacionais (estação de trabalho). Normalmente as taxas de transmissão encontradas são de 100Mbps a 1000Mbps.
- **MAN (*metropolitan area network – rede metropolitana*):** uma MAN é uma rede de área metropolitana que abrange uma área geográfica maior, como uma cidade. Ela é usada para interconectar várias LANs dentro de uma região metropolitana. Um exemplo é a infraestrutura de rede usada por uma empresa de telecomunicações para interconectar várias LANs em diferentes bairros ou áreas de uma cidade. Isso permite a prestação de serviços de internet de alta velocidade em uma área metropolitana. Para exemplificar esse tipo de abrangência, há as redes Wi-Max (redes wi-fi de longo alcance) disponibilizadas em algumas cidades.
- **WAN (*wide area network – rede mundial*):** uma WAN é uma rede que se estende por uma vasta área geográfica, como um país ou continente. Ela é usada para conectar redes locais em locais distantes, geralmente por meio de serviços de telecomunicações. A internet é um exemplo típico de uma WAN, conectando redes locais e metropolitanas em todo o mundo. Os provedores de serviços de internet (ISPs) usam WANs para conectar cidades, países e continentes, permitindo comunicações globais. Sua velocidade de transmissão pode variar, pois são encontrados diversos meios e capacidades de links entre os nós.

- **SAN (storage area network – rede de armazenamento):** uma SAN é uma rede dedicada ao armazenamento de dados e a dispositivos de armazenamento, como discos rígidos e arrays de armazenamento. Ela permite o acesso e a gestão centralizada de recursos de armazenamento em uma rede separada da LAN principal. Empresas que gerenciam grandes volumes de dados, como data centers, utilizam SANs para conectar servidores a dispositivos de armazenamento compartilhados. Isso permite o armazenamento centralizado e a recuperação de dados de forma eficiente. Entre as abrangências encontradas, esta é a mais incomum, pois as tecnologias de análise de grandes volumes de dados para aplicação comercial são recentes.

Tanenbaum, Feamster e Wetherall (2021) explicam que as redes distribuídas podem abranger uma área geográfica dentro de uma organização, cidade, país ou continente, tendo como objetivo interligar um conjunto de dispositivos a fim de que algumas aplicações sejam executadas aos usuários. De uma forma mais abrangente, as redes podem ser definidas como geograficamente distribuídas (WAN), em que diversas LANs estão interligadas.

## Redes sem fio (Wi-Fi)

De acordo com Nunes (2017), redes sem fio, ou Wi-Fi, são tecnologias que permitem a conexão de equipamentos a uma rede de computadores sem a necessidade de cabos físicos. Essas redes utilizam ondas de rádio para transmitir dados entre os equipamentos, proporcionando mobilidade e flexibilidade. Os roteadores Wi-Fi são usados para criar pontos de acesso à rede sem fio em ambientes domésticos, empresariais e públicos. As redes Wi-Fi são amplamente utilizadas para conectar equipamentos como smartphones, laptops, tablets e smart TVs à internet e a outras redes, proporcionando conveniência e conectividade. No entanto, elas também apresentam desafios de segurança e podem sofrer interferências em ambientes lotados.

A internet sem fio se popularizou na maioria dos lares e locais de grande fluxo de pessoas, como terminais, restaurantes, praças etc. A tecnologia parece nova, porém a sua primeira aplicação data de 1901, segundo Tanenbaum, Feamster e Wetherall (2021), tendo sido utilizada para transmissão da mensagem de um navio para o litoral por código Morse. Nas redes atuais, há dois tipos de aplicações:

- **LAN sem fio:** são sistemas dotados por um modem de rádio e uma antena para a transmissão dos dados. A sua abrangência em área livre deve ficar restrita a um prédio, campus ou escritório, dependendo de quantos retransmissores são utilizados na topologia. O padrão de comunicação utilizado para as LANs é conhecido por IEEE 802.11, ou seja, wireless ou wi-fi (sem fio).
- **WAN sem fio:** são antenas de transmissão potentes o suficiente para cobrir uma rede geograficamente distribuída, com uma abrangência de uma cidade por exemplo. As velocidades podem variar conforme as características técnicas de transmissão e recepção do sinal. No Brasil, as operações pela tecnologia são conhecidas por WI-Max.

A vantagem da rede sem fio é a mobilidade: os dispositivos podem ser conectados sem fio, permitindo mobilidade dentro da área de cobertura. A implementação é relativamente simples, sem a necessidade de cabos físicos. Atualmente está amplamente disponível em locais públicos, residências e empresas. A desvantagem é alcance limitado de uma rede sem fio em comparação com redes com fio; especialmente em ambientes com muitas obstruções, redes sem fio podem sofrer interferências de dispositivos ou redes vizinhas, afetando o desempenho.

Há também a questão de segurança: as redes sem fio podem ser vulneráveis a invasões se não forem devidamente protegidas. As redes sem fio encontram-se em residências, escritórios, aeroportos, cafés e locais públicos para fornecer conectividade à internet e permitir que dispositivos como smartphones, laptops e tablets se conectem à rede sem a necessidade de cabos. Elas também são usadas em ambientes industriais para dar suporte a dispositivos móveis e à automação.

## Vamos Exercitar?

Agora vamos a resolução do estudo de caso proposto no início dessa aula, sobre a implementação da topologia de estrela na pequena empresa

Com base na recomendação da topologia de estrela, a seguir estão os passos a serem seguidos para implementar com sucesso essa topologia na pequena empresa:

### **Passo 1: planejamento da topologia de estrela**

Antes de qualquer implementação, é crucial realizar um planejamento detalhado da topologia de estrela. Isso inclui determinar a localização do *hub* central, identificar os pontos de acesso Wi-Fi necessários e dimensionar a capacidade da rede de acordo com as necessidades da empresa.

### **Passo 2: seleção de equipamentos**

Neste estágio, é essencial adquirir os equipamentos necessários, que incluem um *hub* central (*switch* ou roteador), pontos de acesso Wi-Fi, cabos de rede e outros dispositivos relevantes. Certifique-se de escolher equipamentos de qualidade que atendam às especificações da rede.

### **Passo 3: configuração do *hub* central**

Configure o *hub* central de acordo com as necessidades da rede. Isso inclui a configuração de portas, VLANs, segurança de rede, QoS (qualidade de serviço) e outras configurações relevantes. Também é importante garantir que o hub tenha uma fonte de alimentação de backup para manter a operação da rede em caso de falha de energia.

### **Passo 4: instalação dos pontos de acesso Wi-Fi**

Coloque os pontos de acesso Wi-Fi em locais estratégicos dentro do escritório para garantir uma cobertura adequada. Configure cada ponto de acesso para que ele esteja sincronizado com o *hub* central e forneça uma rede Wi-Fi segura. Defina senhas fortes e utilize criptografia para proteger a rede sem fio.

## Passo 5: teste e monitoramento

Após a instalação, realize testes para garantir que a rede esteja funcionando conforme o planejado. Isso inclui verificar a conectividade dos dispositivos, testar a mobilidade dentro do escritório e verificar a velocidade da rede. Além disso, configure um sistema de monitoramento para acompanhar o desempenho da rede e detectar possíveis problemas.

## Passo 6: treinamento dos usuários

Certifique-se de que os funcionários estejam cientes das mudanças na rede e forneça treinamento, se necessário. Explique como se conectar à rede sem fio, como manter as melhores práticas de segurança e como relatar problemas.

## Passo 7: implementação de medidas de segurança

Para garantir a segurança da rede, implemente medidas como firewalls, sistemas de detecção de intrusos e autenticação forte. Certifique-se de que as configurações de segurança estejam atualizadas e monitore constantemente a rede em busca de atividades suspeitas.

## Passo 8: manutenção contínua

A manutenção contínua é essencial. Realize atualizações de firmware e software regularmente, faça backup das configurações da rede e esteja preparado para lidar com problemas que possam surgir.

Com a implementação da topologia de estrela e a conclusão dos passos acima, a pequena empresa terá uma rede confiável, fácil de gerenciar e que oferece mobilidade aos seus funcionários. Certifique-se de que a equipe de TI esteja preparada para lidar com quaisquer desafios que possam surgir e continue monitorando a rede para garantir seu desempenho e segurança a longo prazo.

## Saiba mais

As redes de computadores abrangem diversas topologias, como estrela, anel e barramento, e podem ser categorizadas em PAN, LAN, MAN, WAN e SAN de acordo com sua escala geográfica. Além disso, as redes sem fio desempenham um papel crucial na conectividade atual, permitindo a comunicação sem cabos e viabilizando a mobilidade dos dispositivos. A seguir, confira algumas dicas de materiais de estudo complementar para seu aprendizado:

- Artigo [A educação na era da internet: entrevista com Michel Maffesoli](#), da revista Educação Temática Digital.
- Artigo [Tecnologias de informação móveis, sem fio e ubíquas: definições, estado-da-arte e oportunidades de pesquisa](#), da Revista de Administração Contemporânea.
- Artigo [Cidades inteligentes e mobilidade urbana: atores e práticas na cidade de Recife/PE](#), da Revista de Gestão e Secretariado.
- Filme: Silicon Cowboys (Caubóis do Silício). Direção: Jason Cohen. Produção: Ross M. Dinerstein. Estados Unidos: Campfire. 2016. DVD (77 min.). Em 1982, três amigos do Texas lançaram o computador portátil Compaq, uma tecnologia que logo os levou à batalha contra a IBM, uma das companhias de tecnologia mais poderosas do mundo que acaba com todos os seus concorrentes. O documentário conta sobre a Compaq, um concorrente improvável que alterou o futuro da computação e ajudou a moldar o mundo como conhecemos hoje.

## Referências

ALVES, F. L. *et al.* A educação na era da internet: entrevista com Michel Maffesoli. **Educação Temática Digital**, Campinas, v. 24, n. 1, 2022. Disponível em: <https://periodicos.sbu.unicamp.br/ojs/index.php/etd/article/view/8665214>. Acesso em: 2 abr. 2024.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 3<sup>a</sup> ed. Porto Alegre: Bookman, 2006.

KUROSE, J. F. **Redes de computadores e a internet: uma abordagem top-down**. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

NOGUEIRA, P.; *et al.* Cidades inteligentes e mobilidade urbana: atores e práticas na cidade de Recife/PE. **Revista de Gestão e Secretariado**, São Paulo, v. 14, n. 4, 2023. Disponível em: <https://ojs.revistagesec.org.br/secretariado/article/view/2025>. Acesso em: 2 abr. 2024.

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

SACCOL, A.; REINHARD, N. Tecnologias de informação móveis, sem fio e ubíquas: definições, estado-da-arte e oportunidades de pesquisa. **Revista de Administração Contemporânea**, Rio de Janeiro, v. 11, n. 4, 2007. Disponível em: <https://www.scielo.br/j/rac/a/wqFxPyfrPL6zgcBf4yZPzBq/?format=pdf>. Acesso em 2 abr. 2024.

SOUZA, D. C.; *et al.* **Gerenciamento de redes de computadores**. Porto Alegre: Sagah, 2021.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Aula 5

Encerramento da Unidade

### Fundamentos de redes de computadores



#### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

### Ponto de Chegada

Olá, estudante! A competência desenvolvida nesta Unidade é: “Compreender os fatos históricos que levaram à necessidade de comunicação mediante redes de computadores. Quais os meios utilizados na transmissão e comunicação; as possibilidades de implementação de aplicações nas redes; os equipamentos e a suas funções. Por meios desses aspectos básicos, você poderá desenvolver redes locais de pequeno porte”. Para desenvolver essa competência, você deverá primeiramente conhecer os conceitos fundamentais.

### Contexto histórico

A história das redes de computadores se desdobra ao longo das décadas, começando na de 1960 e evoluindo até os dias de hoje:

- **Década de 1961 a 1972:** nesse período inicial, os estudos e avanços iniciais relacionados a redes de computadores começaram a surgir. Isso foi influenciado pelo interesse na transmissão de dados após a Segunda Guerra Mundial.
- **Década de 1972 a 1980:** durante essa fase, houve avanços notáveis, incluindo a expansão da ARPANET (a precursora da internet) e o desenvolvimento de novas tecnologias e protocolos.
- **Década de 1980 a 1990:** a internet cresceu consideravelmente nesse período, juntamente com o desenvolvimento de protocolos-chave. Houve também uma disseminação de

computadores pessoais.

- **Década de 1990 a 2000:** a internet continuou a se expandir e a web se tornou popular. Novas tecnologias de rede surgiram, e houve um aumento na disponibilidade de serviços online, como vídeo sob demanda, VoIP e jogos online.
- **Anos 2000 a 2023:** nesse período mais recente, a internet continuou a crescer, com a proliferação de redes sociais e dispositivos móveis. Também ocorreu a expansão das tecnologias de comunicação, e diversos objetos do cotidiano, como carros e televisores, se tornaram conectados à internet. Isso possibilitou o surgimento de serviços como vídeo sob demanda, VoIP e streaming de música.

## Redes de computadores

São sistemas que conectam dispositivos de computação e de comunicação, permitindo a troca de dados e o compartilhamento de recursos tecnológicos. Essas redes usam protocolos de comunicação para transmitir informações por meio de tecnologias físicas ou sem fio. Elas transcendem distâncias geográficas e possibilitam o compartilhamento global de informações entre equipamentos, pessoas, empresas e organizações, proporcionando uma ampla gama de serviços. Analogamente, as redes de computadores são como estradas que conectam casas (computadores), permitindo a comunicação e o compartilhamento de informações.

Protocolos são as regras de trânsito que garantem a comunicação organizada e segura, enquanto os endereços IP funcionam como números de telefone para identificar computadores. Roteadores direcionam o tráfego de informações, e firewalls atuam como guardas de segurança, controlando o acesso à rede. As redes de computadores são fundamentais para a comunicação digital, possibilitando acesso à internet, redes sociais, mensagens, streaming, trabalho remoto, entre outros. Elas são essenciais para conectar dispositivos e facilitar a comunicação em nosso mundo digital.

## ISP/ Backbone

Os provedores de serviços de internet (ISPs) são organizações que viabilizam o acesso à internet. Eles oferecem uma variedade de serviços, como acesso à web, hospedagem, trânsito de internet e e-mail. O ISP é a ponte entre os usuários e a internet, sem a qual atividades como jogos online, mídias sociais e compras online seriam impossíveis. É como a rua que liga sua casa à “biblioteca” da internet. O ISP atua como um bibliotecário que ajuda a encontrar informações e encaminhar dados saindo de seu dispositivo e entrando nele. Além disso, os ISPs desempenham um papel fundamental na segurança, garantindo que apenas informações seguras circulem em sua “biblioteca”.

O “backbone” é como uma rodovia na rede da internet, permitindo que dados fluam rapidamente entre diferentes partes da rede. As redes locais (LANs) em escolas, empresas e residências se

conectam a esse “backbone”. É como dirigir seu carro até a rodovia para viajar entre cidades. Grandes empresas e provedores de serviços têm acesso direto ao backbone, de modo semelhante a cidades grandes com várias entradas na rodovia, oferecendo conexões rápidas e confiáveis.

O backbone é construído com redundâncias, garantindo que, mesmo em caso de problemas, os dados possam encontrar rotas alternativas para chegar ao destino. O backbone é essencial para a eficiência da internet, pois interconecta diferentes redes e permite a troca de informações. É uma parte fundamental da infraestrutura de rede e permite que a internet funcione de forma eficiente e global.

## Sinais analógicos e digitais

Sinais analógicos e digitais são duas formas de transmitir dados em redes de computadores:

- **Sinal analógico:** é uma onda eletromagnética que assume infinitos valores ao longo do tempo, caracterizada por sua amplitude (intensidade), frequência (quantidade de ciclos) e fase (formato da onda). No entanto, em redes modernas, o uso de sinais analógicos é raro devido às limitações de velocidade e qualidade de sinal, sendo substituído por tecnologias digitais mais eficazes.
- **Sinal digital:** é o método predominante nas redes atuais, representando dados em forma de bits (0 ou 1). A representação digital permite maior capacidade de transmissão de informações e é resistente a interferências. O processo de comunicação digital envolve a codificação dos dados em 0s e 1s, e é amplamente usado em redes de computadores, de LANs à Internet global.

## Transmissão guiada

- **Cabo de par trançado (*twisted pair*):** nesse tipo, os fios são enrolados de forma helicoidal, o que reduz a interferência, permitindo a transmissão de sinais analógicos e digitais. Existem diferentes categorias de cabos, como CAT 5, 5e, 6 e 7, cada uma com diferentes larguras de banda e níveis de desempenho. O cabo de par trançado é comum em redes locais (LANs).
- **Cabo coaxial (*coaxial cable*):** o cabo coaxial é usado em redes e sistemas de televisão a cabo. Ele consiste em um núcleo de cobre revestido por um condutor metálico, isolado por uma camada dielétrica e protegido por uma camada externa. O cabo coaxial é capaz de transmitir dados a distâncias maiores e com maior velocidade do que o par trançado, além de ser menos suscetível a ruídos. Existem duas variedades: coaxial 10Base2, para taxas de 10 Mbps em segmentos de até 185 metros, e cabo 10Base5, adequado para redes de banda larga com alcance de até 500 metros.
- **Fibra óptica (*optical fiber*):** a fibra óptica é amplamente usada em redes de alta velocidade e comunicações de longa distância. Ela é composta por filamentos de vidro ou plástico que

transmitem dados na forma de luz. A fibra óptica é conhecida por sua alta largura de banda e imunidade a interferências eletromagnéticas. Quando os dados são recebidos, o sinal óptico é convertido em sinal elétrico. Esse meio de transmissão pode atingir velocidades de até 10 terabytes por segundo.

## Transmissão não guiado

- **Rádio:** usado em torres de transmissão para enviar sinais a antenas receptoras. Sofre atenuação de obstáculos e interferências climáticas, o que pode afetar a qualidade do sinal.
- **Micro-ondas:** neste tipo de transmissão, as ondas viajam em linha reta, exigindo visada direta entre as antenas. É adequado para distâncias de até 80km em áreas planas.
- **Wi-Fi (*Wireless Fidelity*):** redes Wi-Fi usam ondas de rádio para transmitir dados sem fio; são amplamente usadas em LANs e conexões à internet sem fio.
- **Bluetooth:** uma tecnologia de curto alcance usada para conectar dispositivos como fones de ouvido, teclados e smartphones.
- **Redes celulares:** incluindo 4G e 5G, fornecem dados móveis em dispositivos móveis para acesso à internet e comunicação de voz.
- **Satélites:** esse tipo de rede usa satélites de comunicação para transmitir sinais de rádio de longa distância, como transmissões de TV via satélite e comunicações globais.
- **Redes *mesh* sem fio:** dispositivos comunicam-se autonomamente, formando redes auto-organizadas, usadas em redes de sensores, IoT e áreas urbanas.
- **Infravermelho (IR):** usado em comunicação ponto a ponto de curto alcance, como controles remotos de TV.
- **Zigbee:** padrão de comunicação sem fio usado em automação residencial.
- **NFC (*Near Field Communication*):** comunicação de curto alcance para troca de informações entre dispositivos próximos.

## Hardwares básicos: placas de rede, modem, hub e switch

A base da conectividade moderna é formada pelas redes de computadores, que permitem a comunicação global, compartilhamento de dados e acesso a recursos em tempo real. Para viabilizar essa conexão, diversos componentes de hardware desempenham funções cruciais. Nesta seção, exploraremos os principais hardwares essenciais em ambientes de rede de computadores.

- **Placas de rede (*Network Interface Cards – NICs*):** esses dispositivos de entrada/saída (E/S) se conectam a dispositivos de rede, como hubs, roteadores, switches e bridges, por meio de cabeamento. As NICs podem ser integradas à placa-mãe e se encaixar em slots de diferentes formatos, como PCI, PCI Express, ISA e USB. Elas desempenham um papel crucial no tratamento de endereçamento durante a transmissão e recepção de mensagens.

- **Modem:** um modem é responsável pela modulação e demodulação de sinais, permitindo a transmissão de dados. Existem diferentes tipos de modems, incluindo modems residenciais com conexões por fio, 4G/5G e fibra óptica, que podem ter Wi-Fi integrado. Eles são amplamente utilizados para acesso à internet.
- **Hub:** os *hubs* são dispositivos que distribuem sinais de conexão na rede interna. No entanto, eles operam como repetidores de sinal, replicando informações para todas as portas. Isso pode levar a problemas de desempenho, já que todas as mensagens são enviadas para todos os dispositivos conectados.
- **Switch:** os *switches* também têm várias portas, mas diferem dos *hubs* porque possuem controle de colisão em cada porta. Isso permite que eles direcionem mensagens para portas específicas, melhorando o desempenho e reduzindo a ocupação da largura de banda.
- **Roteador:** os roteadores contêm microprocessadores que gerenciam o tráfego de pacotes de dados e analisam o endereçamento lógico (TCP/IP). Eles formam tabelas lógicas de dispositivos na rede, evitando colisões de dados. Os roteadores também são usados para roteamento de mensagens e são essenciais na comunicação de redes de computadores.
- **Bridges (pontes):** as pontes são dispositivos semelhantes a *switches*; são usadas para conectar duas redes locais (LANs). Elas são úteis quando é necessário interligar redes distintas.
- **Gateway:** os *gateways* são dispositivos ou software que atuam como interfaces entre redes diferentes, permitindo a comunicação e a transferência de informações entre elas. Eles traduzem protocolos de comunicação e regras para que redes incompatíveis se tornem compatíveis.

## Modos de transmissão

- **Simplex:** a transmissão ocorre em apenas uma direção, ou seja, unidirecional.
- **Half-duplex:** a transmissão ocorre em ambas as direções, mas não simultaneamente. Os dispositivos alternam entre transmitir e receber.
- **Full duplex:** a transmissão é bidirecional e ocorre simultaneamente, permitindo a transmissão e recepção de dados ao mesmo tempo.
- **Multiplexação:** permite que vários sinais compartilhem o mesmo meio de transmissão, como TDM (*Time-Division Multiplexing*) e FDM (*Frequency-Division Multiplexing*).

## Topologias de redes de computadores

- **Topologia de malha:** nesta configuração, cada dispositivo da rede possui uma conexão direta dedicada a todos os outros dispositivos, proporcionando alta redundância e confiabilidade, mas também aumentando a complexidade e custo. É útil em redes de *data centers*.

- **Topologia em estrela:** cada dispositivo se conecta a um ponto central, como um *hub*, roteador ou *switch*. Isso simplifica a gestão, mas a falha no ponto central pode paralisar a rede. É comum em redes de escritórios e domésticas.
- **Topologia em barramento:** os dispositivos se conectam a um tronco central (backbone) em um arranjo ponto a ponto. Isso é simples e de baixo custo, mas pode ter conflitos de colisão e limitações de distância. Usado em redes Ethernet tradicionais.
- **Topologia em anel:** cada dispositivo está conectado ao dispositivo mais próximo, com os dados percorrendo o anel até atingir o destino. Oferece eficiência em termos de largura de banda, mas a falha em um nó pode afetar a rede inteira. Utilizado em redes *Token Ring* e redes de fibra óptica.
- **Topologia híbrida:** combina elementos de diferentes topologias para atender a necessidades específicas. É usado em redes de grande escala que exigem flexibilidade e redundância, como *campi* universitários.

## Classificação de redes por alcance

- **PAN (Personal Area Network – rede pessoal):** rede de curto alcance para dispositivos pessoais, como smartphones e laptops, permitindo a conexão e a comunicação em curtas distâncias; por exemplo, fones de ouvido bluetooth.
- **LAN (Local Area Network – rede local):** abrange uma área geográfica limitada, como um escritório, permitindo a conexão de dispositivos locais para compartilhar recursos e informações.
- **MAN (Metropolitan Area Network – rede metropolitana):** interconecta várias LANs em uma área metropolitana maior, usando serviços de telecomunicações, como infraestrutura para internet de alta velocidade na cidade.
- **WAN (Wide Area Network – rede mundial):** estende-se por vastas áreas geográficas, conectando redes locais em grandes distâncias; um exemplo é a própria internet, com uso de serviços de telecomunicações em nível global.
- **SAN (Storage Area Network – rede de armazenamento):** rede dedicada ao armazenamento de dados, utilizada para conectar servidores a dispositivos de armazenamento compartilhados, permitindo o armazenamento centralizado e eficiente de dados.
- **Redes sem fio (Wi-Fi):** utilizam ondas de rádio para conectar dispositivos a uma rede de computadores, oferecendo mobilidade e flexibilidade, mas apresentando desafios de segurança e possíveis interferências em ambientes lotados. Amplamente utilizadas em residências, empresas e locais públicos para conexão sem fio a dispositivos, como smartphones e laptops.

**É Hora de Praticar!**

Este conteúdo é um vídeo!



Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Ao configurar sua rede doméstica com Wi-Fi, você pode compartilhar a internet e recursos entre dispositivos de maneira conveniente. Lembre-se de manter suas configurações de segurança atualizadas para proteger sua rede contra ameaças. À medida que você adquire mais conhecimento em redes de computadores, poderá explorar configurações avançadas e expandir sua rede conforme necessário.

Agora, para aplicar seus conhecimentos, você deverá montar uma rede doméstica para compartilhar a internet e recursos com outros dispositivos, como smartphones e laptops. A história das redes de computadores ao longo das décadas forneceu uma base para você entender os princípios básicos necessários para criar essa rede. Neste estudo de caso, vamos explorar como configurar sua rede doméstica com Wi-Fi.

## Objetivo:

- Configurar uma rede doméstica com Wi-Fi para compartilhar a internet e recursos entre dispositivos.
- Você pode propor diferentes formas de solução e chegar ao mesmo objetivo. Qual foi o seu modelo de configuração? Mão à obra!
- Como a evolução das redes de computadores ao longo das décadas afetou diretamente a maneira pela qual as pessoas se comunicam, trabalham e acessam informações? Quais são os marcos mais significativos nesse processo de evolução?
- Quais são os principais desafios enfrentados na escolha de uma topologia de rede específica para uma determinada aplicação? Como a escolha da topologia pode afetar a eficiência, segurança e escalabilidade da rede?
- Considerando a importância das redes de computadores em nossa vida cotidiana, como a segurança das redes, incluindo a proteção contra invasões e vazamentos de dados, pode ser aprimorada à medida que a tecnologia de rede continua a evoluir? Quais são os principais aspectos a serem considerados nesse contexto?

Estudante, veja a seguir a proposta de resolução para este estudo de caso:

## Passo 1: hardware necessário

Antes de configurar sua rede, você precisará dos seguintes componentes de hardware:

- Modem (fornecido pelo seu provedor de serviços de internet – ISP).
- Roteador Wi-Fi.
- Placas de rede Wi-Fi para dispositivos sem fio, como laptops e smartphones.
- Cabos Ethernet (opcional, para dispositivos com fio).
- Computador para configurar o roteador.

## Passo 2: configurando o roteador Wi-Fi

Conecte o roteador ao modem usando um cabo Ethernet.

Ligue o roteador e espere alguns minutos para que ele inicialize.

No seu computador, abra um navegador da web e digite o endereço IP padrão do roteador (geralmente algo como 192.168.0.1 ou 192.168.1.1). Consulte o manual do roteador para encontrar o endereço correto.

Faça login no painel de controle do roteador usando as credenciais padrão (também no manual). Configure as informações de conexão com a internet fornecidas pelo seu ISP, como nome de usuário e senha.

Configure as configurações Wi-Fi, como o nome da rede (SSID) e a senha. Certifique-se de usar uma senha forte para proteger sua rede.

Salve as configurações e reinicie o roteador, se necessário.

#### **Passo 3: conectando dispositivos**

Ligue seus dispositivos Wi-Fi, como laptops e smartphones.

Procure a rede Wi-Fi que você configurou no passo anterior (SSID) e conecte-se a ela usando a senha.

Se desejar, você também pode conectar dispositivos com fio ao roteador usando cabos Ethernet.

#### **Passo 4: testando a rede**

Abra um navegador da web em seu laptop ou smartphone e verifique se você pode acessar sites.

Certifique-se de que todos os dispositivos estejam conectados à rede e funcionando corretamente.

#### **Passo 5: manutenção e segurança**

Certifique-se de atualizar regularmente o firmware do seu roteador para proteger sua rede contra vulnerabilidades.

Altere as senhas padrão do roteador e do Wi-Fi para algo mais seguro.

Configure medidas de segurança, como firewalls e filtragem de MAC, se desejar.

## REDES DE COMPUTADORES

**1**

### HISTÓRICO

Nas décadas de 60 a 80, houve avanços notáveis, incluindo a expansão da ARPANET e o desenvolvimento de novas tecnologias. A década. Nos anos 2000 até 2023, proliferação de redes sociais e dispositivos móveis.

**2**

### REDES DE COMPUTADORES

São sistemas que conectam dispositivos, permitindo a troca de dados por meio de protocolos. Elas são como estradas que conectam computadores, e os protocolos são as regras de trânsito.

**3**

### ISP/BACKBONE

Os ISP são como pontes que ligam os usuários à internet, oferecendo uma variedade de serviços, incluindo acesso à web, hospedagem e e-mail. O "backbone" é a rodovia da internet, permitindo a rápida transmissão de dados entre diferentes partes da rede.

**4**

### SINAIS/TRANSMISSÕES

Sinais em redes de computadores podem ser analógicos ou digitais. A transmissão de dados pode ser guiada por meio de cabos como par trançado, cabo coaxial e fibra óptica. A transmissão não guiada utiliza tecnologias sem fio, como rádio, micro-ondas, Wi-Fi, Bluetooth, redes celulares (4G e 5G).

**5**

### HARDWARE DE REDE

A base de conectividade moderna é formada pelas redes de computadores, que permitem a comunicação global, compartilhamento de dados e acesso a recursos em tempo real. Para viabilizar essa conexão, diversos componentes de hardware desempenham funções cruciais.

**6**

### TRANSMISSÃO/TOPOLOGIA

Modos de transmissão: Simplex (unidirecional), Half-duplex (alternância entre transmitir e receber) e Full duplex (transmissão simultânea). Multiplexação permite compartilhar o meio de transmissão. Topologias de redes: Malha (alta redundância), Estrela (conexão a um ponto central), Barramento (conexão a um tronco central), Anel (eficiência em largura de banda) e Híbrida (combinação de topologias).

KUROSE, J. F. *Redes de computadores e a internet: uma abordagem top-down*. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

NAKAMURA, E. T. **Segurança da informação e de redes.** Londrina: Editora e Distribuidora Educacional S.A., 2016.

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

OLIVEIRA, D. B.; LUMMERTZ, R. S.; SOUZA, D. C. **Qualidade e desempenho de redes.** Porto Alegre: Sagah, 2019.

SOUZA, D. C.; *et al.* **Gerenciamento de redes de computadores.** Porto Alegre: Sagah, 2021.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores.** 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Unidade 2

### Modelo de Referência ISO/OSI e Arquitetura TCP/IP

#### Aula 1

Modelo de Referência ISO/OSI

#### Modelo de referência ISO/OSI



##### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

#### Ponto de Partida

Olá, estudante!

Vamos aprender sobre as camadas do modelo OSI e a necessidade de padronização em redes de computadores. Considerando as redes de computadores e o modelo OSI, que é fundamental

para entender como as redes funcionam, você será capaz de apontar soluções para os questionamentos a seguir ao fim desta aula:

- O que é o modelo OSI e por que ele é importante em redes de computadores?
- O modelo OSI divide as funções de uma rede em quantas camadas?
- Por que surgiu a necessidade de padronização no campo das redes de computadores?
- Como a padronização ajuda a resolver problemas em redes de computadores?
- Quais os tipos de equipamentos de redes que desempenham funções em camadas específicas do modelo OSI? Em qual camada cada um deles operam?

Você vai conhecer cada área, as camadas do modelo OSI e de suas funções principais. Aprenderá as dificuldades que surgem quando diferentes fabricantes criam dispositivos de rede sem seguir um padrão comum. Verá como a padronização permite a interoperabilidade entre dispositivos de diferentes fabricantes. Estudará os dispositivos que utilizam este padrão, como roteadores, *switches* e firewalls, e sua relação com as camadas do modelo OSI em que operam.

Esses questionamentos o ajudarão a compreender a importância do modelo OSI e como a padronização é essencial para o funcionamento eficiente das redes de computadores, enquanto também enfoca a aplicação prática por meio de equipamentos de redes.

Agora é mão na massa, e vamos responder a essas questões! Bons estudos!

## Vamos Começar!

## O modelo ISO/OSI e a padronização das redes

A compreensão das características técnicas e concepção do modelo de referência OSI permite a compreensão da forma na qual os protocolos de comunicação foram desenvolvidos e como proveem os serviços de rede utilizados diariamente (mensagens instantâneas, e-mail, acesso a sites, streaming, jogos online e diversos outros), possibilitando que você possa configurar os serviços necessários nas redes.

Os passos necessários para desenvolver a padronização podem variar conforme o tipo de aplicação ou a entidade que fará os estudos. Essas entidades que efetuam esse tipo de trabalho estão espalhadas pelo mundo. Podemos destacar as seguintes:

- ISO (*International Organization for Standardization*) – organização não governamental responsável pela padronização. É dividida em: ANSI (American National Standards Institute); ABNT (Associação Brasileira de Normas Técnicas); ANFOR (Associação Francesa); DIN (Associação Alemã).
- EIA (*Electronic Industries Association*) – grupo que visa à padronizações das transmissões elétricas.
- IEEE (*Institute of Electrical and Electronics Engineers*) – a maior organização internacional de desenvolvimento e padronização nas áreas de engenharia elétrica e computação.

- ITU-T (*Telecommunication Standardization Sector*) – entidade responsável pela padronização dos assuntos relacionados a telecomunicações.

Para poder se comunicar, as redes de computadores necessitavam de uma forma padrão que fosse conhecida e usada em todo o mundo. Por esta razão, ocorreu um importante processo de desenvolvimento quando a ISO (*International Standards Organization*), em um profundo estudo com os seus engenheiros, instituiu o modelo de referência OSI (*Open Systems Interconnection – sistemas abertos de conexão*).

Segundo Tanenbaum, Feamster e Wetherall (2021), o desejo da ISO era desenvolver uma forma universal de interconexão de sistemas abertos. Para atender essa forma universal, foi desenvolvido um modelo em sete camadas, que deveria atender aos seguintes requisitos:

- Cada camada deve executar a função à qual foi destinada.
- A função das camadas deve ser escolhida em razão dos protocolos que foram padronizados.
- Os limites entre as camadas devem ser escolhidos a fim de minimizar os esforços do fluxo das mensagens pelas interfaces.
- O número de camadas deve ser do tamanho suficiente para alocar todas as funcionalidades possíveis nas redes.

A ISO, no começo da década dos anos 80, conseguiu reunir algumas empresas para iniciar o projeto de padronizar a forma de comunicação das redes de computadores. Em meados 1984, foi criado um padrão para os hardwares e softwares de alguns fabricantes, como também o modelo de referência para que fossem desenvolvidos os protocolos, para interagir com os dispositivos de rede.

Tanenbaum, Feamster e Wetherall (2021) explicam que o modelo de referência OSI efetua todos os processos necessários para que ocorra a transmissão de dados, fazendo com que as camadas (*layers*) nele existentes efetuem a divisão dos processos lógicos. Isso significa que um determinado fabricante tem a liberdade de desenvolver o seu protocolo, desde que utilize como referência os parâmetros determinados pelo OSI, o que é conhecido como “Protocolo Proprietário”.

Com todo esse desenvolvimento, a ISO criou o modelo de referência OSI (*Open Systems Interconnection – sistemas abertos de conexão*), um marco para os protocolos de comunicação, utilizados nos serviços consumidos diariamente pela rede e internet. Podemos conhecer a arquitetura do modelo a seguir:

7	<b>Aplicação</b>
6	<b>Apresentação</b>
5	<b>Sessão</b>
4	<b>Transporte</b>
3	<b>Rede</b>
2	<b>Enlace</b>

1	Física
---	--------

Quadro 1 | Modelo de referência OSI. Fonte: elaborado pelo autor.

De acordo com Kurose (2006), antes da criação do modelo de referência OSI, as redes de computadores eram fragmentadas e heterogêneas, com diferentes fabricantes desenvolvendo sistemas de comunicação incompatíveis entre si. Isso dificultava a interoperabilidade e a expansão das redes, uma vez que era necessário um grande esforço para fazer dispositivos de fabricantes distintos funcionarem juntos.

Nunes (2017) destaca que, nesse cenário, a padronização tornou-se extremamente necessária; o modelo ISO/OSI foi criado para resolver esse problema. Ele divide o processo de comunicação em sete camadas, cada uma com funções específicas e bem definidas, desde a camada física, que lida com a transmissão de bits, até a camada de aplicação, que permite a interação com os aplicativos de usuário.

Essa estrutura padronizada permitiu a criação de redes mais flexíveis e compatíveis, nas quais dispositivos de diferentes fabricantes podiam interagir sem problemas. A padronização facilitou o desenvolvimento de tecnologias de rede, a integração de novos dispositivos e a escalabilidade das redes. A padronização promoveu a inovação, uma vez que os fabricantes puderam se concentrar no aprimoramento das camadas específicas do modelo, sabendo que a interoperabilidade seria mantida.

## Siga em Frente...

### Camadas do modelo ISO/OSI: física, enlace e de rede

O modelo de referência OSI não é exatamente a arquitetura dos protocolos de rede, mas sim uma referência de como os protocolos devem ser estruturados.

<b>Camadas de Meios</b>	<b>3. Rede</b> (Determinação de caminho e endereçamento lógico (IP).)
<b>Pacotes</b>  <b>Quadros</b>	<b>2. Enlace de dados</b> (Endereçame

		nto físico MAC e LLC)
	1. Física (Transmissão de mídia e de sinal binários)	
Bits		

Quadro 2 | Camadas física, enlace e de rede. Fonte: elaborado pelo autor.

Tanenbaum, Feamster e Wetherall (2021) definem assim as características e funcionalidades de cada uma das camadas:

- **Camada física:** nesta camada está definida a forma de transmissão dos bits pelo canal de comunicação. Deve ser determinada a voltagem que representa os bits 0s e 1s, o tempo de duração dos bits (em nanossegundos) e o método de transmissão (*simplex*, *half-duplex* ou *full duplex*). Entre os equipamentos descritos nesta camada estão os hubs, repetidores e cabos. A camada física, a primeira do modelo ISO/OSI, trabalha com a transmissão de bits através de meios físicos, como cabos de cobre, fibras ópticas ou ondas de rádio. Nesta camada, os dispositivos de rede, como computadores e roteadores, convertem os dados em sinais elétricos ou ópticos para que possam ser transmitidos. Um exemplo prático é o cabo Ethernet utilizado para conectar um computador a um *switch*. O cabeamento, as voltagens e a frequência dos sinais são elementos da camada física.
- **Camada de enlace:** os dados provenientes da camada física são transformados em quadros, o que facilita a detecção de erros, para que não sejam repassados à camada de rede. Os dados são divididos em algumas centenas de quadros para assim serem transmitidos. Entre os equipamentos utilizados nesta camada estão as placas de redes (endereço de MAC), os *switches* e bridges. A camada de enlace é responsável pela detecção e correção de erros na comunicação entre dispositivos conectados diretamente. Ela também lida com o controle de acesso ao meio, garantindo que vários dispositivos não transmitam simultaneamente e causem colisões de dados. Um exemplo é o protocolo Ethernet, que opera nessa camada e utiliza endereços MAC (*Media Access Control*) para identificar dispositivos em uma rede local. Quando um dispositivo envia um quadro de dados, a camada de enlace certifica que ele chegue ao destino sem erros e no momento correto.
- **Camada de rede:** a forma como os dados são roteados da origem até o seu destino é definida nesta camada. As tabelas referentes às rotas podem ser estáticas, e os dispositivos vizinhos são responsáveis por manter a tabela de roteamento atualizada. Como em alguns casos, o caminho mais curto não é o mais rápido, pois os links podem possuir diferentes velocidades. O controle do congestionamento (gargalo de rede) também é efetuado nessa camada. A camada de rede, por sua vez, trata do roteamento dos pacotes de dados entre redes distintas. Ela é responsável por determinar o melhor caminho para os dados viajarem de um ponto A para um ponto B através de uma série de roteadores. Um exemplo comum é o protocolo IP (*Internet Protocol*), que opera na camada de rede e usa

endereços IP para identificar dispositivos em diferentes redes. Quando você acessa um site, os pacotes de dados são roteados pela camada de rede através de vários roteadores até chegarem ao servidor web de destino, realizando o seu acesso.

Com exemplos práticos, como o uso de cabos Ethernet, endereços MAC e o protocolo IP, fica mais claro como essas camadas funcionam em conjunto para possibilitar a conectividade em redes modernas.

## **Camadas do modelo ISO/OSI: transporte, sessão, apresentação, aplicação**

Com a aceitação do modelo de referência OSI pelas empresas de hardware, em pouco tempo o mercado já contava com a disponibilidade das normas e padrões. Percebemos isso nos equipamentos como roteadores, smartphones e notebooks, que permitem acesso aos recursos em qualquer infraestrutura de redes de computadores. Segundo Nunes (2017), a camada de transporte assegura a entrega confiável dos dados; a camada de sessão estabelece e mantém a conexão; a camada de apresentação lida com a formatação dos dados; e a camada de aplicação é aquela na qual as aplicações interagem diretamente com o usuário. Tanembaum, Feamster e Wetherall (2021) definem assim as características e funcionalidades de cada uma dessas camadas:

<b>Camadas de Host</b>	Dados	<b>7. Aplicação</b> Processo da rede para o aplicativo
	Dados	<b>6. Apresentação</b> Representação e criptografia de dados
	Dados	<b>5. Sessão</b> Comunicação entre hosts
	Segmentos	<b>4. Transporte</b> Conexões e confiabilidade de ponta a ponta

Quadro 3 | Camadas transporte, sessão, apresentação e aplicação. Fonte: elaborado pelo autor.

- **Camada de transporte:** os dados provenientes da camada de sessão, ao chegar nesta camada, são divididos em unidades menores. Entretanto, o mais importante é a certificação de que os pacotes chegarão corretamente ao seu destino. Contamos também com o tipo de serviço que a camada de sessão deve utilizar, sendo o mais comum a conexão ponto a ponto. A camada de transporte, a quarta camada do modelo, é responsável por certificar a entrega confiável das informações de um ponto a outro. Um exemplo é o protocolo de controle de transmissão (TCP). Ao enviar uma mensagem ou fazer o download de um arquivo, o TCP divide os dados em pacotes, envia-os e certifica que todos os pacotes cheguem ao destino na ordem correta, retransmitindo aqueles que se perderam ou chegaram corrompidos. Isso assegura uma comunicação confiável, fundamental para atividades de rede/internet.
- **Camada de sessão:** os computadores que estão separados geograficamente são conectados nesta camada. São gerenciados diversos serviços, controle de acesso, sincronização e a verificação de status da conexão. A camada de sessão, a quinta camada, mantém e encerra as conexões de comunicação. Considere o exemplo de uma videoconferência: a camada de sessão ajuda a iniciar a conexão, gerencia a comunicação contínua e a encerra quando você sai da reunião. Essa camada também realiza o controle de diálogo e a sincronização de atividades, tornando a comunicação interativa possível.
- **Camada de apresentação:** esta camada analisa a semântica e a sintaxe dos dados transmitidos, ou seja, os diferentes serviços utilizados. Antes de serem intercambiados, analisa-se o tipo de informação, para que seja utilizada a codificação correta durante a conexão. O serviço de tradução (codificação/decodificação) da informação que pode ser utilizado é o ASCII (*American Standard Information Interchange*). A camada de apresentação, a sexta camada, lida com a tradução e formatação dos dados para que possam ser compreendidos pelas aplicações. Caso você envie um documento em PDF, a camada de apresentação pode se encarregar de converter e formatar os dados para que o receptor possa visualizá-los corretamente, independentemente do software ou plataforma usada.
- **Camada de aplicação:** local em que os usuários se comunicam com o computador, responsável por prover a disponibilidade dos recursos no dispositivo destino. Nesta camada, estão definidos os navegadores (IE, Firefox, Chrome, entre outros.), os servidores web (Apache, e-mail etc.) e de banco de dados (MySQL, Oracle, Postgree). A camada de aplicação, a sétima camada, é a camada mais próxima do usuário final e abriga as aplicações dos programas que interagem diretamente com o usuário final. Estão os aplicativos de e-mail, navegadores web, mensageiros instantâneos e muitos outros programas que usamos diariamente para acessar informações e serviços na rede de computadores.

Souza *et al.* (2021) resumem da seguinte forma o modelo de referência ISO/OSI: trata-se de uma estrutura que organiza as funções das redes de computadores em sete camadas. A primeira é a camada física (que lida com a transmissão de bits), passando pela camada de enlace (responsável por detecção e correção de erros), camada de rede (roteia os dados entre redes), camada de transporte (garante a entrega confiável), camada de sessão (gerencia conexões), camada de apresentação (lida com formatação de dados) e, finalmente, a camada de aplicação (onde aplicativos interagem com o usuário). Cada camada tem uma função específica, permitindo a comunicação eficaz e padronizada em redes de computadores.

## Vamos Exercitar?

O modelo OSI (*Open Systems Interconnection*) é um modelo teórico que descreve como as redes de computadores devem funcionar. Ele é importante em redes de computadores porque fornece uma estrutura lógica para entender como os diferentes componentes de uma rede se comunicam, garantindo que a comunicação seja consistente e eficaz. O modelo OSI divide as funções de uma rede em sete camadas:

- **Física:** lida com a transmissão física de dados e a interface com o meio físico, como cabos e sinais elétricos.
- **Enlace de dados:** responsável pelo controle de acesso ao meio e pela detecção e correção de erros.
- **Rede:** roteamento de dados entre diferentes redes e sub-redes.
- **Transporte:** garante a entrega confiável de dados e o controle de fluxo.
- **Sessão:** gerencia as sessões de comunicação entre os dispositivos.
- **Apresentação:** lida com a tradução e criptografia de dados.
- **Aplicação:** fornece interfaces para aplicativos e serviços de rede.

A necessidade de padronização surgiu devido à diversidade de fabricantes e tecnologias em uso nas redes de computadores. Sem padrões, os dispositivos de diferentes fabricantes não poderiam se comunicar eficazmente, resultando em incompatibilidades e dificuldades na configuração de redes. A padronização ajuda a resolver problemas em redes de computadores, proporcionando uma base comum para o desenvolvimento e a interoperabilidade de dispositivos de rede. Por exemplo, a padronização de protocolos de rede, como o TCP/IP, permite que computadores de diferentes fabricantes e sistemas operacionais se comuniquem na internet de maneira eficaz.

Alguns exemplos de equipamentos de redes e suas camadas no modelo OSI são:

- **Roteador:** opera principalmente na camada rede, roteando pacotes de dados entre diferentes redes.
- **Switch:** atua na camada de enlace de dados, tomando decisões com base em endereços MAC para encaminhar dados dentro de uma rede local.
- **Firewall:** normalmente opera na camada de transporte e na camada de aplicação, filtrando o tráfego com base em regras de segurança e controlando o acesso a serviços específicos.

Esses são os conceitos-chave relacionados ao modelo OSI, à padronização e ao papel dos equipamentos de redes em camadas específicas.

## Saiba mais

O modelo de referência ISO/OSI é de extrema importância nas redes de computadores, oferecendo uma estrutura padronizada que permite a compreensão, a interoperabilidade e a evolução das redes. Ele separa as funções em sete camadas, facilitando o desenvolvimento de

tecnologias, garantindo a segurança e promovendo a eficiência das redes, tornando-se uma referência essencial para profissionais e estudantes da área. A seguir, indicações de materiais de estudo complementar para seu aprendizado:

- Artigo [Segurança e privacidade na web 2.0: foco nas redes sociais](#), da Egitalia Sciencia.
- Artigo [Um sistema de comunicação via socket em uma rede WI-FI para controle de um robô de inspeção](#), da revista Holos.
- Filme: We Steal Secrets: The Story of WikiLeaks. (Nós Roubamos Segredos: A História do WikiLeaks). Direção: Alex Gibney. Produção: Alex Gibney; Alexis Bloom; Marc Shmuger. Estados Unidos: Focus Features. 2013. DVD (129 min.). Documentário sobre a atuação do WikiLeaks e o trabalho de Julian Assange à frente da organização. Conta algumas das mais importantes atividades realizadas pelo WikiLeaks e como tudo é visto por instituições oficiais, que querem preservar a confidencialidade de suas informações.

## Referências

KUROSE, J. F. **Redes de computadores e a internet: uma abordagem top-down**. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

LIMA, A. S.; RIBEIRO, S. R; ALMEIDA, L. F.; FUSCHILO, C. Um sistema de comunicação via socket em uma rede WI-FI para controle de um robô de inspeção. **Holos**, Natal, v. 33, n. 2, 2017. Disponível em: <https://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/5737>. Acesso em: 3 abr. 2024.

MONTEIRO, D; ALTURAS, B. Segurança e privacidade na web 2.0: foco nas redes sociais. **Egitalia Sciencia**, v. 6, n. 10, 2012. Disponível em:  
[https://www.researchgate.net/publication/336042473\\_Seguranca\\_e\\_Privacidade\\_na\\_WEB\\_20\\_Foco\\_nas\\_Redes\\_Sociais](https://www.researchgate.net/publication/336042473_Seguranca_e_Privacidade_na_WEB_20_Foco_nas_Redes_Sociais). Acesso em: 3 abr. 2024.

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

SOUZA, D. C.; *et al.* **Gerenciamento de redes de computadores**. Porto Alegre: Sagah, 2021.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Aula 2

Arquitetura TCP/IP

### Arquitetura TCP/IP



## Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

## Ponto de Partida

Olá, estudante!

Em redes de computadores, a arquitetura é a estrutura organizada em camadas e protocolos que define como dispositivos se comunicam. Dois modelos amplamente utilizados são o ISO/OSI, com sete camadas, e o TCP/IP, com quatro. A principal diferença é a complexidade, com o ISO/OSI sendo mais teórico e o TCP/IP mais prático e amplamente adotado na internet. Os serviços podem ser classificados como orientados à conexão (como o TCP) ou sem conexão (como o UDP), e a hierarquia de protocolos organiza as camadas de rede para simplificar o desenvolvimento e a resolução de problemas. As camadas interagem por meio de interfaces definidas, com a camada de aplicação adaptando tipos de dados para transmissão. Esses conceitos são fundamentais para entender e gerenciar redes eficazes.

Podemos considerar o conteúdo a seguir para responder ao final desta aula. Imagine o seguinte cenário: como definir a arquitetura de rede, explicando por que as arquiteturas são importantes no contexto de redes de computadores? Vamos envolver também as camadas no Modelo ISO/OSI: quais as camadas do modelo ISO/OSI e as responsabilidades de cada camada? Como as camadas se comunicam entre si no modelo ISO/OSI?

Quanto às camadas no modelo TCP/IP, quais são elas e quais as funções de cada uma? Comparando as camadas do modelo TCP/IP com as do modelo ISO/OSI, o que é possível você observar?

Comparando os modelos, quais as diferenças entre os modelos ISO/OSI e TCP/IP? Vamos apontar algumas diferenças fundamentais entre os modelos ISO/OSI e TCP/IP. Qual desses modelos é mais amplamente utilizado na prática e por quê?

Avançando para classificação de serviços e hierarquia de protocolos, vamos verificar os serviços e protocolos associados a cada tipo deles. Qual a importância da hierarquia de protocolo? como

os protocolos são organizados em uma hierarquia em uma rede?

Quanto à interação entre camadas e tipos de dados: como as camadas em uma arquitetura de rede se comunicam umas com as outras? A separação em camadas é benéfica para o design de redes? Quais são os principais tipos de dados que são transmitidos em redes de computadores? Qual camada da arquitetura é responsável por encapsular e desencapsular esses tipos de dados? Como esses modelos trabalham nos equipamentos de rede? Quais equipamentos podemos apontar e quais suas funções?

Agora é mão na massa, e vamos responder a essas questões! Bons estudos!

## Vamos Começar!

### Definição, camadas e diferenças; arquitetura TCP/IP versus modelo ISO/OSI

Nesta aula, você vai conhecer o contexto histórico, as características e as funções das camadas do conhecido protocolo TCP/IP. Compreenderá como os protocolos fornecem os serviços que utilizamos em rede e na internet, por meio de aplicações, para entretenimento, trabalho ou estudos.

O modelo OSI é uma estrutura teórica que foi desenvolvida pela ISO (*International Organization for Standardization*) para padronizar a comunicação entre sistemas de computadores. Ele divide o processo de comunicação em sete camadas distintas, cada uma com funções bem definidas.

Por sua vez, arquitetura TCP/IP (*Transmission Control Protocol/Internet Protocol*) é uma abordagem prática e amplamente usada para a comunicação em redes, incluindo a internet. Ela divide a comunicação em quatro camadas e é mais orientada para a implementação do que o modelo OSI.

Arquitetura TCP/IP é a base da internet e a mais comumente utilizada na prática. O Modelo OSI é valioso para compreender os conceitos fundamentais de redes, mas é menos utilizado na implementação do dia a dia.

Tanembaum, Feamster e Wetherall (2021) afirmam que o padrão TCP/IP foi desenvolvido pelo DOD (Departamento de Defesa Americano) para que, em caso de guerras, houvesse a garantia da integridade das mensagens enviadas. Isso é compreensível, uma vez que o envolvimento em diversos conflitos ao longo dos tempos fez com que o exército necessitasse de técnicas relacionadas à comunicação.

A arquitetura do protocolo TCP/IP foi criada e desenvolvida para atender às necessidades de comunicação em uma escala global. Essa arquitetura tornou-se a espinha dorsal da internet. O TCP/IP divide as funções em camadas, permitindo uma abordagem modular que simplifica o

entendimento dos processos de comunicação. Esse protocolo é a base que permite a interconexão de dispositivos e aplicativos, desempenhando um papel crucial no funcionamento da internet e em muitas redes empresariais.

O protocolo TCP/IP teve sua arquitetura desenvolvida em quatro camadas, e um conjunto de processos (aplicações) é utilizado para fornecer diversos serviços. Veja no Quadro 1 a seguir uma comparação entre as camadas do modelo de referência OSI e o protocolo TCP/IP:

<b>7. Aplicação</b>		<b>4. Aplicação</b>
<b>6. Apresentação</b>		
<b>5. Sessão</b>		
<b>4. Transporte</b>		<b>3. Host-to-Host</b>
<b>3. Rede</b>		<b>2. Internet</b>
<b>2. Enlace de dados</b>		
<b>1. Física</b>		<b>1. Acesso à rede</b>

Quadro 1 | Mapeamento do modelo de referência OSI *versus* TCP/IP. Fonte: elaborado pelo autor.

Essa hierarquia de camadas na arquitetura TCP/IP permite a modularização e a separação de responsabilidades em diferentes níveis. Cada camada desempenha um papel específico na transmissão de dados, garantindo que a comunicação seja eficiente e confiável, independentemente da complexidade da rede subjacente. Isso também permite que novos protocolos ou tecnologias sejam adicionados ou substituídos em uma camada sem afetar as demais, facilitando a evolução da infraestrutura de rede.

## Classificação de serviços e hierarquia de protocolos

Segundo Tenenbaum, Feamster e Wetherall (2021), assim como determina o modelo de referência OSI, os protocolos são organizados em pilha ou camada; porém, em todas as redes, a função primordial é fornecer serviços às camadas superiores.

Para isso, o mecanismo utilizado faz com que a camada “x” de um dispositivo se comunique com a camada “x” de outro dispositivo. Basicamente, o protocolo efetua o “intermédio” entre as partes para que seja provida a comunicação.

Quando as informações são transferidas, as camadas processam os seus serviços respectivos. A cada par de camadas existe uma interface, responsável por definir as operações e os serviços

que a camada inferior tem que encaminhar à camada superior. Ao projetar as interfaces nas redes, a carga de trabalho das informações que devem ser passadas entre as camadas é reduzida, pois, dessa forma, só é necessário oferecer o mesmo conjunto de serviços entre os dispositivos que estão se comunicando.

De acordo com Nunes (2017), os protocolos presentes nas redes de computadores estão ligados aos serviços utilizados rotineiramente nelas. Por exemplo, ao utilizar um aplicativo em um celular, são necessários diversos protocolos, como o TCP/IP, DNS, NTP, entre outros, para que algum tipo de serviço funcione.

Para isso, podemos definir a função de cada uma das camadas do protocolo TCP/IP como:

- **Camada de aplicação (*Application Layer*)**: nesta camada, é definido como os programas vão se comunicar com as diversas aplicações disponíveis nas redes de computadores. É também responsabilidade dessa camada efetuar o gerenciamento da interface com que o usuário vai interagir ao usar a aplicação. A camada de aplicação é a camada mais próxima do usuário. Ela lida com as interações diretas entre os programas e serviços que o usuário utiliza, como navegadores da web, clientes de e-mail e aplicativos de mensagens. Também é nela que os protocolos de aplicação, como o HTTP (para páginas da web) e o SMTP (para e-mails), são implementados. Esta camada é responsável pela comunicação de alto nível, tornando possível a interação entre programas em computadores diferentes. Outros protocolos utilizados nesta camada:

1. **Telnet**: o seu significado é “*telephone network*”, tendo como função principal efetuar a conexão remota utilizando um terminal (no Windows, o prompt de comando).
2. **FTP (*File Transfer Protocol*)**: tem como objetivo efetuar a transferência de arquivos entre dois dispositivos.
3. **SNMP (*Simple Network Management Protocol*)**: é um protocolo muito utilizado por administradores de redes, pois pode ser um aliado na coleta e na manipulação de algumas informações geradas. Possibilita ao responsável pela rede saber se algum evento inesperado ocorre.

- **Camada de transporte (*Host-to-host Layer*)**: é idêntica à camada de transporte do modelo de referência OSI; responsabiliza-se por fornecer, gerenciar e terminar uma conexão ponto a ponto. Ao efetuar o gerenciamento da conexão, visa-se certificar a integridade das informações pelo sequenciamento dos pacotes segmentados para efetuar o envio/recebimento das mensagens.

A camada de transporte é responsável por garantir a entrega confiável de dados de uma máquina para outra. Ela utiliza dois principais protocolos: o TCP (*Transmission Control Protocol*), que fornece comunicação confiável ponto a ponto, e o UDP (*User Datagram Protocol*), que oferece comunicação mais rápida, mas sem garantia de entrega. Esta camada controla o fluxo de dados, divisão e reagrupamento de pacotes, e também o controle de erros.

A principal função do TCP é segmentar as mensagens originadas na camada de aplicação, e numerá-las. Quando recebe o fluxo das mensagens, o dispositivo faz a reconstrução a partir dos números adicionados no cabeçalho do protocolo. O TCP também deve confirmar o recebimento; ao enviar uma mensagem, o dispositivo receptor deve confirmar o recebimento, pois, dessa forma, é possível reenviar os segmentos não recebidos.

1. **Estabelecer a conexão:** antes de iniciar o envio das mensagens, o protocolo TCP deve estabelecer a conectividade, já que esse tipo de transmissão é orientada à conexão.

2. **Escolher um caminho confiável:** apesar de ser *full-duplex*, o protocolo através das tabelas de roteamento procura sempre o melhor caminho para transporte de suas mensagens.

Segundo Tanembaum, Feamster e Wetherall (2021), todas essas características encontradas no protocolo TCP/IP é que fazem dele o de maior confiabilidade na transmissão das mensagens. Por isso, esse protocolo é utilizado para transmissões do tipo elástico, ou seja, aquelas requisições em que a confirmação do recebimento das mensagens é essencial para que não ocorra a degradação do serviço. Exemplo: quando um usuário acessa um site, se não houver a confirmação do recebimento de todos os segmentos, a página pode não ser montada, ou ser montada com falhas.

- **Camada de rede (*Internet Layer*):** segue o objetivo da camada de rede do modelo de referência OSI; é responsável por definir o endereçamento dos dispositivos por meio do IP e certificar o roteamento dos pacotes através das redes.

A camada de rede é aquela na qual ocorre o roteamento e o encaminhamento de dados através de redes interconectadas. Ela utiliza endereços IP para determinar o melhor caminho para os pacotes de dados alcançarem seu destino. O protocolo IP (*Internet Protocol*) é um exemplo de protocolo usado nesta camada. Ela é responsável por transmitir pacotes de dados entre diferentes redes, o que é fundamental para a comunicação em escala global.

- **Camada de acesso à rede (*Network Access Layer*):** desempenha a mesma função da camada física e da de enlace no modelo de referência OSI. Efetua o monitoramento do tráfego e analisa o endereçamento de hardware antes da transmissão pelo meio físico.

A camada de acesso à rede é a camada mais baixa do modelo TCP/IP e lida com a interface direta com o meio físico, como cabos, Wi-Fi ou fibras ópticas. Implementa protocolos que variam de acordo com o tipo de tecnologia de rede em uso, como Ethernet, Wi-Fi, DSL, entre outros. Certifica que os dados sejam transmitidos fisicamente de forma apropriada, preparando-os para a transmissão pela camada de rede. Protocolos usados por ela são:

- **IP (*Internet Protocol*):** protocolo principalmente responsável por fornecer o endereçamento para os dispositivos nas redes de computadores.
- **ICMP (*Internet Control Message Protocol*):** o objetivo é gerenciar os erros no processamento dos datagramas do protocolo IP. Com destaque para:

1. **Buffer Full:** aponta quando um buffer atingiu a sua capacidade máxima de processamento.

2. **Hops:** apresenta quantos saltos são necessários para que uma mensagem possa alcançar o seu destino.
  3. **Ping:** mecanismo para saber se a interface de rede está ativa ou inativa.
  4. **Traceroute:** utilizado para mapear os saltos, fornecendo informações como o tempo entre os nodos e o seu respectivo nome.
- **ARP (Address Resolution Protocol):** tem a função de permitir conhecer o endereço físico da placa de rede, segundo o seu IP.
  - **RARP (Reverse Address Resolution Protocol):** tem função contrária à do ARP, deve encontrar o endereço lógico, segundo o endereço físico (placa de rede do dispositivo).

Segundo Kurose (2006), basicamente as duas principais funções da camada de internet são efetuar o roteamento dos pacotes e fornecer uma interface de rede às camadas superiores. Na camada de rede, também é necessário haver portas lógicas para permitir a comunicação com a camada de transporte.

## Siga em Frente...

## Interação entre as camadas e tipos de dados

A interação entre as camadas na arquitetura TCP/IP é fundamental para garantir a comunicação de dados em uma rede. Cada camada desempenha um papel específico e se comunica com as camadas adjacentes para cumprir seu propósito.

No processo de transmissão nas redes, é utilizada a técnica de encapsulamento das mensagens. Para criar uma analogia, é como se os dados fossem embrulhados para depois serem transmitidos. O modelo de referência OSI indica que uma camada de transmissão se comunique com a sua camada “vizinha” do dispositivo receptor; esse processo é repetido até que as camadas de sessão, apresentação e aplicação possam interpretar e exibir o conteúdo dos dados ao usuário.

Segundo Tanembaum, Feamster e Wetherall (2021), as quatro camadas inferiores (física, enlace, rede e transporte) possuem nomes específicos para o tratamento dos dados. Kurose (2006) define os passos necessários para que ocorram o envio e a recepção das mensagens. A seguir, como as camadas interagem umas com as outras:

- **Camada de aplicação e camada de transporte:** interagem estreitamente. Os aplicativos enviam dados para a camada de transporte para que eles sejam divididos em segmentos (no caso do TCP) ou datagramas (no caso do UDP). A camada de transporte adiciona informações de controle, como portas de origem e destino, ao cabeçalho dos segmentos ou datagramas. Essas informações são usadas para encaminhar os dados para o aplicativo correto na camada de aplicação do destino.

- **Camada de transporte e camada de rede:** a camada de transporte geralmente não se comunica diretamente com a camada de rede, mas envia os segmentos ou datagramas à camada de rede para a transmissão. A camada de transporte depende da camada de rede para rotear os segmentos ou datagramas até o destino correto com base no endereço IP de destino.
- **Camada de rede e camada de enlace:** a camada de rede encaminha os pacotes (datagramas IP) para a camada de enlace, que é responsável pela transmissão física dos dados. A camada de enlace adiciona os cabeçalhos de enlace, como endereços MAC, a fim de direcionar os quadros de dados para o dispositivo final na rede local.
- **Camada de enlace e meio físico:** a camada de enlace interage com o meio físico da rede para transmitir os quadros. Ela controla o acesso ao meio e lida com a detecção de colisões em redes Ethernet tradicionais, por exemplo. Os quadros são convertidos em sinais elétricos ou ópticos que são transmitidos fisicamente através de cabos ou meios sem fio.

Nunes (2017) explica que essas interações entre as camadas certificam que as informações sejam encapsuladas, transmitidas e entregues corretamente em uma rede. À medida que os dados trafegam de um dispositivo para outro, eles passam por todas as camadas, sendo encapsulados em camadas inferiores à medida que descem na pilha e desencapsulados nas camadas superiores à medida que sobem na pilha. Essa abordagem em camadas permite que a arquitetura TCP/IP seja flexível, escalável e interoperável, tornando-a a base da comunicação na internet e em muitas redes de computadores.

Lembre-se de que esta é apenas uma descrição dos processos que o modelo de referência OSI fornece para a estruturação dos protocolos de comunicação. OSI não é protocolo, mas sim um guia de desenvolvimento para comunicação em redes de computadores.

## Vamos Exercitar?

Nesta aula, tivemos uma base sólida para redes de computadores, ajudando você a entender os conceitos fundamentais e a diferença entre os modelos ISO/OSI e TCP/IP, bem como a importância dos serviços, a hierarquia de protocolos e os equipamentos de redes. Esse conteúdo propicia a compreensão dos conceitos de redes de computadores e a diferenciação entre os modelos ISO e TCP/IP.

Podemos concluir que uma arquitetura de rede é uma estrutura organizada em camadas e protocolos, a qual define como os dispositivos de rede se comunicam. Ela estabelece padrões e diretrizes para a transmissão de dados, permitindo que diferentes dispositivos e sistemas se comuniquem de maneira eficaz em uma rede de computadores. As arquiteturas de rede são importantes porque fornecem uma estrutura unificada que facilita a interoperabilidade entre dispositivos e sistemas de rede, promovendo a comunicação eficiente e segura.

As sete camadas do modelo ISO/OSI são: física, enlace de dados, rede, transporte, sessão, apresentação e aplicação. Elas se comunicam entre si por meio de interfaces bem definidas,

passando dados e controle de uma camada para a próxima.

As quatro camadas do modelo TCP/IP são: interface de rede, internet, transporte e aplicação. Elas são mais simplificadas em comparação com as do modelo ISO/OSI, o que facilita sua implementação.

Destacamos a seguir as diferenças entre os Modelos ISO/OSI e TCP/IP. O modelo ISO/OSI tem sete camadas, enquanto o TCP/IP tem quatro. O modelo ISO/OSI é mais abstrato e teórico, enquanto o TCP/IP é mais prático e amplamente implementado. O TCP/IP foi desenvolvido antes do modelo ISO/OSI e é a base da internet. O modelo TCP/IP é mais amplamente utilizado na prática devido à sua simplicidade e histórico de sucesso na internet.

Quanto à classificação de serviços e hierarquia de protocolos, podemos ressaltar que serviços orientados à conexão envolvem a criação de uma conexão antes da transmissão de dados (exemplo: TCP). Serviços sem conexão não requerem uma conexão prévia (exemplo: UDP). Exemplos de serviços orientados à conexão incluem transferência de arquivos e navegação na web (usando HTTP), enquanto serviços sem conexão são adequados para transmissão de vídeo ao vivo e jogos online (usando UDP).

Hierarquia de protocolos refere-se à organização das camadas e protocolos em uma pilha de rede, garantindo que cada camada tenha responsabilidades claras e distintas. Por exemplo, na camada de aplicação, temos protocolos como HTTP, FTP e SMTP, que oferecem serviços de alto nível aos aplicativos. A camada de transporte inclui TCP e UDP, que gerenciam a entrega de dados entre sistemas, enquanto a camada de rede roteia pacotes IP entre redes.

As camadas interagem por meio de interfaces bem definidas. Cada camada recebe dados da camada superior e adiciona informações de controle necessárias. A camada inferior recebe os dados, realiza sua função específica e encaminha os dados para a próxima camada. A separação em camadas é benéfica, pois permite a modularidade e a substituição de camadas sem afetar outras, e facilita a depuração e o desenvolvimento de novos serviços.

Tipos de dados comuns em redes incluem textos, arquivos, áudio, vídeo e comandos de controle. A camada de aplicação é responsável por encapsular e desencapsular esses tipos de dados, adaptando-os para transmissão na rede, se necessário. Equipamentos de rede incluem roteadores, *switches*, *hubs*, firewalls, servidores, modems e pontos de acesso sem fio. Roteadores roteiam pacotes entre redes; *switches* comutam tráfego dentro de uma rede, firewalls protegem contra ameaças, servidores fornecem serviços, modems conectam redes diferentes e pontos de acesso sem fio possibilitam conectividade sem fio em redes.

## Saiba mais

A importância das arquiteturas de rede na comunicação moderna reside na padronização e na capacidade de permitir que diferentes dispositivos e sistemas se comuniquem de maneira eficiente e segura, tornando possível a globalização da internet e a conectividade de dispositivos

em todo o mundo. A compreensão das camadas e protocolos ajuda a solucionar problemas de rede, pois permite isolar e diagnosticar problemas em um nível específico, além de facilitar o desenvolvimento e a manutenção de redes mais robustas e eficazes. A seguir, mais conteúdo complementar para aprofundar seu conhecimento:

- Artigo [Protocolos de autenticação e controle de acesso para aplicação das forças armadas e órgãos de segurança pública em redes móveis 4G/LTE e 5G](#), página 616, da revista Revista Ibérica de Sistemas e Tecnologias de Informação.
- Artigo [Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação](#), da Revista Ibérica de Sistemas e Tecnologias de Informação.
- Filme: Pirates of Silicon Valley. (Piratas da Informática: Piratas do Vale do Silício). Direção: Martyn Burke. Produção: Leanne Moore. Estados Unidos: TNT. 1999. DVD (95 min.). Retrata a ascensão da Apple e da Microsoft, as duas maiores empresas de informática do planeta. Em busca da liderança do mercado, Steve Jobs (Noah Wyle) e Bill Gates (Anthony Michael Hall), fundadores das empresas, enfrentam-se em uma guerra de bastidores.

## Referências

GEORG, M. A. C. *et al.* Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. **Revista Ibérica de Sistemas e Tecnologias de Informação**, Brasília, ed. 54, 2022. Disponível em:  
[https://www.researchgate.net/publication/370189315\\_Os\\_desafios\\_da\\_Seguranca\\_Cibernetica\\_no\\_setor\\_publico\\_federal\\_do\\_Brasil\\_estudo\\_sob\\_a\\_otica\\_de\\_gestores\\_de\\_tecnologia\\_da\\_informacao](https://www.researchgate.net/publication/370189315_Os_desafios_da_Seguranca_Cibernetica_no_setor_publico_federal_do_Brasil_estudo_sob_a_otica_de_gestores_de_tecnologia_da_informacao). Acesso em: 3 abr. 2024.

KUROSE, J. F. **Redes de computadores e a internet**: uma abordagem top-down. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

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

TANEMBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

RICARDO, J.; DIAS, U. Protocolos de autenticação e controle de acesso para aplicação das forças armadas e órgãos de segurança pública em redes móveis 4G/LTE e 5G. **Revista Ibérica de Sistemas e Tecnologias de Informação**, Brasília, ed. 49, 2022. Disponível em:  
<http://www.risti.xyz/issues/risti49.pdf>. Acesso em: 3 abr. 2024.

## Aula 3

Camadas e Protocolos da Arquitetura TCP/IP: Camadas de Enlace e de Rede

## Camadas e protocolos da arquitetura TCP/IP: camadas de enlace e de Rede



### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

### Ponto de Partida

Olá, estudante!

A disciplina de redes de computadores é voltada para compreender como os sistemas de comunicação de dados funcionam. No âmbito das redes, a camada de enlace desempenha um papel importante. Mas, afinal, qual é o papel dela em redes de computadores? Ela facilita a comunicação entre dispositivos na mesma rede, garantindo que os quadros de dados sejam entregues de forma confiável. Para isso, faz uso de protocolos como Ethernet, Wi-Fi e PPP. Como esses protocolos contribuem para essa entrega confiável?

Além disso, na camada de rede, o protocolo IP (*Internet Protocol*) assume o papel de rotear pacotes na internet e fornecer endereçamento lógico. O que exatamente significa esse endereçamento lógico e como o protocolo IP o realiza? E por que existem diferentes formatos de endereços IP? Como essa diferenciação afeta a rede? A divisão de redes em sub-redes é uma prática comum na organização de endereços IP em redes locais. Por que é importante fazer essa divisão? Como isso contribui para a organização e gestão das redes?

No contexto da disciplina de redes, também analisamos os protocolos da camada de aplicação. O ICMP, por exemplo, é utilizado para relatar erros de comunicação e verificar a conectividade com comandos como o “ping”. Qual é a importância do “ping” na solução de problemas de rede? O IGMP é fundamental em redes *multicast*, permitindo a gestão de grupos de membros que desejam receber tráfego *multicast* específico. Como exatamente funciona o *multicast* e qual é o papel do IGMP nesse cenário? O ARP é crucial para mapear endereços IP para endereços MAC em uma rede local. Como essa tradução de endereços contribui para a comunicação entre dispositivos na mesma rede?

Da mesma forma, protocolos de roteamento desempenham um papel essencial. Entre eles, encontram-se RIP, OSPF e BGP. O que são protocolos de roteamento e como eles ajudam a determinar as rotas mais eficientes na transmissão de pacotes em redes maiores? Quais fatores, como escalabilidade e convergência, são levados em consideração na escolha desses protocolos? A escolha entre RIP e OSPF, por exemplo, depende das necessidades específicas da rede. Como as necessidades da rede afetam a escolha entre esses protocolos?

A interconexão de redes locais em uma rede global, como a internet, é alcançada por meio de roteadores que encaminham pacotes com base nos endereços IP. Como esse encaminhamento ocorre e como as redes locais se conectam para criar uma rede global interconectada?

Por fim, a camada de enlace é vital para a comunicação interna em uma rede local. Mas por que é importante gerenciar o acesso ao meio compartilhado e garantir a entrega confiável de quadros entre dispositivos na mesma rede? Como essas funções da camada de enlace se encaixam no funcionamento geral das redes de computadores?

Vamos responder a todos esses questionamentos! Bons estudos!

## Vamos Começar!

## Protocolos e serviços da camada de enlace

Segundo Kurose (2006), a camada de enlace de dados é a segunda camada do modelo OSI (*Open Systems Interconnection*). É responsável pela comunicação entre equipamentos diretamente conectados em uma rede de computadores. Atua na transmissão confiável de informações, garantindo que os bits sejam transmitidos de forma eficiente e sem erros entre os dispositivos finais, como computadores, roteadores e *switches*. Para cumprir essa função, a camada de enlace utiliza protocolos e serviços específicos. Dois dos principais são:

**Entrega de quadros:** a camada de enlace divide os dados em pacotes chamados de “quadros” e os envia para o equipamento de destino. Cada quadro contém informações, como endereços MAC (*Media Access Control*), para identificar o emissor e o destinatário. O serviço de entrega de quadros certifica que os dados sejam entregues corretamente ao dispositivo de destino.

**Controle de acesso ao meio:** coordena o acesso ao meio de transmissão compartilhado, como um cabo ou uma rede sem fio. Os protocolos de controle de acesso ao meio garantem que os dispositivos na rede transmitam seus dados de maneira ordenada, evitando colisões de dados. Um exemplo disso é o protocolo CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), usado em redes Ethernet para evitar colisões de quadros.

Outros exemplos de protocolos e serviços comuns na camada de enlace:

- **Ethernet:** é um dos protocolos mais amplamente utilizados na camada de enlace. Define como os quadros são encapsulados e transmitidos em redes com fio. Cada equipamento

na rede possui um endereço MAC exclusivo que é usado para identificá-lo. Os *switches* Ethernet operam nesta camada para encaminhar quadros com base nos endereços MAC.

- **Wi-Fi (IEEE 802.11):** para redes sem fio, o padrão IEEE 802.11 define como os dados são transmitidos entre dispositivos. É responsável pela entrega de quadros e pelo gerenciamento da conectividade sem fio e da segurança.
- **PPP (Point-to-Point Protocol):** utilizado para estabelecer conexões ponto a ponto, como aquelas criadas por modems discados. Atua na autenticação e na configuração da conexão, como a transmissão confiável de dados.
- **HDLC (High-Level Data Link Control):** um protocolo de enlace de dados que oferece entrega confiável de dados. É amplamente utilizado em linhas de comunicação dedicadas e redes privadas.
- **Frame relay:** este protocolo é projetado para redes de alta velocidade e baixa latência, como redes WAN (*Wide Area Network*). Ele oferece um serviço de entrega de quadros eficiente e é menos complexo do que outros protocolos, a exemplo do PPP.

Em resumo, a camada de enlace de dados é responsável pela comunicação de rede, garantindo que os dados sejam transmitidos de forma confiável entre dispositivos. Protocolos como Ethernet, Wi-Fi, PPP, HDLC e Frame Relay são responsáveis pela operação eficaz das redes de computadores, e oferecem serviços que vão desde a entrega de quadros até o controle de acesso ao meio. Esses protocolos desempenham um papel crucial nas redes modernas, garantindo a conectividade e a comunicação eficiente entre dispositivos.

Tanenbaum, Feamster e Wetherall (2021) descrevem a camada de enlace como aquela que lida com a comunicação entre dispositivos diretamente conectados em uma rede de computadores. Ela apresenta os seguintes elementos-chave relacionados aos protocolos e serviços da camada de enlace:

- **Quadros (Frames):** os dados são divididos em quadros (*frames*). Cada quadro é uma unidade de dados independente que contém informações sobre o endereço MAC do emissor e do destinatário, bem como os próprios dados.
- **Endereços MAC (Media Access Control):** cada dispositivo de rede possui um endereço MAC exclusivo que o identifica na rede. O endereço MAC é usado para determinar a quem um quadro pertence e para onde ele deve ser entregue. O serviço da camada de enlace envolve a entrega de quadros com base nos endereços MAC.
- **Controle de acesso ao meio:** a camada de enlace atua no controle de acesso ao meio físico de transmissão. Vários dispositivos competem pelo uso do meio de transmissão, como cabos ou canais de rádio. Protocolos de controle de acesso ao meio, como CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) em redes Ethernet, garantem que a comunicação ocorra de maneira organizada, evitando colisões de quadros.
- **Detecção e correção de erros:** protocolos como o CRC (*Cyclic Redundancy Check*) são usados para verificar a integridade dos dados nos quadros transmitidos. Caso um erro seja detectado, o quadro pode ser descartado, ou solicita-se uma retransmissão.
- **Controle de fluxo:** visa garantir que um emissor não sobrecarregue um destinatário com dados em uma taxa que ele não possa processar. Isso é especialmente importante em comunicações ponto a ponto.

**Exemplo de uma rede Ethernet:** dois computadores, A e B, desejam se comunicar em uma rede Ethernet. O computador A encapsula os dados em um quadro Ethernet, incluindo o endereço MAC de A como o emissor e o endereço MAC de B como o destinatário. O quadro é então transmitido na rede.

Um *switch* Ethernet na rede recebe o quadro e o encaminha para o computador B, usando o endereço MAC de destino. Isso ilustra o serviço de entrega de quadros baseado em endereços MAC. Se houver colisões de quadros na rede, o protocolo CSMA/CD detectará e lidará com as colisões, permitindo uma comunicação eficiente. Quando o computador B recebe o quadro, ele verifica a integridade dos dados por meio do CRC. Se o quadro estiver livre de erros, o computador B processa os dados; caso contrário, o quadro é descartado ou uma retransmissão pode ser solicitada. Esses são alguns dos conceitos-chave para entender a camada de enlace e seus protocolos e serviços em ação.

## Protocolos e serviços da camada de rede: o protocolo IP

A camada de rede é a terceira camada do modelo OSI; ela é responsável por rotear pacotes de dados de uma origem para um destino. O protocolo IP é a espinha dorsal da internet e é responsável por rotear pacotes de dados de forma eficiente entre dispositivos em diferentes redes. O IP atribui um endereço único a cada dispositivo na rede, chamado de endereço IP e utilizado para identificá-los. Segundo Kurose (2006), o IP é o endereço lógico feito para que um dispositivo possa se comunicar com qualquer outro dispositivo, independentemente de sua localização geográfica.

Utilizado para roteamento de pacotes, quando um equipamento, como um computador, envia dados para outro dispositivo em uma rede, o IP é responsável por determinar a melhor rota para os dados alcançarem o destino. Isso envolve a análise dos endereços IP de origem e destino, juntamente com informações de roteamento, para determinar a próxima parada dos pacotes. Cada roteador em uma rede toma decisões de encaminhamento com base nas informações do cabeçalho IP. Existem duas versões principais do IP em uso: IPv4 (*Internet Protocol version 4*) e IPv6 (*Internet Protocol version 6*). Em IPv4, os endereços são representados em formato decimal, como “192.168.1.1”; enquanto em IPv6, eles são representados em formato hexadecimal, como “2001:0db8:85a3:0000:0000:8a2e:0370:7334”.

Tanenbaum, Feamster e Wetherall (2021) explicam que o protocolo IP funciona dividindo os dados em pacotes chamados datagramas. Cada datagrama contém informações, incluindo o endereço IP de origem e destino, juntamente com os próprios dados. Quando um dispositivo envia um datagrama, este passa por roteadores intermediários. Cada roteador consulta tabelas de roteamento para determinar a melhor rota para o datagrama, com base no endereço IP de destino. Os roteadores encaminham o datagrama de um salto (*hop*) para outro, até que ele alcance seu destino.

O IP fornece entrega de pacote não confiável e sem conexão para a internet. Trata cada pacote de informações de forma independente. Não é confiável porque não garante entrega, não requer

reconhecimentos a partir do host de envio, do host de recebimento ou de hosts intermediários. As conexões físicas de uma rede transferem informações em um quadro com um cabeçalho e dados. O IP usa um datagrama de internet que contém informações semelhantes ao quadro físico e que também possui um cabeçalho contendo endereços IP tanto da origem quanto do destino dos dados.

O datagrama é encapsulado em quadros de camadas inferiores, como Ethernet, e transmitido pela rede e roteado por dispositivos intermediários até chegar ao seu destino, onde é desencapsulado e os dados são entregues aos aplicativos apropriados. Isso possibilita a comunicação eficiente e escalável na internet. Os pacotes de saída automaticamente têm um cabeçalho IP prefixado a eles. Os pacotes recebidos têm seu cabeçalho IP removido antes de serem enviados para os protocolos de nível superior. O protocolo IP prevê o endereçamento universal de hosts na rede Internet.

Bits															
0	4	8	16	19	31										
Version	Length	Type of Service	Total Length												
Identification			Flags	Fragment Offset											
Time to Live	Protocol		Header Checksum												
Source Address															
Destination Address															
Options															
Data															

Figura 1 | Cabeçalho do pacote IP. Fonte: Kurose (2006, [s. p.]).

O IP permite que as redes sejam divididas em sub-redes menores para melhor gerenciamento de endereços. Isso é útil em redes de grande escala, nas quais é necessário um controle granular dos endereços IP. O IP conta com suporte de qualidade de serviço (QoS), permitindo que a rede dê prioridade a determinados tipos de tráfego, como voz sobre IP (VoIP) ou vídeo em tempo real, para garantir uma experiência de comunicação de alta qualidade.

A transição para IPv6 também é um desenvolvimento significativo. Com a crescente escassez de endereços IPv4, o IPv6 foi desenvolvido para fornecer um espaço de endereçamento muito maior, com capacidade para um número praticamente ilimitado de dispositivos conectados à internet.

Siga em Frente...

## Outros protocolos e serviços da camada de aplicação: ICMP, IGMP, ARP e protocolos de roteamento

Tanenbaum, Feamster e Wetherall (2021) explicam que a camada de aplicação é a camada superior do modelo OSI; ela é responsável por fornecer serviços e protocolos para as aplicações de software que funcionam em dispositivos finais, como computadores, servidores e outros dispositivos de rede. Vamos explorar alguns desses protocolos e serviços, como ICMP, IGMP, ARP e protocolos de roteamento, com exemplos de utilização e funcionamento.

- **ICMP (Internet Control Message Protocol)**: é um protocolo usado para comunicações de controle e diagnóstico na internet. Ele não é usado para transferência de dados, mas sim para relatar erros, verificar a disponibilidade de dispositivos e outras funções de controle. Exemplos de utilização incluem o comando “ping” para verificar a conectividade e a resposta de dispositivos na rede e mensagens de erro ICMP, como “Time Exceeded” (“tempo excedido”) ou “Destination Unreachable” (“destino fora de alcance”).
- **IGMP (Internet Group Management Protocol)**: é um protocolo usado para controlar o tráfego de *multicast* em redes IP. Ele permite que os dispositivos em uma rede comuniquem ao roteador ou *switch* que desejam receber tráfego *multicast* de um grupo específico. Um exemplo de utilização é em streaming de vídeo ao vivo, quando vários dispositivos desejam receber a mesma transmissão ao mesmo tempo. Ele gerencia a entrega eficiente do tráfego *multicast* a grupos específicos de dispositivos.
- **ARP (Address Resolution Protocol)**: é um protocolo usado para mapear endereços IP para endereços MAC em redes locais. Quando um dispositivo na rede precisa enviar um pacote para outro dispositivo na mesma rede, ele usa o ARP para descobrir o endereço MAC correspondente ao endereço IP de destino. Isso é essencial para a comunicação em redes locais. Por exemplo, quando um computador deseja enviar dados para outro na mesma rede, ele usa o ARP para descobrir o endereço MAC do destino antes de enviar os pacotes.

## Protocolos de roteamento

Na camada de aplicação, protocolos de roteamento não são executados, mas sua configuração e gerenciamento podem ser uma parte importante da administração da rede. Exemplos de protocolos de roteamento incluem o OSPF (*Open Shortest Path First*) e o BGP (*Border Gateway Protocol*), que são protocolos de roteamento usados em roteadores para determinar as melhores rotas para encaminhar o tráfego.

De acordo com Nunes (2017), protocolos de roteamento, como OSPF e BGP, são executados em roteadores a fim de determinar as rotas mais eficientes para o encaminhamento de pacotes. Eles consideram fatores como métricas, topologia da rede e políticas de roteamento para tomar

decisões em relação ao encaminhamento do tráfego. Existem vários protocolos de roteamento; porém, os principais, mais conhecidos, utilizados e citados em redes de computadores incluem:

- **OSPF (*Open Shortest Path First*)**: é amplamente utilizado em redes empresariais e ISPs. Trata-se de um protocolo de roteamento baseado em estado de enlace; é escalável e altamente eficiente. O OSPF é projetado para calcular rotas com base na topologia da rede e oferece recursos avançados de convergência rápida.
- **BGP (*Border Gateway Protocol*)**: utilizado na internet global para rotear tráfego entre sistemas autônomos (ASes). Ele é fundamental para determinar as rotas de tráfego na internet e é altamente escalável.
- **RIP (*Routing Information Protocol*)**: protocolo de roteamento distante baseado em vetores de distância. Embora não seja tão comum como no passado, ainda é encontrado em algumas redes menores. RIP é fácil de configurar, mas tem limitações em termos de escalabilidade.
- **EIGRP (*Enhanced Interior Gateway Routing Protocol*)**: protocolo de roteamento da Cisco que combina características de protocolos de estado de enlace e vetores de distância. Ele é amplamente utilizado em redes que usam equipamentos Cisco e oferece rápida convergência.
- **IS-IS (*Intermediate System to Intermediate System*)**: protocolo de roteamento baseado em estado de enlace que é utilizado principalmente em redes de grande escala, como ISPs e redes de telecomunicações. É semelhante ao OSPF em muitos aspectos.
- **RIPv2 e RIPvNG**: RIPv2 é uma versão aprimorada do RIP, que dá suporte ao roteamento IPv4. O RIPvNG (*RIP Next Generation*) é a versão correspondente para o IPv6. Ambos são usados em redes menores ou em cenários de transição para o IPv6.

Esse são alguns dos protocolos de roteamento mais conhecidos e amplamente utilizados. A escolha do protocolo depende do tamanho e das necessidades específicas da rede. Redes menores podem usar protocolos mais simples, como RIP, enquanto redes maiores e mais complexas normalmente se beneficiam de protocolos como OSPF, BGP e EIGRP. Além desses, existem outros protocolos de roteamento específicos para cenários ou equipamentos particulares, mas os mencionados acima são os mais predominantes em redes empresariais e na internet global.

## Vamos Exercitar?

A camada de enlace em redes de computadores desempenha um papel essencial ao facilitar a comunicação entre dispositivos na mesma rede, garantindo que os quadros de dados sejam entregues de forma confiável. Para isso, utiliza protocolos como Ethernet, Wi-Fi e PPP, sendo particularmente relevante na comutação de pacotes, na qual os dados são divididos em unidades menores para transmissão. Na camada de rede, o protocolo IP (*Internet Protocol*) assume o papel de rotear pacotes na internet e fornecer endereçamento lógico. Ele é identificado pelo formato dos endereços, como o IPv4 com 32 bits e o IPv6 com 128 bits. A divisão de redes em sub-redes é uma prática comum para organizar endereços IP em redes locais.

Além disso, outros protocolos da camada de aplicação desempenham funções específicas. O ICMP é utilizado para relatar erros de comunicação e verificar a conectividade com comandos como o “ping”. O IGMP é fundamental em redes *multicast*, permitindo a gestão de grupos de membros que desejam receber tráfego *multicast* específico. O ARP, por sua vez, é crucial para relacionar endereços IP a endereços MAC em uma rede local, possibilitando a comunicação entre dispositivos na mesma rede. Adicionalmente, protocolos de roteamento como o RIP, OSPF e BGP são empregados para determinar as rotas mais eficientes na transmissão de pacotes em redes maiores, considerando fatores como escalabilidade e convergência.

A escolha entre RIP e OSPF, por exemplo, depende das necessidades específicas da rede. Enquanto o RIP é mais simples, o OSPF oferece escalabilidade e convergência mais rápidas. A interconexão de redes locais em uma rede global, como a internet, é alcançada por meio de roteadores que encaminham pacotes com base nos endereços IP, criando uma rede global interconectada. A camada de enlace é vital para a comunicação interna em uma rede local, gerenciando o acesso ao meio compartilhado e garantindo a entrega confiável de quadros entre dispositivos na mesma rede. Portanto, essas camadas e protocolos desempenham papéis fundamentais na infraestrutura de comunicação das redes de computadores.

## Saiba mais

Os protocolos e serviços dessas camadas desempenham papéis cruciais nas redes de computadores. Na camada de enlace, garantem a comunicação eficaz e segura dentro de uma rede local, enquanto o protocolo IP, na camada de rede, é a base da comunicação entre redes distintas na internet. Além disso, protocolos como ICMP, IGMP, ARP e os protocolos de roteamento são essenciais para resolver problemas, otimizar o tráfego e alocar recursos de rede, garantindo o funcionamento adequado das comunicações em todo o sistema. A seguir, mais conteúdo complementar para aprofundar seu conhecimento:

- Artigo [Emprego dual – civil e militar – do 5G na defesa brasileira: uma proposta para o SISFRON, sob domínio do Exército](#), da Revista Ibérica de Sistemas e Tecnologias de Informação.
- Artigo [Arquitetura de segurança em aplicações baseadas em web services](#), da revista HOLOS.
- Filme: The Great Hack. (Privacidade Hackeada). Direção: Jehane Noujaim Karim Amer. Produção: Geralyn Dreyfous; Jamie Wolf (II); Judy Korin; Karim Amer. Estados Unidos: Netflix. 2019. DVD (113 min.). Dados, indiscutivelmente o bem mais valioso do mundo, estão sendo armados para travar guerras culturais e políticas. O obscuro mundo da exploração de dados é descoberto através de jornadas pessoais imprevisíveis de jogadores em lados diferentes da história explosiva de dados da Cambridge Analytica/Facebook.

## Referências

KUROSE, J. F. **Redes de computadores e a internet: uma abordagem top-down.** 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

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

OLIVEIRA, R. C. F. Emprego dual – civil e militar – do 5G na defesa brasileira: uma proposta para o SISFRON, sob domínio do Exército. **Revista Ibérica de Sistemas e Tecnologias de Informação**, Brasília, ed. 49, 2022. Disponível em: [https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante\\_de\\_publicacao-1.pdf](https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-1.pdf). Acesso em 3 abr. 2024.

SILVA, R.; CUNHA, J. Arquitetura de segurança em aplicações baseadas em web services. HOLOS, Natal, v. 21, n. 3, 2005. Disponível em: <https://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/77>. Acesso em: 3 abr. 2024.

TANEMBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores.** 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Aula 4

Camadas e Protocolos da Arquitetura TCP/IP: Camadas de Transporte e Aplicação

### Camadas e protocolos da arquitetura TCP/IP: camadas de transporte e aplicação



#### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

## Ponto de Partida

Olá, estudante!

Vamos explorar os protocolos de redes de computadores nas camadas de transporte e aplicação. Na camada de transporte, destacamos o TCP e o UDP, discutindo sua importância para a confiabilidade da transmissão. Na camada de aplicação, veremos protocolos como o HTTP, SMTP, POP3 e TLS, destacando suas funções, como transferência de recursos da web, envio e recebimento de e-mails, e segurança nas comunicações online. Além disso, veremos outros protocolos, como NTP, DNS, SSH e FTP, que desempenham papéis específicos na interconexão de redes. Em um mundo cada vez mais conectado, a comunicação eficaz e segura na internet é essencial. Nesse contexto, protocolos desempenham um papel fundamental na camada de transporte e na camada de aplicação das redes de computadores.

No coração da transmissão de dados, estão os protocolos da camada de transporte, como o *Transmission Control Protocol* (TCP) e o *User Datagram Protocol* (UDP). O TCP é conhecido por sua confiabilidade, garantindo que os dados sejam entregues sem erros. No entanto, ele introduz alguma sobrecarga devido à necessidade de estabelecer conexões e confirmar cada pacote com o “*Acknowledgment number*” (“número de confirmação”) no cabeçalho do TCP. Isso nos leva à pergunta: qual a importância desse campo para a confiabilidade da transmissão? O campo “*Acknowledgment number*” é crucial para o TCP, pois permite que o remetente saiba quais pacotes foram recebidos com sucesso. Se um pacote não é confirmado, o remetente reenvia-o, garantindo que os dados sejam entregues de forma confiável. A confiabilidade do TCP é essencial em muitos cenários, mas se estivéssemos desenvolvendo um aplicativo de chat em tempo real, como o WhatsApp, para o qual a entrega rápida de mensagens é crucial?

No caso de um aplicativo de chat em tempo real, a velocidade de entrega é fundamental. Aqui, o UDP, que é menos confiável, porém mais rápido. Por isso, pode ser uma escolha mais adequada. A decisão depende das prioridades do aplicativo, e a justificativa dessa escolha deve levar em consideração a natureza das mensagens a serem enviadas.

Na camada de aplicação, protocolos como o *Hypertext Transfer Protocol* (HTTP), o *Simple Mail Transfer Protocol* (SMTP), o *Post Office Protocol* (POP3) e o *Transport Layer Security* (TLS) desempenham papéis distintos. O HTTP é usado para transferir dados da web, enquanto o SMTP e o POP3 gerenciam o envio e recebimento de e-mails. O TLS, por sua vez, oferece segurança adicional nas comunicações online. O HTTP é responsável pela transferência de recursos da web, permitindo que navegadores solicitem e exibam páginas da internet. O SMTP é usado para enviar e-mails, enquanto o POP3 é utilizado para recuperar e-mails de um servidor. E o TLS?

O *Transport Layer Security* (TLS) é fundamental para a segurança online, criptografando as comunicações para proteger dados sensíveis. Isso é essencial em transações financeiras e em qualquer situação em que a privacidade dos dados seja crítica.

Além disso, há os protocolos como o *Network Time Protocol* (NTP) para sincronização de relógios de rede, o *Domain Name System* (DNS) para traduzir nomes de domínio em endereços IP, o *Secure Shell* (SSH) para acesso remoto seguro e o *File Transfer Protocol* (FTP) para transferência de arquivos. O NTP mantém a precisão dos relógios de rede, o DNS é crucial na resolução de nomes de domínio, o SSH oferece segurança em acessos remotos e o FTP, apesar de menos seguro, é útil em situações específicas.

Assim, em um mundo de redes interconectadas, compreender a complexidade e as nuances dos protocolos é essencial para garantir a eficácia, a confiabilidade e a segurança das comunicações online, independentemente de qual protocolo ou serviço seja usado.

Bons estudos!

## Vamos Começar!

## Protocolos da camada de transporte: TCP e UDP

Segundo Tanenbaum, Feamster e Wetherall (2021), as características encontradas no protocolo TCP fazem dele o de maior confiabilidade na transmissão das mensagens. Esse protocolo é utilizado para transmissões do tipo elástico, requisições em que a confirmação do recebimento das mensagens é essencial para que não ocorra a degradação do serviço. Quando um usuário acessa um site, se não houver a confirmação do recebimento de todos os segmentos, a página pode não ser montada, ou ser montada com falhas. Para compreensão da estrutura do protocolo TCP, observe a Figura 1 a seguir:

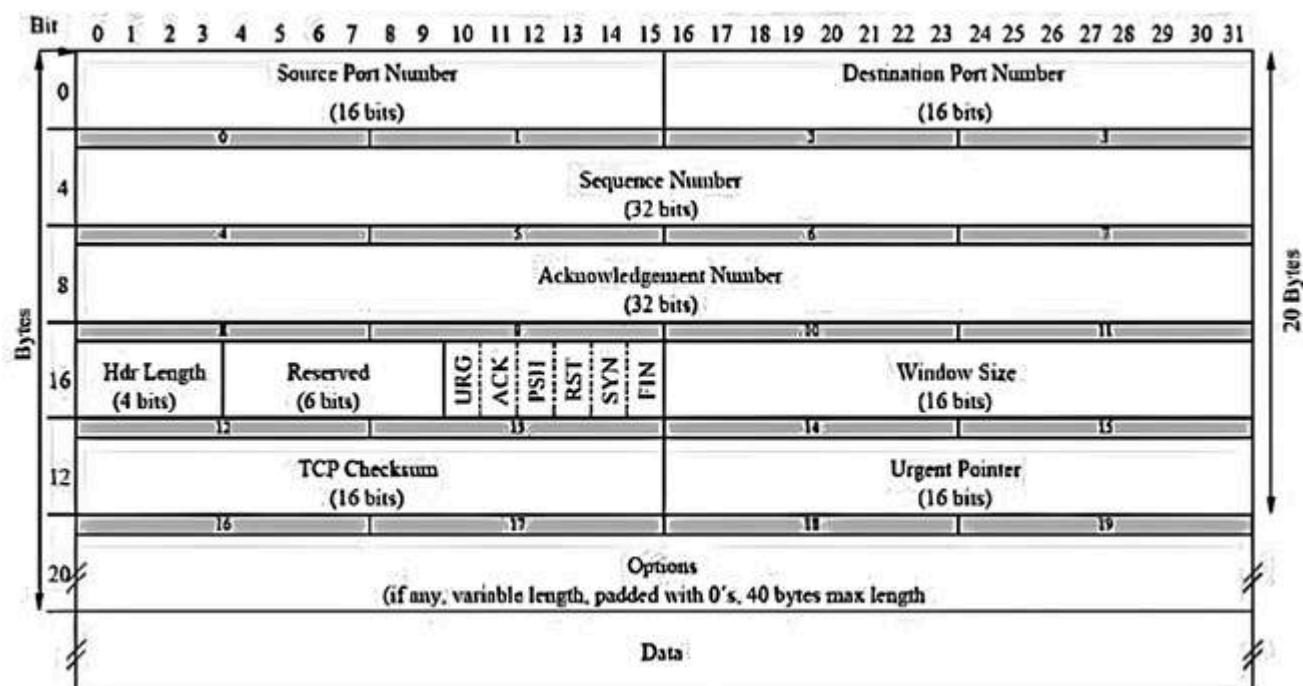


Figura 1 | Cabeçalho TCP. Fonte: Tanenbaum, Feamster e Wetherall (2021, [s. p.]).

Cada campo do cabeçalho tem as respectivas funções:

- **Source port number** (número da porta de origem): número da porta lógica na qual a aplicação está localizada.
- **Destination port number** (número da porta de destino): número da porta lógica na qual está a aplicação do dispositivo destino.
- **Sequence number** (número sequencial): número que sequencia os segmentos transmitidos/recebidos.
- **Acknowledgement number** (número de confirmação): número de confirmação de conexão.
- **Header length** (comprimento do cabeçalho): define o comprimento do cabeçalho TCP.
- **Reserved** (reservado): campo reservado.
- **Code bits**: campos responsáveis por gerenciar o início e o encerramento das conexões.
- **Windows** (janelas): tamanho da janela de dados que mede a capacidade de recebimento do remetente.
- **TCP checksum**: faz checagem de controle de erros (redundante).
- **Urgent pointer** (marcação de urgência): determina os dados críticos, aqueles com maior prioridade na transmissão.
- **Option** (opção): na qual é definido o tamanho máximo do segmento.
- **Data** (dados): os dados transmitidos.

Por sua vez, o UDP (*User Datagram Protocol*) é considerada uma versão simplificada do protocolo TCP. Dessa forma, não utiliza muito a largura da banda disponível, devido a não efetuar a confirmação do recebimento das mensagens, razão pela qual é considerada como um protocolo de transmissão não confiável. Para entender a estrutura do protocolo UDP, veja a Figura 2 a seguir:

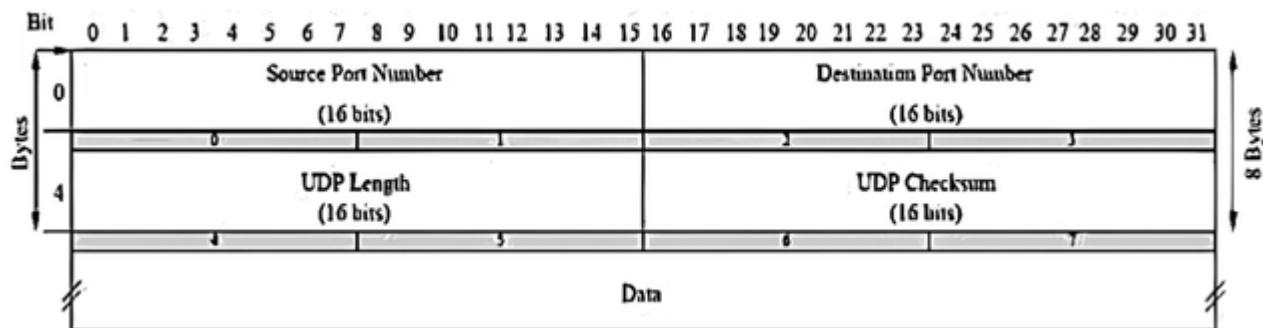


Figura 2 | Cabeçalho UDP. Fonte: Tanenbaum, Feamster e Wetherall (2021, [s. p.]).

De acordo com Tanenbaum, Feamster e Wetherall (2021), o protocolo UDP recebe as mensagens provenientes das camadas superiores, divide em segmentos e as transmite, porém a numeração para sequenciar não é adicionada. Ao receber as mensagens, caso um segmento não seja recebido, o protocolo UDP ignora o fato. Isso ocorre na utilização são os serviços do tipo streaming. Veja no Quadro 1 a seguir a comparação dos protocolos:

TCP	UDP
Serviço orientado à conexão	Serviço sem conexão

Garante a entrega por meio da confirmação de recebimento, pois os dados são sequenciados.	Não garante o recebimento, pois os dados não são sequenciados.
O programa que utiliza o TCP possui um transporte confiável.	A garantia de recebimento do software que utiliza o protocolo UDP deve ser garantida pelo programa.
Transmissão lenta e necessita de maior largura de banda	Transmissão rápida e ocupa menos largura de banda
Comunicação ponto a ponto.	Suporte a comunicação <i>multicast</i> .

Quadro 1 | Comparação TCP *versus* UDP. Fonte: adaptado pelo autor a partir de Tanenbaum, Feamster e Wetherall (2021, [s. p.]).

Nunes (2017) também destaca que o TCP e o UDP têm aplicabilidades diferentes. O TCP é indicado para conexões do tipo elástico, em que é necessária a confirmação de recebimento e retransmissão em caso de falha. O protocolo UDP é indicado para os serviços streaming, em que não é necessária a confirmação do recebimento das mensagens: serviços como jogos online, filmes *on demand* e músicas online utilizam esse protocolo.

### Siga em Frente...

## Protocolos e serviços da camada de aplicação: HTTP, SMTP, POP3, TLS

Kurose (2006) explica que camada de aplicação em redes de computadores engloba uma diversidade de protocolos e serviços essenciais para a comunicação e transferência de dados na internet. O HTTP (*Hypertext Transfer Protocol*) é usado na navegação na web, permitindo a transferência de páginas da web e recursos associados. O SMTP (*Simple Mail Transfer Protocol*) é utilizado para o envio de e-mails, enquanto o POP3 (*Post Office Protocol 3*) permite que os clientes de e-mail recebam mensagens em suas caixas de entrada. O TLS (*Transport Layer Security*) é uma camada de segurança que protege a privacidade e integridade dos dados em trânsito, garantindo conexões seguras na web e em outros serviços.

O HTTP é um protocolo utilizado para acessar conteúdo web na rede mundial de computadores. Viabiliza a transferência ponto a ponto entre clientes e servidores em serviços do tipo elástico e streaming (multimídia). Veja a Figura 3 a seguir:

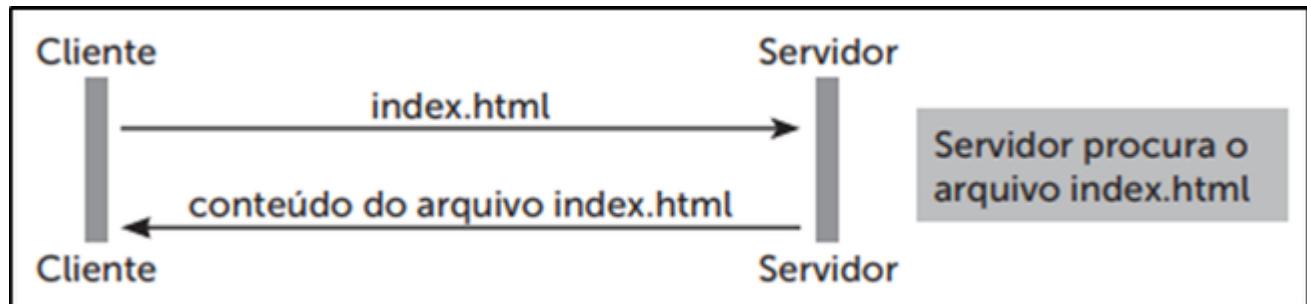


Figura 3 | Protocolo HTTP. Fonte: adaptada pelo autor a partir de Tanenbaum, Feamster e Wetherall (2021, [s. p.]).

Um computador efetua uma solicitação para acessar um site aloocado em um servidor HTTP, quando o usuário digita o endereço do site disponível na internet. Ao receber a solicitação, o servidor envia a resposta, e o usuário visualiza o conteúdo por meio de um navegador web.

Para hospedagem de sites, sistemas web, jogos online, entre outras aplicações, o mercado possui diversas empresas que disponibilizam hospedagem gratuita. No Quadro 2 a seguir, é demonstrado o endereço do host (nome dado à hospedagem web) e os serviços disponíveis.

Host	Serviços
000webhost.com	HTPP, e-mail, banco de dados e FTP.
freehostia.com/hosting.html	HTPP, e-mail.
hostinger.com	HTPP, e-mail e FTP.
Servidorgratuito.com	HTPP, e-mail, banco de dados e FTP.

Quadro 2 | Hospedagens. Fonte: adaptado pelo autor a partir de Kurose (2006, [s. p.]).

SMTP é a sigla para *Simple Mail Transfer Protocol* (protocolo simples de transferência de e-mail). É o protocolo utilizado para efetuar a transferência de e-mail de um servidor para outro. Veja a Figura 4 a seguir:

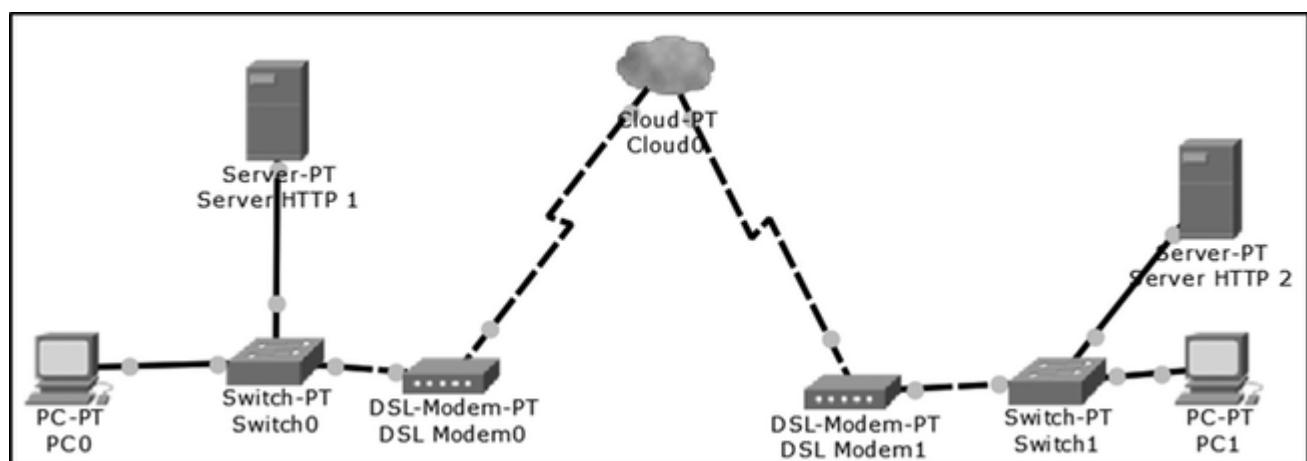


Figura 4 | Simple Mail Transfer Protocol (protocolo simples de transferência de e-mail). Fonte: adaptada pelo autor a partir de Nunes (2017, p. 78).

Neste caso, o usuário A do “PC0” possui uma conta de e-mail localizada no “Server HTTP 1”; por sua vez, no “PC1”, o usuário B possui uma conta de e-mail no “Server HTTP 2”. Quando o usuário A escreve uma mensagem ao usuário B, esta primeiramente é enviada para o “Server HTTP 1” e, depois disso, o protocolo SMTP se encarrega de transferi-la para o “Server HTTP 2”, possibilitando que o usuário B acesse a mensagem. Para que isso ocorra, o acesso aos e-mails pode ser efetuado via web, usando o HTTP. Este servidor HTTP, por sua vez, acessa o servidor SMTP, no qual estão alocadas as mensagens.

O POP3 (*Post Office Protocol*), está na terceira versão. O protocolo permite que o usuário descarregue em seu equipamento as mensagens que estejam localizadas em um servidor de e-mail. Quando as operadoras de internet não ofereciam conexões banda larga, alguns programas, como Outlook ou Thunderbird, tinha esse objetivo. Por sua vez, o IMAP (*Internet Messaging Access Protocol*), como ocorre com o POP3, sincroniza as mensagens alocadas em um servidor de e-mail, porém se mantém conectado a fim de sincronizar as mensagens recebidas, em tempo real.

A TLS (*Transport Layer Security*) é uma camada de segurança que fornece criptografia e autenticação para proteger as comunicações em redes, incluindo a internet. É utilizada para criar conexões seguras, como HTTPS (HTTP seguro), protegendo a privacidade e a integridade dos dados transmitidos. Isso torna mais difícil a interceptação de informações.

Segundo Nunes (2017), quando você faz uma compra online e insere informações de pagamento em um site, a TLS é usada para criar uma conexão segura entre o seu navegador e o servidor do site. Isso certifica que suas informações de pagamento sejam criptografadas e protegidas contra interceptação por terceiros enquanto estão sendo transmitidas pela internet. Elementos da TLS:

- **Criptografia:** a TLS usa técnicas de criptografia para codificar os dados transmitidos entre o cliente e o servidor.
- **Autenticação:** a TLS permite a autenticação mútua entre o cliente e o servidor. Isso certifica que o cliente esteja se conectando ao servidor correto e que o servidor possa verificar a identidade do cliente.
- **Integridade dos dados:** a TLS também certifica que os dados não tenham sido alterados durante a transmissão. Utiliza funções *hash* criptográficas para verificar a integridade dos dados e detectar qualquer alteração accidental ou maliciosa.
- **Versões do protocolo:** a TLS possui várias versões, sendo as mais comuns a TLS 1.0, 1.1, 1.2 e 1.3. As versões mais recentes tendem a ser mais seguras e eficientes.
- **Configuração e certificados:** para estabelecer uma conexão segura com TLS, os servidores web geralmente precisam de certificados SSL/TLS emitidos por autoridades de certificação confiáveis. Esses certificados validam a identidade do servidor e garantem a autenticidade da conexão.

## Protocolos e serviços da camada de aplicação: NTP, DNS, SSH, FTP

De acordo com Kurose (2006), a camada de aplicação em redes de computadores engloba protocolos e serviços essenciais, como NTP para sincronização de tempo, DNS para traduzir nomes de domínio em endereços IP, SSH para acesso remoto seguro e FTP para transferência de arquivos. Vamos conhecer um pouco mais sobre esses protocolos.

O *Network Time Protocol* (NTP), protocolo de tempo de redes, tem como função sincronizar os relógios dos servidores, roteadores e computadores das redes. Para fazer com que ocorra a sincronia, os servidores NTP são estruturados por uma topologia hierarquizada em camadas, entre as quais existe um mecanismo de consulta de tempo para o ajuste preciso. Os dispositivos solicitam a atualização do tempo para os servidores. Um servidor NTP pode ser configurado para sincronizar os relógios de todos os dispositivos em uma rede corporativa, garantindo que todas as transações e eventos sejam registrados com precisão, mantendo os relógios no horário correto.

Nunes (2017) define que o protocolo DNS tem como função principal efetuar a tradução do número IP para o nome de domínios dentro de um servidor DNS. Veja o Quadro 3 a seguir:

Nome de domínio	IP Correspondente
kroton.com.br	87.86.214.62
google.com.br	216.58.202.131
teleco.com	64.14.55.148
cert.br	200.160.7.17

Quadro 3 | DNS. Fonte: adaptado pelo autor a partir de Nunes (2017, p. 82).

A hierarquia dos domínios é dividida em três pontos:

- **Domínio genérico:** os registros seguem conforme os segmentos do site, que podem ser: .com, .net, .org, .edu, .gov, etc.
- **Domínio de países:** é utilizada a abreviatura com dois caracteres para identificar em qual país o domínio foi registrado, podendo ser: br (Brasil), us (Estados Unidos), ar (Argentina), etc.
- **Domínio reverso:** faz o processo reverso à consulta ao servidor DNS. Quando um servidor recebe uma solicitação, é feita uma consulta em sua “tabela”, que, por sua vez, encaminha a solicitação do cliente, apontando para o servidor relacionado ao endereço digitado pelo usuário, sendo utilizado o endereço IP.

O resolvelor do nome de domínio basicamente precisa responder como uma aplicação do tipo cliente/servidor, que tem a capacidade de mapear e encaminhar as solicitações de acesso a sites por meio do endereço ou número IP fornecido.

O protocolo SSH (*Secure Shell*) é utilizado para efetuar acesso remoto em outro dispositivo, por meio de um terminal, assim como o *prompt* de comando do DOS. A grande diferença para as outras técnicas de acesso remoto (Telnet e RSH) está relacionada com a segurança. Ao fazer um acesso remoto em um equipamento, a transmissão de dados recebe uma criptografia que pode variar conforme o algoritmo de encriptação, a fim de certificar a integridade do que é compartilhado. Um administrador de sistema pode usar SSH para se conectar a um servidor remotamente e realizar tarefas de administração, como configurar o servidor ou solucionar problemas.

O FTP (*File Transfer Protocol*) é um protocolo utilizado para a transferência de arquivos entre um cliente e um servidor. Ele permite a cópia de arquivos de um sistema para outro, seja localmente ou pela internet. O FTP é usado em diversos cenários, incluindo a publicação de conteúdo da web, o compartilhamento de arquivos e a distribuição de software. Existem duas variantes principais, FTP padrão (inseguro) e FTPS (FTP Seguro), que adiciona criptografia para proteger a transmissão de dados sensíveis. Um designer gráfico pode usar um cliente FTP para fazer upload de arquivos de imagem para um servidor web, por exemplo, tornando-os acessíveis ao público na internet.

## Vamos Exercitar?

Os protocolos da camada de transporte desempenham um papel crucial na comunicação de dados em redes. Dois dos protocolos mais notáveis nesta camada são o TCP (*Transmission Control Protocol*) e o UDP (*User Datagram Protocol*), cada um com características distintas.

O TCP é conhecido por ser orientado à conexão, o que significa que ele estabelece uma conexão antes de iniciar a transmissão. Além disso, o TCP oferece garantias de entrega confiável, empregando mecanismos de retransmissão e confirmação de recebimento. Isso torna o TCP ideal para aplicativos que demandam alta confiabilidade, como transferência de arquivos e navegação na web. Através do campo “*Acknowledgement number*” no cabeçalho do TCP, o remetente pode acompanhar o número de sequência do próximo byte esperado, permitindo a retransmissão de segmentos não confirmados.

Por outro lado, o UDP é um protocolo sem conexão, o que significa que não há estabelecimento de conexão. No entanto, ele não oferece garantias de entrega, tornando-o mais apropriado para aplicativos que podem tolerar alguma perda de dados, como streaming de vídeo e jogos online. Para aplicativos de chat em tempo real, como o WhatsApp, a escolha do UDP se justifica pela necessidade de entrega rápida de mensagens. No entanto, é importante observar que o aplicativo de chat deve implementar seu próprio mecanismo de garantia de entrega, já que o UDP não fornece essa funcionalidade por padrão.

Mudando o foco para a camada de aplicação, vários protocolos desempenham funções específicas na transmissão de dados:

O HTTP (*Hypertext Transfer Protocol*) é amplamente utilizado para acessar conteúdo na web, permitindo a transferência de páginas da web e recursos associados.

O SMTP (*Simple Mail Transfer Protocol*) é essencial para o envio de e-mails, enquanto o POP3 (*Post Office Protocol 3*) é empregado pelos clientes de e-mail para receber mensagens em suas caixas de entrada. O SMTP lida com o envio de mensagens, enquanto o POP3 lida com a recepção.

O TLS (*Transport Layer Security*) desempenha um papel fundamental na segurança das comunicações online, fornecendo criptografia para proteger os dados transmitidos, autenticação para verificar a identidade do cliente e a integridade dos dados, garantindo que não tenham sido alterados durante a transmissão.

Na mesma camada, encontramos protocolos como o NTP (*Network Time Protocol*), que sincroniza os relógios em redes para garantir a precisão na marcação de transações e eventos. Além disso, o DNS (*Domain Name System*) é vital, pois traduz nomes de domínio em endereços IP, permitindo a resolução de nomes na internet.

Por último, o SSH (*Secure Shell*) é utilizado para acesso remoto seguro a dispositivos, protegendo a transmissão de dados por meio da criptografia e garantindo a autenticidade e integridade da conexão. Já o FTP (*File Transfer Protocol*) é empregado para a transferência de arquivos entre clientes e servidores, tornando-se uma escolha valiosa quando a segurança adicional é necessária, podendo ser implementada através do FTPS. Todos esses protocolos e serviços desempenham papéis vitais nas comunicações em rede, garantindo que os dados sejam transmitidos com eficácia e segurança.

## Saiba mais

A importância das arquiteturas de rede na comunicação moderna reside na padronização e na capacidade de permitir que diferentes dispositivos e sistemas se comuniquem de maneira eficiente e segura, tornando possível a globalização da internet e a conectividade de dispositivos em todo o mundo. A compreensão das camadas e protocolos ajuda a solucionar problemas de rede, pois permite isolar e diagnosticar problemas em um nível específico, além de facilitar o desenvolvimento e a manutenção de redes mais robustas e eficazes. A seguir, mais conteúdo complementar para aprofundar seu conhecimento.

- Artigo [Tunelamento DNS: metodologia de detecção para ambiente em nuvem computacional](#), p. 395, da Revista Ibérica de Sistemas e Tecnologias de Informação.
- Artigo [Uma análise de desempenho da rede metropolitana de telemedicina dos hospitais universitários da cidade de Natal-RN/Brasil](#), da revista HOLOS.
- Filme: Snowden. (Snowden: Herói ou Traidor). Direção: Oliver Stone. Produção: Moritz Borman, Eric Kopeloff, Philip Schulz-Deyle, Fernando Sulichin. Estados Unidos: Pathê. 2016. DVD (134 min.). Depois de trabalhar durante anos na Agência de Segurança Nacional,

Edward Snowden decide entregar documentos secretos de ações de invasão de privacidade do governo dos Estados Unidos.

## Referências

BORGES, L. S. B.; *et al.* Tunelamento DNS: metodologia de detecção para ambiente em nuvem computacional. **Revista Ibérica de Sistemas e Tecnologias de Informação**, Brasília, ed. 57, 2023.

KUROSE, J. F. **Redes de computadores e a internet**: uma abordagem top-down. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

MEDEIROS, R. M.; *et al.* Uma análise de desempenho da rede metropolitana de telemedicina dos hospitais universitários da cidade de Natal-RN/Brasil. **HOLOS**, Natal, v. 30, n. 4. 2014. Disponível em: <https://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/987>. Acesso em: 3 abr. 2024.

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

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Aula 5

Encerramento da Unidade

## Modelo de referência ISO/OSI e arquitetura TCP/IP



### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

## Ponto de Chegada

Olá, estudante! A competência desta Unidade é “Compreender a importância do modelo OSI de referência, que facilitou o desenvolvimento e a estruturação das redes; reconhecer e categorizar os serviços de rede, a estrutura hierárquica dos protocolos e a relevância dos protocolos TCP/IP na garantia da comunicação entre as redes. Dessa forma, será viável adquirir conhecimento sobre determinados serviços fundamentais nas redes de computadores e configurá-los. Por meios desses aspectos básicos, você poderá desenvolver redes locais de pequeno porte”. Para desenvolvê-la, você deverá primeiramente conhecer os conceitos fundamentais.

## O modelo ISO/OSI e a padronização das redes

O modelo ISO/OSI e a padronização das redes atuam na compreensão do desenvolvimento e funcionamento dos protocolos de comunicação que dão suporte aos serviços de rede usados diariamente, como mensagens instantâneas, e-mail, acesso a sites, streaming e jogos online.

Antes da criação do modelo de referência OSI, as redes de computadores eram fragmentadas e incompatíveis devido a diferentes fabricantes desenvolvendo sistemas de comunicação próprios. Isso dificultava a interoperabilidade e a expansão das redes, tornando essencial a padronização. Ela foi realizada por várias entidades, incluindo a ISO (*International Organization for Standardization*), ANSI, ABNT, ANFOR, DIN, EIA, IEEE e ITU-T, cada uma com seu foco de padronização específico, como transmissões elétricas, engenharia elétrica, computação e telecomunicações.

O modelo de referência OSI, estabelecido pela ISO, consiste em sete camadas, cada uma com funções específicas e bem definidas, desde a camada física que lida com a transmissão de bits, até a camada de aplicação, que permite a interação com os aplicativos de usuário. Isso forneceu uma estrutura padronizada que facilitou a interoperabilidade, tornando possível que dispositivos de diferentes fabricantes interagissem sem problemas.

## Camadas do modelo ISO/OSI: física, enlace e de rede

O modelo de referência OSI, apesar de não ser uma arquitetura de protocolos de rede em si, fornece uma estrutura fundamental para o desenvolvimento desses protocolos. Ele é composto por sete camadas, sendo as três primeiras as mais cruciais para a compreensão das redes de computadores.

A camada física, a primeira do modelo, lida com a transmissão de bits pelos meios de comunicação, determinando voltagens que representam 0s e 1s, a duração dos bits e o método

de transmissão. Isso envolve a conversão de dados em sinais elétricos ou ópticos, considerando cabeamento, voltagens e frequência de sinais.

A camada de enlace transforma os dados da camada física em quadros, facilitando a detecção de erros. Além disso, lida com o controle de acesso ao meio para evitar colisões de dados.

A camada de rede é responsável pelo roteamento dos dados da origem ao destino, determinando o caminho mais eficiente e atualizando tabelas de roteamento. O controle de congestionamento também é tratado nessa camada, garantindo a eficiência da rede.

Em conjunto, essas camadas desempenham papéis fundamentais para possibilitar a conectividade em redes modernas. O modelo OSI serve como um guia para a estruturação de protocolos de rede, garantindo uma abordagem organizada e eficaz na transmissão de dados.

## Camadas do modelo ISO/OSI: transporte, sessão, apresentação, aplicação

A camada de transporte, a quarta, assegura a entrega confiável de dados, dividindo-os em unidades menores e certificando-se de que cheguem corretamente ao destino.

A camada de sessão, a quinta, gerencia conexões entre computadores geograficamente separados e controla aspectos como sincronização e verificação do status da conexão. Isso é essencial para aplicativos que exigem comunicação interativa, como videoconferências.

A camada de apresentação, a sexta, lida com a semântica e a sintaxe dos dados transmitidos, garantindo que a codificação e a decodificação corretas sejam aplicadas durante a conexão. Isso permite que diferentes tipos de informações sejam trocados, independentemente do software ou plataforma utilizada.

A camada de aplicação, a sétima, é a mais próxima do usuário final e abriga os aplicativos que permitem a comunicação direta com o usuário, como navegadores da web, clientes de e-mail e programas de banco de dados.

O modelo ISO/OSI oferece uma estrutura sólida que facilita a compreensão e o desenvolvimento de sistemas de rede, permitindo a interconexão de dispositivos em diferentes infraestruturas. A padronização proporcionada pelo modelo ISO/OSI é fundamental para a interoperabilidade dos sistemas em um ambiente cada vez mais conectado.

## Definição, camadas e diferenças: arquitetura TCP/IP *versus* modelo ISO/OSI

A arquitetura TCP/IP, amplamente usada na prática, é a base da internet. Essa arquitetura se tornou a espinha dorsal da internet e permite a interconexão de dispositivos e aplicativos, desempenhando um papel fundamental em redes empresariais e na internet.

Essa hierarquia de camadas na arquitetura TCP/IP permite modularização e separação de responsabilidades em diferentes níveis, garantindo eficiência e confiabilidade na comunicação. Ela também facilita a evolução da infraestrutura de rede, pois novos protocolos ou tecnologias podem ser adicionados ou substituídos em uma camada sem afetar as demais.

## Classificação de serviços e hierarquia de protocolos

Cada camada se comunica com a correspondente em outro dispositivo, intermediando a comunicação. Na prática, os protocolos em redes estão ligados aos serviços cotidianos, como o TCP/IP, DNS e NTP, que permitem o funcionamento de aplicativos.

A camada de aplicação lida com a interação direta entre programas e serviços usados pelo usuário, como navegadores e clientes de e-mail. Protocolos como HTTP e SMTP são implementados nesta camada.

A camada de transporte assegura a entrega confiável de dados entre máquinas. O TCP oferece comunicação confiável, enquanto o UDP é mais rápido, mas não garante a entrega.

A camada de rede lida com roteamento e encaminhamento de dados entre redes. O protocolo IP é usado nesta camada.

A camada de acesso à rede é a mais baixa e lida diretamente com o meio físico. Protocolos variam com a tecnologia de rede usada, como Ethernet e Wi-Fi.

Essas camadas garantem que a comunicação seja eficiente e confiável, permitindo que novos protocolos sejam adicionados sem afetar as outras camadas.

## Protocolos e serviços da camada de enlace

A camada de enlace de dados, a segunda camada no modelo OSI, é responsável pela comunicação entre dispositivos diretamente conectados em uma rede de computadores.

Dois principais serviços são prestados pela camada de enlace:

- **Entrega de quadros:** a camada de enlace divide os dados em pacotes chamados “quadros” e os envia para o equipamento de destino. Cada quadro contém informações, como endereços MAC (*Media Access Control*), para identificar o remetente e o destinatário. Esse serviço garante que os dados sejam entregues corretamente ao dispositivo de destino.
- **Controle de acesso ao meio:** esse serviço coordena o acesso a um meio de transmissão compartilhado, como um cabo ou uma rede sem fio. Os protocolos de controle de acesso ao meio garantem que os dispositivos na rede transmitam seus dados de maneira ordenada, evitando colisões de dados. Um exemplo desse controle é o protocolo CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), usado em redes Ethernet para evitar colisões de quadros.

Além desses serviços, diversos protocolos e padrões estão associados à camada de enlace, incluindo:

- **Ethernet:** amplamente utilizado, define como os quadros são encapsulados e transmitidos em redes com fio. Cada dispositivo possui um endereço MAC exclusivo para identificação. Os *switches* Ethernet operam nesta camada para encaminhar quadros com base nos endereços MAC.
- **Wi-Fi (IEEE 802.11):** para redes sem fio, o padrão IEEE 802.11 define como os dados são transmitidos entre dispositivos, gerenciando a conectividade sem fio e a segurança.
- **PPP (*Point-to-Point Protocol*):** usado para estabelecer conexões ponto a ponto, como as criadas por modems discados. Atua na autenticação e configuração da conexão, bem como na transmissão confiável de dados.
- **HDLC (*High-Level Data Link Control*):** oferece entrega confiável de dados e é amplamente utilizado em linhas de comunicação dedicadas e redes privadas.
- **Frame Relay:** projetado para redes de alta velocidade e baixa latência, como WANs, oferece um serviço de entrega de quadros eficiente e é menos complexo do que outros protocolos, como o PPP.

## Protocolos e serviços da camada de rede: o protocolo IP

A camada de rede, a terceira no modelo OSI, é responsável por rotear pacotes de dados de uma origem para um destino na rede. O IP atribui a cada dispositivo um endereço único, conhecido como endereço IP. Ele é utilizado para identificar e localizar esses dispositivos.

O *Internet Protocol*, ou IP, é um endereço lógico que permite aos dispositivos se comunicarem independentemente de sua localização geográfica. Quando um dispositivo envia dados para outro na rede, o IP é responsável por determinar a melhor rota para os dados alcançarem o destino. Isso envolve a análise dos endereços IP de origem e destino, juntamente com informações de roteamento, para determinar a próxima parada dos pacotes. Cada roteador em uma rede toma decisões de encaminhamento com base nas informações do cabeçalho IP.

O protocolo IP divide os dados em pacotes chamados datagramas, que contêm informações, incluindo o endereço IP de origem e destino, juntamente com os próprios dados. Esses datagramas são roteados por roteadores intermediários, que consultam tabelas de roteamento para determinar a melhor rota com base no endereço IP de destino. Os datagramas são encaminhados de um salto (*hop*) para outro até alcançarem o destino.

O IP fornece entrega de pacotes não confiável e sem conexão, tratando cada pacote de informações de forma independente. Isso significa que não garante a entrega e não requer confirmações dos hosts de envio, recebimento ou intermediários. Os pacotes IP são encapsulados em quadros de camadas inferiores, como Ethernet, transmitidos pela rede e roteados até o destino, onde são desencapsulados e os dados são entregues aos aplicativos apropriados.

## Outros protocolos e serviços da camada de aplicação: ICMP, IGMP, ARP e protocolos de roteamento

Alguns dos protocolos e serviços mencionados incluem:

- **ICMP (Internet Control Message Protocol)**: é usado para comunicações de controle e diagnóstico na internet. Não é usado para transferência de dados, mas sim para relatar erros, verificar a disponibilidade de dispositivos e realizar funções de controle.
- **IGMP (Internet Group Management Protocol)**: é usado para controlar o tráfego de *multicast* em redes IP. Permite que os dispositivos em uma rede comuniquem ao roteador ou *switch* que desejam receber tráfego *multicast* de um grupo específico.
- **ARP (Address Resolution Protocol)**: é usado para mapear endereços IP para endereços MAC em redes locais. Quando um dispositivo na rede precisa enviar um pacote para outro dispositivo na mesma rede, ele usa o ARP para descobrir o endereço MAC correspondente ao endereço IP de destino.

Alguns dos principais protocolos de roteamento mencionados incluem:

- **OSPF (Open Shortest Path First)**: é amplamente utilizado em redes empresariais e ISPs (*Internet Service Providers*). Protocolo baseado em estado de enlace que é escalável e altamente eficiente. Foi projetado para calcular rotas com base na topologia da rede e oferece recursos avançados de convergência rápida.
- **BGP (Border Gateway Protocol)**: protocolo de roteamento utilizado na internet global para rotear tráfego entre sistemas autônomos (ASes). É altamente escalável e fundamental para determinar as rotas de tráfego na internet.
- **RIP (Routing Information Protocol)**: protocolo de roteamento distante baseado em vetores de distância. Embora não seja tão comum como no passado, ainda é encontrado em algumas redes menores.
- **RIPv2 e RIPvNG**: RIPv2 é uma versão aprimorada do RIP que dá suporte ao roteamento IPv4. RIPvNG (RIP Next Generation) é a versão correspondente para o IPv6. Ambos são

usados em redes menores ou em cenários de transição para o IPv6.

## Protocolos da camada de transporte: TCP e UDP

O TCP (Protocolo de Controle de Transmissão) é um serviço orientado à conexão. Estabelece-a entre o remetente e o receptor antes da transferência de dados. O TCP garante a entrega confiável dos dados por meio de confirmações de recebimento e retransmissões em caso de perda. Características desse protocolo:

- **Garantia de entrega:** o TCP garante que os dados sejam entregues ao destinatário na ordem correta e sem erros. Isso é essencial para aplicativos em que a integridade e a ordem dos dados são críticas.
- **Transmissão lenta e necessita de maior largura de banda:** devido à sobrecarga de controle e garantias de entrega, o TCP pode ser mais lento e consumir mais largura de banda do que o UDP.
- **Comunicação ponto a ponto:** o TCP é projetado para comunicações ponto a ponto, nas quais um remetente se comunica diretamente com um receptor. Uso comum em aplicativos como transferência de arquivos, acesso remoto, navegação na web e qualquer aplicativo que requer entrega confiável e ordenada de dados.

UDP (*User Datagram Protocol*) é um serviço que não estabelece uma conexão antes da transferência de dados. Ele não oferece garantia de entrega ou controle de fluxo e não garante o recebimento. O UDP não fornece confirmações de recebimento, o que significa que os dados podem ser perdidos ou chegar fora de ordem. Isso é adequado para aplicativos em que a latência é mais crítica do que a garantia de entrega.

## Protocolos e serviços da camada de aplicação: HTTP, SMTP, POP3, TLS

- **HTTP (*Hypertext Transfer Protocol*):** usado para navegação na web, permitindo a transferência de páginas da web e recursos associados.
- **SMTP (*Simple Mail Transfer Protocol*):** utilizado para o envio de e-mails. Permite a transferência de e-mails de um servidor para outro.
- **POP3 (*Post Office Protocol 3*) e IMAP (*Internet Message Access Protocol*):** POP3 é usado para descarregar mensagens de um servidor de e-mail para um dispositivo do usuário. IMAP permite sincronizar as mensagens em tempo real entre o servidor e o dispositivo do usuário, mantendo as mensagens no servidor.
- **TLS (*Transport Layer Security*):** camada de segurança que fornece criptografia e autenticação para proteger comunicações em redes, incluindo a internet.

## Protocolos e serviços da camada de aplicação: NTP, DNS, SSH, FTP

- **NTP (Network Time Protocol)**: usado para sincronizar relógios em servidores, roteadores e computadores em redes. Funciona por meio de servidores NTP hierarquizados que fornecem atualizações de tempo precisas para dispositivos.
- **DNS (Domain Name System)**: traduz nomes de domínio em endereços IP. Hierarquia dos domínios é dividida em genéricos (ex: .com), de países (ex: .br), e reversos para mapear endereços IP.
- **SSH (Secure Shell)**: usado para acesso remoto seguro a outros dispositivos, como servidores. Fornece criptografia para proteger a transmissão de dados durante a conexão.
- **FTP (File Transfer Protocol)**: usado para transferência de arquivos entre um cliente e um servidor. Permite a cópia de arquivos localmente ou pela internet. Existem duas variantes principais: FTP padrão (inseguro) e FTPS (seguro), que adiciona criptografia para proteger a transmissão de dados sensíveis.

### É Hora de Praticar!



#### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Ao configurar sua rede doméstica, você pode compartilhar a internet e recursos entre dispositivos de maneira conveniente e manter suas configurações de segurança atualizadas para proteger sua rede contra ameaças. À medida que você adquire mais conhecimento em redes de computadores, poderá explorar configurações avançadas. Neste estudo de caso, vamos explorar como configurar utilizar protocolos e serviços.

Vamos entender as diferenças entre o TCP e o UDP em termos de características e funcionalidades. Imagine que você está configurando uma rede de escritório e precisa decidir entre o TCP e o UDP para transmitir dados entre os computadores. Que fatores você consideraria ao tomar essa decisão? Você deve apontar três fatores e explicar por que são importantes.

Na configuração servidor web em sua rede local para hospedar um site da sua empresa, qual protocolo da camada de aplicação (HTTP ou HTTPS) você usaria para garantir a segurança da comunicação entre os clientes e o servidor? Explique por quê.

Além do servidor web, você recebeu a tarefa de configurar um servidor de e-mail para sua empresa. Descreva a diferença entre os protocolos SMTP e POP3 e explique quando cada um

deles é usado.

Devido a ataques cibernéticos, a empresa em que você trabalha está preocupada com a segurança das comunicações e deseja proteger os dados transmitidos pela rede. Qual protocolo de segurança da camada de aplicação você usaria para criptografar as comunicações HTTP: TLS ou SSL? Explique a diferença entre eles.

Nos servidores de rede em sua empresa, você precisa manter o tempo sincronizado com precisão. Qual protocolo da camada de aplicação você usaria para sincronizar o tempo em sua rede e por quê?

Seu departamento de TI precisa configurar um serviço de tradução de nomes de domínio para endereços IP na rede. Qual protocolo da camada de aplicação você usaria para essa finalidade e qual equipamento de rede desempenharia um papel fundamental nesse serviço?

Outra demanda de sua empresa: você precisa configurar um servidor remoto que permita acesso seguro a outros dispositivos na rede. Qual protocolo da camada de aplicação você usaria para fornecer acesso remoto seguro e qual tipo de equipamento de rede seria essencial para essa configuração?

Por fim, você está configurando um servidor para compartilhamento de arquivos na sua rede. Qual protocolo da camada de aplicação você usaria para permitir que os clientes façam o upload e download de arquivos, e como um roteador na rede pode facilitar o acesso a esse servidor?

Você pode propor diferentes formas de solução e chegar ao mesmo objetivo. Qual foi o seu modelo de configuração? Mão à obra!

Como ter uma compreensão mais sólida dos protocolos da camada de transporte, bem como dos protocolos e serviços da camada de aplicação em redes de computadores?

Lembre-se de que a escolha do protocolo e do equipamento de rede adequados depende dos requisitos específicos de sua rede e de seus objetivos de segurança e desempenho.

As diferenças entre TCP e UDP são as seguintes: o TCP (*Transmission Control Protocol*) é um protocolo orientado à conexão que oferece confiabilidade na entrega de dados, garantindo que os pacotes cheguem na ordem correta e sem erros. O UDP (*User Datagram Protocol*), por outro lado, é não orientado à conexão, o que significa que ele não garante a entrega confiável dos pacotes nem a ordem em que eles são entregues. Fatores para escolher entre TCP e UDP incluem a natureza dos dados, sua sensibilidade à ordem e necessidade de entrega confiável. Se essas características são necessárias, o TCP é a escolha apropriada. Se a perda de alguns pacotes não é crítica (como em transmissões de vídeo), o UDP pode ser mais adequado. Por exemplo, videoconferências podem usar UDP para minimizar a latência, enquanto transferências de arquivos confiáveis podem usar TCP.

Para garantir a segurança da comunicação entre clientes e servidores web, é recomendável usar o HTTPS (*HTTP Secure*), que utiliza o protocolo TLS (*Transport Layer Security*) para criptografar os dados em trânsito. Isso garante a confidencialidade e integridade dos dados transmitidos.

SMTP (*Simple Mail Transfer Protocol*) é usado para enviar e-mails, enquanto o POP3 (*Post Office Protocol*, versão 3) é usado para recuperar e-mails. SMTP é usado para enviar e-mails do cliente para o servidor, enquanto o POP3 é usado para baixar e-mails do servidor para o cliente.

Para criptografar as comunicações HTTP, é recomendado usar o TLS (*Transport Layer Security*), pois o SSL (*Secure Sockets Layer*) é considerado obsoleto. Ambos TLS e SSL são protocolos que fornecem segurança na camada de transporte, mas o TLS é mais seguro e atualizado.

O protocolo NTP (*Network Time Protocol*) é usado para sincronizar o tempo em redes. Ele garante que todos os dispositivos da rede estejam em sincronia com um relógio de referência.

O protocolo DNS (*Domain Name System*) é usado para traduzir nomes de domínio em endereços IP. Um equipamento fundamental nesse serviço é o servidor DNS, que armazena informações de mapeamento nome-domínio para consulta.

O SSH (*Secure Shell*) é usado para fornecer acesso remoto seguro a outros dispositivos na rede. Um firewall ou roteador pode facilitar o acesso ao bloquear ou permitir o tráfego SSH, direcionando-o para o dispositivo correto.

O protocolo FTP (*File Transfer Protocol*) é usado para permitir o upload e download de arquivos em um servidor. Um roteador pode ser configurado para encaminhar o tráfego FTP para o servidor de arquivos a fim de que os clientes possam acessar os arquivos com sucesso.

## ISO/OSI E ARQUITETURA TCP/IP

**1**

### O MODELO ISO/OSI E A PADRONIZAÇÃO DAS REDES

O modelo ISO/OSI e a padronização das redes atuam na compreensão do desenvolvimento e funcionamento dos protocolos de comunicação.

**2**

### ARQUITETURA TCP/IP

A arquitetura TCP/IP é a base da internet e é amplamente usada na prática.

**3**

### HIERARQUIA DE PROTOCOLOS

Cada camada se comunica com a camada correspondente em outro dispositivo, intermediando a comunicação.  
Protocolos e serviços da camada de enlace

**4**

### O PROTOCOLO IP

A camada de rede, a terceira camada no modelo OSI, é responsável por rotear pacotes de dados de uma origem para um destino na rede.

**5**

### PROTOCOLOS E SERVIÇOS

Camada de aplicação:  
ICMP, IGMP, ARP, HTTP, SMTP, POP3, TLS, NTP,  
DNS, SSH, FTP

Figura 1 | ISO/OSI e arquitetura TCP/IP. Fonte: elaborada pelo autor.

KUROSE, J. F. **Redes de computadores e a internet:** uma abordagem top-down. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

NAKAMURA, E. T. **Segurança da informação e de redes.** Londrina: Editora e Distribuidora Educacional S.A., 2016.

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

OLIVEIRA, D. B.; LUMMERTZ, R. S.; SOUZA, D. C. **Qualidade e desempenho de redes.** Porto Alegre: Sagah, 2019.

SOUZA, D. C.; *et al.* **Gerenciamento de redes de computadores.** Porto Alegre: Sagah, 2021.

TANEMBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores.** 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Unidade 3

### Arquitetura e Tecnologias de Redes

#### Aula 1

Ethernet: Tecnologia e Protocolos de Camada Física e de Enlace



#### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

#### Ponto de Partida

Olá, estudante!

A disciplina de Redes de Computadores explora os fundamentos e aplicações das redes de comunicação, abrangendo conceitos desde topologias e protocolos até segurança e gerenciamento de redes. Compreender a importância desses conceitos é crucial na era digital, em que a conectividade é vital para organizações e indivíduos. Ao longo deste curso, buscamos não apenas transmitir conhecimento, mas também fornecer um ambiente de aprendizado inclusivo e colaborativo. Você será encorajado a explorar, questionar e aplicar os conceitos aprendidos, promovendo assim uma compreensão sólida e prática do mundo das redes de computadores.

Os “domínios de broadcast” desempenham um papel crucial no funcionamento das redes de computadores, permitindo a comunicação de dados em uma rede local. Eles são definidos pelas áreas ou segmentos de uma rede local nos quais todos os dispositivos recebem pacotes de broadcast, que são mensagens destinadas a todos os equipamentos na mesma rede. Para compreender os domínios de broadcast, é importante considerar conceitos como endereços MAC exclusivos para identificar dispositivos na camada de enlace, o tráfego de broadcast para descobrir outros equipamentos e anunciar serviços, e a função dos *switches*, que encaminham pacotes apenas para a porta em que o dispositivo de destino está conectado, melhorando a eficiência da rede. Uma questão que surge é: como o controle dos domínios de broadcast afeta a segurança e a eficiência das redes de computadores?

Domínios de colisão referem-se a áreas em uma rede de computadores nas quais pacotes de dados podem colidir uns com os outros, causando interferência e perda de dados. Isso é especialmente relevante em redes Ethernet baseadas no protocolo CSMA/CD, nas quais os dispositivos compartilham o mesmo meio físico para transmitir dados. Quando ocorrem colisões, os dispositivos envolvidos interrompem a transmissão, aguardam um período aleatório e tentam novamente para evitar colisões contínuas. No entanto, com o avanço da tecnologia, colisões se tornaram menos comuns em redes modernas, devido ao uso de *switches* que segmentam o meio físico em domínios de colisão separados para cada porta, minimizando assim esse problema. No entanto, uma questão que se levanta é: como as tecnologias de rede continuam a evoluir, será que o conceito de domínios de colisão ainda é relevante em redes modernas, ou estamos nos aproximando de um ponto em que colisões se tornarão completamente obsoletas?

A Ethernet é uma tecnologia fundamental em redes de computadores, atuando nas camadas física e de enlace do modelo OSI. Ela oferece uma variedade de velocidades e métodos de comutação. A camada física cuida da transmissão de bits, caracterizando o meio de transmissão, codificação dos dados e topologia da rede. A camada de enlace controla o acesso ao meio e lida com a segmentação de quadros. A Ethernet oferece velocidades de 10 Mbps a 100 Gbps, e a comutação pode ser feita por *hubs* (com alto risco de colisões) ou *switches* (com domínios de colisão separados, melhorando o desempenho). Como a escolha da velocidade e do método de comutação Ethernet pode impactar o desempenho e a eficiência de uma rede?

Bons estudos!

## Vamos Começar!

### Domínios de broadcast

Os “domínios de broadcast” são importante parte do funcionamento de redes de computadores; eles trabalham com a comunicação de dados em uma rede local. Para compreender os domínios de broadcast, veremos primeiramente os endereços MAC, tráfego de broadcast e *switches*.

Segundo Kurose (2006), cada equipamento de rede, como computadores, impressoras, roteadores e switches, possui um endereço MAC (*Media Access Control*) exclusivo. Esse endereço é gravado na placa de rede do dispositivo e é usado para identificá-lo na camada de enlace de dados do modelo OSI.

Quando um equipamento na rede deseja enviar um pacote de dados para todos os outros equipamentos na mesma rede, ele envia esse pacote como um “pacote de broadcast”. Os pacotes de broadcast são destinados a todos os equipamentos na rede e são identificados pelo endereço MAC especial, por exemplo, “ff:ff:ff:ff:ff:ff”. Isso é usado para descobrir outros equipamentos na rede ou para anunciar serviços.

Os *switches* são equipamentos de rede que operam na camada de enlace (camada 2 do modelo OSI) e são projetados para encaminhar pacotes com base nos endereços MAC. Eles aprendem quais equipamentos estão conectados a cada uma de suas portas e, em vez de transmitir pacotes de broadcast para todas as portas, eles encaminham os pacotes apenas para a porta à qual o dispositivo de destino está conectado, tendo ganho de performance na rede.

Tanenbaum, Feamster e Wetherall (2021) explicam que um domínio de broadcast é uma área ou segmento de uma rede local no qual todos os equipamentos recebem pacotes de broadcast. Em outras palavras, é o escopo de equipamentos que podem ouvir e responder a pacotes de broadcast enviados na rede.

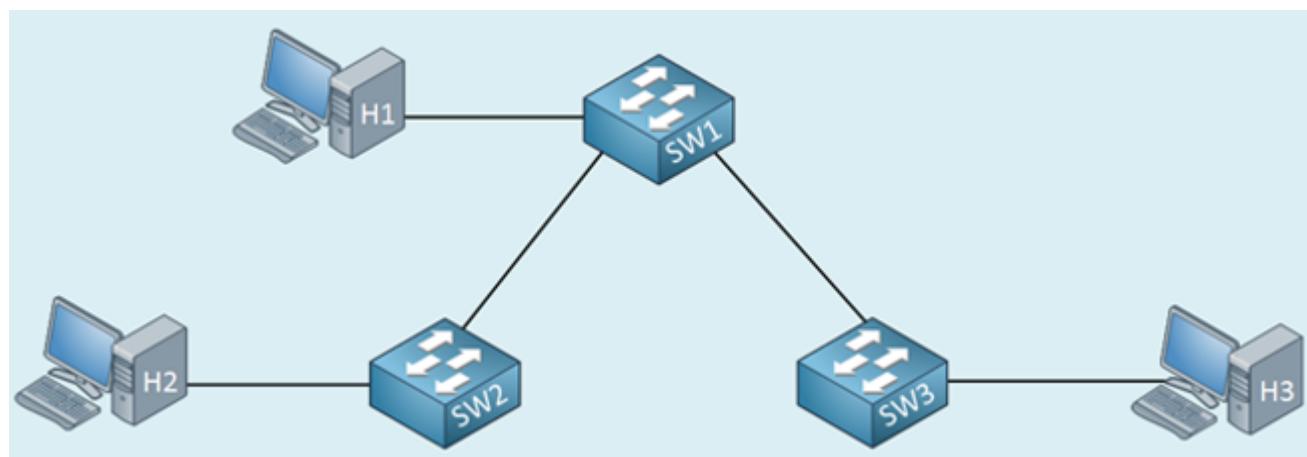


Figura 1 | Domínio de broadcast. Fonte: Tanenbaum, Feamster e Wetherall (2021, [s. p.]).

Normalmente, um *switch* divide uma rede local em vários domínios de broadcast. Isso ocorre porque os *switches* isolam o tráfego de broadcast, enviando pacotes de broadcast apenas para as portas que têm dispositivos que precisam desses pacotes. Isso ajuda a reduzir o tráfego desnecessário na rede e melhora a eficiência.

Portanto, cada segmento de rede conectado a uma porta de *switch* individual forma seu próprio domínio de broadcast. Se houver dois *switches* interconectados, eles compartilharão informações sobre endereços MAC para garantir que os pacotes de broadcast sejam encaminhados apenas para as em que dispositivos relevantes estão conectados.

O conceito de domínios de broadcast é totalmente utilizado para o projeto e a manutenção de redes locais, garantindo que o tráfego seja controlado e restrito apenas aos equipamentos que realmente precisam dessas mensagens.

Rede	1º IP válido	Último IP Válido	Broadcast
192.168.0.0	192.168.0.1	192.168.0.62	192.168.0.63
192.168.0.64	192.168.0.65	192.168.0.126	192.168.0.127
192.168.0.128	192.168.0.129	192.168.0.190	192.168.0.191
192.168.0.192	192.168.0.193	192.168.0.254	192.168.0.255

Quadro 1 | Tabela de sub-redes. Fonte: elaborado pelo autor.

De acordo com Nunes (2017), considerando as sub-redes, o último endereço é reservado para mensagens do tipo broadcast (última coluna). Ele indica a difusão de um pacote para todos os equipamentos da rede (se ele for enviado a uma sub-rede, então somente aos equipamentos dela o receberão). Ao receber a mensagem, o equipamento deve “ler” o pacote e verificar se lhe pertence. Se pertencer a ele, a mensagem é respondida; caso contrário, o pacote é descartado. Exemplo: ao ligarmos um computador em uma rede, é emitido uma mensagem de broadcast solicitando um endereço IP ao servidor DHCP. Os computadores e demais equipamentos descartam a solicitação e, então, o servidor DHCP responde ao pedido, atribuindo um endereço ao computador ou equipamento conectado.

## Domínios de colisão

Domínios de colisão, em redes de computadores, são áreas em uma rede nas quais os pacotes de dados podem colidir uns com os outros, causando interferência e resultando em perda de dados e ineficiência na transmissão. O conceito de domínios de colisão é fundamental para o projeto e gerenciamento de redes, especialmente em redes Ethernet baseadas no protocolo CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), que era mais comum em redes com fio.

Em uma rede Ethernet, todos os equipamentos compartilham o mesmo meio físico (como um cabo) para transmitir e receber dados. Quando vários equipamentos tentam transmitir ao mesmo tempo, pode ocorrer uma colisão, pois os sinais se sobrepõem. Para reduzir o impacto das colisões, as redes Ethernet segmentam o meio físico em domínios de colisão menores.

Para entender como as colisões ocorrem, é útil seguir o processo de transmissão de dados em uma rede Ethernet com CSMA/CD:

- **Escuta do meio (*Carrier Sense*):** verifica se o meio de comunicação está ocupado ou livre. Se o meio estiver livre, o dispositivo tenta iniciar a transmissão.
- **Transmissão de dados:** o equipamento começa a enviar os dados.
- **Colisão detectada:** se dois ou mais equipamentos iniciam a transmissão simultaneamente, a detecção de colisão ocorre. Isso é feito quando os equipamentos monitoram o meio para garantir que não haja colisões durante a transmissão.
- **Notificação de colisão:** quando uma colisão é detectada, todos os equipamentos envolvidos interrompem imediatamente a transmissão e enviam um sinal de colisão para alertar os outros equipamentos na rede.
- **Espera e retentativa:** após a colisão, os equipamentos esperam um período aleatório antes de tentar transmitir novamente. Isso ajuda a evitar colisões contínuas.

Souza *et al.* (2021) destacam que colisões são um problema em redes Ethernet com muitos equipamentos ou tráfego intenso. Elas podem causar atrasos e reduzir o desempenho da rede. Entretanto, com o aumento da velocidade das redes e a evolução das tecnologias de comutação, as colisões se tornaram menos comuns e menos problemáticas em redes contemporâneas. Isso ocorre porque os *switches* Ethernet e redes sem fio mais recentes evitam a maioria das colisões ao criar domínios de colisão separados para cada porta, permitindo que os dispositivos transmitam e recebam dados sem conflitos.

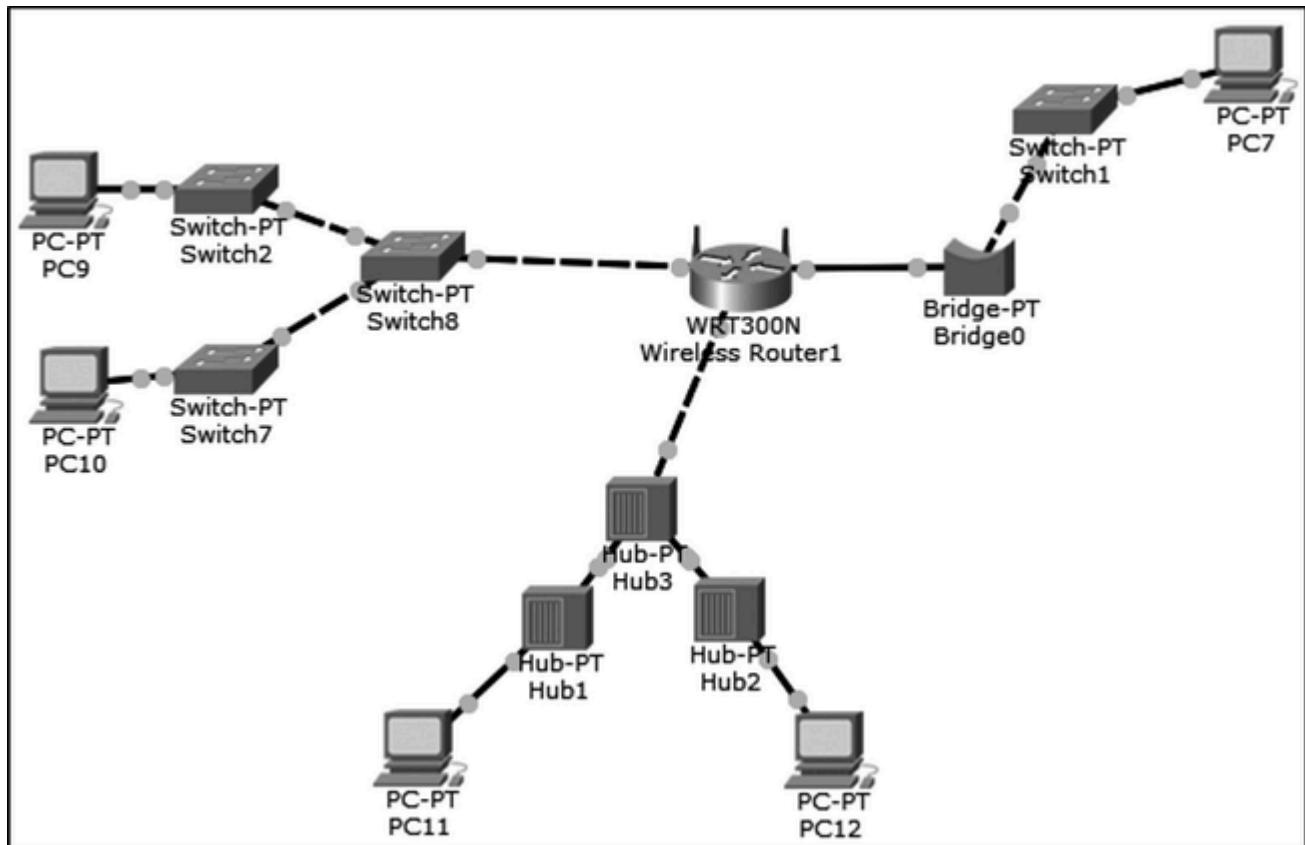


Figura 2 | Topologia com domínio de colisão. Fonte: adaptada de Nunes (2017, [s. p.]).

Dominando os conceitos e as características da rede do tipo Ethernet, é possível recuperar o termo “colisão”, utilizado nas explicações ao longo desta aula. Tanembaum, Feamster e Wetherall (2021) destacam que os dois tipos de ocorrências de colisões nas redes Ethernet são:

- No domínio de colisão, os pacotes têm a possibilidade de efetuar a colisão uns com os outros. Essa ocorrência é um dos fatores principais da degradação dos serviços; se o equipamento que realiza o domínio de colisão for cascadatao, a rede pode sofrer maiores consequências.
- No domínio de broadcast, determina-se o limite a que o pacote pode chegar, ou seja, um dispositivo em uma rede local é capaz de efetuar a comunicação com outro sem que seja utilizado um roteador.

Segundo Nunes (2017), as mensagens de broadcast são utilizadas pelas operadoras de celular para marketing dos seus serviços oferecidos. Em alguns países, são utilizadas para alertas de emergência como enchentes, ameaça de desastres naturais, entre outros. No entanto, sistemas como Android e IOS podem ser bloqueados para não receber tais mensagens de broadcast. Algumas tecnologias que se relacionam com as colisões e as mensagens de broadcast incluem:

- **Hubs:** como são equipamentos que repetem as mensagens para todas as portas, formam um único domínio de colisão e broadcast.

- **Roteadores:** são equipamentos concebidos na camada 3 do protocolo TCP/IP – por padrão quebram o domínio de broadcast.
- **Switch:** este equipamento é capaz de formar um domínio de colisão em cada uma de suas portas, em um único domínio de broadcast.
- **Bridge:** este equipamento pode separar domínios de colisão. Como os *switches*, formam um único domínio de broadcast.

O roteador pode separar os domínios de broadcast. Na topologia apresentada na Figura 2, há três domínios. Quanto ao domínio de colisão, verificamos que:

- Abaixo do roteador, a topologia é conectada apenas por *hubs*, formando, assim, um único domínio de colisão e broadcast
- À esquerda do roteador há dois domínios de colisão, pois os dispositivos estão ligados em um *switch*.
- À direita do roteador há um domínio de colisão ligado no único *switch*; portanto são quatro domínios de colisão.

Suponha que você tenha um escritório com vários computadores conectados a um único *switch*. Todos esses computadores compartilham a mesma conexão do *switch*, formando um único domínio de colisão. Se dois computadores A e B tentarem transmitir dados ao mesmo tempo, uma colisão pode ocorrer, resultando em perda de dados. Entretanto, caso haja outro *switch* interconectando mais computadores em uma sala próxima, essa sala agora formará um segundo domínio de colisão. Caso dois computadores na sala 1 tentem transmitir dados ao mesmo tempo, não afetarão os computadores na sala 2, pois eles estão em domínios de colisão diferentes.

Segundo Souza *et al.* (2021), para evitar colisões em redes Ethernet, muitas organizações utilizam *switches* em vez de *hubs*. Os switches dividem os domínios de colisão, permitindo que os equipamentos transmitam e recebam dados de forma eficiente. Cada porta de um *switch* é geralmente um domínio de colisão separado; isso significa que as colisões são minimizadas, tornando as redes mais rápidas e confiáveis.

**Siga em Frente...**

## Operação, velocidades, comutação

A Ethernet é uma tecnologia amplamente usada em redes de computadores, responsável pela transmissão confiável de dados em uma variedade de ambientes. Tanembaum, Feamster e Wetherall (2021) explicam que a Ethernet opera nas camadas física e de enlace do modelo OSI e tem várias variantes que diferem em termos de velocidades, meios de transmissão e métodos de comutação. Vamos explorar esses aspectos em detalhes:

### 1. Camada física:

A função da Ethernet na camada física é ser responsável pela transmissão dos bits de dados no meio físico, como cabos de cobre, fibra óptica ou comunicação sem fio. Define as características elétricas e mecânicas da transmissão, a forma de onda elétrica usada, a codificação dos dados e a topologia da rede. Um exemplo de camada física Ethernet é a Ethernet 1000BASE-T, que opera em cabos de par trançado e utiliza sinais elétricos para transmitir dados a uma velocidade de 1 gigabit por segundo (1 Gbps).

## 2. Camada de enlace (*Link Layer*):

A função da Ethernet na camada de enlace é ser responsável pelo controle de acesso ao meio (MAC – *Media Access Control*), gerenciando como os equipamentos compartilham o meio de transmissão e garantindo que não ocorram colisões de dados. Também lida com a segmentação e reassemblagem de quadros Ethernet. A Ethernet 802.3 é um exemplo amplamente utilizado na camada de enlace. Define os quadros Ethernet, que consistem em cabeçalhos e trailers que contêm informações de endereço MAC de origem e destino, tipo de protocolo e dados. Um exemplo é o quadro Ethernet comutado, que é um quadro de dados encaminhado por um *switch* Ethernet.

## 3. Velocidades:

A Ethernet oferece uma ampla variedade de velocidades, desde 10 Mbps (Ethernet 10BASE-T) até 100 Gbps (Ethernet 100GBASE-T) e além. Essa velocidade é um dos principais fatores que determina o desempenho da rede, e as escolhas dependem das necessidades específicas. Por exemplo, redes domésticas podem usar Ethernet de 1 Gbps, enquanto data centers podem adotar 10 Gbps ou 100 Gbps para dar suporte grandes volumes de tráfego.

## 4. Comutação:

A comutação na Ethernet refere-se ao método de encaminhamento de quadros Ethernet de uma porta de switch para outra. Existem dois principais métodos de comutação:

- **Comutação de hub:** em redes antigas, como Ethernet 10BASE-T com *hubs* (também conhecida como *hub* Ethernet), os quadros eram repetidos para todas as portas do *hub*. Isso criava um único domínio de colisão, o que tornava a rede suscetível a colisões e reduzia o desempenho.
- **Comutação de switch:** em redes modernas, os *switches* Ethernet são amplamente utilizados. Eles operam na camada de enlace e encaminham quadros com base nos endereços MAC. Isso cria domínios de colisão separados por porta, o que melhora significativamente o desempenho e a eficiência da rede.

Em uma rede com *switches* Ethernet, quando um equipamento A na porta 1 do *switch* deseja se comunicar com um equipamento B na porta 2, o *switch* encaminha diretamente o quadro de A para B, sem afetar outros dispositivos na rede.

## Vamos Exercitar?

O controle de domínios de broadcast desempenha um papel essencial na segurança e eficiência das redes de computadores, minimizando o tráfego desnecessário e protegendo informações sensíveis. Com o avanço das tecnologias de rede e o uso generalizado de *switches*, as colisões se tornaram menos problemáticas, tornando as redes mais rápidas e confiáveis. A escolha da velocidade e do método de comutação Ethernet é crucial para atender às necessidades específicas da rede, com *switches* sendo preferíveis para melhorar o desempenho e a eficiência, especialmente em ambientes com tráfego intenso.

O controle dos domínios de broadcast, ajuda a reduzir o tráfego desnecessário na rede, melhorando o desempenho geral, uma vez que os pacotes de broadcast são encaminhados apenas para as portas com dispositivos relevantes. Isso evita sobrecarregar a rede com mensagens que não são relevantes para a maioria dos dispositivos. Além disso, o controle de domínios de broadcast é fundamental para a segurança, pois limita a exposição de informações sensíveis a dispositivos não autorizados. Portanto, a capacidade de controlar e restringir o tráfego de broadcast é essencial para manter redes locais seguras e eficientes.

Os *switches* segmentam o meio físico em domínios de colisão separados, o que minimiza as colisões. Além disso, a crescente velocidade das redes e a evolução das tecnologias de comutação também desempenham um papel crucial na redução de colisões. Portanto, embora o conceito de domínio de colisão ainda seja relevante em algumas configurações de rede, em muitos casos, as colisões se tornaram menos comuns e menos problemáticas, tornando as redes mais rápidas e confiáveis.

A velocidade da Ethernet determina a taxa de transferência de dados e, portanto, deve ser selecionada com base nas necessidades específicas da rede. Redes domésticas podem se beneficiar de velocidades de 1 Gbps, enquanto data centers podem exigir 10 Gbps ou até 100 Gbps para dar suporte a grandes volumes de tráfego.

Quanto ao método de comutação, a decisão entre o uso de *hubs* ou *switches* é crucial. A comutação por *hubs*, com um único domínio de colisão, é propensa a colisões e pode prejudicar o desempenho da rede, especialmente em ambientes com tráfego intenso. Por outro lado, a comutação por *switches*, que cria domínios de colisão separados por porta, melhora significativamente o desempenho e a eficiência da rede, minimizando colisões e permitindo uma comunicação direta e eficaz entre dispositivos. Portanto, a escolha adequada desses aspectos é fundamental para garantir um funcionamento eficiente e confiável da rede.

## Saiba mais

O gerenciamento dos segmentos de difusão exerce um papel crucial na segurança e eficiência das redes de computadores, controlando o tráfego redundante e protegendo informações confidenciais. Quanto aos segmentos de colisão, embora ainda tenham relevância em algumas configurações, tornaram-se menos problemáticos devido ao avanço tecnológico e à ampla

aceitação de switches, que dividem o meio físico. A seleção da taxa e do método de comutação Ethernet é de suma importância para otimizar o desempenho da rede, sendo switches a opção preferível devido à sua capacidade de minimizar conflitos e facilitar a comunicação eficaz entre dispositivos. Vamos estudar os conteúdos adicionais a seguir:

- Artigo [Análise de Desempenho em Redes IEEE 802.3 Aplicado para Sistema de Tempo Real](#), da revista Holos.
- Artigo [Monitoração do Desempenho de Redes de Automação usando SNMP](#), da Tecnologia em Metalurgia e Materiais.
- Filme: The Imitation Game (Jogo da Imitação). Direção: Morten Tyldum. Produção: Teddy Schwarzman, Nora Grossman, Ido Ostrowsky. Estados Unidos: The Weinstein Company. 2014. DVD (114 min.). Baseado na história real do lendário criptoanalista inglês Alan Turing, considerado o pai da computação moderna, narra a tensa corrida contra o tempo de Turing e sua brilhante equipe no projeto Ultra para decifrar os códigos de guerra nazistas e contribuir para o final do conflito.

## Referências

FONSECA, M. O; *et al.* Monitoração do Desempenho de Redes de Automação usando SNMP. **Tecnologia em Metalurgia e Materiais**, São Paulo, v. 3, n.1, p. 1-6, jul./set. 2006. Disponível em: <https://tecnologiammm.com.br/article/10.4322/tmm.00301001/pdf/1573492069-3-1-1.pdf>. Acesso em: 04 abr. 2024.

KUROSE, J. F. **Redes de computadores e a internet**: uma abordagem top-down. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

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

SOUZA, D. C.; *et al.* **Gerenciamento de redes de computadores**. Porto Alegre: Sagah, 2021.

TANEMBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

VALENTIM, R. A. M.; *et al.* Análise de Desempenho em Redes IEEE 802.3 Aplicado para Sistema de Tempo Real. **Holos**, Natal, v. 27, n. 3, 2011. Disponível em: <https://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/520> . Acesso em: 4 abr. 2024.

## Aula 2

Protocolo IPv4: Conceitos e Divisão de Endereços IP

## Protocolo IPv4: conceitos e divisão de endereços IP



### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

### Ponto de Partida

Olá, estudante!

O protocolo de internet versão 4 (IPv4) é amplamente utilizado para rotear dados na internet e redes locais, atribuindo endereços IP a dispositivos e encaminhando pacotes de dados entre eles. Um endereço IPv4 consiste em 32 bits e é representado em notação decimal separada por pontos (por exemplo, 192.168.1.1). Essa é a forma de representação amigável para leitura humana; contudo, internamente, os dispositivos o usam em sua forma binária. Os endereços IPv4 são divididos em classes (A, B, C, D e E) com base no número inicial da primeira oitava. As máscaras de sub-rede são usadas para dividir a parte de rede e a parte do host de um endereço IP.

Além disso, existem endereços IP públicos e privados, sendo os últimos reservados para redes privadas e não roteáveis na internet. Há também endereços especiais, como o de *loopback* (127.0.0.1), usado para testar a pilha de protocolos. No entanto, o conceito de classes está em desuso em favor do uso de máscaras de sub-rede variáveis. Como a transição para o IPv6, que oferece um espaço de endereçamento muito maior, afetou a utilização do IPv4 e as considerações relacionadas à atribuição de endereços IP?

Um pacote IPv4 é uma unidade de dados utilizada para transmitir informações na internet e em redes locais que empregam o protocolo de internet versão 4 (IPv4). Cada pacote contém informações cruciais para o roteamento e entrega de dados entre dispositivos na rede. O cabeçalho IPv4, uma parte essencial de um pacote, possui vários campos, incluindo versão, comprimento do cabeçalho, tipo de serviço, comprimento total, identificação, *flags*, offset de fragmento, tempo de vida, protocolo, *checksum* do cabeçalho, endereço IP de origem e endereço IP de destino.

Em adição, ele pode conter opções extras, como registro de rota e *timestamp*. A carga útil do pacote contém os dados reais transmitidos, como segmentos TCP ou datagramas UDP, dependendo do protocolo indicado no campo “Protocolo”. O *checksum* do pacote é usado para verificar a integridade de todo o pacote, e a fragmentação é opcional para dividir pacotes muito grandes. O encapsulamento permite adicionar cabeçalhos de protocolos de transporte adicionais, como TCP ou UDP, conforme necessário.

Como a migração para o protocolo de internet versão 6 (IPv6) impacta a estrutura e os recursos dos pacotes em comparação com o IPv4, considerando que o IPv6 foi desenvolvido para enfrentar as limitações de endereçamento do IPv4 e oferecer suporte a uma internet mais ampla e em crescimento?

Classes de endereços em redes de computadores referem-se à estrutura de alocação de endereços IP no protocolo de internet versão 4 (IPv4). Os endereços IPv4 consistem em 32 bits, divididos em quatro octetos, permitindo cerca de 4,3 bilhões de endereços IP únicos. No entanto, o esgotamento desse espaço levou à adoção do IPv6, que oferece um número praticamente infinito de endereços IP de 128 bits. As classes de endereços originalmente facilitavam a alocação de endereços, mas sua utilidade diminuiu com a introdução do CIDR (*Classless Inter-Domain Routing*), que permite alocações mais flexíveis e eficientes. As classes de endereços incluem Classe A, B, C, D (para *multicast*) e E (para fins experimentais). Como o uso eficiente de endereços IP pode ser alcançado em um mundo com uma demanda crescente por conectividade, considerando o esgotamento dos endereços IPv4 e a necessidade de transição para o IPv6?

Bons estudos!

## Vamos Começar!

### Definição e notação protocolo IPv4

O protocolo de internet versão 4 (IPv4) é o protocolo de rede mais amplamente utilizado para rotear dados pela internet e redes locais. É responsável pela atribuição de endereços IP aos equipamentos em uma rede e pelo encaminhamento de pacotes de dados entre esses dispositivos.

Nunes (2017) ressalta que devemos considerar conceitos e notações importantes relacionados ao IPv4. Um endereço IPv4 é um número de 32 bits usado para identificar exclusivamente um dispositivo em uma rede. Geralmente é representado em notação decimal separada por pontos, por exemplo, (192.168.1.1). Essa notação é a forma mais comum de representar endereços IPv4: consiste em quatro grupos de números decimais separados por pontos, variando de 0 a 255 em cada grupo.

É importante notar que, devido à escassez de endereços IPv4, muitas redes estão migrando para o IPv6, que utiliza endereços de 128 bits para oferecer um espaço de endereçamento muito

maior. No entanto, o IPv4 ainda é amplamente usado em todo o mundo. Cada endereço IPv4 é um número binário de 32 bits. O formato decimal é apenas uma representação mais amigável para a leitura humana. Internamente, os roteadores e dispositivos operam com os endereços IP em sua forma binária. Cada grupo de números na notação decimal de ponto representa um octeto de 8 bits do endereço IP. Isso significa que cada octeto varia de 0 a 255. Por exemplo, o endereço “192.168.1.1” é dividido em quatro octetos: 192, 168, 1 e 1. Os endereços IPv4 são divididos em classes, com base no número inicial da primeira oitava. Existem cinco classes principais: A, B, C, D e E, cada uma com seu próprio intervalo de endereços.

A máscara de sub-rede é usada para dividir a parte de rede e a parte do host de um endereço IP. É representada da mesma maneira que um endereço IP, por exemplo, “255.255.255.0”. A máscara é uma sequência de 32 bits, na qual os bits 1 representam a parte da rede e os bits 0 representam a parte do host. Por exemplo, uma máscara de sub-rede “255.255.255.0” (ou “prefixo /24”) indica que os primeiros 24 bits são a parte de rede, enquanto os últimos 8 bits são a parte do host.

Segundo Tanenbaum, Feamster e Wetherall (2021), endereços IP públicos usados na internet global são únicos em todo o mundo. Endereços IP privados são reservados para uso em redes privadas e não são roteáveis na internet. Isso permite que várias redes usem os mesmos endereços IP privados sem conflitos. Além dos blocos mencionados anteriormente, existem outros, como 169.254.0.0/16 (usado para configuração automática de IP) e 127.0.0.0/8 (usado para *loopback*).

O endereço de *loopback* (127.0.0.1) é usado para testar a pilha de protocolos em um dispositivo. Os pacotes enviados para este endereço são direcionados de volta para o próprio dispositivo, permitindo que os aplicativos testem suas próprias conexões de rede.

Kurose (2006) explica que as classes de endereços IP eram usadas para determinar o tamanho da parte de rede e da parte do host de um endereço. No entanto, o conceito de classes está em desuso em favor do uso de máscaras de sub-rede variáveis. Ainda assim, é útil entender as classes. Existem três blocos de endereços IP reservados para uso em redes privadas. Cada classe tem um intervalo de endereços e é destinada a um tipo específico de uso.

O endereço de broadcast é usado para enviar dados para todos os dispositivos na mesma rede. Exemplo: 192.168.1.255. Os roteadores são dispositivos que encaminham pacotes de dados entre redes. Eles usam tabelas de roteamento para determinar a rota mais adequada para encaminhar pacotes. Por exemplo, se você envia dados para o endereço de broadcast 192.168.1.255, todos os dispositivos na rede 192.168.1.0 receberão os dados.

**Siga em Frente...**

**Pacote IPv4**

De acordo com Kurose (2006), um pacote IPv4, também conhecido como datagrama IPv4, é uma unidade de dados usada para transmitir informações na internet e em redes locais que utilizam o IPv4. Cada pacote IPv4 contém informações importantes para o roteamento e entrega de dados entre equipamentos na rede.

#### Bloco 1

Version	IHL	Type of Service	Total Length
Identification			Flags
Time to Live		Protocol	Header Checksum
Source Address			
Destination Address			
Options (+ Padding)			
Data (Variable)			

#### Bloco 2

Total Length
Fragment Offset
Header Checksum
Source Address
Destination Address
Options (+ Padding)
Data (Variable)

Quadro 1 | Cabeçalho IPv4. Fonte: adaptada de Nunes (2017, [s. p.]).

seguir, os principais campos de um pacote IPv4:

- **Cabeçalho IPv4:** é a parte inicial de um pacote IPv4 e contém informações de controle e metadados. Tem um tamanho fixo de 20 bytes, mas pode ser estendido com opções adicionais que aumentam seu tamanho total.
- **Versão (4 bits):** indica a versão do protocolo (IPv4 é 4).
- **Comprimento do cabeçalho (4 bits):** indica o tamanho do cabeçalho em palavras de 32 bits. Geralmente, seu valor é 5, indicando 20 bytes, mas pode ser maior, se houver opções no cabeçalho.
- **Tipo de serviço (8 bits):** define a qualidade de serviço, como prioridade e tratamento diferenciado.
- **Comprimento total (16 bits):** indica o tamanho total do pacote, incluindo o cabeçalho e os dados.
- **Identificação (16 bits):** identifica exclusivamente um pacote, facilitando a reordenação de pacotes em caso de fragmentação.
- **Flags (3 bits):** usados para controlar a fragmentação de pacotes.

- **Offset de fragmento (13 bits)**: indica a posição do fragmento dentro do pacote original.
- **Tempo de vida (TTL – 8 bits)**: representa o número máximo de saltos (*hops*) que o pacote pode fazer antes de ser descartado.
- **Protocolo (8 bits)**: indica o protocolo de camada superior (por exemplo, TCP, UDP) para o qual o pacote está entregando os dados.
- **Checksum do cabeçalho (16 bits)**: um valor de verificação de integridade do cabeçalho.
- **Endereço IP de origem (32 bits)**: o endereço IP do remetente.
- **Endereço IP de destino (32 bits)**: o endereço IP do destinatário.
- **Opções**: este campo é opcional, usado para incluir informações adicionais no cabeçalho, como registro de rota, *timestamp*, entre outros.

Segundo Souza *et al.* (2021), a carga útil do pacote contém os dados que estão sendo transmitidos. Isso pode ser um segmento de TCP, um datagrama UDP ou qualquer outro tipo de dados, dependendo do protocolo indicado no cabeçalho IPv4. Dois outros conceitos importantes são:

- **Fragmentação**: quando um pacote é muito grande para ser transmitido por uma rede em uma única unidade, ele pode ser fragmentado em pedaços menores. Os campos “flags” e “offset de fragmento” no cabeçalho IPv4 são usados para controlar e reconstruir os fragmentos.
- **Encapsulamento**: o pacote IPv4 pode ser encapsulado em camadas adicionais, como o cabeçalho do protocolo de controle de transmissão (TCP) ou o cabeçalho do protocolo de datagrama de usuário (UDP), dependendo do protocolo de transporte utilizado. Isso permite que os dados sejam entregues com sucesso e roteados adequadamente através da rede.

## Classes de endereços

O IPv4 é a quarta revisão do protocolo de internet; é amplamente utilizado para roteamento de pacotes de dados na internet e em redes locais. Os endereços IPv4 são compostos por 32 bits, divididos em quatro octetos, o que resulta em cerca de 4,3 bilhões de endereços IP únicos. No entanto, devido ao crescimento exponencial da Internet e das redes, o espaço de endereçamento IPv4 se esgotou, levando à adoção do IPv6, que usa endereços de 128 bits, proporcionando uma quantidade virtualmente infinita de endereços IP.

Nunes (2017) explica que, com o esgotamento dos endereços IPv4, muitas organizações usam técnicas como *Network Address Translation* (NAT) para compartilhar um único endereço IPv4 público entre vários dispositivos em uma rede privada. Além disso, a transição para o IPv6 está em andamento para garantir que haja endereços IP suficientes para suportar o crescimento contínuo da Internet. O IPv6 usa endereços muito mais longos e oferece uma capacidade de endereçamento virtualmente infinita em comparação com o IPv4.

As classes de endereços em redes de computadores, conforme definidas no Protocolo IPv4, desempenham um papel importante na estrutura e alocação de endereços IP. Elas foram originalmente criadas para facilitar a administração e a alocação de endereços IP, mas a sua utilidade diminuiu com a introdução do CIDR (*Classless Inter-Domain Routing*).

CIDR (*Classless Inter-Domain Routing*) é uma metodologia utilizada para atribuir e gerenciar endereços IP e blocos de endereços IP de maneira mais eficiente do que o método tradicional baseado em classes, que era usado antes da introdução do CIDR. Com o CIDR, os administradores de rede podem criar sub-redes personalizadas e agrupar endereços IP de forma mais flexível, levando em consideração as necessidades específicas de suas redes.

Tanembaum, Feamster e Wetherall (2021) ressaltam que a principal característica do CIDR é a substituição do antigo sistema baseado em classes (classes A, B e C) por uma notação mais flexível que inclui um endereço IP seguido por uma barra (/) e um número que indica quantos bits da parte de rede do endereço são fixos. Isso permite a criação de sub-redes de tamanhos variados. Os exemplos incluem:

- **Classe A:** os endereços IP começam com um bit 0, variando de 0.0.0.0 a 127.255.255.255. A classe A é a classe mais ampla e permite alocar muitos endereços. O primeiro octeto (8 bits) é reservado para a identificação da rede. Isso significa que existem  $2^7$  ou 128 redes classe A possíveis. Os três octetos estantes (24 bits) são usados para identificar dispositivos na rede. Isso permite cerca de 16,7 milhões de dispositivos em cada rede classe A. A classe A é frequentemente usada por organizações de grande escala devido ao grande espaço de endereço disponível.
- **Classe B:** os endereços IP começam com os dois bits 10, variando de 128.0.0.0 a 191.255.255.255. A classe B é usada para redes de tamanho intermediário. Os dois primeiros octetos (16 bits) são usados para identificar a rede. Isso permite  $2^{14}$  ou cerca de 16.000 redes classe B. Os dois últimos octetos (16 bits) são usados para identificar dispositivos na rede. Isso permite cerca de 65.000 dispositivos em cada rede classe B. A classe B é frequentemente usada por organizações de médio porte.
- **Classe C:** os endereços IP começam com os três bits 110, variando de 192.0.0.0 a 223.255.255.255. A classe C é a classe mais comum para redes pequenas e médias. Os três primeiros octetos (24 bits) são usados para identificar a rede. Isso permite  $2^{21}$  ou cerca de 2 milhões de redes classe C. O último octeto (8 bits) é usado para identificar dispositivos na rede. Isso permite 254 dispositivos em cada rede classe C. A classe C é frequentemente usada por pequenas empresas e redes residenciais.
- **Classe D:** reservada para endereços *multicast*. Eles são usados para enviar dados para grupos de dispositivos que se inscreveram em um grupo *multicast* específico. Isso é útil para streaming de vídeo, comunicações em grupo e outros aplicativos. Esses endereços não são usados para identificar redes ou dispositivos individuais.
- **Classe E:** reservada para fins experimentais. Não é usada na internet pública nem para fins de endereçamento convencional.

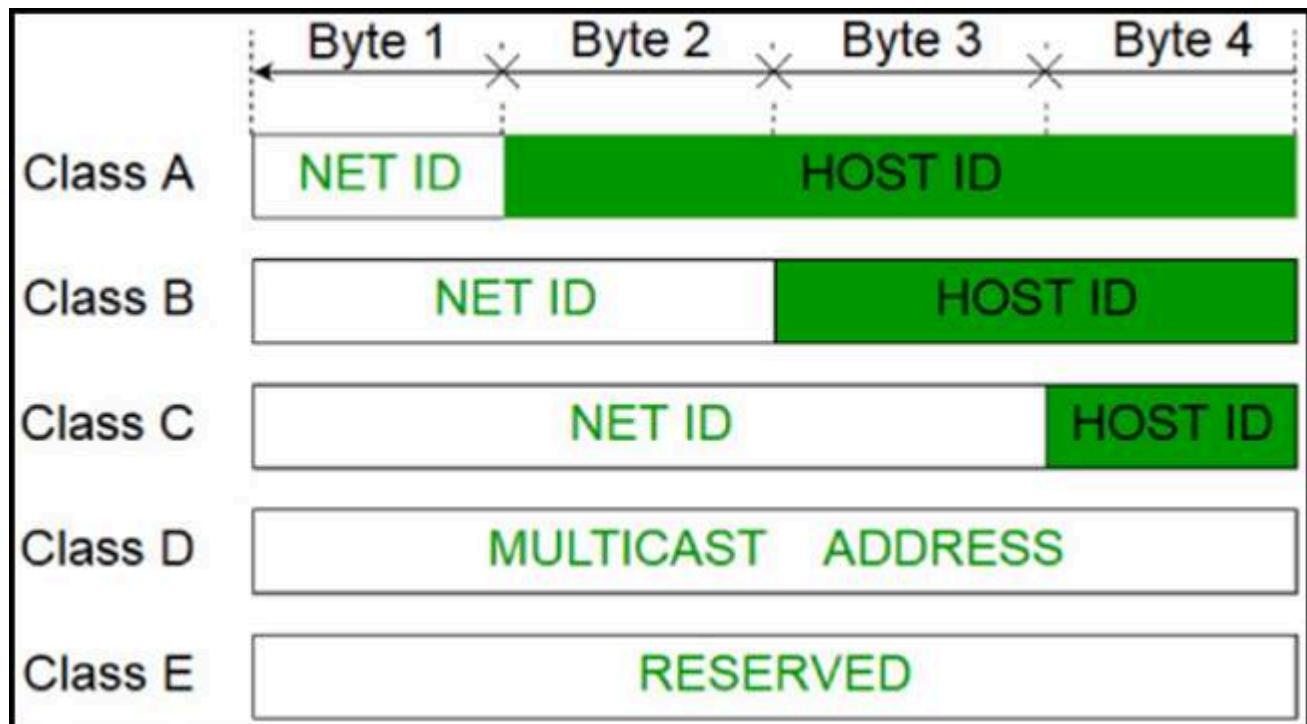


Figura 2 | Tabela de classes. Fonte: Kumar e Miglani ([s. d., s. p.]).

A utilização de classes de endereços tem limitações significativas em termos de alocação eficiente de endereços IP. Muitas vezes, as organizações não precisam de todos os endereços disponíveis em uma classe inteira, resultando em um uso ineficiente do espaço de endereçamento.

## Vamos Exercitar?

A transição para o IPv6, que oferece um espaço de endereçamento muito maior em comparação com o IPv4, impactou significativamente a utilização do IPv4 e as considerações relacionadas à atribuição de endereços IP. Com o esgotamento dos endereços IPv4 de 32 bits, tornou-se imperativo adotar o IPv6, que utiliza endereços de 128 bits, para atender às crescentes demandas da internet e suportar o crescimento exponencial de dispositivos conectados. Isso significa que, à medida que a transição para o IPv6 avança, o IPv4 gradualmente perde sua predominância.

No entanto, o IPv4 ainda é amplamente usado, e a coexistência de ambos os protocolos é uma realidade. É essencial que organizações e provedores de serviços de internet planejem e gerenciem a transição de IPv4 para IPv6 de maneira eficiente, garantindo a interoperabilidade entre os dois protocolos e a continuidade das operações de rede. Além disso, a adoção do IPv6 levanta questões sobre segurança, compatibilidade e custos associados à atualização de infraestruturas e dispositivos para acomodar o novo protocolo. Portanto, a transição para o IPv6 é uma mudança substancial que exige um planejamento cuidadoso e um acompanhamento contínuo para garantir uma transição suave e eficaz.

A migração para o IPv6 impacta a estrutura e recursos dos pacotes em comparação com o IPv4 de várias maneiras. O IPv6 utiliza endereços de 128 bits, resolvendo o problema de esgotamento de endereços do IPv4. Seu cabeçalho simplificado melhora a eficiência e o desempenho da rede, e recursos de segurança, como integridade e autenticação de pacotes, tornam a rede mais segura. O suporte aprimorado para Qualidade de Serviço (QoS) é essencial para aplicativos sensíveis à latência. O IPv6 também simplifica o uso de *multicast* e oferece suporte aprimorado para dispositivos móveis e mobilidade. Em resumo, o IPv6 é essencial para enfrentar os desafios da internet moderna, e a migração cuidadosa é crucial para aproveitar seus benefícios.

O uso eficiente de endereços IP em um mundo com crescente demanda por conectividade, com o esgotamento dos endereços IPv4 e com a necessidade de transição para o IPv6, pode ser alcançado principalmente por meio do uso de técnicas como o CIDR (*Classless Inter-Domain Routing*). O CIDR permite que os administradores de rede criem sub-redes personalizadas e aloquem endereços de forma mais flexível, levando em consideração as necessidades específicas de suas redes. Isso significa que as organizações podem utilizar apenas a quantidade necessária de endereços IP, evitando o uso ineficiente de um bloco de endereços de classe inteira. Além disso, a transição contínua para o IPv6, que oferece um vasto espaço de endereçamento, é essencial para atender à crescente demanda por endereços IP em um mundo cada vez mais conectado.

## Saiba mais

Estudante, veja a seguir, dicas de materiais de estudo complementar para seu aprendizado:

- Artigo [A governança não estatal da internet e o direito brasileiro](#), da Revista de Direito Administrativo.
- Filme: Blackhat. (Hackers, 2015). Direção: Michael Mann. Produção: Alex Garcia, Eric McLeod. Estados Unidos: Universal Studios. 2015. DVD (133 min.). Um hacker, preso por cometer crimes virtuais, é retirado da prisão para encontrar o homem que roubou seu código e invadiu o sistema interno de um grande banco americano, provocando uma série de eventos drásticos no mercado internacional de ações.

## Referências

KUMAR, M.; MIGLANI, G. Introdução de endereçamento ip classful. **Acervo Lima**, [s. d.]. Disponível em: <https://acervolima.com/introducao-de-enderecameto-ip-classful/>. Acesso em: 11 abr. 2024.

KUROSE, J. F. **Redes de computadores e a internet**: uma abordagem top-down. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

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

SOUZA, D. C.; et al. **Gerenciamento de redes de computadores**. Porto Alegre: Sagah, 2021.

SUNDFELD, C.; ROSILHO, A. A governança não estatal da internet e o direito brasileiro. **Revista de Direito Administrativo**, Rio de Janeiro, v. 270, p. 41-79, set./dez. 2015. Disponível em: <https://repositorio.fgv.br/server/api/core/bitstreams/b361d8ac-20af-4d94-bd35-abdeff9321a/content>. Acesso em 4 abr. 2024.

TANEMBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Aula 3

Protocolo IPv4: Redes e Sub-redes

### Protocolo IPv4: redes e sub-redes



#### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

## Ponto de Partida

Olá, estudante!

A divisão de uma rede em sub-redes é uma prática essencial na gestão e eficiência das redes de computadores. Isso é feito através da aplicação de máscaras de sub-rede, nas quais os bits "1" indicam a parte da rede e os bits "0" identificam os hosts. A quantidade de bits usados para identificar as sub-redes e os hosts determina o número de sub-redes criadas e o número máximo de dispositivos em cada uma. Essa segmentação melhora o tráfego, a segurança, o desempenho e a gestão da rede, permitindo a alocação eficiente de endereços IP. Roteadores são necessários para permitir a comunicação entre as sub-redes, e a documentação detalhada é crucial para

facilitar a administração da rede. Como escolher o número ideal de bits para identificar as sub-redes, considerando as necessidades específicas da rede e dos dispositivos a serem conectados?

Quanto ao cálculo da máscara de sub-rede em redes de computadores, uma vez que endereços IP podem ser representados binariamente, fica patente a importância de segmentar redes em sub-redes. O cálculo de sub-redes é exemplificado com uma rede de classe C, mostrando os passos para determinar a quantidade de sub-redes desejadas, os hosts por sub-rede e a nova máscara de sub-rede. Temos a necessidade de reservar o primeiro e o último endereço para identificação da rede e o broadcast, respectivamente. Como o cálculo de sub-redes pode ser aplicado em redes de classe A e B, e quais são as considerações específicas para essas classes?

A atribuição de endereços IP em redes de computadores é essencial, com o DHCP permitindo a alocação dinâmica de endereços IP e configurações de rede, o que simplifica a administração. Por outro lado, o NAT possibilita que vários dispositivos compartilhem um único endereço IP público para acesso à internet, substituindo os endereços IP privados dos dispositivos internos. O DHCP é amplamente utilizado em redes domésticas, empresariais, de convidados e móveis, enquanto o NAT é essencial em redes com escassez de endereços IP públicos. Como a transição para o IPv6 está impactando a necessidade e o uso do NAT em redes, e quais são os desafios e vantagens dessa mudança em termos de atribuição de endereços IP e configuração de rede?

É o que você vai aprender nesta aula, vamos lá?

Bons estudos!

## Vamos Começar!

## Divisão de uma rede em sub-redes

Segundo Kurose (2006), os endereçamentos utilizados nas redes foram divididos em classes para utilização de acordo com o número de dispositivos, conforme é possível observar a seguir.

### Bloco 1

	8 bits	8 bits	8 bits
Classe A	NET	HOST	HOST
Classe B	NET	NET	HOST
Classe C	NET	NET	NET
Classe D	Classe reservada para endereços de multicast		
Classe E	Classe reservada para pesquisa		

**Bloco 2**

8 bits	Intervalo
HOST	0 – 127
HOST	128 – 191
HOST	192 - 223
Classe reservada para endereços de multicast	
Classe reservada para pesquisa	

Quadro 1 | Classes de endereço IP. Fonte: adaptada de Kurose (2006, [s. p.]).

Para melhorar a gestão e a eficiência das redes, é comum dividir uma rede em sub-redes (ou *subnets*). Essa divisão é feita por meio da aplicação de máscaras de sub-rede e está relacionada à arquitetura e tecnologias de redes.

**1. Máscaras de sub-rede:**

As máscaras de sub-rede são um componente fundamental na divisão de uma rede. Elas são compostas por uma sequência de bits, na qual os bits “1” indicam a parte da rede, e os bits “0” indicam a parte do host.

Uma máscara de sub-rede é geralmente representada em formato de notação decimal, como “255.255.255.0”, que, em binário, seria “11111111.11111111.11111111.00000000”. Isso significa que os primeiros 24 bits são dedicados à identificação da rede e os últimos 8 bits são para identificar hosts.

**2. Divisão de rede em sub-redes:**

Para dividir uma rede em sub-redes, você precisa escolher quantos bits da máscara de sub-rede serão usados para identificar as sub-redes e quantos bits serão deixados para identificar os hosts.

Suponha que você tenha a rede 192.168.1.0 com uma máscara de sub-rede 255.255.255.0 (24 bits para a rede e 8 bits para o host). Se você deseja dividir essa rede em quatro sub-redes, você precisa adicionar 2 bits para identificar as sub-redes, resultando em uma nova máscara de sub-rede 255.255.255.192 (ou /26 em notação CIDR). Isso significa que você terá 6 bits para identificar hosts em cada sub-rede.

**3. Exemplos de divisão de rede em sub-redes:**

**Exemplo 1:** divisão da rede 192.168.1.0/24 em duas sub-redes.

**Máscara de sub-rede original:** 255.255.255.0 (ou /24).

**Nova máscara de sub-rede:** 255.255.255.128 (ou /25).

**Duas sub-redes resultantes:** 192.168.1.0/25 e 192.168.1.128/25.

**Exemplo 2:** divisão da rede 10.0.0.0/16 em quatro sub-redes.

**Máscara de sub-rede original:** 255.255.0.0 (ou /16).

**Nova máscara de sub-rede:** 255.255.192.0 (ou /18).

**Quatro sub-redes resultantes:** 10.0.0.0/18, 10.0.64.0/18, 10.0.128.0/18 e 10.0.192.0/18.

## 4. Usos de sub-redes:

A divisão de redes em sub-redes é útil para segmentar o tráfego, melhorar a segurança, otimizar o desempenho e facilitar a gestão da rede. Permite também alocar endereços IP de forma mais eficiente e designar sub-redes para diferentes departamentos, equipes ou finalidades.

## 5. Escolhendo o número de bits para a sub-rede:

A escolha do número de bits para identificar as sub-redes afeta diretamente a quantidade de sub-redes que podem ser criadas e o número de hosts em cada sub-rede. Para determinar o número de bits a serem usados, você pode usar a fórmula  $2^x$ , sendo "x" é o número de bits adicionais. Por exemplo, se você adiciona 2 bits, pode criar  $2^2 = 4$  sub-redes.

**Exemplo 3:** divisão da rede 192.168.1.0/24 em quatro sub-redes.

**Máscara de sub-rede original:** 255.255.255.0 (ou /24).

**Nova máscara de sub-rede:** 255.255.255.192 (ou /26).

**Quatro sub-redes resultantes:** 192.168.1.0/26, 192.168.1.64/26, 192.168.1.128/26 e 192.168.1.192/26.

## 6. Número de hosts em cada sub-rede:

A quantidade de bits reservados para identificar os hosts em uma sub-rede determina o número máximo de dispositivos que podem ser conectados a ela. Em geral, o número de hosts em uma sub-rede é  $2^n - 2$ , sendo "n" é o número de bits usados para identificar os hosts. A subtração de 2 ocorre porque o endereço de rede (todos os bits de host iguais a 0) e o endereço de broadcast (todos os bits de host iguais a 1) não podem ser atribuídos a dispositivos.

**Exemplo 4:** se uma sub-rede usa uma máscara de sub-rede /27 ( $32 - 27 = 5$  bits para hosts), pode ter até  $2^5 - 2 = 30$  hosts.

## 7. Roteamento entre sub-redes:

Para que as sub-redes se comuniquem entre si, você precisará de um roteador. O roteador age como um *gateway* entre as sub-redes, encaminhando o tráfego entre elas. Para isso, o roteador deve ter interfaces em cada sub-rede, cada uma configurada com um endereço IP pertencente à respectiva sub-rede.

## 8. Documentação e gerenciamento:

Ao dividir uma rede em sub-redes, é fundamental manter documentação detalhada sobre a configuração, alocando faixas de endereços IP, máscaras de sub-rede, roteadores, e outras informações pertinentes. Isso facilita a gestão da rede e a resolução de problemas.

## Cálculo da máscara de sub-rede

A contagem dos números IP vai de 0 a 255, podendo se representar pelos valores: 128, 64, 32, 16, 8, 4, 2, e 1. Se efetuarmos a soma desses valores, teremos 255; ou seja, é possível representar qualquer endereço de rede binariamente, no intervalo de 0 a 255. Para efetuar a conversão, é necessário fazer a somatória dos bits ligados nos valores que se desejam representar. Observe o exemplo a seguir, em que o endereço 192.168.0.22 foi convertido em binário.

Bloco 1

	128	64	32
192	1	1	0
168	1	0	1
0	0	0	0
22	0	0	0

Bloco 2

16	8	4	2
0	0	0	0
0	1	0	0
0	0	0	0
1	0	1	1

Bloco 3

1
0
0
0
0

Quadro 2 | Conversão para binário. Fonte: adaptado de Nunes (2017, [s. p.]).

No primeiro octeto, foram ligados apenas os números 128 e 64, resultando em 192, que é a primeira parte do endereço IP. Portanto, é possível representar todos os endereços utilizados nas redes de computadores baseadas em IPv4. Dessa forma, o endereço IP 192.168.0.22 pode ser representado em binário como: 11000000.10101000.00000000.00010110.

# REDES DE COMPUTADORES

Segundo Tanenbaum, Feamster e Wetherall (2021), também conhecida como *subnet*, essa técnica permite a segmentação de uma rede em diversas sub-redes, que podem ser isoladas das demais ou não. Isso permite que o administrador dentro de uma faixa de IP possa ter:

- **Redução do tráfego de rede**, pois os nodos dentro das sub-redes fazem domínio de broadcast, mensagens enviadas para todos os nodos da rede.
- **Simplificação no gerenciamento da rede**, pois facilita-se a identificação de falhas pelo mapeamento do endereço da sub-rede.
- **Controle dos recursos da rede**, pois possibilita-se “enxergar” uma grande rede, como diversas LANs isoladas.

Em diversas empresas, é necessário dividir alguns setores em financeiro, recursos humanos, tecnologia da informação, entre outros. As motivações podem estar ligadas à segurança, ao controle ou ao gerenciamento. O intuito de desenvolver redes em sub-redes pode estar na necessidade de alocação de mais recursos, para garantir que os serviços prioritários fiquem disponíveis. Exemplo: isolar em uma sub-rede uma impressora utilizada por todos os departamentos permite que o usuário não enfrente filas de impressão, aumentando, assim, a disponibilidade do recurso na rede.

Para calcular as sub-redes, vamos tomar de exemplo uma rede de classe C, em que a faixa de IP utilizada deve ser 192.168.0.0; e a máscara padrão, 255.255.255.0, sendo desejado fazer quatro sub-redes. Para isso, Tanembaum, Feamster e Wetherall (2021) definem os seguintes passos:

**1. Faça a conversão da máscara de rede para binário:** 255.255.255.0 ☐  
11111111.11111111.11111111.00000000.

**2. Efetue o cálculo da quantidade de hosts possível em cada uma das sub-redes**, em que “n” é o número de bits necessário para determinar:

- **Rede:**  $2^n = 2^2 = 4$ ; ou seja, para fazer quatro sub-redes, será necessário “tomar emprestados” dois bits da máscara de rede.
- **Hosts por sub-rede:**  $2^n = 2^6 = 64$ ; ou seja, cada sub-rede poderá utilizar 64 endereços. Você deve estar se perguntando: por que  $2^6$ ? De onde surgiu o 6? Lembre-se de que para converter os octetos, são utilizados os valores 128, 64, 32, 16, 8, 4, 2, 1; portanto, se, para determinar o número de redes, foram emprestados 2 bits, então sobraram 6 bits para determinar o número de hosts.

**3. Construa a tabela de sub-redes.** Vale aqui ressaltar que, dentro da faixa de uma sub-rede, o primeiro endereço não deve ser utilizado, pois é reservado para identificação da rede, e o último é utilizado para broadcast.

Rede	1º IP Válido	Último IP Válido	Broadcast
192.168.0.0	192.168.0 .1	192.168.0 .62	192.168.0 .63

192.168.0.64	192.168.0 .65	192.168.0 .126	192.168.0 .127
192.168.0.128	192.168.0 .129	192.168.0 .190	192.168.0 .191
192.168.0.192	192.168.0 .193	192.168.0 .254	192.168.0 .255

Quadro 3 | Tabelas de sub-redes. Fonte: adaptada de Nunes (2017, [s. p.]).

Nesse exemplo, repare na primeira linha: o endereço de rede atribuído foi 192.168.0.0; já na segunda rede, foi utilizado o 192.168.0.64. Dessa forma, o endereço de Broadcast da primeira rede tem que ser um anterior ao endereço de rede da segunda linha, isto é, 192.168.0.63. Os IPs válidos, ou seja, os que podem ser utilizados nos dispositivos, estão entre o intervalo dos endereços de rede e de broadcast.

**4. Determine a nova máscara de rede;** para determinar o número de rede, foi necessário “tomar emprestados” dois bits da máscara. Dessa forma, se a máscara padrão convertida no passo 1 foi 11111111.11111111.11111111.00000000, ao tomarmos emprestados 2 bits, temos que:

#### Bloco 1

128	64	32	16
1	1	0	0

#### Bloco 2

8	4	2	1
0	0	0	0

Quadro 4 | Conversão de máscara. Fonte: adaptada de Nunes (2017, [s. p.]).

Com a soma dos bits ligados, teremos  $128 + 64 = 192$ . Portanto, na nova máscara de sub-rede que vai permitir segmentar a rede em quatro partes, deve ser utilizado o número 255.255.255.192. Em binário, poderíamos representá-lo por: 11111111.11111111.11111111.11000000 (contando-se os bits ligados, tem-se 26 bits). Com base nessa representação, é possível expressar um endereço e a sua respectiva máscara, por exemplo: 192.168.0.1/26. Ou seja, são representados o endereço IP 192.168.0.1 utilizado para identificar um dispositivo e a sua respectiva máscara de rede 255.255.255.192. Para utilizar essa técnica para desenvolvimento de sub-redes nas classes A e B, deve-se seguir o mesmo conceito apresentado para a classe C.

Siga em Frente...

## Atribuição de endereço IP: DHCP e NAT

A atribuição de endereços IP é uma parte fundamental da configuração de redes de computadores. Existem duas tecnologias-chave que desempenham papéis importantes nesse processo: DHCP (*Dynamic Host Configuration Protocol*) e NAT (*Network Address Translation*).

### DHCP (*Dynamic Host Configuration Protocol*):

O DHCP é um protocolo usado para atribuir dinamicamente endereços IP e outras informações de configuração de rede, como máscara de sub-rede, gateway padrão e servidores DNS, aos dispositivos em uma rede. Isso simplifica a administração de redes, permitindo que os dispositivos obtenham suas configurações de rede automaticamente, em vez de demandar a configuração manual de cada dispositivo individualmente.

Quando um dispositivo for conectado à rede, ele normalmente inicia um processo de solicitação de endereço IP. O dispositivo envia uma solicitação de DHCP para um servidor DHCP na rede local. O servidor DHCP recebe a solicitação, verifica o pool de endereços IP disponíveis e atribui um ao dispositivo. Além do endereço IP, o servidor DHCP também pode fornecer informações adicionais, como máscara de sub-rede, gateway padrão e servidores DNS. O dispositivo aceita as informações de configuração fornecidas pelo servidor DHCP e configura automaticamente sua interface de rede.

Suponha que você tenha uma rede local com vários dispositivos, incluindo computadores, smartphones e impressoras. Você configura um servidor DHCP na rede para atribuir endereços IP automaticamente. Quando um novo dispositivo se conecta à rede, ele solicita um endereço IP ao servidor DHCP, que o fornece juntamente com outras informações de configuração necessárias.

O servidor DHCP é um componente essencial no processo. Ele pode ser um roteador, um servidor dedicado ou até mesmo um dispositivo integrado a um roteador doméstico. O servidor DHCP mantém um pool de endereços IP disponíveis para atribuição. Quando um dispositivo solicita um endereço IP, o servidor verifica se há um endereço livre no pool. O servidor DHCP pode atribuir configurações específicas para dispositivos com base em seus endereços MAC (chamado de reserva DHCP) ou em critérios específicos definidos pelo administrador. As mensagens DHCP incluem quatro etapas: descoberta, oferta, solicitação e confirmação. Essas etapas permitem que o dispositivo cliente negocie a atribuição de endereço IP com o servidor DHCP.

Cenários de uso do DHCP:

- **Redes domésticas:** o DHCP é comumente usado em roteadores domésticos para atribuir endereços IP a dispositivos conectados à rede Wi-Fi ou com fio.
- **Redes empresariais:** em redes corporativas, o DHCP é usado para fornecer configurações de rede apropriadas a dispositivos, como computadores, telefones IP e dispositivos IoT.
- **Redes de convidados:** empresas e hotéis frequentemente usam o DHCP para atribuir temporariamente endereços IP aos dispositivos dos visitantes.
- **Redes móveis:** operadoras de telefonia móvel usam o DHCP para atribuir endereços IP a dispositivos móveis quando se conectam à rede 3G, 4G ou 5G.

## NAT (*Network Address Translation*):

O NAT é uma tecnologia que permite que muitos dispositivos em uma rede local compartilhem um único endereço IP público para se comunicar com a internet. Isso é particularmente útil quando você tem uma rede doméstica ou empresarial com vários dispositivos internos, mas apenas um endereço IP público fornecido pelo provedor de internet.

Dispositivos internos, como computadores, usam endereços IP privados dentro da rede local. Um dispositivo conhecido como um roteador NAT está conectado entre a rede local e a internet. Quando um dispositivo interno envia uma solicitação para a internet, o roteador NAT substitui o endereço IP privado do dispositivo pelo endereço IP público do roteador. O roteador mantém uma tabela de tradução que rastreia as conexões para garantir que as respostas da internet sejam enviadas de volta para o dispositivo interno correto.

Imagine uma rede doméstica com vários dispositivos, como laptops, tablets e smartphones. A rede tem um único endereço IP público fornecido pelo provedor de internet. O roteador NAT permite que todos esses dispositivos compartilhem o mesmo endereço IP público para acessar a internet. O NAT traduz os endereços IP privados dos dispositivos internos em um único endereço IP público, tornando possível para eles acessar a internet e receber respostas de volta.

O roteador NAT age como intermediário entre a rede local e a internet. Ele possui uma interface interna com um endereço IP privado e uma interface externa com um endereço IP público. Quando um dispositivo interno inicia uma solicitação para a Internet, o roteador NAT modifica o endereço de origem da solicitação, substituindo o endereço IP privado pelo seu endereço IP público. O roteador mantém uma tabela de tradução que rastreia as conexões. Quando a resposta da solicitação chega, o roteador reverte a tradução, encaminhando a resposta para o dispositivo interno correto. O NAT pode ser estático (uma tradução fixa para um dispositivo específico) ou dinâmico (mapeamento de portas) para permitir que múltiplos dispositivos compartilhem o mesmo endereço IP público usando portas diferentes.

Cenários de uso de NAT:

- **Redes domésticas:** roteadores residenciais usam NAT para permitir que vários dispositivos, como computadores, consoles de jogos e smartphones, compartilhem uma única conexão

de internet.

- **Redes empresariais:** NAT é usado para permitir que dispositivos internos acessem a internet através de um único endereço IP público.
- **Redes IPv4 esgotadas:** com o esgotamento de endereços IPv4, o NAT se tornou uma solução temporária para permitir que muitos dispositivos compartilhem um número limitado de endereços IP públicos.
- **Segurança de rede:** o NAT age como um firewall “ocultando” os endereços IP internos da rede e dificultando que dispositivos externos acessem diretamente dispositivos internos não solicitados.
- **IPv6:** vale ressaltar que, com a adoção crescente do IPv6, o qual oferece um espaço de endereço muito mais amplo, a necessidade de NAT está diminuindo em redes IPv6, já que cada dispositivo pode ter seu próprio endereço IP público. Isso simplifica a configuração de rede e elimina algumas das limitações do NAT. No entanto, o NAT ainda é amplamente usado em redes IPv4 devido à escassez de endereços IPv4 públicos.

## Vamos Exercitar?

A escolha do número ideal de bits para identificar as sub-redes é um aspecto crucial na divisão de uma rede em sub-redes. Para determinar o número de bits a serem usados, você deve considerar as necessidades específicas da rede e dos dispositivos a serem conectados. Isso envolve avaliar o tamanho da rede, a quantidade de sub-redes necessárias e o número máximo de dispositivos em cada sub-rede. Além disso, é importante levar em conta as futuras expansões da rede, para garantir que a escolha seja escalável. Portanto, a resposta a esse questionamento depende das características e requisitos individuais de cada rede, e é uma decisão estratégica que requer análise cuidadosa.

Para aplicar o cálculo de sub-redes em redes de classe A e B, o processo é semelhante ao explicado para a classe C. No entanto, há algumas considerações específicas para essas classes:

- **Classe A** (por exemplo, 10.0.0.0):  
A máscara padrão para a classe A é 255.0.0.0.  
O cálculo das sub-redes em classe A envolve a “tomada emprestada” de bits dos octetos do endereço IP, da esquerda para a direita.  
Você pode usar a mesma lógica de calcular a quantidade de bits necessários para representar o número de sub-redes desejado e o número de hosts por sub-rede.
- **Classe B** (por exemplo, 172.16.0.0):  
A máscara padrão para a classe B é 255.255.0.0.  
O processo de cálculo de sub-redes em classe B segue princípios semelhantes, mas você “empresta” bits do primeiro e segundo octetos do endereço IP.

Para aplicar o cálculo de sub-redes em classes A e B, você deve considerar quantos bits são necessários para representar as sub-redes desejadas e quantos bits são deixados para os hosts em cada sub-rede, seguindo a mesma lógica de “tomar emprestado” bits dos octetos da máscara

padrão. A nova máscara de sub-rede resultante será determinada com base na quantidade de bits emprestados.

A transição para o IPv6 está reduzindo a necessidade do uso do NAT em redes, uma vez que o IPv6 oferece um amplo espaço de endereçamento. Ele permite que cada dispositivo tenha um endereço IP público exclusivo. Isso simplifica a atribuição de endereços e a configuração de rede, eliminando a escassez de endereços IPv4 públicos que levou ao uso extensivo do NAT. No entanto, a migração para o IPv6 apresenta desafios, como a necessidade de atualizar infraestruturas de rede e garantir a compatibilidade com sistemas legados, tornando a coexistência de IPv6 e IPv4 comuns durante a transição.

## Saiba mais

A segmentação de redes em sub-redes é crucial para a gestão eficiente de redes de computadores, com máscaras de sub-rede dividindo a rede em partes e melhorando tráfego e segurança. A escolha do número de bits depende das necessidades da rede. O cálculo de máscaras é exemplificado em redes de classe C e se aplica a classes A e B. A atribuição de endereços IP é essencial, com DHCP para alocação dinâmica e NAT para compartilhar um único IP público. A transição para o IPv6 afeta a necessidade e uso do NAT, com desafios e vantagens em termos de atribuição de endereços IP e configuração de rede. A seguir, algumas dicas de materiais de estudo complementar para seu aprendizado:

- Artigo [Aplicação de melhores práticas de gestão e segurança para monitoração de ativos de infraestrutura](#), da Revista Ibérica de Sistemas e Tecnologias de Informação.
- Artigo [Monitoramento residencial utilizando o Zabbix e o padrão IEEE 802.15.4](#), da revista Holos.
- Filme: The Girl with the Dragon Tattoo. (Millennium: Os Homens que Não Amavam as Mulheres). Direção: David Fincher. Produção: Michael Lynton e Amy Pascal. Estados Unidos: Sony Pictures Entertainment. 2011. DVD (158 min.). O difamado jornalista Mikael Blomkvist (Daniel Craig) aceita o convite para investigar um assassinato de 40 anos atrás não solucionado, a pedido do tio da vítima, o industrial sueco Henrik Vanger (Christopher Plummer). Enquanto isso, a hacker tatuada Lisbeth Salander (Rooney Mara) é contratada para investigar Blomkvist e descobre a verdade por trás da conspiração que levou o jornalista a cair em desgraça. Unidos pelo destino, a dupla improvável descobre uma história secreta de assassinato e abuso sexual que compromete o passado da família Vanger, enquanto eles se aproximam de um mal silencioso que espera para engolir ambos.

## Referências

KUROSE, J. F. **Redes de computadores e a internet**: uma abordagem top-down. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

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

OLIVEIRA, F. B.; *et al.* Aplicação de melhores práticas de gestão e segurança para monitoração de ativos de infraestrutura. **Revista Ibérica de Sistemas e Tecnologias de Informação**, Lousada, ed. 62, 2023.

ROMEIRO, W; COSTA, F. Monitoramento residencial utilizando o Zabbix e o padrão IEEE 802.15.4. **Holos**, Natal, v. 32, n. 1, 2016. Disponível em:  
<https://www2.ifrn.edu.br/ojs/index.php/HOTOS/article/view/2439>. Acesso em: 4 abr. 2024.

SOUZA, D. C.; *et al.* **Gerenciamento de redes de computadores**. Porto Alegre: Sagah, 2021.

TANEMBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Aula 4

Protocolo IPv6

### Protocolo IPv6



#### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

### Ponto de Partida

Olá, estudante!

O IPv6 (*Internet Protocol Version 6*) é a próxima geração do protocolo de internet (IP), destinado a substituir o IPv4. Enquanto o IPv4 utiliza endereços de 32 bits e dá suporte a aproximadamente 4,3 bilhões de endereços, o IPv6 utiliza endereços de 128 bits, o que fornece um espaço de endereço substancialmente maior, permitindo um número virtualmente ilimitado de dispositivos

conectados à internet. IPv6 foi projetado para resolver vários dos problemas associados ao esgotamento dos endereços IPv4 e para fornecer uma série de melhorias em relação a seu predecessor. Como as redes e os provedores de internet estão lidando com a coexistência do IPv6 e IPv4 e quais são os desafios enfrentados durante esse período de transição?

O cabeçalho IPv6 é a parte essencial de um pacote de dados que contém informações necessárias para roteamento e entrega de pacotes. É mais simplificado em comparação com o IPv4, melhorando a eficiência e velocidade de processamento nos roteadores. O cabeçalho IPv6 inclui campos como versão, classe de tráfego, identificação de fluxo, tamanho dos dados do *payload*, próximo cabeçalho, limite de saltos, endereço IP de origem e endereço IP de destino.

A simplificação do cabeçalho no IPv6 é notável, pois utiliza apenas oito campos, em comparação com os 14 do IPv4. Além disso, veremos os diferentes tipos de endereços IPv6, como *unicast* (incluindo o endereço global público, endereço local de ligação e endereço local exclusivo), *multicast*, *anycast*, *loopback* e endereços usados durante a transição do IPv4 para o IPv6. Como a simplificação do cabeçalho e os diversos tipos de endereços do IPv6 afetam diretamente a eficiência, escalabilidade e capacidade de suportar a expansão da internet e a crescente diversidade de dispositivos conectados?

No contexto da coexistência e interoperabilidade entre os protocolos IPv4 e IPv6, várias técnicas de transição desempenham um papel fundamental. A técnica *Dual Stack* permite que dispositivos operem simultaneamente com IPv4 e IPv6. O tunelamento encapsula pacotes IPv6 em pacotes IPv4 (ou vice-versa) para permitir a comunicação entre dispositivos não nativamente compatíveis. O NAT64 traduz endereços IPv6 para IPv4 para facilitar a comunicação, a tradução de protocolo converte pacotes entre IPv4 e IPv6, e o DS-Lite é útil para ISPs que desejam migrar para IPv6. Essas técnicas facilitam a coexistência entre protocolos e garantem uma transição suave. No entanto, surge a questão da persistente dependência do NAT em redes IPv4 devido à escassez de endereços IPv4 públicos, o que pode afetar a transição. Como superar esse obstáculo de forma eficaz no processo de adoção do IPv6?

Bons estudos!

## Vamos Começar!

### Introdução ao protocolo IPv6: definição e objetivos

Tanenbaum, Feamster e Wetherall (2021) explicam que o IPv6 (*Internet Protocol Version 6*) é a próxima geração do protocolo de internet (IP), destinado a substituir o IPv4. Enquanto o IPv4 utiliza endereços de 32 bits e dá suporte a aproximadamente 4,3 bilhões de endereços, o IPv6 utiliza endereços de 128 bits, o que fornece um espaço de endereço substancialmente maior, permitindo um número virtualmente ilimitado de dispositivos conectados à internet. IPv6 foi projetado para resolver vários dos problemas associados ao esgotamento dos endereços IPv4 e para fornecer uma série de melhorias em relação a seu predecessor.

Inicialmente, o IPv6 surge no cenário de redes de computadores para suprir as necessidades do IPv4. Segundo Tanembaum, Feamster e Wetherall (2021), o novo protocolo deve:

- Resolver a escassez de endereços.
- Simplificar o cabeçalho, facilitando o processamento dos pacotes e o aumento da velocidade do envio/recebimento.
- Tornar opcionais os campos obrigatórios do cabeçalho, facilitando, assim, o roteamento dos pacotes.
- Garantir a segurança das transmissões, tornando o IPsec obrigatório.

Quando os engenheiros se reuniram para o desenvolvimento do novo protocolo, chamado de IPng (*Internet Protocol Next Generation* – protocolo de internet da nova geração), as suas características foram definidas por meio das RFCs.

- **RFC 2460:** especificações do IPv6 (12/1998).
- **RFC 2461:** especificações de descoberta de vizinhos IPv6 (*Neighbor Discovery IPv6*).
- **RFC 4291:** definição da estrutura do IPv6 (01/2006).
- **RFC 4443:** especificações do ICMPv6 (*Internet Control Message Protocol*).

O endereçamento do protocolo IPv6 possui 128 bits (o IPv4 possui apenas 32 bits), o que possibilita  $2^{128}$  endereços possíveis, ou ainda 340 undecilhões. O seu formato é dividido em oito grupos com quatro dígitos hexadecimais, conforme pode ser observado:

8000:0000:0010:0000:0123:4567:89AB:CDEF (o IPv4 é dividido em quatro grupos com 8 bits cada, ex.: 192.168.0.100). Segundo Kurose (2006), os protocolos possuem diferenças entre as duas versões, conforme se observa no Quadro 1 a seguir.

Versão / Itens	IPv4	IPv6
Quantidade de endereços	$2^{32}$	$2^{128}$
Quantidade de campos	14	8
MTU mínimo	576 bytes	1.280 bytes
Representação do endereço	4 Grupos com 8 bits	8 Grupos com 16 bits
Tamanho do endereço (bits)	32	128
Roteamento	Tabela de roteamento grande	Efetuado pelo cabeçalho de extensão
Segurança	IPSec facultativo	IPSec obrigatório
Qualidade de serviço (QoS)	Sem garantia	Através dos campos, classe de tráfego e identificação de Fluxo
Cabeçalho	Uso do checksum	Mais simplificado

Quadro 1 | Diferenças entre IPv4 e IPv6. Fonte: adaptada de Nunes (2017, [s. p.]).

Segundo Souza *et al.* (2021), IPv6 e IPv4 vão coexistir por muitos anos. Esse cenário gerou um novo problema, pois não é possível “abandonar” o protocolo IPv4 e começar a utilizar somente o protocolo IPv6. Tanenbaum, Feamster e Wetherall (2021) explicam que, nesse longo período de transição, os administradores de redes e os provedores de internet preveem a possibilidade de alguns impactos nas redes, o que demanda algumas medidas:

- **Gerenciamento de falhas:** os administradores devem efetuar um plano de contingência para que as redes continuem operando com o IPv4 e IPv6.
- **Gerenciamento de contabilização:** devem-se recalcular os limites de utilização dos recursos, pois, com os dois protocolos em operação, o consumo muda em relação às redes somente com IPv4.
- **Gerenciamento de configuração:** para permitir que os dois protocolos convivam nas redes, são necessárias diversas configurações.
- **Gerenciamento de desempenho:** com a mudança de cenário (redes com os dois protocolos operando), o desempenho da rede necessita de adaptações para garantia do acordo de nível de serviço (SLA – *Service Level Agreement*).
- **Gerenciamento de segurança:** o administrador deve optar por alguma técnica que garanta a interoperabilidade sem gerar riscos à segurança da rede e/ou de usuários.

Tanenbaum, Feamster e Wetherall (2021) explicam que, em razão da necessidade do período de coexistência entre os dois protocolos, as redes podem apresentar três possíveis cenários: rede IPv4 pura, rede IPv6 pura ou rede com pilha dupla (*dual stack*). Com isso, foi necessário planejar a estratégia de migração dos protocolos para que o impacto da transição não compromettesse a qualidade dos serviços providos.

Para resolver esse problema, a IETF formou grupo de trabalho denominado IPv6 Operations, a fim de que fossem desenvolvidas algumas normas e diretrizes para redes IPv4/IPv6. Com isso, o mecanismo de pilha dupla foi normatizado na RFC 1933.

A principal diferença entre o IPv4 e o IPv6 é o tamanho do endereço. O IPv6 utiliza um formato de endereço de 128 bits, dividido em oito grupos de quatro dígitos hexadecimais. Exemplo de um endereço IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Isso permite um espaço de endereço enorme, tornando-o mais adequado para a crescente demanda de dispositivos conectados à internet.

Para facilitar a leitura de endereços IPv6, a notação abreviada é comumente usada. Pares de grupos contíguos de zeros podem ser omitidos uma vez, e os zeros iniciais em cada grupo podem ser omitidos. Por exemplo, o endereço IPv6 2001:0db8:85a3:0000:0000:8a2e:0370:7334 pode ser abreviado como 2001:db8:85a3::8a2e:370:7334.

O IPv6 define vários tipos de endereços, incluindo endereços *unicast* (um para um), *multicast* (um para muitos) e *anycast* (um para o mais próximo de muitos). Esses diferentes tipos de endereços são usados para fins específicos, como comunicação direta entre dispositivos ou broadcasting de informações para vários dispositivos.

O IPv6 simplifica a configuração de endereços em dispositivos, permitindo a autoconfiguração. Os dispositivos podem gerar automaticamente seus próprios endereços IPv6, o que simplifica a implantação e a manutenção de redes.

O IPv6 inclui recursos de segurança aprimorados em comparação com o IPv4, incluindo a capacidade de criptografar o tráfego de ponta a ponta por meio do uso de extensões de cabeçalho de autenticação e criptografia (AH e ESP).

## Objetivos do IPv6

De acordo com Souza *et al.* (2021), o objetivo principal do IPv6 é fornecer um espaço de endereço muito maior em comparação com o IPv4. Isso é fundamental devido ao esgotamento dos endereços IPv4, o que limita a capacidade de expansão da Internet.

- Com mais endereços disponíveis, o IPv6 facilita a expansão da internet, permitindo que um número crescente de dispositivos e redes seja conectado sem esgotar rapidamente os endereços disponíveis.
- A autoconfiguração no IPv6 simplifica a configuração de dispositivos, reduzindo a necessidade de configurações manuais e simplificando a implantação de redes.
- O IPv6 incorpora recursos de segurança aprimorados, como autenticação e criptografia, que podem ajudar a proteger a integridade e a confidencialidade dos dados transmitidos na internet.
- Com um espaço de endereço mais amplo e melhor escalabilidade, o IPv6 é projetado para atender às necessidades das futuras aplicações e dispositivos conectados, como a internet das coisas (IoT).

O IPv6 foi projetado para enfrentar os desafios do IPv4, fornecendo um espaço de endereço expandido, melhor escalabilidade, simplificação de configuração e maior segurança.

**Siga em Frente...**

## Cabeçalho e tipos de endereçamento IPv6

O IPv6 possui um cabeçalho e tipos de endereçamento específicos que o tornam eficaz para roteamento e entrega de dados na internet. Esse cabeçalho é a parte do pacote de dados que contém informações necessárias para o roteamento e a entrega do pacote. O cabeçalho IPv6 é mais simplificado em comparação com o IPv4, o que melhora a eficiência e a velocidade de processamento nos roteadores. O cabeçalho IPv6 contém as seguintes informações:

Segundo Nunes (2017), as especificações desenvolvidas pelos engenheiros da IETF para o IPv6 fizeram com que fosse estruturado o cabeçalho.

**Bloco 1**

Versão	Classe de Tráfego	Identificação de Fluxo
Tamanho dos Dados		Próximo Cabeçalho
Endereço IP de Origem		
Endereço IP de Destino		

**Bloco 2**

Identificação de Fluxo
Limite de Saltos
Endereço IP de Origem
Endereço IP de Destino

Quadro 2 | Estrutura do cabeçalho IPv6. Fonte: adaptada de Nunes (2017, [s. p.]).

Cada campo tem as seguintes funções:

- **Versão (4 bits)**: indica a versão do protocolo, que é sempre 6 para o IPv6.
- **Classe de tráfego (8 bits)**: especifica o tipo de serviço, como qualidade de serviço (QoS) e priorização do tráfego. Isso é usado para diferenciar diferentes tipos de tráfego na rede.
- **Identificação de fluxo (20 bits)**: usada para identificar e agrupar pacotes que pertencem ao mesmo fluxo de tráfego. Isso ajuda a entrega eficiente de pacotes relacionados.
- **Tamanho dos dados do payload (16 bits)**: indica o comprimento dos dados (*payload*) no pacote, excluindo o cabeçalho.
- **Próximo cabeçalho (8 bits)**: indica o tipo do próximo cabeçalho que segue o cabeçalho IPv6. Pode ser um cabeçalho de extensão ou o cabeçalho de transporte, como o cabeçalho TCP ou UDP.
- **Limite de saltos (8 bits)**: funciona de maneira semelhante ao campo TTL (*Time to Live*) do IPv4, mas, em vez de limitar o tempo de vida de um pacote, limita o número de saltos (rotações de roteadores) que o pacote pode fazer na rede. Isso evita loops infinitos.
- **Endereço IP origem (128 bits)**: contém o endereço IPv6 do remetente.
- **Endereço IP destino (128 bits)**: contém o endereço IPv6 do destinatário.

O cabeçalho do IPv6 foi simplificado, pois no IPv4 são utilizados 14 campos, enquanto na nova versão do protocolo são utilizados apenas oito deles.

## Tipos de endereçamento IPv6

Segundo Tanenbaum, Feamster e Wetherall (2021), o IPv6 define vários tipos de endereços para atender a diferentes necessidades na internet. Alguns dos principais incluem:

- O endereço *unicast* é destinado a um único dispositivo. É semelhante ao conceito de endereço IP exclusivo no IPv4. Existem diferentes tipos de endereços *unicast* no IPv6, incluindo *Global Unicast Address* (endereço global público), *Link-Local Address* (endereço local de ligação) e *Unique Local Address* (endereço local exclusivo).
- O endereço *multicast* é usado a fim de enviar dados para um grupo de dispositivos em uma rede. Em vez de transmitir para todos os dispositivos, os pacotes são entregues apenas aos membros do grupo *multicast*.
- O endereço *anycast* é atribuído a um grupo de dispositivos, mas os pacotes são entregues ao dispositivo mais próximo desse grupo. Isso é útil para serviços distribuídos, como servidores de DNS, em que o cliente é roteado para o servidor mais próximo.
- O endereço de *loopback* é usado para permitir que um dispositivo se comunique com ele mesmo. Em IPv6, o endereço de *loopback* é ::1.
- Endereços são usados durante a transição do IPv4 para o IPv6, permitindo que dispositivos IPv4 se comuniquem com dispositivos IPv6.
- Endereço IPv6 de Mapeamento IPv4: É usado para representar endereços IPv4 em notação IPv6. Por exemplo: FFFF:192.0.2.1 representa o endereço IPv4 192.0.2.1.

Esses tipos de endereços e o cabeçalho simplificado do IPv6 tornam o protocolo mais eficiente, escalável e adequado para suportar a expansão da internet e a crescente diversidade de dispositivos conectados.

## Coexistência e interoperabilidade: técnicas de transição

A coexistência e a interoperabilidade entre os protocolos IPv4 e IPv6 são aspectos críticos durante o período de transição para a adoção generalizada do IPv6. Isso ocorre porque, durante essa fase de transição, muitos dispositivos e redes continuarão a usar o IPv4, enquanto outros começarão a adotar o IPv6. Existem várias técnicas de transição que permitem a esses dois protocolos operar de forma conjunta.

Kurose (2006) explica que a técnica *Dual Stack* envolve a implantação de ambos os protocolos IPv4 e IPv6 em dispositivos, roteadores e redes. Isso permite que os dispositivos se comuniquem usando ambos os protocolos. Quando um dispositivo *dual-stack* se conecta a outro dispositivo com suporte a IPv6, eles usarão IPv6 para se comunicar. Da mesma forma, quando se conectam a dispositivos IPv4, usarão IPv4. Exemplo: um roteador *dual-stack* está configurado com endereços IPv4 e IPv6. Quando um dispositivo com suporte IPv6 se conecta a ele, eles se comunicam por meio do IPv6. Se um dispositivo com suporte apenas IPv4 se conectar a esse roteador, a comunicação ocorre através do IPv4.

O tunelamento envolve encapsular pacotes IPv6 em pacotes IPv4 ou vice-versa para permitir a comunicação entre dispositivos ou redes que não são nativamente compatíveis com o protocolo-alvo. Existem diferentes métodos de tunelamento, incluindo 6in4, 6to4, Teredo e ISATAP. Exemplo: se uma rede está usando IPv6, mas precisa se comunicar com uma rede que só

suporta IPv4, um túnel IPv6 para IPv4 pode ser configurado para encapsular o tráfego IPv6 e transmiti-lo sobre uma rede IPv4. Isso permite que a comunicação ocorra entre as duas redes.

O NAT64 é uma técnica que permite a dispositivos IPv6 se comunicar com dispositivos IPv4, usando uma tradução de endereços. O NAT64 traduz os endereços IPv6 em endereços IPv4, permitindo que os dispositivos IPv6 acessem recursos na internet que só têm endereços IPv4. Exemplo: se um dispositivo IPv6 deseja acessar um servidor que possui apenas um endereço IPv4, o NAT64 atua como intermediário, traduzindo as solicitações IPv6 em solicitações IPv4. Isso permite a comunicação entre dispositivos de diferentes protocolos.

O DS-Lite é uma técnica que permite a dispositivos em uma rede usar IPv6 para se comunicar com a internet; ela converte tráfego IPv4 em pacotes IPv6. Isso é útil para provedores de serviços de internet (ISPs) que desejam adotar IPv6, mas ainda têm muitos clientes usando IPv4.

Exemplo: um ISP que implementa o DS-Lite permite que seus clientes usem IPv6 para acessar a internet. Quando esses clientes acessam recursos IPv4, o DS-Lite converte automaticamente o tráfego para IPv6 e encaminha para a internet, proporcionando uma experiência de usuário transparente.

Essas técnicas de transição são cruciais para permitir a coexistência e a interoperabilidade entre os protocolos IPv4 e IPv6 durante o período de transição. Elas permitem que redes e dispositivos com diferentes níveis de suporte a IPv4 e IPv6 se comuniquem efetivamente, garantindo uma transição suave para o IPv6 à medida que o IPv4 se esgota. No entanto, o NAT ainda é amplamente usado em redes IPv4 devido à escassez de endereços IPv4 públicos.

## Vamos Exercitar?

A coexistência de IPv6 e IPv4 apresenta desafios para redes e provedores de internet, exigindo estratégias como a implementação de pilha dupla. Os desafios incluem o gerenciamento de falhas, recalibração de recursos, configurações complexas, adaptações de desempenho e garantia de segurança. É crucial planejar cuidadosamente a transição para evitar interrupções nos serviços e garantir a qualidade durante o período de coexistência. O IPv6 Operations e as normas da IETF desempenham um papel importante na facilitação desse processo.

A simplificação do cabeçalho IPv6 em relação ao IPv4, juntamente com a variedade de tipos de endereços IPv6, desempenha um papel crucial na eficiência, escalabilidade e adaptação às crescentes demandas da internet e à diversidade de dispositivos conectados. A redução de campos no cabeçalho melhora a eficiência no roteamento e processamento de dados, enquanto os tipos de endereços, como *unicast*, *multicast* e *anycast* permitem uma conectividade mais flexível, tornando o IPv6 adequado para lidar com o crescimento da internet e a diversificação de aplicativos e dispositivos.

Para superar a dependência contínua do NAT em redes IPv4 devido à escassez de endereços IPv4 públicos durante a transição para o IPv6, é crucial adotar práticas de alocação de endereços IPv4 mais eficientes, promover a migração gradual para o IPv6, fazer uso de tecnologias de

transição, como NAT64, implementar Carrier-Grade NAT (CGN) de forma estratégica, e investir em educação e conscientização para acelerar a adoção do IPv6. Essas estratégias visam lidar com os desafios associados à escassez de endereços IPv4 e facilitar uma transição suave para o IPv6, crucial para a evolução das redes de computadores.

## Saiba mais

Estudante, veja a seguir, dicas de materiais de estudo complementar para seu aprendizado:

- Artigo [\*Saúde ocupacional e ambientes de vida melhorados com recurso à Internet das Coisas\*](#), da Revista Ibérica de Sistemas e Tecnologias de Informação.
- Artigo [\*Trajetórias tecnológicas da indústria de telefonia móvel: um exame prospectivo de tecnologias emergentes\*](#), de Economia e Sociedade.
- Filme: The Social Dilemma. (O Dilema das Redes). Direção: Jeff Orlowski. Produção: Larissa Rhodes. Estados Unidos: Netflix. 2020. DVD (94 min.). Pessoas por trás do Google, Twitter, Facebook, Instagram e YouTube revelam como essas plataformas estão reprogramando a civilização, expondo o que está escondido no outro lado da tela.

## Referências

KUROSE, J. F. **Redes de computadores e a internet: uma abordagem top-down**. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

MARQUES, G.; PITARMA, R. Saúde ocupacional e ambientes de vida melhorados com recurso à Internet das Coisas. **Revista Ibérica de Sistemas e Tecnologias de Informação**, Lousada, ed. 19, 2019. Disponível em: [https://www.researchgate.net/profile/Rui-Pitarma/publication/335653524\\_Occupational\\_health\\_and\\_enhanced\\_living\\_environments\\_through\\_Internet\\_of\\_Things/links/5d72316d4585151ee4a0de81/Occupational-health-and-enhanced-living-environments-through-Internet-of-Things.pdf](https://www.researchgate.net/profile/Rui-Pitarma/publication/335653524_Occupational_health_and_enhanced_living_environments_through_Internet_of_Things/links/5d72316d4585151ee4a0de81/Occupational-health-and-enhanced-living-environments-through-Internet-of-Things.pdf). Acesso em 4 abr. 2024.

NERIS JUNIOR, C.; FUCIDJI, J. R.; GOMES, R. Trajetórias tecnológicas da indústria de telefonia móvel: um exame prospectivo de tecnologias emergentes. **Economia e Sociedade**, Campinas, v. 23, n. 2, 2014. Disponível em: <https://www.scielo.br/j/ecos/a/xLX4ZnNfTHbBTBJ9VqHLJmB>. Acesso em 4 abr. 2024.

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

SOUZA, D. C.; et al. **Gerenciamento de redes de computadores**. Porto Alegre: Sagah, 2021.

TANEMBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Aula 5

Encerramento da Unidade

### Arquitetura e tecnologias de redes



#### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

### Ponto de Chegada

Olá, estudante! A competência desta Unidade é “Detalhar as classes de endereço IP e efetuar o cálculo de sub-rede; identificar as características das redes Ethernet; refletir sobre quão importante é o protocolo de comunicação IPv6 para evolução dos serviços e aplicações nas redes e conhecer quais são as dificuldades no período de coexistência e interoperabilidade entre IPV4 e IPV6. Tais entendimentos possibilitam o cálculo e a implementação de redes divididas por faixas de endereçamento IP”. A partir dela, é possível adquirir conhecimentos sobre como utilizar serviços essenciais em redes de computadores. Para criar redes locais, é vital que você domine os conceitos fundamentais em primeiro lugar.

### Domínios de broadcast

Os domínios de broadcast são uma parte crucial das redes de computadores, sendo essenciais para a comunicação de dados em uma rede local. Eles estão relacionados aos endereços MAC, tráfego de broadcast e switches.

Endereços MAC, que são exclusivos para cada dispositivo de rede, são usados para identificar dispositivos na camada de enlace de dados do modelo OSI.

O tráfego de broadcast ocorre quando um dispositivo envia um pacote de dados para todos os outros na mesma rede, identificado pelo endereço MAC especial “ff:ff:ff:ff:ff:ff”. Isso é usado para descobrir outros dispositivos na rede ou para anunciar serviços.

*Switches* operam na camada de enlace e encaminham pacotes com base nos endereços MAC, direcionando-os apenas para a porta do dispositivo de destino, melhorando o desempenho da rede.

Domínios de broadcast são áreas em uma rede local onde todos os dispositivos recebem pacotes de broadcast. *Switches* dividem a rede em vários domínios de broadcast, enviando pacotes apenas para as portas relevantes, reduzindo o tráfego desnecessário e melhorando a eficiência.

Os domínios de broadcast são fundamentais para o projeto e manutenção de redes locais, controlando o tráfego e garantindo que as mensagens sejam direcionadas apenas para os dispositivos que precisam delas.

Além disso, endereços de broadcast são usados para enviar mensagens para todos os equipamentos de uma rede ou sub-rede, como no caso de solicitar um endereço IP ao servidor DHCP em uma rede local.

## Os domínios de colisão

Os domínios de colisão são áreas em redes de computadores em que pacotes de dados podem colidir, causando interferências e ineficiências na transmissão. Isso é especialmente relevante em redes Ethernet que utilizam o protocolo CSMA/CD. As colisões ocorrem quando dispositivos tentam transmitir dados ao mesmo tempo, interrompendo a transmissão.

Em redes Ethernet, todos os dispositivos compartilham o mesmo meio físico, e as colisões podem ocorrer quando vários dispositivos tentam transmitir simultaneamente. A segmentação em domínios de colisão menores é uma abordagem para reduzir colisões.

Atualmente, com *switches* Ethernet e tecnologias sem fio avançadas, as colisões se tornaram menos comuns em redes contemporâneas, pois os dispositivos criam domínios de colisão separados para cada porta, minimizando conflitos e melhorando o desempenho.

Os domínios de colisão são distintos dos domínios de broadcast, nos quais pacotes são enviados para todos os dispositivos na rede, enquanto os domínios de colisão lidam com a possibilidade de colisões durante a transmissão de dados. *Switches* desempenham um papel crucial na redução de colisões em redes Ethernet, tornando a transmissão mais eficiente e confiável.

## Operação, velocidades, comutação

A Ethernet é uma tecnologia amplamente utilizada em redes de computadores, operando nas camadas física e de enlace do modelo OSI. Ela oferece uma variedade de velocidades e métodos de comutação. Na camada física, a Ethernet lida com a transmissão de dados em meios físicos, como cabos de cobre e fibra óptica, enquanto na camada de enlace, ela gerencia o acesso ao meio e previne colisões. As velocidades Ethernet variam de 10 Mbps a 100 Gbps, dependendo das necessidades da rede. A comutação de *hub*, que cria um único domínio de colisão, é usada em redes antigas com *hubs*, enquanto a comutação de *switch* é amplamente empregada em redes modernas, dividindo a rede em domínios de colisão separados por porta, o que aumenta o desempenho e a eficiência da rede.

## O Protocolo de Internet versão 4 (IPv4)

O Protocolo de Internet versão 4 (IPv4) é amplamente utilizado para rotear dados em redes locais e na internet. Ele atribui endereços IP aos dispositivos e encaminha pacotes de dados entre eles. Um endereço IPv4 é um número de 32 bits representado em notação decimal separada por pontos, como “192.168.1.1”, com quatro grupos de números variando de 0 a 255. As classes de endereços IP foram usadas para determinar o tamanho das partes de rede e host, mas agora máscaras de sub-rede variáveis são mais comuns.

Endereços IP públicos são únicos globalmente, enquanto os endereços IP privados são reservados para redes privadas e não roteáveis na internet. Isso permite que várias redes usem os mesmos endereços IP privados sem conflitos. Além disso, existem endereços especiais, como 169.254.0.0/16 para configuração automática e 127.0.0.1 (*loopback*) para testar conexões de rede local.

A máscara de sub-rede divide endereços IP em partes de rede e host, representada por uma sequência de 32 bits com bits 1 para a parte da rede e bits 0 para a parte do host. Roteadores encaminham pacotes entre redes usando tabelas de roteamento, enquanto o endereço de broadcast, como 192.168.1.255, envia dados para todos os dispositivos na mesma rede.

## Um pacote IPv4

Um pacote IPv4 é uma unidade de dados usada na internet e em redes locais que usam o IPv4. O cabeçalho IPv4 contém informações cruciais para o roteamento e entrega de dados, incluindo versão, comprimento do cabeçalho, tipo de serviço, comprimento total, identificação, *flags*, offset de fragmento, tempo de vida, protocolo, *checksum* do cabeçalho, endereço IP de origem, endereço IP de destino e opções (opcional).

A carga útil do pacote contém os dados reais transmitidos, como segmentos de TCP ou datagramas UDP, dependendo do protocolo indicado no campo “Protocolo” do cabeçalho IPv4.

O *checksum* do pacote verifica a integridade de todo o pacote, incluindo cabeçalho e carga útil. A fragmentação é usada quando um pacote é muito grande para ser transmitido em uma única unidade, sendo dividido em fragmentos controlados pelos campos “Flags” e “Offset de Fragmento”.

O pacote IPv4 pode ser encapsulado em camadas adicionais, como os cabeçalhos do TCP ou UDP, de acordo com o protocolo de transporte utilizado, garantindo a entrega e o roteamento adequados dos dados pela rede.

## Classes de endereços

O IPv4 usa endereços de 32 bits, divididos em quatro octetos, totalizando cerca de 4,3 bilhões de endereços IP únicos. O esgotamento desses endereços levou à adoção do IPv6, com 128 bits, oferecendo uma quantidade virtualmente infinita de endereços. Classes de endereços IPv4, como A, B, C, eram usadas para administração, mas foram substituídas pelo CIDR, que permite a criação de sub-redes personalizadas. Exemplos das classes incluem A (para grandes organizações), B (para médias) e C (para pequenas e médias). Classes D são para *multicast*, e classe E para fins experimentais. No entanto, as classes de endereços têm limitações na alocação eficiente de endereços, levando ao uso ineficiente do espaço de endereçamento.

## Divisão de uma rede em sub-redes

A divisão de uma rede em sub-redes é um processo importante para a gestão eficiente de endereços IP. Isso é realizado por meio da aplicação de máscaras de sub-rede, nas quais os bits “1” indicam a parte da rede, e os bits “0” indicam a parte do host. A divisão em sub-redes ajuda a segmentar o tráfego, a melhorar a segurança, a otimizar o desempenho e a facilitar a gestão da rede.

Para dividir uma rede em sub-redes, é necessário escolher o número de bits a serem usados para identificar as sub-redes e os bits restantes para identificar os hosts. As máscaras de sub-rede são representadas em notação decimal, como “255.255.255.0” (ou /24 em notação CIDR). A quantidade de bits usados para identificar os hosts determina o número máximo de dispositivos em cada sub-rede.

A comunicação entre sub-redes requer um roteador, que atua como *gateway* entre elas, encaminhando o tráfego. É importante manter documentação detalhada sobre a configuração, incluindo faixas de endereços IP, máscaras de sub-rede e informações sobre roteadores, para

facilitar a gestão da rede e solucionar problemas. A escolha do número de bits para identificar as sub-redes afeta diretamente a quantidade de sub-redes criadas e o número de hosts em cada uma. Por exemplo, ao adicionar 2 bits, é possível criar 4 sub-redes.

## Cálculo da máscara de sub-rede

O cálculo da máscara de sub-rede é uma técnica fundamental para segmentar uma rede em sub-redes, permitindo uma melhor gestão e otimização dos recursos. Inicialmente, é importante entender que os números IP vão de 0 a 255 e podem ser representados como potências de 2, como 128, 64, 32, 16, 8, 4, 2 e 1, com uma soma total de 255.

A conversão de endereços IP para binário é realizada atribuindo valores de potência de 2 aos bits apropriados. Por exemplo, o endereço 192.168.0.22 é convertido em binário, de modo que o primeiro octeto (8 bits) é representado como 128 + 64, resultando em 192.

A segmentação de redes em sub-redes é útil para reduzir o tráfego de rede, simplificar a gestão, controlar recursos e aumentar a disponibilidade de serviços. Para calcular sub-redes, é necessário seguir um processo, como no exemplo de uma rede de classe C:

- Converter a máscara de rede para binário (exemplo: 255.255.255.0 ☐ 11111111.11111111.11111111.00000000).
- Calcular a quantidade de bits necessários para representar as sub-redes (usando a fórmula  $2^n$ , onde "n" é o número de bits adicionais). No exemplo, 2 bits são necessários para quatro sub-redes.
- Construir a tabela de sub-redes, na qual o primeiro e o último endereço não devem ser usados (um é reservado para identificação de rede e outro para broadcast).
- Determinar a nova máscara de rede com base nos bits adicionados (no exemplo, a máscara é 255.255.255.192 ou /26 em notação CIDR).

Essa técnica pode ser aplicada a classes A e B da mesma maneira. Ela permite criar sub-redes personalizadas para atender às necessidades específicas de alocação de recursos e gestão da rede.

## Atribuição de endereço IP: DHCP e NAT

A atribuição de endereços IP desempenha um papel essencial na configuração de redes de computadores, com duas tecnologias-chave desempenhando papéis importantes nesse processo: DHCP (*Dynamic Host Configuration Protocol*) e NAT (*Network Address Translation*).

**DHCP (Dynamic Host Configuration Protocol):** O DHCP é um protocolo usado para atribuir dinamicamente endereços IP e outras configurações de rede, como máscara de sub-rede, gateway padrão e servidores DNS, aos dispositivos em uma rede. Isso simplifica a administração de redes, permitindo que os dispositivos obtenham suas configurações de rede automaticamente, em vez de configurá-las manualmente. Os dispositivos solicitam um endereço IP ao servidor DHCP na rede e recebem as configurações necessárias.

## Cenários de uso do DHCP:

- Redes domésticas.
- Redes empresariais.
- Redes de convidados.
- Redes móveis.

**NAT (Network Address Translation):** O NAT é uma tecnologia que permite a vários dispositivos em uma rede compartilhar um único endereço IP público para acessar a internet. Os dispositivos internos usam endereços IP privados, e um roteador NAT atua como intermediário, traduzindo os endereços IP privados em um único endereço IP público para comunicação com a internet. Isso é útil em redes com vários dispositivos internos, mas com apenas um endereço IP público fornecido pelo provedor de internet.

## Cenários de uso de NAT:

- Redes domésticas.
- Redes empresariais.
- Redes com esgotamento de endereços IPv4.
- Segurança de rede.
- Transição de redes para IPv6.

Embora o NAT tenha sido uma solução temporária em redes IPv4 devido à escassez de endereços públicos, o crescimento da adoção do IPv6, que oferece um espaço de endereço mais amplo, está reduzindo a necessidade de NAT. No entanto, ele ainda é amplamente usado em redes IPv4 para permitir que vários dispositivos compartilhem um único endereço IP público.

## Introdução ao protocolo IPv6: definição e objetivos

O IPv6 (*Internet Protocol version 6*) é a próxima geração do protocolo de internet, destinado a substituir o IPv4. Enquanto o IPv4 utiliza endereços de 32 bits e suporta cerca de 4,3 bilhões de endereços, o IPv6 utiliza endereços de 128 bits, proporcionando um espaço de endereço virtualmente ilimitado para dispositivos conectados à internet. O IPv6 foi projetado para resolver problemas relacionados ao esgotamento de endereços IPv4 e fornecer melhorias. Objetivos do IPv6:

- Resolver a escassez de endereços.
- Simplificar o cabeçalho para acelerar o processamento de pacotes.
- Tornar campos do cabeçalho opcionais para facilitar o roteamento.
- Garantir a segurança das transmissões, tornando o IPsec obrigatório.

O endereçamento IPv6 possui 128 bits, divididos em oito grupos de quatro dígitos hexadecimais, permitindo um vasto espaço de endereço. O IPv6 coexistirá com o IPv4 durante um longo período de transição, e isso requer planejamento para gerenciar redes com ambos os protocolos.

O IPv6 foi padronizado por meio de RFCs, incluindo RFC 2460, que especifica o IPv6, e RFC 2461, que define a descoberta de vizinhos IPv6, entre outras. A notação abreviada é comumente usada para facilitar a leitura dos endereços IPv6; esse protocolo incorpora recursos de segurança aprimorados, como criptografia.

Os objetivos do IPv6 incluem fornecer um espaço de endereço mais amplo para expandir a internet, simplificar a configuração de dispositivos, melhorar a segurança e atender às necessidades de futuras aplicações e dispositivos conectados, como a internet das coisas (IoT).

## Cabeçalho e tipos de endereçamento IPv6

O IPv6 possui um cabeçalho simplificado e tipos de endereçamento específicos para melhorar a eficácia no roteamento e na entrega de dados na internet. Inclui informações como:

- Versão (sempre 6).
- Classe de tráfego (para qualidade de serviço e priorização).
- Identificação de fluxo (agrupa pacotes relacionados).
- Tamanho dos dados do *payload* (comprimento dos dados no pacote).
- Próximo cabeçalho (indica o tipo do próximo cabeçalho).
- Limite de saltos (limita o número de roteadores que um pacote pode atravessar).
- Endereço IP de origem.
- Endereço IP de destino.
- O IPv6 simplificou o cabeçalho em comparação com o IPv4, que tem 14 campos.

O IPv6 define diferentes tipos de endereços, como:

- *Unicast* (para um único dispositivo).
- *Multicast* (para um grupo de dispositivos).
- *Anycast* (entregue ao dispositivo mais próximo em um grupo).
- *Loopback* (para comunicação interna em um dispositivo).
- Endereço de mapeamento IPv4 (para representar endereços IPv4 em notação IPv6).

Esses tipos de endereços e o cabeçalho simplificado tornam o IPv6 mais eficiente, escalável e adequado para suportar a expansão da internet e a diversidade de dispositivos conectados.

## Coexistência e interoperabilidade: técnicas de transição

Durante o período de transição para a adoção generalizada do IPv6, a coexistência e interoperabilidade entre os protocolos IPv4 e IPv6 são essenciais. Existem várias técnicas de transição que permitem que esses dois protocolos operem juntos:

- **Dual Stack:** esta técnica envolve a implantação de ambos os protocolos IPv4 e IPv6 em dispositivos e redes, permitindo que eles se comuniquem usando ambos os protocolos.
- **Tunelamento:** envolve encapsular pacotes IPv6 em pacotes IPv4 (ou vice-versa) para permitir a comunicação entre dispositivos ou redes que não são nativamente compatíveis com o protocolo-alvo.
- **NAT64:** permite que dispositivos IPv6 se comuniquem com dispositivos IPv4, traduzindo endereços IPv6 em endereços IPv4.
- **Tradução de protocolo:** envolve a conversão de pacotes IPv4 em pacotes IPv6 (ou vice-versa) para permitir a comunicação direta entre dispositivos que usam protocolos diferentes.
- **DS-Lite:** é útil para provedores de serviços de internet (ISPs) que desejam adotar IPv6, permitindo que os clientes usem IPv6 para se comunicar com a internet, mas convertendo tráfego IPv4 em pacotes IPv6.

Essas técnicas garantem uma transição suave para o IPv6 à medida que o IPv4 se esgota, permitindo que redes e dispositivos com diferentes níveis de suporte a IPv4 e IPv6 se comuniquem efetivamente.

## É Hora de Praticar!



## Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Suponha que você está administrando uma rede local de escritório com vários departamentos, e você deseja otimizar a eficiência e o desempenho da rede. Responda às seguintes perguntas:

- O que são domínios de broadcast, e por que são importantes na gestão de uma rede local?
- Como os *switches* operam na camada de enlace e como eles ajudam a melhorar a eficiência de uma rede local?
- Qual é a diferença entre domínios de broadcast e domínios de colisão, e por que ambos são relevantes ao projetar uma rede local?

Agora, imagine que você está planejando uma expansão da rede local para acomodar mais dispositivos e departamentos. Você decide dividir a rede em sub-redes para melhorar a segmentação e o controle do tráfego. Responda às seguintes perguntas:

- Como a divisão de uma rede em sub-redes pode ajudar a melhorar a gestão da rede e o desempenho?
- Explique o processo de cálculo da máscara de sub-rede ao dividir uma rede em sub-redes menores. Dê um exemplo usando uma rede de classe C.
- Quais são os benefícios de utilizar DHCP e NAT na atribuição de endereços IP em uma rede local? Em que cenários cada uma dessas tecnologias é mais apropriada?

Finalmente, você decide que é hora de migrar para o IPv6. Responda às seguintes perguntas:

- Quais são os objetivos principais do IPv6 em comparação com o IPv4?
- Explique a diferença entre os tipos de endereços IPv6, como *unicast*, *multicast* e *anycast*.
- Quais são as técnicas de transição que podem ser usadas para permitir a coexistência e interoperabilidade entre IPv4 e IPv6 em uma rede durante o período de transição?

Você pode responder a essas questões com base nas informações fornecidas no texto e em seu conhecimento sobre redes de computadores. Você pode propor diferentes formas de solução e chegar ao mesmo objetivo. Qual foi o seu modelo de configuração? Mão à obra!

Como os domínios de broadcast e colisão impactam o funcionamento eficiente das redes locais, e como as práticas de divisão em sub-redes e cálculo de máscaras de sub-rede podem otimizar a alocação de endereços IP? Além disso, como a transição do IPv4 para o IPv6 é crucial para atender às crescentes demandas de endereçamento, e quais técnicas de transição garantem uma coexistência suave desses protocolos, permitindo a interoperabilidade entre redes IPv4 e IPv6?

Estudante, veja a seguir a proposta de resolução para este estudo de caso:

### **Domínios de broadcast, *switches* e domínios de colisão:**

- a) Os domínios de broadcast são áreas em uma rede local nas quais todos os dispositivos recebem pacotes de broadcast. Eles são importantes na gestão de uma rede local, pois controlam o tráfego de broadcast, garantindo que as mensagens sejam direcionadas apenas para os dispositivos que precisam delas. Isso evita congestionamento de rede e melhora a eficiência, uma vez que reduz o tráfego desnecessário. Além disso, os domínios de broadcast são fundamentais para descobrir outros dispositivos na rede e para anunciar serviços.
- b) Os *switches* operam na camada de enlace e desempenham um papel crucial na melhoria do desempenho de uma rede local. Eles encaminham pacotes com base nos endereços MAC, direcionando-os apenas para a porta do dispositivo de destino, em vez de transmitir para toda a rede. Isso divide a rede em vários domínios de colisão, reduzindo a possibilidade de colisões e melhorando a eficiência, uma vez que os dispositivos podem transmitir simultaneamente em portas separadas do *switch*.
- c) Domínios de broadcast lidam com a distribuição de pacotes de broadcast, que são enviados para todos os dispositivos na mesma rede, a fim de descobrir outros dispositivos ou anunciar serviços. Domínios de colisão, por outro lado, tratam da possibilidade de colisões durante a transmissão de dados. Eles são relevantes porque, em redes Ethernet, as colisões podem ocorrer quando vários dispositivos tentam transmitir simultaneamente em um único domínio de colisão. A segmentação em domínios de colisão menores é uma abordagem para reduzir colisões e melhorar o desempenho da rede.

### **Divisão de rede em sub-redes, cálculo de máscara de sub-rede, atribuição de endereço IP:**

- a) A divisão de uma rede em sub-redes ajuda a melhorar a gestão da rede, otimiza o desempenho, facilita a segurança e permite um controle mais granular do tráfego. Isso é alcançado usando máscaras de sub-rede para dividir a rede em segmentos menores, nos quais os bits "1" identificam a parte da rede e os bits "0" identificam a parte do host. Cada sub-rede pode ser tratada como uma rede independente, tornando a rede global mais eficiente.
- b) O processo de cálculo da máscara de sub-rede envolve a conversão da máscara de rede em notação decimal para binário e a determinação do número de bits adicionais necessários para representar as sub-redes desejadas. Por exemplo, para criar quatro sub-redes, você adicionaria 2 bits, resultando em uma máscara de sub-rede correspondente. Construir uma tabela de sub-redes ajuda a determinar os intervalos de endereços disponíveis para cada sub-rede.
- c) O DHCP (*Dynamic Host Configuration Protocol*) é uma tecnologia usada para atribuir dinamicamente endereços IP e outras configurações aos dispositivos em uma rede. É apropriado para redes nas quais a configuração automática de endereços é desejada, como em redes domésticas, empresariais e móveis.

O NAT (*Network Address Translation*) é uma técnica que permite a vários dispositivos em uma rede compartilhar um único endereço IP público para acessar a internet. Ele é útil quando um provedor de internet fornece apenas um endereço IP público. O NAT traduz endereços IP privados em um único endereço IP público, permitindo que vários dispositivos internos acessem a internet.

### **IPv6, cabeçalho, tipos de endereçamento e transição:**

- a) Os principais objetivos do IPv6 em comparação com o IPv4 são resolver a escassez de endereços IPv4, simplificar o cabeçalho para acelerar o processamento de pacotes, tornar

campos do cabeçalho opcionais para facilitar o roteamento e garantir a segurança das transmissões tornando o IPsec obrigatório.

b) O IPv6 define diferentes tipos de endereços, como *unicast* (para um único dispositivo), *multicast* (para um grupo de dispositivos), *anycast* (entregue ao dispositivo mais próximo em um grupo) e *loopback* (para comunicação interna em um dispositivo).

c) Técnicas de transição, como Dual Stack, tunelamento, NAT64, tradução de protocolo e DS-Lite, permitem a coexistência e interoperabilidade entre IPv4 e IPv6 em uma rede durante o período de transição. Essas técnicas permitem que dispositivos e redes com diferentes níveis de suporte a IPv4 e IPv6 se comuniquem efetivamente.

# ARQUITETURA E TECNOLOGIAS DE REDES

**1**

## ETHERNET: TECNOLOGIA E PROTOCOLOS DE CAMADA FÍSICA E DE ENLACE

Domínios de broadcast; Domínios de colisão;  
Operação, velocidades, comutação

**2**

## PROTÓCOLO IPV4: CONCEITOS E DIVISÃO DE ENDEREÇOS IP

Definição e notação; Pacote IPv4; Classes de Endereços

**3**

## PROTÓCOLO IPV4: REDES E SUB-REDES

Divisão de uma rede em sub-redes  
Cálculo da máscara de sub-rede  
Atribuição de endereço IP: DHCP e NAT

**4**

## PROTÓCOLO IPV6

Introdução ao protocolo IPv6: definição e objetivos  
Cabeçalho e tipos de endereçamento IPv6  
Coexistência e interoperabilidade: Técnicas de transição

Figura 1 | Arquitetura e tecnologias de redes. Fonte: elaborada pelo autor.

KUROSE, J. F. **Redes de computadores e a internet:** uma abordagem top-down. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

NAKAMURA, E. T. **Segurança da informação e de redes.** Londrina: Editora e Distribuidora Educacional S.A., 2016.

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

OLIVEIRA, D. B.; LUMMERTZ, R. S.; SOUZA, D. C. **Qualidade e desempenho de redes.** Porto Alegre: Sagah, 2019.

SOUZA, D. C.; *et al.* **Gerenciamento de redes de computadores.** Porto Alegre: Sagah, 2021.

TANEMBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores.** 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Unidade 4

### Gerência de Redes

#### Aula 1

##### Gerência de Redes e Padrões



#### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

#### Ponto de Partida

Olá, estudante!

O gerenciamento de redes de computadores tem o objetivo de garantir a confiabilidade, desempenho e segurança dos serviços oferecidos. Existem duas abordagens principais para gerenciamento de redes: a gerência única, que utiliza um conjunto integrado de ferramentas, e sistemas de gerência, que são ferramentas específicas para monitorar diferentes serviços. Três princípios essenciais incluem a coleta de dados, análise e diagnóstico, e controle de eventos. A ISO desenvolveu um modelo de gerenciamento dividido em cinco áreas: gerenciamento de desempenho, falhas, configuração, contabilização e segurança.

A arquitetura de gerenciamento de redes envolve entidade gerenciadora, dispositivos gerenciados e protocolo de gerenciamento. O protocolo SNMP (*Simple Network Information Protocol*) é utilizado para monitorar dispositivos e serviços de rede, enquanto o TMN (*Telecommunications Management Network*) é uma estrutura composta por arquiteturas informacional, funcional e física; ele permite o gerenciamento eficaz da rede. Podemos questionar como essas abordagens e princípios podem ser aplicados na prática para garantir o funcionamento eficiente e seguro de uma rede de computadores.

A técnica de *sniffing* em redes de computadores consiste na interceptação e registro de dados de tráfego de rede; ele pode incluir informações confidenciais, como senhas e conteúdo de comunicações. Essa técnica pode ser aplicada em diferentes camadas do modelo OSI, sendo mais comum nas camadas de enlace de dados e rede. O *sniffing* pode ser realizado por meio de programas instalados em computadores, visando capturar fluxos de dados específicos, como e-mails, logins e histórico de internet. Como um administrador de rede pode mitigar os riscos associados às técnicas de *sniffing* e garantir a segurança dos dados de uma rede, especialmente em ambientes em que informações confidenciais são transmitidas?

A gerência de redes com fluxos IP envolve a coleta e análise em tempo real de informações sobre o tráfego de rede, sendo fundamental para o monitoramento, solução de problemas, otimização de recursos e segurança de redes. Duas tecnologias proeminentes para essa finalidade são o IPFIX (*Internet Protocol Flow Information Export*) e o NetFlow. O IPFIX é uma evolução do NetFlow da Cisco, caracterizado por ser mais flexível e interoperável, permitindo a coleta de informações de fluxo de uma variedade de dispositivos de diferentes fabricantes.

Já o próprio NetFlow, desenvolvido pela Cisco, é uma tecnologia implementada em roteadores e *switches*, coletando informações detalhadas sobre o tráfego IP, endereços, portas, protocolos e duração das conexões, com aplicações abrangendo desde o gerenciamento de tráfego até a segurança da rede, planejamento de capacidade e resolução de problemas. As tecnologias de IPFIX e NetFlow são utilizadas para identificar e solucionar problemas de tráfego e, ao mesmo tempo, melhorar a eficiência e a segurança da rede da organização. Quais passos e qual a importância dessas tecnologias nesse processo?

Bons estudos!

## Vamos Começar!

## Padrões de gerência e elementos: SNMP e o TMN

Kurose (2006) define gerenciamento como ações de coordenação dos dispositivos físicos (computadores, servidores, etc.) e lógicos (protocolos, endereços e serviços), visando à confiabilidade dos serviços e buscando desempenho aceitável e a segurança das informações. O gerenciamento de redes visa oferecer, integrar e coordenar os elementos de hardware, software e usuários, a fim de monitorar, testar, configurar, avaliar e obter o controle da rede. A gerência de rede pode ser feita de duas formas basicamente:

- **Única gerência:** são um conjunto de ferramentas de monitoramento e/ou controle de dispositivos e/ou serviços, integrados em uma única solução.
- **Sistemas de gerência:** são ferramentas de monitoramento ou controle de dispositivos ou serviços. As ferramentas possuem funções específicas, auxiliando os administradores de redes no monitoramento de diversos serviços.

Para que o gerenciamento possa ter elementos para garantir o seu funcionamento, Kurose (2006) destaca três princípios:

- **Coleta de dados:** responsável por coletar automaticamente dados parametrizados pelo administrador de redes
- **Análise e diagnóstico:** organizar os dados coletados a fim de gerar informações que permitam a tomada de decisão. A análise pode ser feita manualmente, ou automatizada. A intenção é um diagnóstico correto do problema para que seja feita a correção no menor tempo possível.
- **Controle:** após o diagnóstico correto do problema, busca tomar ações a fim de cessar, mitigar ou minimizar os impactos. O administrador de redes deve ter o controle para que o mesmo evento não comprometa a qualidade ou funcionamento da rede e/ou serviços.

Segundo Kurose (2006), a ISO (*Internacional Organization for Standardization*) desenvolveu um modelo de gerenciamento de redes, divididos em cinco áreas:

- **Gerenciamento de desempenho:** quantificar, medir, informar, analisar e controlar o desempenho de dispositivos, serviços e segurança.
- **Gerenciamento de falhas:** registrar, detectar e reagir às falhas ocorridas nas redes. O compromisso maior é tratar de imediato as falhas transitórias da rede. Isso ocorre diariamente, quando há interrupções de serviços, hospedagem, falha de hardware e softwares de nodos.
- **Gerenciamento de configuração:** permite que o administrador saiba quais são os dispositivos utilizados na rede e as suas respectivas configurações. Nessa área de gerenciamento, estão contidos o planejamento dos IPs e as sub-redes.
- **Gerenciamento de contabilização:** permite a especificação, o registro e controle de acesso. Também define as quotas de utilização, balanceamento de carga.
- **Gerenciamento de segurança:** é efetuar o controle de acesso aos recursos via mecanismos de segurança, métodos de mascaramento de mensagens e políticas de prevenção e segurança.

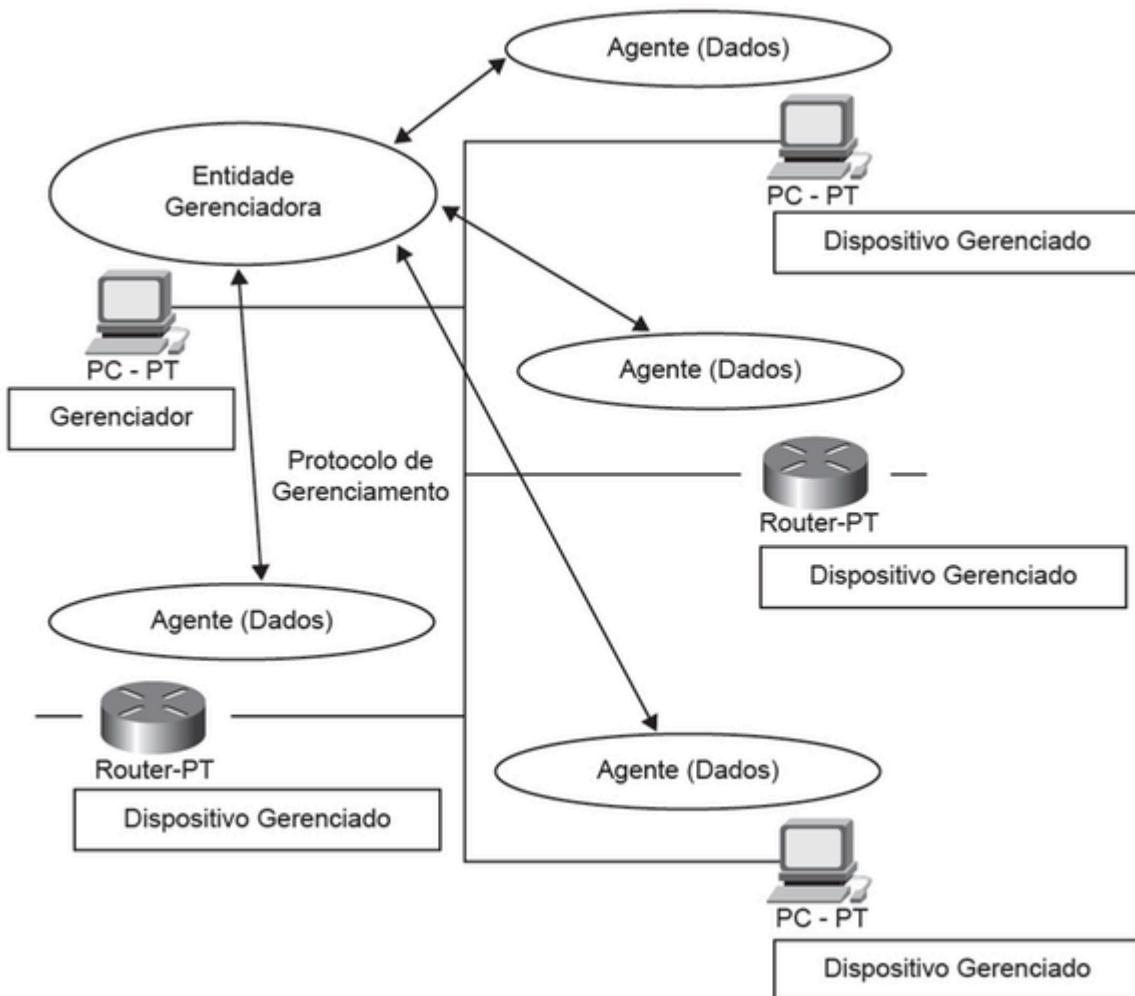


Figura 1 | Arquitetura de gerenciamento de redes. Fonte: adaptada de Kurose (2006, [s. p.]).

A estrutura da imagem tem os seguintes componentes:

- **Entidade gerenciadora:** é o meio pelo qual o administrador de redes interage com a interface de gerenciamento, podendo realizar as atividades de coleta de dados, processamento e análise para posterior tomada de decisão.
- **Dispositivo gerenciado:** é um dispositivo situado em uma rede gerenciada, o qual pode ser monitorado, por exemplo: servidores, sensores, switches, etc.
- **Protocolo de gerenciamento de rede:** é executado entre a entidade gerenciadora e os dispositivos gerenciados, permitindo que os agentes possam informar a entidade gerenciadora sobre a ocorrência de erros, falhas ou alguma violação de segurança.

## SNMP (*Simple Network Information Protocol*)

Nunes (2017) explica que o protocolo SNMP é definido pela RFC 3410. A sua primeira versão (SNMPv1) foi lançada em 1988; ela foi definida nas RFCs 1065, 1066 e 1067. Hoje, utiliza-se o protocolo SNMPv3, atualizado em dezembro de 2002. O protocolo é utilizado para efetuar o monitoramento dos dispositivos de redes e os serviços. Permite que equipamentos com diversas arquiteturas e sistemas operacionais possam utilizá-lo. Utiliza quatro componentes básicos:

1. Os nodos gerenciados (agentes).
2. As estações de gerenciamento (gerente).
3. As informações de gerenciamento (MIB).
4. O protocolo de gerenciamento (SNMP).

O MIB (*Management Information Base*) é um banco de dados (lógico) que efetua o armazenamento de informações de configuração e status dos equipamentos gerenciáveis. Pode fornecer informações como: nome, atributos e possíveis operações. Observe os processos envolvidos no SNMP:

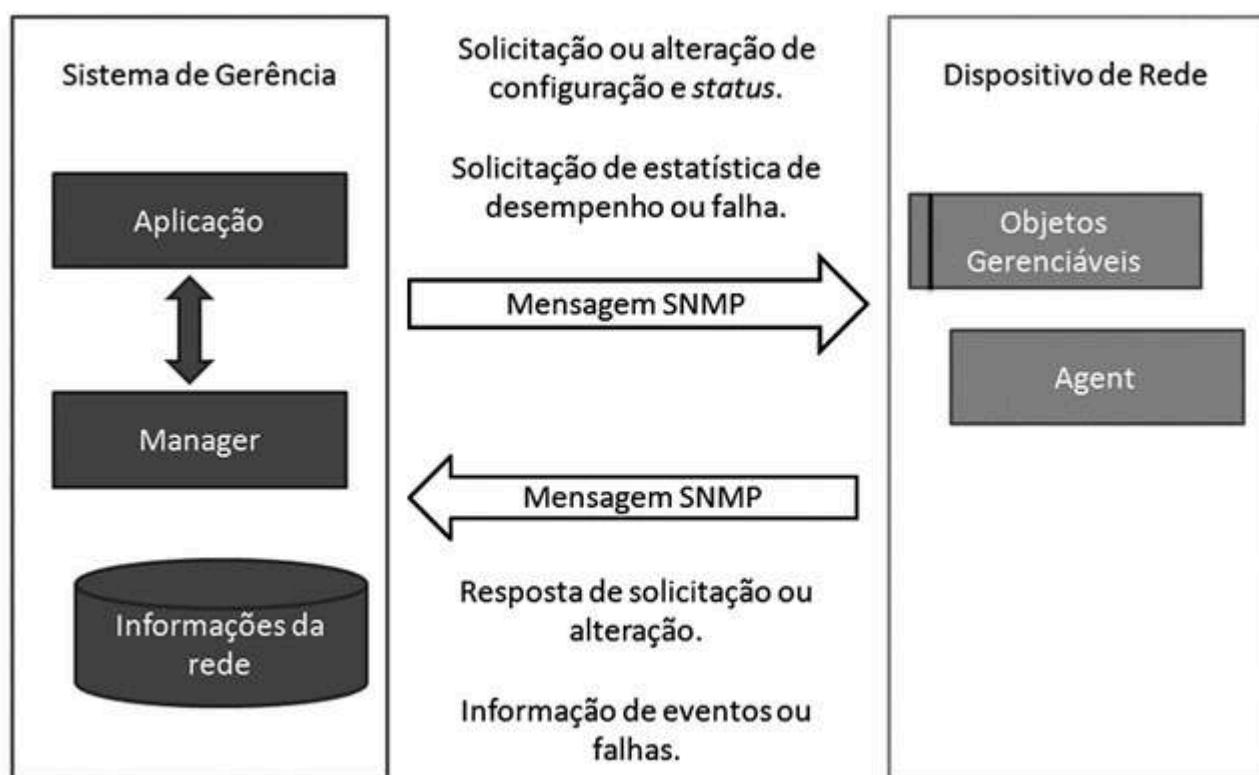


Figura 2 | Arquitetura de gerenciamento de redes. Fonte: adaptada de Nunes (2017, [s. p.]).

O SNMP é instalado nos equipamentos gerenciáveis da rede, os agentes que se comunicam diretamente com o MIB e respondem às solicitações efetuadas pelo gerente. Caso ocorra algum evento inesperado, uma notificação é enviada ao gerente.

## TMN (*Telecommunications Management Network*)

Tanenbaum, Feamster e Wetherall (2021) detalham que este modelo de gerenciamento está estruturado em três arquiteturas, as quais podem ser implementadas juntas ou separadas, conforme a necessidade do administrador de rede. São elas:

- **Arquitetura informacional:** as informações são trocadas entre os agentes e gerentes por meio de um protocolo de gerência de rede. Porém, não é utilizado somente um protocolo para prover o gerenciamento, uma vez que cada interface definida na arquitetura física pode utilizar um protocolo adequado à necessidade.
- **Arquitetura funcional:** define quais serão as funções e os objetivos na gerência de rede, com os seguintes blocos adicionados: sistema de suporte à operação (OSF); elemento de rede (NEF); estação de trabalho (WSF); adaptador Q (QAF); elemento mediador (MF); e rede de comunicação de dados (DCN).
- **Arquitetura física:** define as interfaces que garantem a compatibilidade dos equipamentos. Elas são divididas em:
  1. **Interface Q:** entre os blocos OSF, WSF, QAF, MF e NF.
  2. **Interface F:** para ligar as estações de trabalho, WSF.
  3. **Interface X:** entre os blocos OSF e WSF.
  4. **Interface G:** abrange um escopo mais amplo, incluindo impressoras, servidores e outros equipamentos. Pode oferecer um nível de gerenciamento mais limitado para dispositivos não relacionados à rede.
  5. **Interface M:** permite o gerenciamento completo de dispositivos de rede não TMN pela rede TMN, se concentra em dispositivos de rede não TMN.

**Siga em Frente...**

## Técnica de *sniffing*

De acordo com Souza *et al.* (2021), a palavra *sniff* vem do inglês e significa farejar. A ferramenta efetua a interceptação e o registro dos dados. Existem casos em que é possível decodificar o conteúdo dos pacotes capturados. Esse recurso é utilizado pelos administradores de rede para checar se uma rede está trabalhando dentro dos parâmetros definidos. Refere-se à prática de interceptar e analisar o tráfego de rede para obter informações sobre os dados transmitidos.

Um programa de *sniffing* instalado em um computador visa capturar os fluxos especificados em sua configuração, que podem ser: e-mail, logins, textos, histórico de internet, entre outros dados.

- **Sniffing na camada de enlace de dados (camada 2):** um invasor pode colocar uma placa de rede em modo de captura, o que permite que ela capture todos os pacotes que passam por uma rede local (LAN). Isso pode revelar informações confidenciais, como senhas ou conteúdo de comunicações.

- **Sniffing na camada de rede (camada 3):** um atacante pode capturar pacotes IP que trafegam na rede. Isso pode ser usado para monitorar o tráfego, identificar dispositivos na rede ou até mesmo redirecionar o tráfego.

O SMI (*Structure of Management Information*) é uma parte do protocolo SNMP (*Simple Network Management Protocol*), usado para gerenciar dispositivos de rede. O SMI não está diretamente relacionado a técnicas de *sniffing*. Ele define a estrutura e a semântica dos objetos gerenciados em um sistema de gerenciamento de rede. O SNMP permite que administradores de rede coletem informações sobre dispositivos de rede e configurem esses dispositivos remotamente. As técnicas de *sniffing* são métodos para interceptar e analisar o tráfego de rede, enquanto o SMI é uma parte do protocolo SNMP que define a estrutura de informações gerenciadas. Eles não estão diretamente relacionados entre si. O SNMP pode ser afetado por técnicas de *sniffing* se o tráfego SNMP for interceptado, mas o SMI em si não é uma técnica de *sniffing*.

Segundo Tanenbaum, Feamster e Wetherall (2021), as técnicas de *sniffing* podem ser usadas em qualquer camada do modelo OSI, mas são mais comuns nas camadas de enlace de dados e rede:

- **ARP Spoofing:** envolve a manipulação do protocolo de resolução de endereços (ARP) para associar o endereço MAC de um invasor a um endereço IP legítimo na rede. O ARP é usado para relacionar endereços IP a endereços MAC na rede. Quando um dispositivo precisa comunicar com outro na mesma rede local, ele consulta a tabela ARP para obter o endereço MAC associado a um determinado endereço IP. O invasor envia pacotes ARP falsificados, informando que o endereço IP de uma vítima está associado ao seu próprio endereço MAC. Assim, o tráfego destinado à vítima é redirecionado para o invasor. Ao realizar ARP Spoofing, ele pode interceptar o tráfego entre um computador e um roteador, obtendo acesso a informações sensíveis, como senhas.
- **Packet sniffing com ferramentas de software:** esta técnica envolve o uso de software especializado para capturar e analisar pacotes de rede em uma rede local ou segmento de rede. Ferramentas como o Wireshark permitem capturar pacotes de rede e analisar o tráfego em tempo real, ou posteriormente. Isso pode ser usado para monitorar a atividade da rede, diagnosticar problemas de conectividade ou, em casos maliciosos, para capturar informações confidenciais transmitidas pela rede. Um administrador de rede pode usar o Wireshark para monitorar o tráfego de uma rede e identificar problemas de desempenho. No entanto, um invasor também pode usar a mesma ferramenta para capturar senhas ou informações sensíveis de usuários.

## Gerência de redes com fluxos IP: IPFIX e NetFlow

A gerência de redes com fluxos IP é uma abordagem que envolve a coleta e análise de informações sobre o tráfego de rede em tempo real. É ideal para monitoramento, solução de problemas, otimização de recursos e segurança de redes. Duas tecnologias amplamente

utilizadas para essa finalidade são IPFIX (*IP Flow Information Export*) e NetFlow. Ambas as tecnologias são usadas para coletar dados sobre o tráfego de rede em forma de fluxos.

Nunes (2017) explica que o IPFIX é baseado no NetFlow da Cisco, mas é mais flexível e interoperável, permitindo a coleta de informações de fluxo de uma variedade de dispositivos de diferentes fabricantes. Tem padrão aberto, que permite a interoperabilidade entre equipamentos de rede de diferentes fabricantes. É uma tecnologia que monitora fluxos de tráfego através de um *switch* ou roteador. Interpreta o tráfego para determinar o cliente, servidor, protocolo e porta que é utilizada.

O NetFlow é uma tecnologia criada pela Cisco e implementada em roteadores e switches, para coletar informações de tráfego IP e monitorar dados de rede. Ele permite a coleta de informações sobre o tráfego de rede, endereços IP de origem e destino, portas, protocolos, volumes de tráfego e duração das conexões. O monitoramento do tráfego gera estatísticas que representam os dados de fluxo na rede. As operações de rede e segurança compreendem quem se comunica com quem, quando, por quanto tempo e com que frequência. Na linguagem de um ambiente de rede de dados, são monitorados volumes de dados, tempo, portas e protocolos. Isso pode ser enriquecido com medições de latência e dados da camada de aplicação para uma variedade de protocolos. Muito utilizado para gerenciamento de tráfego, segurança de rede, planejamento de capacidade, resolução de problemas, auditoria e conformidade.

## Vamos Exercitar?

A aplicação eficaz dos princípios de gerenciamento de redes, como coleta de dados, análise, diagnóstico e controle, envolve a implementação de sistemas de gerenciamento, como SNMP e TMN. Isso permite aos administradores de rede monitorar dispositivos e serviços, garantir o desempenho adequado, identificar e corrigir falhas rapidamente, planejar configurações, controlar o acesso e reforçar a segurança. Essas abordagens, junto com protocolos específicos, são essenciais para administrar redes de computadores complexas de maneira eficiente e segura.

Um administrador de rede pode implementar várias medidas de segurança para mitigar os riscos associados às técnicas de *sniffing*. Algumas estratégias incluem a criptografia dos dados transmitidos na rede a fim de torná-los ilegíveis para possíveis invasores, o monitoramento constante do tráfego de rede em busca de atividades suspeitas usando ferramentas de detecção de intrusões, e a implementação de autenticação forte, como autenticação de dois fatores, para impedir o acesso não autorizado. É essencial manter sistemas e software atualizados com as últimas correções de segurança e educar os usuários sobre práticas seguras, como evitar abrir links ou baixar arquivos de fontes não confiáveis. Essas medidas combinadas ajudam a garantir a segurança dos dados em uma rede, mesmo em ambientes onde informações confidenciais são transmitidas.

Para solucionar os desafios de desempenho na rede, o administrador pode começar implementando as tecnologias de IPFIX e NetFlow para coletar dados detalhados sobre o tráfego

de rede em tempo real. Com o IPFIX, a vantagem seria a interoperabilidade com dispositivos de diferentes fabricantes, tornando-o flexível para a coleta de informações de fluxo. Já o NetFlow fornece detalhes sobre endereços IP de origem e destino, portas, protocolos e duração das conexões. Essas tecnologias seriam cruciais para a identificação de gargalos de tráfego, análise de padrões de utilização e detecção de possíveis ameaças de segurança.

É possível analisar os dados coletados para identificar quais aplicativos ou protocolos estão consumindo mais largura de banda, onde ocorrem os congestionamentos e como otimizar a alocação de recursos. As informações do NetFlow avaliam a segurança da rede, identificam comportamentos anômalos e monitoram o tráfego em busca de atividades suspeitas.

## Saiba mais

A gerência de redes e os padrões desempenham um papel crucial na organização e monitoramento eficazes de sistemas de comunicação. O SNMP (Simple Network Management Protocol) e o TMN (Telecommunications Management Network) são componentes fundamentais. O SNMP é amplamente utilizado para coletar informações e gerenciar dispositivos de rede, enquanto o TMN oferece uma estrutura mais abrangente para a gerência de telecomunicações. A técnica de sniffing, que envolve a interceptação e análise de pacotes de dados em uma rede, é uma ferramenta poderosa para entender o tráfego e identificar problemas de segurança ou desempenho. Além disso, a gerência de redes com fluxos IP, como IPFIX e NetFlow, permite a coleta de dados de tráfego em tempo real, oferecendo informações valiosas para a análise e otimização da rede. Essas abordagens e padrões desempenham um papel fundamental na garantia de operações de rede eficazes, seguras e confiáveis. Vamos estudar os conteúdos adicionais a seguir:

- Artigo [Segurança e privacidade na web 2.0: foco nas redes sociais](#), da Egitania sciencia, disponível na Biblioteca Virtual, no parceiro [ProQuest](#).
- Artigo [Aplicação de melhores práticas de gestão e segurança para monitoração de ativos de infraestrutura](#), da Revista Ibérica de Sistemas e Tecnologias de Informação, disponível na Biblioteca Virtual, no parceiro ProQuest.
- Filme: Ex Machina (Ex Machina: Instinto Artificial). Direção: Alex Garland. Produção: Alton Reich; Andrew Macdonald. Estados Unidos: A24. 2014. DVD (108 min.). Em um refúgio nas montanhas, mantido por um talentoso bilionário da internet, um jovem participa de uma estranha experiência: testar a inteligência artificial, inserida no corpo de uma bela garota robô. Mas a experiência se torna uma sinistra batalha psicológica: um triângulo amoroso, no qual a lealdade está dividida entre homem e máquina.

## Referências

KUROSE, J. F. **Redes de computadores e a internet: uma abordagem top-down**. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

MONTEIRO, D. Segurança e privacidade na web 2.0: foco nas redes sociais. **Egitania sciencia**, Guarda, ed. 10, 2012.

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

OLIVEIRA, F. B.; *et al.* Aplicação de melhores práticas de gestão e segurança para monitoração de ativos de infraestrutura. **Revista Ibérica de Sistemas e Tecnologias de Informação**, Lousada, ed. 62, 2023.

SOUZA, D. C.; *et al.* **Gerenciamento de redes de computadores**. Porto Alegre: Sagah, 2021.

TANEMBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Aula 2

Gerência de Falhas e Segurança

### Gerência de falhas e segurança



#### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

### Ponto de Partida

Olá, estudante!

Veremos a importância da gerência de falhas e segurança em redes de computadores, destacando aspectos-chave, como a distribuição, armazenamento e criptografia. Na distribuição, é essencial detectar e resolver problemas de conectividade e desempenho, sendo necessário

implementar medidas de autenticação e controle de acesso. Além disso, redes de entrega de conteúdo (CDNs) desempenham um papel crucial na disseminação global de recursos. No contexto de armazenamento, a disponibilidade e a integridade dos dados são fundamentais, com estratégias como redundância e backups.

A criptografia é destacada como um componente crucial para proteger a confidencialidade e integridade dos dados em repouso e em trânsito, incluindo escolha de algoritmos, gerenciamento de chaves e considerações de desempenho. Técnicas como SSL/TLS e VPNs são mencionadas como exemplos de aplicação de criptografia em redes. Caso fosse um administrador de uma empresa com uma rede de grande escala que lida com informações sensíveis, como você garantiria a segurança e a integridade dos dados distribuídos, levando em consideração os conceitos de controle de acesso, monitoramento de tráfego, redundância de dados, backup e criptografia? Além disso, como você lidaria com a gestão de chaves de criptografia para proteger as comunicações e os dados armazenados? Qual seria a sua estratégia para assegurar que a rede seja resiliente a falhas e que os dados permaneçam seguros?

Você verá ainda as distinções entre falhas e erros em sistemas de comunicação de dados. Abordaremos erros de transmissão, como interferência, distorção e atenuação, que podem ocorrer, bem como as categorias de erros, como erros em um único bit, erros em rajadas e erros indefinidos. Além disso, são mencionados métodos de detecção e correção de erros, como correção antecipada de erros (FEC) e correção de erros por retransmissão. Trataremos também conceitos relacionados à previsão de falhas em hardware, como o tempo médio entre falhas (MTBF) e o tempo médio para reparos (MTTR).

Essas informações são essenciais para que você compreenda e resolva problemas de falhas e erros em redes de computadores. Assim, você poderá garantir a confiabilidade da comunicação de dados em sua rede, considerando a ocorrência de falhas e erros. Como você aplicaria os conceitos que serão discutidos sobre falhas e erros para garantir a qualidade da comunicação em sua rede? Além disso, como você escolheria entre os métodos de correção de erros, como correção antecipada de erros (FEC) e correção de erros por retransmissão, para otimizar o desempenho e a confiabilidade da rede? Explique também como você utilizaria as técnicas de tempo médio entre falhas (MTBF) e tempo médio para reparos (MTTR) para prever e lidar com as falhas de hardware em sua rede.

O monitoramento envolve a avaliação contínua do desempenho e da segurança da rede, incluindo a supervisão do tráfego, análise de logs e monitoramento de dispositivos. A manutenção é proativa, abrangendo atualizações de software, substituição de hardware defeituoso e aplicação de políticas de segurança. A correção é a resposta imediata a eventos de falha ou ameaças de segurança detectados durante o monitoramento. Essas práticas trabalham em conjunto para garantir a confiabilidade e a integridade das operações de rede, tornando-a resiliente a problemas futuros. Além disso, o controle de acesso à rede (NAC) desempenha um papel importante na segurança, ajudando a evitar intrusões e a identificar dispositivos vulneráveis.

O uso eficaz dessas estratégias e ferramentas é essencial para manter uma rede de computadores confiável e segura. Após o aprendizado do conteúdo, como você planejaria e

implementaria estratégias de monitoramento, manutenção e correção para garantir a segurança e a integridade da rede? Que ferramentas e práticas você utilizaria para detectar possíveis falhas e ameaças de segurança, realizar manutenções preventivas e corrigir problemas emergentes? Como a tecnologia de controle de acesso à rede (NAC) pode ser incorporada para aprimorar a segurança da rede? Ao final dessa aula veremos como essas medidas contribuiriam para um funcionamento confiável e seguro da rede em sua organização.

Bons estudos!

## Vamos Começar!

### Distribuição, armazenamento, criptografia

A gerência de falhas na distribuição envolve a detecção, notificação e resolução de problemas em uma rede distribuída. A detecção de falhas é essencial para identificar problemas de conectividade ou desempenho em vários pontos da rede.

A distribuição em redes de computadores é o processo de compartilhar recursos, informações e serviços entre dispositivos interconectados. Isso inclui o compartilhamento de impressoras, arquivos e aplicativos, possibilitando uma colaboração eficiente. Para garantir a segurança nesse contexto, são necessárias medidas como autenticação, controle de acesso e segurança na distribuição, como firewalls e VPNs.

Souza *et al.* (2021) ressaltam que redes P2P permitem aos dispositivos compartilhar informações diretamente entre si, enquanto o balanceamento de carga optimiza o desempenho, distribuindo o tráfego entre servidores. Além disso, as redes de entrega de conteúdo (CDNs) espalham conteúdo globalmente para melhorar o acesso a recursos, como imagens e vídeos. Redes sociais, IoT e mídias sociais são exemplos de distribuição em larga escala, que envolvem o compartilhamento de informações e interações em todo o mundo.

Exemplos de técnicas de distribuição de gerenciamento de falhas incluem:

- **Controle de acesso:** a implementação de políticas de controle de acesso garante que apenas usuários autorizados tenham acesso a recursos específicos. Isso pode ser alcançado por meio de senhas, autenticação de dois fatores (2FA) ou certificados digitais.
- **SNMP (*Simple Network Management Protocol*):** SNMP é um protocolo amplamente utilizado para monitorar dispositivos de rede, como roteadores e *switches*. Ele permite que os administradores coletem informações sobre o estado de dispositivos de rede e definam alarmes para notificar sobre falhas.
- **Monitoramento de tráfego de rede:** ferramentas de monitoramento de tráfego, como o Wireshark, podem ser usadas para capturar e analisar o tráfego de rede em busca de problemas, como congestionamento, perda de pacotes e erros de transmissão.

A gerência de falhas relacionada ao armazenamento está principalmente associada à disponibilidade e integridade dos dados em sistemas de armazenamento de rede, como servidores de arquivos e sistemas de armazenamento em nuvem.

Segundo Nunes (2017), o armazenamento em redes de computadores é uma parte da infraestrutura de TI, permitindo o compartilhamento de dados, recursos e informações entre dispositivos interconectados. Abrange o compartilhamento de arquivos, pastas e uso de serviços de armazenamento em nuvem para acesso remoto. A segurança dos dados é uma preocupação, com a implementação de medidas como criptografia, políticas de retenção e backups seguros para proteger os dados contra perda e acesso não autorizado. A redundância e a tolerância a falhas são usadas para garantir a disponibilidade contínua dos dados, enquanto o gerenciamento eficaz de dados e a escalabilidade são fundamentais para garantir a organização e a adaptação às crescentes demandas de armazenamento. Exemplos:

- **Redundância de dados:** para garantir a disponibilidade contínua dos dados, as organizações implementam práticas como RAID (*Redundant Array of Independent Disks*) para criar cópias redundantes de dados em vários discos.
- **Backup e recuperação de desastres:** a realização de backups regulares e a criação de planos de recuperação de desastres são essenciais para garantir a recuperação de dados em caso de falhas.
- **Controle de acesso:** para proteger dados sensíveis, é importante implementar medidas de controle de acesso, como autenticação e autorização, para garantir que apenas usuários autorizados acessem os dados.
- **Políticas de retenção e descarte seguro:** a implementação de políticas para retenção de dados e seu descarte seguro é essencial para garantir que informações sensíveis não sejam mantidas indefinidamente, mas sejam adequadamente eliminadas quando não forem mais necessárias.

Segundo Tanenbaum, Feamster e Wetherall (2021), quatro grupos contribuíram para o surgimento e o aprimoramento dos métodos de criptografia: os militares, os diplomatas, as pessoas “comuns” que gostam de guardar memórias e os amantes. O maior volume de contribuição adveio dos militares, uma vez que eles tinham interesses como estratégia de comunicação em período de guerra.

Basicamente, o processo consiste em transformar uma mensagem de texto com uma chave parametrizada, cuja saída é um texto cifrado, com o uso de um algoritmo criptográfico. Se a mensagem for capturada e o interceptor não possuir a chave, não conseguirá fazer o processo inverso, que possibilite ler o conteúdo da mensagem. Neste momento, vale a pena conceituar três termos:

- **Criptoanálise:** arte de solucionar (“desvendar”) as mensagens cifradas.
- **Criptografia:** arte de criar mensagens cifradas.
- **Criptologia:** estudos acerca de criptoanálise e os métodos de criptografia.

Tanenbaum, Feamster e Wetherall (2021) sugerem um modelo matemático para representar o processo de criptografia, em que, tanto na função de criptografia, quanto na de descriptografia,

há uma chave aplicada a uma função matemática.

Outra forma de proteger uma mensagem é utilizar a técnica de esteganografia, que pode ser definida como a arte de esconder dentro de outro arquivo aparentemente inofensivo alguma mensagem; se esta for interceptada, não será possível detectá-la.

De acordo com Kurose (2006), a criptografia em redes de computadores é uma técnica fundamental que protege a confidencialidade, integridade e autenticidade dos dados transmitidos e armazenados. Utiliza algoritmos de criptografia simétrica e assimétrica, bem como funções de *hash*, para transformar informações em um formato ilegível, que só pode ser revertido com a chave apropriada. A criptografia é amplamente aplicada em redes para garantir a segurança das comunicações, autenticar usuários, proteger dados em repouso e em trânsito e verificar a integridade dos dados. No entanto, o gerenciamento de chaves, a escolha de algoritmos fortes e a consideração do desempenho são desafios importantes na implementação eficaz da criptografia. Exemplos de criptografia em redes incluem:

- **SSL/TLS (*Secure Sockets Layer/Transport Layer Security*)**: esses protocolos são usados para criptografar a comunicação entre navegadores da web e servidores, garantindo que os dados transmitidos sejam seguros e protegidos contra interceptação.
- **VPN (*Virtual Private Network*)**: as VPNs usam criptografia para criar túneis seguros através dos quais o tráfego de rede pode ser transmitido com segurança pela internet ou redes públicas.
- **Criptografia de dados em repouso**: para proteger dados armazenados em dispositivos ou servidores, a criptografia de dados em repouso é usada. Por exemplo, discos rígidos criptografados garantem que, se um dispositivo for perdido ou roubado, os dados ainda permaneçam seguros.

## Siga em Frente...

## Falhas *versus* erros

Segundo Nunes (2017), sistemas de comunicação de dados estão sujeitos a falhas e erros. Podem ocorrer em equipamentos físicos ou em transmissão. Mesmo quando são feitos exaustivos testes de erros ou de stress de rede, tais ocorrências ainda podem aparecer nas estruturas das redes de computadores. Os erros de transmissão são divididos em três categorias:

- **Interferência**: são radiações eletromagnéticas capazes de causar ruído, o que, por sua vez, degrada os sinais de rádio ou os sinais que trafegam pelo meio cabulado.
- **Distorção**: normalmente os dispositivos físicos de transmissão, como os cabos, geram a distorção dos sinais. O excesso dela é capaz de causar desde a degradação do serviço até a perda de sinal.
- **Atenuação**: em meios não guiados, a atenuação se dá quando o sinal necessita atravessar barreiras físicas (parede, vidro, fibra, etc.); também é causada pela distância entre o

receptor e a antena. Já no meio guiado, só a distância é o fator de degradação dos serviços.

Segundo Kurose (2006), em 1984, o cientista americano Claude Shannon publicou as bases matemáticas para determinar a capacidade máxima de transmissão por um canal físico com uma banda passante, em uma determinada relação sinal/ruído. Os erros ocorridos na comunicação de dados não podem ser eliminados por completo, porém aqueles relacionados à transmissão podem ser facilmente detectados, permitindo, assim, que sejam corrigidos automaticamente.

Para efetuar o tratamento desses erros, existe uma relação de custo-benefício, pois é adicionada uma sobrecarga no processo de transmissão.

- **Erro em um único bit:** apenas um bit sofre uma alteração e os outros permanecem preservados. A degradação do serviço ocorre por um período curto. O erro de um único bit (*single-bit-error*) causa uma degradação com menor duração, porém, dependendo do que está sendo transmitido, pode ser mais ou menos degradante. Por exemplo, se o erro acontecer quando se está assistindo a um filme por streaming, ocorre um travamento momentâneo, ou seja, uma pequena fração da cena é pulada.
- **Erro em rajada:** vários bits sofrem alterações. A degradação do serviço ocorre por um longo período. Como são transmitidos em rajadas, para contabilizá-los, após a ocorrência de um erro, considera-se um bloco de oito bits. Os erros em rajada têm um tempo de duração maior em relação ao erro em único bit. Normalmente a degradação do serviço pode ser sensível tanto nas transmissões de streaming, quanto no acesso a sites. Por exemplo, a comunicação utilizada em jogos online é feita em rajada; na ocorrência de erros, em casos mais leves, pode apenas acontecer uma paralisação temporária no jogo, e, após um tempo, retoma-se a partida. Nos casos extremos, quando os erros ocorridos nas transmissões em rajada se repetem continuamente, a conexão pode ser perdida.
- **Indefinido:** a transmissão que chega ao receptor é ambígua (valores fora do escopo). Podem ocorrer diversos períodos de degradação do serviço.

Souza *et al.* (2021) destacam que, quando os erros são detectados, é necessário efetuar a correção deles. Para que isso ocorra, o número de bits corrompidos deve ser determinado. São possíveis dois métodos de correção de erros:

- **Correção antecipada de erros (FEC – *Forward Error Correction*):** são utilizados bits redundantes (por métodos de codificação), possibilitando que o receptor “adivinhe” os bits.
- **Correção de erros por retransmissão:** quando o receptor encontra um erro, solicita ao emissor para realizar o reenvio da mensagem, processo esse que se repete até que se esteja livre de erro.

Tanenbaum, Feamster e Wetherall (2021) definem que as falhas em sistemas computacionais são respostas incorretas em relação ao que foi projetado como saída, podendo ser definidas por alguns especialistas como defeito. Essas falhas podem ser geradas por fator humano, meios de transmissão, hardware, lógico (software), entre outros. Para auxiliar os profissionais de

tecnologia da informação a prever as falhas de hardware, por meio de análise estatística de dados históricos dos dispositivos de uma rede, são utilizadas as técnicas:

- **Tempo médio entre falhas (MTBF – Mean Time Between Failures):** é uma previsão por modelo estatístico/matemático do tempo médio entre as falhas. É útil para os profissionais de tecnologia da informação, uma vez que prevê as manutenções necessárias.

$$MTBF = \frac{\sum(Final - Início)}{\text{Número de falhas}}$$

$$MTBF = \frac{\sum(Final - Início)}{\text{Número de falhas}}$$

- **Tempo médio para reparos (MTTR – Mean Time To Repair):** é uma previsão por modelo estatístico/matemático do tempo médio para efetuar reparo após a ocorrência de falha.

$$MTTR = \frac{\text{Tempo parado por falha}}{\text{Número de falhas}}$$

$$MTTR = \frac{\text{Tempo parado por falha}}{\text{Número de falhas}}$$

Dessa forma, é possível prever, por meio dos cálculos efetuados com os dados históricos/estatísticos, quando os equipamentos apresentarão uma falha e seu tempo de indisponibilidade.

## Monitoramento, manutenção e correção

Em redes de computadores, a gerência de falhas e segurança desempenha um papel crucial para garantir o funcionamento confiável e seguro da rede. Três pontos-chave desse contexto incluem: o monitoramento, a manutenção e a correção.

O monitoramento é a prática diária de observar e avaliar o desempenho, a disponibilidade, a integridade da infraestrutura e a segurança de rede de computadores. Pode ser realizado por meio de ferramentas de monitoramento que coletam dados e estatísticas sobre o tráfego na rede, sobre a utilização de recursos, sobre a integridade dos equipamentos e sobre outras configurações.

Nunes (2017) ressalta que podemos acompanhar do uso de largura de banda da rede para identificar problemas, como gargalos; também é possível a supervisão de equipamentos em

busca de indicadores de falhas ou vulnerabilidades. Além disso, pode-se realizar a análise de logs de segurança para detectar atividades suspeitas e tomar ações para mitigar uma situação de perigo para uma organização, buscando identificar problemas potenciais antes que eles afetem a operação normal da rede. Exemplos:

- **Supervisão de tráfego de rede:** monitorar a utilização da largura de banda, identificando gargalos de tráfego ou picos de utilização que possam impactar o desempenho.
- **Monitoramento de equipamentos:** acompanhar o status de roteadores, switches, servidores e outros dispositivos para identificar falhas de hardware, altas temperaturas ou outros indicadores de problemas.
- **Análise de logs:** verificar logs de eventos e segurança para detectar atividades incomuns, tentativas de intrusão ou problemas de configuração.
- **Monitoramento de segurança:** acompanhar as aplicações de segurança da rede em busca de ameaças, identificando atividades suspeitas e garantindo a conformidade com políticas de segurança.

Segundo Nunes (2017), a manutenção envolve ações proativas e preventivas para garantir que a rede funcione de maneira eficiente, e permaneça confiável e segura. Isso inclui realização de atualizações de software, correções de segurança, substituição de hardware defeituoso e aplicação de políticas de conformidade. A manutenção é aplicada para regular atualizações de segurança nos sistemas, substituir cabos degradados antes que causem falhas, implementar de políticas de senha fortes e realizar a manutenção preventiva de servidores para evitar paralisações. A manutenção é essencial para evitar falhas e problemas futuros. Exemplos:

- **Atualizações de software:** manter sistemas operacionais, aplicativos e firmware atualizados com as últimas correções de segurança e melhorias de desempenho.
- **Substituição de hardware:** trocar dispositivos de rede defeituosos ou com falhas, como switches ou discos rígidos, para evitar interrupções.
- **Gestão de ativos:** manter um inventário de ativos de rede, rastreando dispositivos, licenças de software e datas de expiração.
- **Políticas de conformidade:** aplicar políticas de segurança, como senhas fortes, autenticação de dois fatores e políticas de retenção de dados, para garantir a conformidade com padrões de segurança.

A correção é a resposta a eventos de falha ou incidentes de segurança que foram identificados por meio do monitoramento. Envolve ação imediata para resolver problemas e restaurar a funcionalidade da rede. Podemos considerar as ações como a restauração de um servidor após uma falha, a aplicação de correções de segurança para remediar vulnerabilidades identificadas e a resposta a um ataque cibernético, como a remoção de malware e a mitigação de ameaças. Exemplos:

- **Recuperação de desastres:** restaurar a operação normal da rede após uma falha, como a recuperação de dados de um backup em caso de perda de dados.
- **Resposta a incidentes de segurança:** tomar medidas para conter e mitigar ameaças de segurança, como a remoção de malware, investigação de uma violação de dados ou bloqueio de contas comprometidas.

- **Correção de erros de configuração:** identificar e corrigir configurações incorretas que possam levar a problemas de segurança ou desempenho.

Segundo Tanenbaum, Feamster e Wetherall (1997), os logs são ferramentas importantes para os administradores de redes, pois são recursos de fácil implementação que podem fornecer um histórico para análise. Os geradores de logs devem obedecer a uma regra simples: manter os dispositivos sincronizados ao servidor NTP. Os registros de logs devem ser armazenados em servidores locais ou remotos, e as suas informações podem ser acessadas online e/ou offline. Além do armazenamento dos registros, algumas práticas se fazem fundamentais:

- A inspeção dos logs deve ser uma rotina de trabalho.
- Devem-se investigar as causas dos logs nocivos à segurança e ao funcionamento da rede.
- Devem-se estabelecer padrões de funcionamento para facilitar a análise dos logs.

Tanenbaum, Feamster e Wetherall (1997) acrescentam que o NAC (*Network Access Control*) é um recurso muito importante para auxiliar o gerenciamento da segurança em redes. Tal ferramenta auxilia o administrador de redes nas seguintes tarefas:

- Controlar acesso à rede, contra pessoas ou equipamentos não autorizados.
- Evitar intrusões fraudulentas, cujo intuito é o roubo de informações sigilosas.
- Detectar dispositivos vulneráveis ou infectados que possam colocar a rede em risco de alguma forma.

Tais técnicas permitem que os dispositivos e usuários que necessitem conectar-se à rede sejam identificados e, se possuírem credenciais, sejam autorizados a fazê-lo. Assim, torna-se possível verificar o status e a atualização de antivírus, as aplicações, os softwares, etc.

A gerência de falhas e segurança em redes de computadores é voltada para manter a confiabilidade e a integridade das operações. O monitoramento envolve a observação constante do desempenho da rede e a detecção de possíveis problemas. Esse processo inclui a supervisão de tráfego, análise de logs e monitoramento de dispositivos para identificar irregularidades e ameaças de segurança.

A manutenção é uma prática preventiva que visa evitar problemas futuros. Ela inclui a aplicação de atualizações de software, a substituição de hardware defeituoso e a garantia de conformidade com políticas de segurança. Por fim, a correção é a resposta a falhas ou incidentes de segurança identificados durante o monitoramento. Envolve ação imediata para restaurar a funcionalidade da rede, como a recuperação de desastres, a resposta a incidentes de segurança e a correção de erros de configuração.

## Vamos Exercitar?

Como administrador de uma empresa com uma rede de grande escala que trata de informações sensíveis, a estratégia poderia abranger medidas como controle de acesso rigoroso,

monitoramento de tráfego para detecção precoce de anomalias, redundância de dados através do uso de RAID e backups regulares, implementação abrangente de criptografia tanto para comunicações quanto para dados em repouso, com uma gestão de chaves sólida para garantir a segurança das chaves. Destaque para a resistência a falhas, com redundância de hardware, planos de contingência e procedimentos de recuperação de desastres bem definidos para garantir a disponibilidade contínua da rede e a integridade dos dados. Auditorias regulares e atualizações de segurança seriam parte integrante dessa estratégia em evolução.

Para garantir a segurança e a integridade dos dados distribuídos em uma rede de grande escala, um administrador deve adotar diversas medidas. Além das já citadas anteriormente, a gestão de chaves de criptografia é fundamental para assegurar a segurança, e a resiliência a falhas pode ser alcançada por meio de técnicas como tempo médio entre falhas (MTBF) e tempo médio para reparos (MTTR) para prever e lidar com problemas de hardware, garantindo que a rede funcione de forma confiável e contínua.

É possível utilizar ferramentas para monitoramento de rede de computadores e para supervisionar o tráfego, a integridade dos dispositivos e analisar logs de segurança. A manutenção preventiva incluiria atualizações regulares de software, substituição de hardware defeituoso e aplicação de políticas de segurança. A correção responderia a incidentes identificados durante o monitoramento. Além disso, seria possível incorporar a tecnologia de Controle de Acesso à Rede (NAC) para controlar o acesso de dispositivos e usuários à rede, melhorando a segurança. Essas medidas contribuiriam para um funcionamento confiável e seguro da rede, garantindo a integridade dos dados e a confidencialidade das informações.

## Saiba mais

A gerência de falhas e segurança em redes de computadores é essencial para garantir um ambiente confiável e protegido. A distribuição, armazenamento e criptografia desempenham papéis importantes na proteção de informações sensíveis, assegurando que os dados sejam armazenados e transmitidos com segurança. A distinção entre falhas e erros destaca a necessidade de identificar e corrigir problemas em uma rede. O monitoramento contínuo, a manutenção preventiva e a correção ágil de incidentes são práticas vitais para garantir o funcionamento confiável e seguro de uma rede, enquanto a tecnologia de Controle de Acesso à Rede (NAC) pode ser incorporada para fortalecer ainda mais a segurança. Portanto, um conjunto abrangente de estratégias e práticas que abrangem esses elementos é fundamental para proteger informações críticas em ambientes de rede. Vamos estudar os conteúdos adicionais a seguir:

- Artigo [Visão Geral do e-Governo: Segurança e Privacidade dos Dados Pessoais](#), da Revista Ibérica de Sistemas e Tecnologias de Informação, disponível na Biblioteca Virtual no parceiro [Proquest](#),
- Artigo [Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação](#), da Revista Ibérica de Sistemas e Tecnologias de Informação, disponível na Biblioteca Virtual no parceiro [Proquest](#),

- Filme: The Social Dilemma (O Dilema das Redes). Direção: Jeff Orlowski. Produção: Larissa Rhodes. Estados Unidos: Netflix. 2020. DVD (94 min.). Pessoas por trás do Google, Twitter, Facebook, Instagram e YouTube revelam como essas plataformas estão reprogramando a civilização, expondo o que está escondido no outro lado da tela.

## Referências

GEORG, M. A. C. ; *et al.* Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. **Revista Ibérica de Sistemas e Tecnologias de Informação**, Lousada, ed. 54, 2022.

KUROSE, J. F. **Redes de computadores e a internet**: uma abordagem top-down. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

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

SOUZA, D. C.; *et al.* **Gerenciamento de redes de computadores**. Porto Alegre: Sagah, 2021.

TANEMBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

VICTOR, J.; *et al.* Visão Geral do e-Governo: Segurança e Privacidade dos Dados Pessoais. **Revista Ibérica de Sistemas e Tecnologias de Informação**, Lousada, ed. 60, 2023.

## Aula 3

Gerência de Desempenho, Configuração e Contabilização



### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

## Ponto de Partida

Olá, estudante!

Gargalos, tempo de resposta, latência e *jitter* são conceitos-chave em redes de computadores. Gargalos representam pontos de estrangulamento na rede, enquanto o tempo de resposta é crucial para a eficiência. A latência é a soma do tempo de transmissão e propagação, impactando a comunicação em tempo real. *Jitter* é a variação na entrega de pacotes. Podemos questionar: como minimizar a latência em redes e garantir uma transmissão mais consistente, especialmente em aplicações sensíveis ao tempo, como videoconferências e jogos online, mantendo uma boa qualidade de serviço?

Indicadores de desempenho, como utilização, tráfego e *throughput*, desempenham um papel crucial na gestão de falhas e segurança em redes de computadores. Para avaliar o desempenho da rede, os engenheiros de redes frequentemente realizam testes de qualidade, observando aspectos como a taxa máxima suportada, o tempo de deslocamento de pacotes e o tempo de recuperação de falhas. A reconfigurabilidade das redes é muito utilizada, uma vez que os perfis de tráfego mudam frequentemente, exigindo a capacidade de acomodar novos serviços, crescimento de tráfego, novas tecnologias e padronização.

A vazão (*throughput*) representa a quantidade de dados transferidos em um determinado tempo, influenciada pela topologia da rede, número de usuários e taxa das interfaces de rede. A perda de pacotes, devido ao esgotamento de capacidade de armazenamento dos roteadores, pode ocorrer à medida que a rede cresce. A disponibilidade é essencial, descrevendo a capacidade de manter os serviços de rede em execução sem interrupções.

A qualidade de serviço (QoS) busca otimizar a utilização dos recursos disponíveis, considerando fatores como latência, *jitter*, perda de pacotes e largura de banda disponível. Uma pergunta relevante é como equilibrar efetivamente esses indicadores para garantir um desempenho ótimo da rede, considerando as necessidades em constante evolução e mantendo a disponibilidade e a qualidade dos serviços?

O VLAN Trunk Protocol (VTP) é uma ferramenta fundamental na gestão de redes de computadores, especialmente em ambientes que fazem uso de VLANs (*Virtual Local Area Networks*) para segmentar o tráfego de rede e aprimorar segurança e desempenho. O VTP, desenvolvido pela Cisco, estabelece uma estrutura cliente-servidor em que todas as alterações de configuração de VLAN ocorrem no servidor, que posteriormente replica essas alterações para os clientes.

Esse protocolo simplifica a configuração e a manutenção de VLANs em uma rede, permitindo que as informações de configuração, como nomes e números de VLAN, sejam automaticamente

propagadas para todos os *switches* na rede. Isso economiza tempo e reduz erros humanos, além de garantir a consistência nas configurações de VLAN em todos os dispositivos da rede. O VTP opera em três modos principais: servidor, cliente e transparente, dependendo da função de cada switch na rede. Isso torna a gestão de VLANs mais eficiente e confiável, especialmente em redes complexas.

Como as redes podem garantir a segurança e a integridade das informações de configuração de VLAN quando usam o VTP, considerando que ele é um protocolo que replica automaticamente essas informações para todos os *switches* na rede? Quais medidas de segurança e autenticação podem ser implementadas para evitar possíveis ameaças à integridade das configurações de VLAN por meio do VTP?

É o que veremos a seguir, vamos lá?

Bons estudos!

## Vamos Começar!

## Gargalos, tempo de resposta, latência ou atrasos, *jitter*

Nunes (2017) explica que gargalos se referem a pontos de estrangulamento em uma rede de computadores, nos quais o tráfego é restringido ou limitado. Podem ocorrer em qualquer ponto da rede, como links de baixa largura de banda ou roteadores/servidores com recursos limitados. Gargalos podem levar a congestionamento e redução no desempenho da rede. Na rede mundial de computadores, são fenômenos bem comuns, já que os serviços providos diariamente podem sofrer falhas ou perdas. Por exemplo, o gargalo pode ocorrer nos últimos dias de entrega da declaração de imposto de renda, quando o grande número de chegadas simultâneas de informações pode deixar o serviço indisponível, embora o problema também possa ocorrer por falha na aplicação.

Gargalos em redes de computadores são responsáveis pela degradação dos serviços, razão pela qual, ao se pensar na estruturação das topologias, o administrador deve procurar mecanismos que garantam a disponibilidade das aplicações. Podemos imaginar uma rede corporativa em que a conexão de internet de entrada possui uma largura de banda de 100Mbps, mas várias estações de trabalho estão transmitindo vídeo de alta definição simultaneamente. O link de entrada se tornaria o gargalo, resultando em desempenho insatisfatório.

De acordo com Souza *et al.* (2021), gargalos podem ocorrer em diferentes pontos de uma rede. Além dos exemplos já mencionados, outros pontos de estrangulamento incluem servidores sobrecarregados, com recursos de CPU insuficientes, e switches congestionados. Gargalos de tráfego podem resultar em perda de pacotes e tempos de resposta mais longos. Em uma rede de data center, um servidor de banco de dados central pode se tornar um gargalo se muitas consultas simultâneas forem feitas a ele, causando latência significativa para os usuários. Para gerenciar gargalos, você pode implementar平衡amento de carga, de modo que o tráfego é

distribuído uniformemente entre vários servidores para evitar sobrecarga. Isso é particularmente útil em data centers e sites da web com alto tráfego.

Por sua vez, o tempo de resposta é o intervalo de tempo entre a emissão de um pedido e a recepção de uma resposta. Baixos tempos de resposta são desejáveis, pois indicam eficiência e responsividade na rede. O tempo de resposta é crítico em muitas aplicações, como comércio eletrônico e sistemas de controle em tempo real. Reduzi-lo é essencial para melhorar a experiência do usuário. Quando você faz uma pesquisa no mecanismo de busca, como o Google, o tempo que leva para obter os resultados é o tempo de resposta. É essencial que ele seja rápido para uma experiência de usuário satisfatória.

Em um sistema de negociação de ações, por exemplo, o tempo de resposta é vital. Atrasos podem resultar em oportunidades de negociação perdidas ou em preços desatualizados, afetando as decisões dos traders. Otimizar o tempo de resposta envolve aprimorar a infraestrutura de rede, usar tecnologias de cache e otimizar o código de aplicação para minimizar consultas a bancos de dados ou serviços externos, além equipamentos de hardware robusto para aguentar o tráfego na rede.

Latência (atraso) em redes de computadores, segundo Souza *et al.* (2021), é o intervalo de tempo entre o momento que o emissor enviou o pacote e o recebimento da confirmação do pacote por parte do receptor. O tempo que o receptor gasta no processamento do pacote não deve ser utilizado no cálculo da latência. A latência pode ser considerada:

$$\text{Latência} = \text{Tempo de transmissão} + \text{Tempo de propagação}.$$

Em que:

$$\begin{aligned}\text{Tempo de transmissão} &= \text{Dimensão do pacote (bits)} \\ &\quad / \text{Velocidade da Transmissão (bps)}.\end{aligned}$$

$$\begin{aligned}\text{Tempo de propagação} &= \text{Dimensão do Canal (Km)} \\ &\quad / \text{Velocidade de Propagação (Km/s)}.\end{aligned}$$

$$\begin{aligned}\text{Tempo de transmissão} &= \text{Dimensão do pacote (bits)} / \\ &\quad \text{Velocidade da Transmissão (bps)}.\end{aligned}$$

$$\begin{aligned}\text{Tempo de propagação} &= \text{Dimensão do Canal (Km)} / \\ &\quad \text{Velocidade de Propagação (Km/s)}.\end{aligned}$$

A latência de ida e volta (*round-trip latency*), que representa o período necessário para um pacote de dados percorrer o trajeto de um ponto A para um ponto B e regressar ao ponto A, constitui a métrica crucial para diversos aplicativos. Diminuir a latência é essencial para aprimorar a eficácia das comunicações. Nos sistemas de navegação por satélite, a demora é vital. Uma latência substancial pode ocasionar atrasos nas informações de posicionamento, prejudicando a navegação em tempo real.

Nas videochamadas ou jogos online, esse fator também é considerado. Se ocorrer uma demora elevada, os participantes podem vivenciar retardos nas conversas ou nos movimentos do jogo, o que pode prejudicar a experiência. Para minimizar a demora, redes de alta velocidade, como redes de fibra óptica, são uma opção. Além disso, a utilização de CDNs (Redes de Distribuição de Conteúdo) contribui para reduzir a demora, ao armazenar conteúdo em servidores próximos aos utilizadores.

Os atrasos em uma rede podem incluir atrasos de transmissão, atrasos de propagação e atrasos de processamento. Os atrasos de transmissão ocorrem devido à velocidade de transmissão; os atrasos de propagação são causados pela distância física entre os pontos e os atrasos de processamento ocorrem quando dispositivos de rede processam os dados. Ao fazer uma chamada de voz pela internet (VoIP), o atraso de transmissão pode ocorrer se a conexão estiver congestionada. O atraso de propagação pode acontecer em chamadas internacionais, devido à distância física entre os locais de chamada.

Atrasos de transmissão, propagação e processamento podem ocorrer em diferentes camadas da rede. Atrasos de processamento são geralmente mais controláveis, enquanto os outros dependem de fatores físicos. Em sistemas de monitoramento de tráfego rodoviário, atrasos de processamento podem ocorrer se os algoritmos de detecção de veículos forem inefficientes, atrasando a tomada de decisões críticas. Para gerenciar atrasos, é necessário otimizar os processos de rede e utilizar algoritmos eficientes. Em relação aos atrasos de transmissão, o uso de redes de alta velocidade e protocolos de compressão de dados pode ajudar.

Segundo Kurose (2006), há dois outros tipos de atrasos que podem provocar latência: o tempo de processamento e o tempo de enfileiramento (gargalos). No entanto, esses dois tempos só podem ser aferidos em uma rede com utilização de tráfego significativamente elevado. O aumento da latência (atraso) e a perda de pacotes nas transmissões sofrem interferências devido, entre outros fatores, à:

- Distância entre os nodos.
- Distância da antena (em transmissão sem fio).
- Qualidade dos links (cabeado ou sem fio).

É fato que esses tipos de ocorrências podem se mostrar como um dos maiores degradadores dos serviços encontrados nas redes de computadores.

*Jitter*, de acordo com Nunes (2017), pode ser definido como a variação no tempo e na sequência de entrega dos pacotes devido à variação da latência na rede. A influência do *jitter* é mais sensível para a qualidade de serviço quando se tem a necessidade de garantia na entrega dos pacotes em períodos definidos. O *jitter* é analisado na periodicidade na transmissão dos pacotes, como também na variação da entrega dos pacotes.

O *Jitter* pode levar a uma experiência do utilizador instável, especialmente em comunicações em tempo real, como videochamadas e chamadas de áudio. Em uma videochamada, se os pacotes de áudio e vídeo tiverem uma oscilação significativa, você pode notar interrupções e irregularidades na qualidade da chamada, com a voz ou o vídeo cortando e tremendo. Em

comunicações em tempo real, como chamadas de voz sobre IP (VoIP) e videoconferências, pode resultar em perturbações na qualidade do áudio ou vídeo. Na telemedicina, o *jitter* pode prejudicar a qualidade da comunicação entre médicos e pacientes, tornando o diagnóstico preciso uma tarefa problemática em consultas remotas.

Para lidar com o *jitter*, é preciso dar prioridade ao tráfego em tempo real, empregar buffers adaptativos e implementar tecnologias de qualidade de serviço (QoS) para assegurar que as comunicações sensíveis ao tempo tenham prioridade, garantindo uma transmissão de pacotes mais consistente.

## Siga em Frente...

### Indicadores: utilização, tráfego, *throughput*

Uma das maiores dificuldades encontradas é ajustar os parâmetros de desempenho da rede para que se possam suprir as necessidades. Segundo Tanembaum, Feamster e Wetherall (2021), em diversas situações, os engenheiros de redes necessitam avaliar desde a estrutura da rede até os dispositivos individualmente, para então realizar testes probatórios de qualidade.

Em geral, os testes de desempenho são feitos por meio da injeção de um determinado tráfego na rede, permitindo assim que o administrador de rede analise as saídas. Vários aspectos podem ser observados, e entre outros:

- Taxa máxima suportada.
- Tempo de deslocamento de um pacote.
- Tempo de recuperação a falhas.

Um software muito utilizado por administradores de redes para analisar vazão, latência, *jitter* e perda de pacotes é o Iperf (Jperf em Linux). Esse programa faz a análise da rede e do seu desempenho, por meio das ferramentas disponíveis e configuradas, para enviar pacotes de tamanhos variáveis conforme o experimento a ser realizado. Ao utilizar alguns tipos de ferramentas, é possível compreender quais dados são utilizados, o horário de maior consumo dos recursos, entre outros pontos. Isso possibilita a compreensão do perfil dos usuários e adequação da rede a fim de atender aos serviços prioritários. Quando pensamos no quesito “desempenho da rede”, não importa muito o tipo de serviço que se esteja utilizando. Porém, quanto aos protocolos de redes, principalmente o TCP/IP e UDP, sabemos que todos eles têm funcionamento, tamanho e, consequentemente, ocupam mais ou menos recursos da rede.

Tanembaum, Feamster e Wetherall (2021) explicam que as redes devem ser reconfiguráveis para atender aos perfis de tráfego, que mudam com muita frequência. Para a garantia da continuidade dos serviços da rede e a manutenção da qualidade, os administradores de redes devem permitir:

- Novos serviços.
- Crescimento do tráfego.

- Novas tecnologias.
- Padronização e interoperabilidade entre os protocolos e equipamentos.

Dessa forma, ao conhecer o perfil do tráfego da rede, é possível adequar os recursos às necessidades, ou ainda manter o equilíbrio necessário para obter um nível de qualidade adequado.

Vazão (*throughput*), segundo Nunes (2017), pode ser definida como a quantidade de dados transferidos entre equipamentos de rede, ou mesmo a quantidade de dados processados em determinado tempo. Normalmente é expressa em bits por segundo (bps). Os fatores que interferem na vazão, são: topologia de rede, número de usuários e taxa das interfaces. A vazão poderia ser descrita como a velocidade em que os dados realmente trafegam pela rede. Essa taxa de transferência pode ser menor do que a largura de banda, devido a perdas e atrasos.

Perda de pacotes, de acordo com Tanenbaum, Feamster e Wetherall (2021), acontecem em razão de os roteadores não terem a capacidade de armazenamento de pacotes infinita; após o esgotamento, os pacotes são descartados. À medida que a rede cresce ou a exigência de processamento aumenta devido às aplicações, o nodo passa a ter mais solicitações e, consequentemente, pode ocorrer perda de pacotes.

Quanto à disponibilidade, Nunes (2017) explica que as redes de computadores são compostas por diversos dispositivos, como computadores, servidores, cabeamentos, entre outros, cada um dos quais é um sistema suscetível a falhas. Ou seja, disponibilidade é a descrição da capacidade que equipamentos e redes possuem de forma contínua (sem que haja interrupção), por um período. Nesse sentido, os serviços de rede devem estar disponíveis no maior espaço de tempo possível (janela de disponibilidade).

Tanenbaum, Feamster e Wetherall (2021) definem QoS (*Quality of Service* – qualidade de serviço) como um conjunto de regras, mecanismos e tecnologias que tem o propósito de utilizar os recursos disponíveis de forma eficaz e econômica. Os fatores que determinam diretamente a qualidade de transmissão são: latência, *jitter*, perda de pacotes e largura de banda disponível.

## Introdução ao VLAN Trunk Protocol

O VLAN Trunk Protocol (VTP) é um componente importante em redes de computadores, especialmente em ambientes onde se utilizam VLANs (Virtual Local Area Networks) para segmentar o tráfego de rede e melhorar a segurança e o desempenho.

Um exemplo de configuração de equipamentos é a utilização do VLAN Trunk Protocol. Trata-se de um protocolo de camada 2, desenvolvido pela Cisco, para configuração de VLANs, facilitando, assim, a sua administração. Mas o que é uma VLAN? Nunes (2017) mostra que VLAN é definida como rede local virtual (*virtual lan network*). Trata-se de uma maneira de criar sub-redes de forma

virtual. Se feita em *switchs*, cada uma das interfaces pode ser uma VLAN e ter o seu próprio domínio de broadcast.



Figura 1 | Exemplo de VTP VLAN. Fonte: adaptada de Nunes (2017, [s. p.]).

Basicamente, o VTP (VLAN Trunk Protocol) cria uma estrutura do tipo cliente-servidor, em que as alterações obrigatoriamente são feitas no servidor, o qual, por sua vez, posteriormente, as replica aos clientes. Tal técnica é largamente utilizada pelos administradores de redes.

O VTP é um protocolo de gerência de VLAN desenvolvido pela Cisco para simplificar a configuração e a manutenção de VLANs em uma rede. Ele permite que as informações de configuração da VLAN, como nomes e números de VLAN, sejam propagadas automaticamente para todos os *switches* na rede. Essa propagação automática facilita a adição, remoção ou modificação de VLANs em vários *switches*, economizando tempo e reduzindo erros humanos.

O VTP ajuda a simplificar a configuração de VLANs, permitindo que as informações de configuração sejam definidas em um único *switch*, chamado servidor VTP. Essas informações são então propagadas automaticamente para outros *switches* na rede, conhecidos como clientes VTP. Isso evita a necessidade de configurar manualmente cada *switch* na rede com as mesmas informações de VLAN. Uma das principais vantagens do VTP é evitar inconsistências na

configuração de VLANs. Quando um administrador de rede cria, modifica ou exclui uma VLAN no servidor VTP, as mudanças são replicadas para todos os clientes VTP na rede. Isso ajuda a garantir que todos os *switches* tenham a mesma configuração de VLAN.

O VTP opera em três modos principais: servidor, cliente e transparente. O servidor é responsável por criar e gerenciar as informações de VLAN, o cliente recebe essas informações e o modo transparente repassa as informações, mas não as processa localmente. O modo a ser usado em um *switch* depende da função que ele desempenhará na rede.

## Vamos Exercitar?

Para minimizar a latência em redes e garantir uma transmissão mais consistente, especialmente em aplicações sensíveis ao tempo, como videoconferências e jogos online, é necessário adotar diversas estratégias. Isso inclui o uso de redes de alta velocidade, implementação de protocolos de qualidade de serviço (QoS) para priorizar o tráfego sensível ao tempo, otimização de rotas de rede para reduzir o tempo de propagação e o uso de caches e CDNs para armazenar conteúdo próximo aos usuários, diminuindo o tempo de transmissão. Além disso, a escolha de hardware e equipamentos de rede eficientes é fundamental. A questão central é como equilibrar efetivamente essas estratégias para atender às necessidades específicas de cada aplicação, garantindo uma experiência do usuário satisfatória, considerando as restrições de recursos e limitações de orçamento.

Para equilibrar efetivamente indicadores de desempenho, como utilização, tráfego, *throughput*, latência, *jitter* e perda de pacotes, na gestão de redes de computadores, é adotar uma abordagem abrangente que inclua monitoramento contínuo, planejamento de capacidade, implementação de QoS, tolerância a falhas, otimização de desempenho, análise de tráfego, treinamento da equipe e atualização tecnológica. O desafio central é encontrar o equilíbrio certo entre esses elementos para atender às necessidades da organização e manter a disponibilidade, qualidade de serviço e segurança da rede, considerando a constante evolução das demandas e recursos disponíveis.

Para garantir a segurança e a integridade das informações de configuração de VLAN ao utilizar o VLAN Trunk Protocol (VTP), algumas medidas podem ser adotadas. Uma abordagem seria a implementação de autenticação e controle de acesso rigorosos para os dispositivos que operam no modo servidor VTP, a fim de impedir acesso não autorizado às configurações. Além disso, a segmentação da rede e a aplicação de listas de controle de acesso (ACLs) podem ajudar a restringir o tráfego VTP a áreas específicas da rede.

Outra medida de segurança seria a configuração de senhas de domínio VTP, que devem ser consistentes entre os dispositivos VTP confiáveis. Assim, somente dispositivos com a senha correta podem participar do domínio VTP e propagar configurações. É importante também manter a supervisão constante das configurações e auditorias regulares para identificar possíveis anomalias e garantir a conformidade com as políticas de segurança da rede. Portanto,

embora o VTP simplifique a configuração de VLANs, é vital adotar práticas seguras para garantir que esse processo não comprometa a segurança da rede.

## Saiba mais

A gerência de desempenho em redes de computadores envolve a monitorização de elementos críticos como gargalos, tempo de resposta, latência, atrasos e jitter, bem como a análise de indicadores como utilização, tráfego e throughput. Esses aspectos são fundamentais para assegurar uma comunicação eficiente e confiável na rede. Além disso, a introdução do VLAN Trunk Protocol (VTP) é relevante, pois possibilita a segmentação da rede em VLANs para uma gestão mais eficaz dos recursos, embora seja necessário um cuidadoso processo de configuração e contabilização. Essa disciplina desempenha um papel crucial na otimização do desempenho da rede e na garantia de sua capacidade de atender às necessidades dos usuários e aplicações. Veja as indicações de conteúdo complementar a seguir:

- Artigo [\*Sobre a utilização de mediadores semânticos para monitoramento de qualidade de serviço na web\*](#), da revista Holos.
- Artigo [\*Sistema para a identificação de aglomerações operando em Redes IoT e Fog Computing\*](#), da Revista Ibérica de Sistemas e Tecnologias de Informação, disponível na Biblioteca Virtual, no parceiro Proquest.
- Filme: Her (Ela). Direção: Spike Jonze. Produção: Samantha Morton. Estados Unidos: Warner Bros. Pictures. 2013. DVD (125 min.). Em um futuro próximo na cidade de Los Angeles, Theodore Twombly (Joaquin Phoenix) é um homem complexo e emotivo que trabalha escrevendo cartas pessoais e tocantes para outras pessoas. Com o coração partido após o final de um relacionamento, ele começa a ficar intrigado com um novo e avançado sistema operacional que promete ser uma entidade intuitiva e única. Ao iniciá-lo, ele tem o prazer de conhecer “Samantha”, uma voz feminina perspicaz, sensível e surpreendentemente engraçada. A medida em que as necessidades dela aumentam junto com as dele, a amizade dos dois se aprofunda em um eventual amor um pelo outro.

## Referências

DIAS, B. S. S.; et al. Sistema para a identificação de aglomerações operando em Redes IoT e Fog Computing. **Revista Ibérica de Sistemas e Tecnologias de Informação**, Lousada, ed. 47, 2021.

KUROSE, J. F. **Redes de computadores e a internet**: uma abordagem top-down. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

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

RIBEIRO, C. M. F. A. Sobre a utilização de mediadores semânticos para monitoramento de qualidade de serviço na web. **Holos**, Natal, v. 26, n.1, 2010. Disponível em: <https://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/276>. Acesso em 5 abr. 2024.

SOUZA, D. C.; et al. **Gerenciamento de redes de computadores**. Porto Alegre: Sagah, 2021.

TANEMBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Aula 4

Simulando Redes de Computadores

### Simulando redes de computadores



#### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

### Ponto de Partida

Olá, estudante!

O simulador de redes Cisco Packet Tracer destaca a importância dos simuladores na criação e teste de modelos virtuais de redes. Ele é muito utilizado para a aplicação educacional e, por pesquisadores, para avaliar desempenho e segurança de protocolos. O Packet Tracer é uma ferramenta da Cisco com interface intuitiva, amplamente usada em treinamentos e ambientes de aprendizado prático, permitindo criar topologias complexas, configurar dispositivos e simular tráfego de dados.

Considerando a importância dos simuladores de redes, como o Cisco Packet Tracer, na formação prática de estudantes e profissionais de TI, será que há alguma limitação significativa nesses ambientes virtuais que poderia afetar a aplicação prática do conhecimento adquirido? Até que ponto a simulação reflete com precisão os desafios do ambiente real de redes de computadores?

A infraestrutura em redes de computadores é composta por elementos físicos e lógicos, dispositivos como roteadores e switches, e meios de transmissão, como cabos e conexões sem fio. O simulador destaca a importância da topologia de rede, da gestão de rede, do cabeamento estruturado e de conceitos modernos, como virtualização e redundância. A complexidade da construção da infraestrutura em simuladores ajuda a refletir sobre desafios reais.

As capacidades dos simuladores, incluindo a configuração de parâmetros, introdução de falhas, gerenciamento detalhado de protocolos e análise de desempenho, auxiliam a montar uma rede de computador mais próxima possível do real, abrangendo instalação, seleção de dispositivos, configuração de conexões, teste de conectividade e exploração de recursos avançados, como NAT, ACLs e VLANs.

Como a construção e simulação de uma infraestrutura de rede no Cisco Packet Tracer pode contribuir para o desenvolvimento de habilidades práticas em profissionais de redes, permitindo a configuração detalhada de dispositivos, a análise de desempenho, a introdução de falhas controladas e a implementação de protocolos avançados para lidar com diferentes cenários?

Veremos a importância de configurar serviços e protocolos em simuladores de redes para treinamento e teste. Diversos simuladores, como Cisco Packet Tracer, permitem a criação de topologias virtuais e emulação de dispositivos de rede. A configuração abrange roteadores, switches, serviços (DHCP, DNS, FTP, HTTP) e protocolos de comunicação (TCP/IP). O Cisco Packet Tracer fornece exemplos práticos de configuração; sua flexibilidade permite criar cenários diversos, enquanto a documentação facilita revisões e compartilhamento de conhecimento.

Erros na configuração podem levar a resultados não realistas na simulação. Considerando a simulação detalhada de configurações de redes em ambientes virtuais, como essa abordagem pode ser utilizada para aprimorar a capacidade de resposta em situações de falhas de rede? Como os profissionais de redes podem empregar simuladores para desenvolver estratégias eficazes de recuperação, diagnosticar problemas rapidamente e garantir a continuidade operacional em cenários adversos?

É o que veremos nesta aula, vamos lá?

Bons estudos!

## Vamos Começar!

## Introdução ao simulador de redes Cisco Packet Tracer

Os simuladores de redes de computadores são ferramentas com diversas aplicações e recursos práticos de infraestrutura de redes. Eles permitem a criação e teste de modelos virtuais de redes em um ambiente controlado; são utilizados para projetar e avaliar diferentes topologias de rede antes de implementá-las, economizando recursos e tempo. Os simuladores são valiosos no campo educacional, auxiliando o conhecimento de conceitos de redes. Pesquisadores também

aproveitam essas ferramentas para avaliar o desempenho de protocolos, algoritmos e estratégias de gerenciamento de tráfego.

Segundo Souza *et al.* (2021), um aspecto fundamental dos simuladores de redes é a capacidade de modelar vários componentes de uma rede, como roteadores, *switches*, servidores, computadores e dispositivos móveis, e também o meio físico, representando cabos, fibras ópticas e comunicação sem fio. A simulação permite configurar esses elementos de acordo com as necessidades do projeto.

A capacidade de gerar tráfego de rede simulado é uma característica dos simuladores. Isso permite a avaliação do desempenho da rede em cenários variados, incluindo a simulação de tráfego de voz, dados, vídeo e até mesmo ataques cibernéticos simulados para testar a segurança e a resiliência da rede.

Simuladores de redes geralmente dão suporte a uma ampla gama de protocolos, como TCP/IP, e permitem a configuração de parâmetros específicos. Fornecem um ambiente para a implementação e teste de novos protocolos e algoritmos, para a pesquisa e o desenvolvimento de tecnologia de rede.

Kurose (2006) explica que a maioria dos simuladores oferece recursos de visualização em tempo real, permitindo que os usuários observem o comportamento da rede à medida que ela é simulada. Essas ferramentas frequentemente incluem recursos de análise, permitindo a coleta de dados de desempenho e métricas de rede, que podem ser fundamentais para a avaliação e otimização da rede. Há uma variedade de simuladores de redes disponíveis, tanto comerciais quanto de código aberto.

O Cisco Packet Tracer é amplamente utilizado para simular redes baseadas em equipamentos da Cisco. O GNS3 é uma ferramenta de código aberto que dá suporte a dispositivos de várias marcas e sistemas operacionais. Para pesquisa acadêmica, o NS-3 é uma estrutura de simulação de código aberto que oferece ampla flexibilidade. Outra opção é o OPNET (Riverbed Modeler), uma ferramenta comercial que ajuda a modelar, simular e analisar redes de computadores complexas. Vamos utilizar o Cisco Packet Tracer.

Trata-se de uma ferramenta de simulação de redes desenvolvida pela Cisco, amplamente utilizada no campo de redes de computadores. Oferece uma interface gráfica intuitiva e uma série de recursos que permitem aos estudantes e profissionais de TI projetar, configurar e solucionar problemas em redes virtuais de forma segura e controlada. Com o Packet Tracer, é possível criar topologias de rede complexas, configurar dispositivos como roteadores e *switches*, e simular o tráfego de dados para entender o funcionamento da rede.

O software é utilizado principalmente em laboratórios de treinamento, ambientes de aprendizado prático. Oferece a flexibilidade de configurar uma variedade de dispositivos de rede, de roteadores a PCs, permitindo a configuração de endereços IP, máscaras de sub-rede, roteamento, VLANs e muito mais. Os usuários também podem avaliar o desempenho da rede, identificar problemas de conectividade e explorar conceitos de redes, como protocolos de roteamento e segurança de rede, por meio de cenários predefinidos, ou criando suas próprias configurações.

Para a elaboração prática, você deverá utilizar a ferramenta Cisco Packet Tracer para criar e testar uma rede de computadores proposta. Primeiramente, você deverá fazer download da ferramenta Cisco Packet Tracer, acessando os seguintes sites: [NetAcad](#) ou [MegaNz](#). Faça o cadastro no site da [Cisco](#); será necessário login para utilizar a versão estudante.

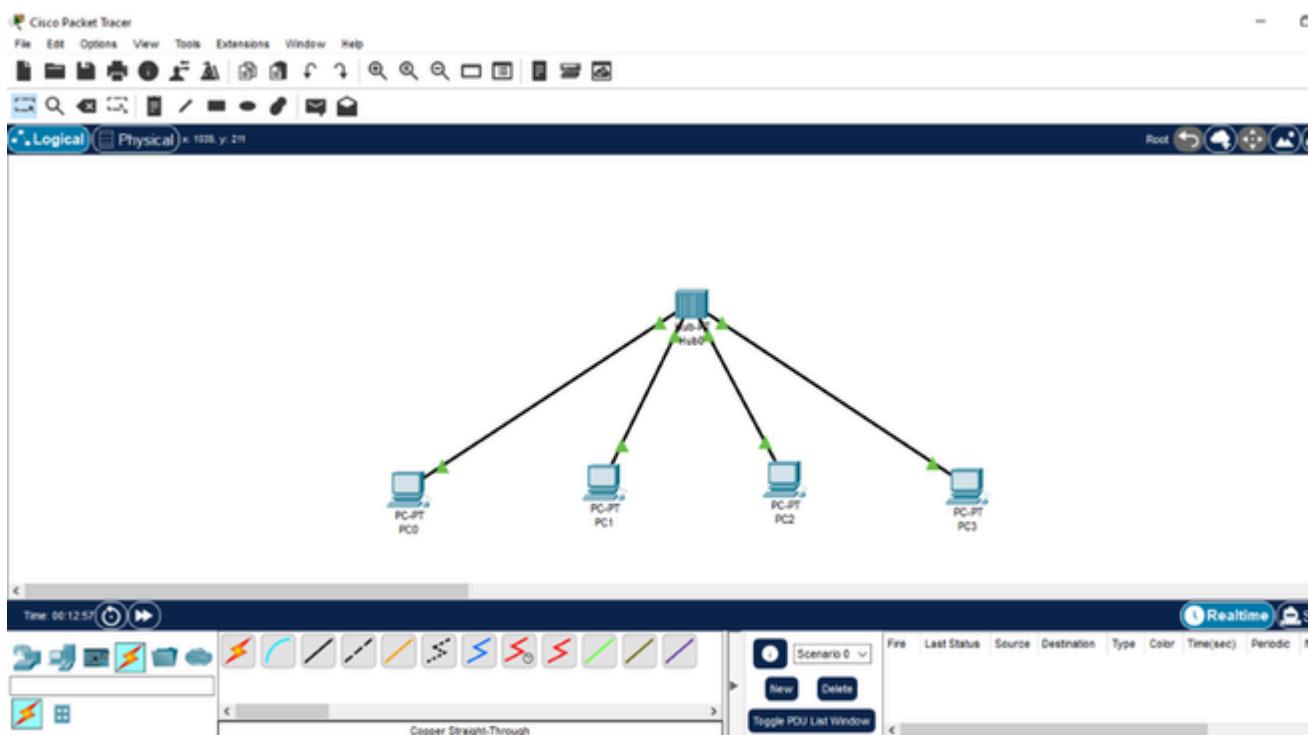


Figura 1 | Home Cisco Packet Tracer. Fonte: captura de tela Home Cisco Packet Tracer.

Nunes (2017) destaca que uma característica essencial do Packet Tracer é sua capacidade de criar um ambiente de simulação completo, incluindo uma variedade de dispositivos de rede, como roteadores, *switches*, computadores e telefones IP. Isso permite que os usuários criem topologias de rede complexas que se assemelham a redes do mundo real, o que proporciona uma experiência prática valiosa. Uma característica particularmente útil do Packet Tracer é a capacidade de simular o tráfego de rede e o comportamento dos pacotes.

Os usuários podem ver como os pacotes são encaminhados, comutados e processados pelos dispositivos de rede. Isso permite uma compreensão profunda de como os dispositivos de rede funcionam e como os protocolos de rede operam na prática. O Packet Tracer está intimamente associado ao programa Cisco Networking Academy, permitindo que estudantes matriculados em cursos da Academy pratiquem e apliquem o conhecimento adquirido diretamente no software. Isso torna o aprendizado mais prático e eficaz.

**Siga em Frente...**

**Construção da infraestrutura de rede no simulador**

Tanembaum, Feamster e Wetherall (2021) explicam que a infraestrutura em redes de computadores abrange o conjunto de elementos físicos e lógicos necessários para estabelecer e manter uma rede de comunicação entre os equipamentos. Os dispositivos de rede, como roteadores, *switches* e firewalls, compõem a estrutura principal da infraestrutura, gerenciando a transmissão de dados. A escolha adequada desses dispositivos e sua configuração atuam no bom funcionamento da rede. Os meios de transmissão atuam com os dados fisicamente transmitidos pela rede. Isso inclui cabos de cobre, fibras ópticas e conexões sem fio, cada um com suas características e aplicações específicas.

A topologia de rede, que pode assumir formas como estrela, anel ou malha, representa o arranjo físico ou lógico dos dispositivos, impactando diretamente na eficiência e na capacidade de expansão da rede. A gestão de rede, por meio de práticas como monitoramento de tráfego e diagnóstico de falhas, contribui para a manutenção da saúde da rede. A implementação de cabeamento estruturado proporciona organização e padronização, facilitando a manutenção e expansão da infraestrutura. Conceitos modernos, como virtualização de rede e redundância, permitem flexibilidade, garantindo disponibilidade contínua.

De acordo com Tanembaum, Feamster e Wetherall (2021), a construção da infraestrutura de rede em simuladores é uma tarefa complexa, para garantir que os ambientes virtuais reflitam com precisão os desafios e cenários encontrados em redes do mundo real. Ao explorar as características avançadas dos simuladores, os profissionais podem aprimorar suas habilidades, testar configurações e desenvolver soluções eficientes para os desafios encontrados nas redes de computadores em um ambiente virtual realista e eficiente para o estudo e teste.

Simuladores geralmente oferecem suporte a uma variedade de topologias de rede, como estrela, anel, barramento, malha, entre outras. Os usuários podem escolher a topologia que melhor se adequa ao cenário que desejam simular. Você poderia configurar uma topologia de rede em estrela, na qual um *switch* central representa a sede da empresa e outros *switches* conectam as filiais. Esses dispositivos podem ser configurados com parâmetros específicos para imitar o comportamento real dos dispositivos de hardware.

Os simuladores permitem a configuração de parâmetros, como endereços IP, máscaras de sub-rede, protocolos de roteamento, tabelas de roteamento e políticas de segurança. Possibilitam a introdução de falhas na rede para avaliar como os dispositivos e protocolos reagem a condições adversas. Podemos simular a desconexão de links, falhas em dispositivos e congestionamentos de tráfego. Introduzindo uma falha em um link de comunicação entre dois roteadores, podemos avaliar a capacidade do protocolo de roteamento se adaptar a mudanças na topologia.

A gerência de redes busca utilizar ferramentas para monitorar o tráfego de rede, analisar estatísticas de desempenho e diagnosticar problemas. Podemos configurar um roteador Cisco no simulador, especificando o modelo do roteador, as interfaces disponíveis, as capacidades de processamento etc. Simuladores permitem a configuração detalhada de protocolos de rede, como OSPF, BGP, RIP, entre outros, incluindo a definição de parâmetros, métricas e políticas de roteamento. Podemos gerar tráfego de voz, vídeo, dados e a avaliação do comportamento da rede sob carga.

Kurose (2006) destaca que ferramentas integradas aos simuladores permitem a análise detalhada do desempenho da rede, monitorização do tráfego, a identificação de gargalos e a otimização de configurações. Eles permitem utilizar ferramentas como Wireshark para analisar pacotes e identificar problemas de comunicação em uma rede simulada. Alguns simuladores incorporam recursos para simular ameaças de segurança, permitindo aos usuários testar políticas de segurança, firewalls e detecção de intrusos.

Passos iniciais para a construção de uma infraestrutura de rede no Cisco Packet Tracer:

- Primeiramente, faça o download do Cisco Packet Tracer no site oficial da Cisco. Instale a ferramenta em seu computador.
- Após a instalação, abra o Cisco Packet Tracer.
- Selecione, arraste e solte os equipamentos. Na barra lateral, você encontrará uma variedade de dispositivos, como roteadores, *switches*, computadores, servidores, entre outros. Arraste e solte os dispositivos desejados para a área de trabalho.
- Use o cabo de conexão disponível no menu lateral para conectar os dispositivos. Clique no dispositivo de origem e, em seguida, no dispositivo de destino para estabelecer uma conexão. Arraste um roteador (exemplo, o "Router 2811") e um *switch* para a área de trabalho. Conecte uma porta do roteador a uma porta do *switch* usando um cabo de conexão.
- Dê um duplo clique no dispositivo para abrir a janela de configuração. Configure os parâmetros, como endereços IP, máscaras de sub-rede e protocolos de roteamento. Por exemplo, configure o endereço IP da interface do roteador e a VLAN no *switch*.
- Após configurar os dispositivos, teste a conectividade. Use comandos de *ping*, por exemplo, para verificar se os dispositivos podem se comunicar. No roteador, use o comando *ping* para testar a conectividade com um dispositivo conectado ao *switch*.
- O Cisco Packet Tracer oferece recursos avançados, como configuração de NAT, ACLs, VLANs, e até mesmo simulação de protocolos mais complexos. Explore esses recursos para obter uma compreensão mais profunda das redes. Configure uma VLAN no *switch* e crie subinterfaces no roteador para lidar com tráfego VLAN.
- Salve o seu projeto.

## Configuração de serviços e protocolos no simulador

Nunes (2017) ressalta que configurar serviços e protocolos em simuladores de redes de computadores tem o objetivo de treinamento e teste. Temos alguns simuladores disponíveis no mercado, como o Cisco Packet Tracer, GNS3, Netkit, Core e EVE-NG. Eles oferecem a capacidade de criar topologias virtuais e emular dispositivos de rede, proporcionando a prática de configurações sem impactar ambientes de produção.

Antes das configurações de serviços e protocolos, é necessário estabelecer a topologia desejada, considerando os roteadores, *switches* e outros equipamentos. Os dispositivos virtuais, que imitam componentes de rede como roteadores, *switches* e servidores, podem então ser

configurados para fornecer serviços específicos. A configuração de roteadores envolve a definição de interfaces, configuração de endereços IP e ajuste de parâmetros de roteamento. Pode incluir protocolos como OSPF, EIGRP ou BGP. Da mesma forma, *switches* podem ser configurados para dar suporte a VLANs e troncos, e para otimizar o encaminhamento por meio de ajustes nas configurações de *spanning tree*.

De acordo com Souza *et al.* (2021), serviços de rede, como DHCP, DNS, FTP e HTTP, podem ser emulados e configurados, seguindo procedimentos semelhantes aos utilizados em ambientes reais. A segurança das configurações também deve ser configurada; há a possibilidade de configurar firewalls e listas de controle de acesso (ACLs) para simular ambientes seguros e testar políticas de segurança. Os simuladores também oferecem recursos, como monitoramento de tráfego, análise estatística de interfaces e simulação de falhas de rede.

A configuração de serviços refere-se à especificação de funcionalidades ou serviços que estarão em execução nos dispositivos de rede simulados. Se você estiver simulando uma rede corporativa, você pode configurar um servidor DHCP para atribuir dinamicamente endereços IP aos dispositivos conectados à rede. Isso pode ser feito definindo parâmetros como faixa de endereços IP, gateway padrão e servidor DNS. Serviços como DHCP e DNS simplificam a gestão da rede, enquanto medidas de segurança, como firewalls e criptografia, são essenciais para proteger a integridade e a confidencialidade dos dados.

Protocolos de comunicação, como TCP/IP, atuam para que os equipamentos de rede possam entender e interpretar corretamente as informações transmitidas. Os endereços IP atribuídos a cada dispositivo possibilitam a identificação única na rede, facilitando o roteamento eficiente dos dados. Os protocolos de comunicação que serão utilizados na simulação, como TCP, UDP, ICMP, OSPF, BGP, etc., podem ser configurados com parâmetros específicos. Na simulação de uma topologia de roteamento, podem-se configurar os roteadores para utilizar o protocolo OSPF, envolvendo a definição de áreas OSPF, configuração de métricas de rota, e outras configurações específicas do OSPF.

Segundo Souza *et al.* (2021), no simulador Cisco Packet Tracer, a configuração de serviços e protocolos pode ser realizada da seguinte maneira. Para configurar um servidor DHCP, você acessaria a configuração do roteador ou *switch*, selecionaria o modo de configuração global e definiria os parâmetros DHCP. Para configurar o protocolo OSPF, você acessaria o modo de configuração de roteador e ativaria o OSPF; em seguida, configuraria detalhes como a ID da área e interfaces associadas. Vamos ao exemplo; nele, configuraremos um roteador, um *switch*, o serviço DHCP e o serviço FTP.

- **Passo 1:** abrindo o Cisco Packet Tracer

Abra o Cisco Packet Tracer no seu computador.

Crie uma nova topologia selecionando “File” e depois “New”.

Arraste um roteador (por exemplo, um “Router 2811”) e um *switch* (por exemplo, um “Switch 2960”) para a área de trabalho.

Conecte os dispositivos arrastando cabos entre as portas, como faria em um ambiente físico.

- **Passo 2:** configurando o roteador:

Clique no roteador para selecioná-lo.

Na janela de configuração, clique em “CLI” para abrir a interface de linha de comando do roteador.

Digite os seguintes comandos para configurar uma interface e o protocolo OSPF:

***enable***

***configure terminal***

***interface gig0/0***

***ip address 192.168.1.1 255.255.255.0***

***exit***

***router ospf 1***

***network 192.168.1.0 0.0.0.255 area 0***

\*\*\*(Esses comandos configuraram a interface GigabitEthernet0/0 com o endereço IP 192.168.1.1/24 e iniciam o OSPF na área 0).

- **Passo 3:** configurando o *switch*:

Clique no *switch* para selecioná-lo.

Na janela de configuração, clique em “CLI” para abrir a interface de linha de comando do *switch*.

Digite os seguintes comandos para ajustar a prioridade do *spanning tree*:

***enable***

***configure terminal***

***spanning-tree vlan 1 priority 4096***

\*\*\*(Esses comandos definem a prioridade do *spanning tree* para a VLAN 1 como 4096.)

- **Passo 4:** configurando o serviço DHCP no roteador:

Clique no roteador para selecioná-lo.

Na janela de configuração, clique em “Config” e, em seguida, em "FastEthernet0/0".

Habilite a interface e configure um pool DHCP:

Habilite a interface.

Escolha um endereço IP para a interface, por exemplo, 192.168.1.1/24.

Abaixo, clique em “DHCP” e configure um pool DHCP, como:

**Pool Name: POOL1**

**Network: 192.168.1.0**

**Subnet Mask: 255.255.255.0**

**Default Router: 192.168.1.1**

- **Passo 5:** configurando o serviço FTP no roteador:

Clique no roteador para selecioná-lo.

Na janela de configuração, clique em “Services” e, em seguida, em “FTP”.

Habilite o serviço FTP e configure um usuário:

Habilite o serviço FTP.

Adicione um usuário, por exemplo, com nome “admin” e senha “secretpassword”.

- **Passo 6:** testando:

Simule um PC ou laptop na topologia.

Configure a interface do PC com DHCP ou manualmente com um endereço IP dentro da faixa definida no pool DHCP.

Abra um cliente FTP em um dispositivo e conecte-se ao roteador usando as credenciais configuradas.

Também contamos com a capacidade de documentar a configuração da rede diretamente no simulador; isso facilita a revisão de configurações, o compartilhamento de conhecimento e a replicação de ambientes específicos. A configuração precisa refletir as características específicas da rede que está sendo simulada. Erros ou configurações inadequadas podem levar a resultados não realistas ou inesperados na simulação. A flexibilidade para configurar serviços e protocolos permite aos usuários criar uma variedade de cenários, desde redes simples até ambientes complexos de larga escala.

## Vamos Exercitar?

Os simuladores de redes, como o Cisco Packet Tracer, são ferramentas valiosas para a formação prática em ambientes controlados; porém, há o questionamento quanto à extensão da fidelidade dessas simulações em relação ao ambiente real de redes de computadores. Existem poucas limitações nos ambientes virtuais de simulação de redes que podem impactar a aplicação prática do conhecimento adquirido. A fidelidade em relação ao ambiente real de redes de computadores, especialmente em situações complexas, pode ser questionada.

A capacidade limitada de simular grandes redes e a falta de imprevisibilidade e eventos não previstos podem reduzir a eficácia das simulações. A representação de ataques cibernéticos pode não abranger completamente a diversidade de ameaças do mundo real. Portanto, os usuários devem estar cientes dessas limitações e buscar complementar a aprendizagem com experiências práticas em ambientes reais para uma preparação mais abrangente, com base no conteúdo aprendido nos simuladores.

A construção e simulação de uma infraestrutura de rede no Cisco Packet Tracer são utilizadas para o desenvolvimento prático de habilidades em profissionais de redes. O simulador oferece a capacidade de configurar dispositivos, analisar o desempenho da rede, introduzir falhas controladas e implementar protocolos. A abordagem prática permite aos usuários testar a rede, diagnosticar problemas, explorar recursos e aprimorar suas habilidades em diversos cenários. Ao salvar projetos, os profissionais podem documentar suas configurações, proporcionando uma valiosa referência para revisão e compartilhamento de conhecimento.

A prática de configuração de redes em ambientes simulados, como exemplificado no Cisco Packet Tracer, desempenha a capacidade de resposta dos profissionais de redes diante de situações de falhas. Ao enfrentar cenários simulados, os profissionais têm a oportunidade de desenvolver habilidades de diagnóstico rápido, praticar estratégias de recuperação e aperfeiçoar conhecimentos de protocolos e serviços. Configurar redes em ambientes simulados proporciona uma compreensão mais profunda de como as tecnologias operam, permitindo a tomada de decisões informadas ao lidar com problemas e implementar soluções eficazes. Torna-se possível utilizar políticas de segurança e redundância, familiarizar-se com diferentes topologias de rede e documentar configurações para facilitar a revisão e a partilha de conhecimento.

## Saiba mais

Os simuladores de redes, como o Cisco Packet Tracer, atuam na formação prática, embora a autenticidade em relação ao ambiente real de redes de computadores suscite questionamentos devido a restrições, como a capacidade limitada de simular redes extensas e a ausência de imprevisibilidade. Embora essas ferramentas permitam a configuração de dispositivos, análise de desempenho e introdução de falhas controladas, a representação de ataques cibernéticos pode não abranger todas as ameaças do mundo real.

É recomendável que os usuários complementem seu aprendizado com experiências práticas em ambientes reais para uma preparação mais abrangente, reconhecendo simultaneamente a eficácia dos simuladores na construção de habilidades de diagnóstico, estratégias de recuperação e conhecimentos de protocolos e serviços em cenários simulados, bem como a capacidade de documentar configurações para revisão e compartilhamento de conhecimento. A seguir, sugerimos mais conteúdo para complementar o conhecimento sobre o tema apresentado:

- Artigo [\*Revista Ibérica de Sistemas e Tecnologias de Informação, da revista Lousada\*](#), disponível na Biblioteca Virtual, no parceiro [\*Proquest\*](#).
- Artigo [\*Análise e gerenciamento de redes usando uma metodologia proativa com Zabbix\*](#), da revista [\*Holos\*](#).
- Filme, Citizenfour (Cidadão quatro). Direção: Laura Poitras. Produção: Dirk Wilutzky. Estados Unidos: The Weinstein Company. 2014. DVD (113 min.) Uma documentarista e um repórter viajam para Hong Kong para o primeiro de muitos encontros com Edward Snowden. Na entrevista, o então analista de sistemas da CIA Edward Snowden apresenta documentos e detalhes sobre o sistema de vigilância global do governo dos EUA pela NSA.
- Para aprofundar o conteúdo, conheça o [\*pequeno curso oficial gratuito através da Academia de Rede Cisco\*](#). É só fazer o cadastro e acompanhar o curso; você pode ir do básico ao avançado.

## Referências

KUROSE, J. F. **Redes de computadores e a internet: uma abordagem top-down**. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

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

SABO, P. H.; CARDIERI, P. Simulador de Subcamada MAC para protocolos do tipo polling. **Revista Ibérica de Sistemas e Tecnologias de Informação**, Lousada, ed. 28, 2020.

SILVA, W.M. C.; *et al.* Análise e gerenciamento de redes usando uma metodologia proativa com Zabbix. **Holos**, Natal, v. 31, n. 8, 2015. Disponível em:  
<https://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/2441>. Acesso em: 5 abr. 2024.

SOUZA, D. C.; *et al.* **Gerenciamento de redes de computadores**. Porto Alegre: Sagah, 2021.

TANEMBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.

## Aula 5

Encerramento da Unidade

### Gerência de redes



#### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Estudante, esta videoaula foi preparada especialmente para você. Nela, você irá aprender conteúdos importantes para a sua formação profissional. Vamos assisti-la?

[Clique aqui](#) para acessar os slides da sua videoaula.

Bons estudos!

### Ponto de Chegada

Olá, estudante! A competência desta Unidade é “Compreender os aspectos gerenciais relacionados à administração e ao gerenciamento das estruturas e dos serviços de redes; compreender como identificar os elementos que podem degradar os serviços; saber como as regras podem garantir qualidade de serviço. Com esses conteúdos, é possível desenvolver uma visão gerencial nas redes de computadores, inclusive utilizando ferramentas de simuladores de redes”. Para desenvolvê-la, é fundamental que você domine os conceitos de gerência.

### Padrões de gerência e elementos: SNMP e o TMN

O gerenciamento de redes, segundo Kurose (2006), envolve a coordenação de dispositivos físicos e lógicos para garantir a confiabilidade, desempenho e segurança dos serviços. Existem duas formas principais de gerenciamento: única gerência, que utiliza ferramentas integradas, e sistemas de gerência, que são ferramentas específicas para monitorar serviços. Três princípios essenciais são destacados: coleta de dados, análise e diagnóstico, e controle. A ISO propõe um modelo de gerenciamento de redes dividido em cinco áreas: desempenho, falhas, configuração, contabilização e segurança.

A arquitetura de gerenciamento de redes inclui entidade gerenciadora (interação do administrador), dispositivo gerenciado (monitorado) e protocolo de gerenciamento (comunicação entre entidade e dispositivos). O SNMP (*Simple Network Information Protocol*), definido pela RFC 3410 e atualizado para SNMPv3 em 2002, é um protocolo usado para monitorar dispositivos e serviços em redes. Envolve nodos gerenciados, estações de gerenciamento, informações de gerenciamento (MIB) e o protocolo SNMP.

O TMN (*Telecommunications Management Network*), de acordo com Tanembaum, Feamster e Wetherall (2021), possui três arquiteturas: informacional (troca de informações entre agentes e gerentes), funcional (definição de funções na gerência de rede) e física (definição de interfaces para garantir compatibilidade entre equipamentos). Cada arquitetura possui blocos específicos, como sistema de suporte à operação, elemento de rede e estação de trabalho. Interfaces, como Q, F, X, G e M, são definidas para assegurar a comunicação entre esses blocos.

## Técnica de *sniffing*

A técnica de *sniffing* (originada da palavra inglesa “*sniff*”, que significa farejar) envolve a interceptação e registro de dados no tráfego de rede para obter informações sobre os dados transmitidos. Administradores de rede utilizam programas de *sniffing* para verificar se uma rede está operando conforme os parâmetros definidos, sendo capazes de capturar e decodificar vários tipos de dados, como e-mails, logins e histórico de internet. Essa prática pode ocorrer em diferentes camadas do modelo OSI, destacando-se nas camadas de enlace de dados e rede.

O ARP Spoofing é uma técnica específica que manipula o protocolo de resolução de endereços (ARP), permitindo ao invasor associar seu próprio endereço MAC a um endereço IP legítimo na rede e redirecionar o tráfego. Além disso, o uso de ferramentas de software, como o Wireshark, possibilita a captura e análise de pacotes de rede, tanto para monitorar a atividade da rede como para potencialmente capturar informações sensíveis, destacando a dualidade dessas técnicas entre a administração legítima e atividades maliciosas na rede.

## Gerência de redes com fluxos IP: IPFIX e NetFlow

A gestão de redes por meio de fluxos IP é uma abordagem que visa à coleta e à análise de informações sobre o tráfego de rede em tempo real; é crucial para monitoramento, resolução de problemas, otimização de recursos e segurança. Duas tecnologias destacadas para essa finalidade são o IPFIX (*Internet Protocol Flow Information Export*) e o NetFlow. O IPFIX, baseado no NetFlow da Cisco, é mais flexível e interoperável, permitindo a coleta de informações de fluxo de diversos dispositivos de diferentes fabricantes, sendo um padrão aberto que promove a interoperabilidade.

Por outro lado, o NetFlow, desenvolvido pela Cisco, é implementado em roteadores e switches para coletar informações detalhadas sobre o tráfego IP, abrangendo dados como endereços IP, portas, protocolos e duração das conexões. Ambas as tecnologias são essenciais para o monitoramento de volumes de dados, tempo, portas, protocolos, segurança de rede e planejamento de capacidade.

## Distribuição, armazenamento, criptografia

A gestão de falhas na distribuição em redes abrange a detecção, notificação e resolução de problemas em diversos pontos, sendo crucial para garantir conectividade e desempenho. A distribuição em redes envolve o compartilhamento de recursos, informações e serviços entre dispositivos interconectados, sendo essencial para uma colaboração eficiente. Medidas de segurança, como autenticação, controle de acesso, firewalls e VPNs, são necessárias para garantir a segurança na distribuição. Redes P2P, balanceamento de carga, CDNs e plataformas globais como redes sociais e IoT exemplificam diferentes formas de distribuição em larga escala. Técnicas de gerenciamento de falhas incluem controle de acesso, SNMP e monitoramento de tráfego de rede.

No contexto de armazenamento em redes de computadores, a gestão de falhas está associada à disponibilidade e integridade dos dados em sistemas de armazenamento, como servidores de arquivos e nuvens. A segurança dos dados é garantida por medidas como criptografia, controle de acesso e backups seguros. Práticas como redundância de dados, backup e recuperação de desastres são essenciais para garantir a continuidade e recuperação de dados em caso de falhas. A criptografia, envolvendo algoritmos simétricos e assimétricos, é fundamental para proteger a confidencialidade, integridade e autenticidade dos dados em redes, sendo aplicada em protocolos como SSL/TLS e VPNs, além de proteger dados em repouso. O gerenciamento eficaz de chaves e a escolha adequada de algoritmos são desafios importantes na implementação da criptografia.

## Falha versus erros

A comunicação de dados em sistemas está sujeita a falhas e erros, podendo ocorrer em equipamentos físicos ou na transmissão, mesmo com testes exaustivos. Os erros de transmissão são categorizados em interferência, distorção e atenuação. Claude Shannon estabeleceu bases matemáticas em 1948 para determinar a capacidade máxima de transmissão por um canal físico. Embora os erros de comunicação não possam ser eliminados completamente, os relacionados à transmissão podem ser detectados e corrigidos.

A detecção de erros implica uma relação de custo-benefício, considerando a sobrecarga no processo de transmissão. Erros em um único bit causam degradação temporária, enquanto erros em rajada afetam o serviço por períodos mais longos, impactando transmissões de streaming e

jogos online. Erros indefinidos resultam em transmissões ambíguas. A correção de erros pode ser realizada antecipadamente com bits redundantes ou por retransmissão.

Falhas em sistemas computacionais, definidas como respostas incorretas em relação ao projeto, podem ser causadas por diversos fatores, incluindo fator humano, meios de transmissão e componentes hardware ou software. Técnicas como tempo médio entre falhas (MTBF) e tempo médio para reparos (MTTR) são utilizadas para prever falhas e tempo de indisponibilidade com base em análise estatística de dados históricos.

## Monitoramento, manutenção e correção

A gestão de falhas e segurança em redes de computadores destaca-se por três componentes essenciais: monitoramento, manutenção e correção. O monitoramento implica na observação diária do desempenho, disponibilidade, integridade e segurança da infraestrutura de rede, utilizando ferramentas para coletar dados sobre tráfego, recursos e configurações. Exemplos incluem a supervisão do uso da largura de banda, análise de logs e monitoramento de segurança.

A manutenção abrange ações preventivas e proativas para garantir eficiência, confiabilidade e segurança, envolvendo atualizações de software, substituição de hardware defeituoso e aplicação de políticas de conformidade. Por fim, a correção é a resposta imediata a eventos de falha ou incidentes de segurança identificados durante o monitoramento, como recuperação de desastres, resposta a incidentes de segurança e correção de erros de configuração. A gestão eficaz desses elementos é fundamental para assegurar a confiabilidade e a integridade das operações de rede.

## Gargalos, tempo de resposta, latência, atrasos e *jitter*

Gargalos em redes de computadores referem-se a pontos de estrangulamento que limitam o tráfego, podendo ocorrer em links de baixa largura de banda, servidores sobrecarregados ou *switches* congestionados. Esses gargalos podem resultar em congestionamento e degradação do desempenho da rede. Para gerenciar gargalos, estratégias como balanceamento de carga podem ser implementadas.

O tempo de resposta, intervalo entre a emissão de um pedido e a recepção de uma resposta, é crucial para eficiência e responsividade na rede. Em aplicações como comércio eletrônico e sistemas de controle em tempo real, baixos tempos de resposta são desejáveis. Otimizar o tempo de resposta envolve melhorar a infraestrutura de rede, usar tecnologias de cache e otimizar o código de aplicação.

Latência, o intervalo de tempo entre o envio e a confirmação do recebimento de um pacote, pode ser calculada como a soma do tempo de transmissão e de propagação. A latência de ida e volta é crucial para diversas aplicações, e reduzi-la é essencial para aprimorar a eficácia das comunicações. Tecnologias como redes de fibra óptica e CDNs ajudam a minimizar a latência.

O *jitter*, variação no tempo e sequência de entrega de pacotes devido à variação na latência, pode afetar a qualidade de serviço em comunicações em tempo real, como videochamadas e chamadas de áudio. Para lidar com o *jitter*, é necessário priorizar o tráfego em tempo real, usar buffers adaptativos e implementar tecnologias de qualidade de serviço (QoS). Interferências na latência e perda de pacotes são influenciadas por fatores como distância entre nodos, distância da antena (em transmissão sem fio) e qualidade dos links (cabeados ou sem fio).

## Indicadores: utilização, tráfego e *throughput*

Na gestão de redes de computadores, ajustar parâmetros de desempenho é desafiador, exigindo avaliação da estrutura da rede e dispositivos. Testes de desempenho incluem injeção de tráfego para analisar aspectos como taxa máxima suportada, tempo de deslocamento de pacotes e tempo de recuperação a falhas. O software Iperf é comumente utilizado para avaliar vazão, latência, *jitter* e perda de pacotes.

Redes devem ser reconfiguráveis devido às mudanças frequentes nos perfis de tráfego, exigindo acomodação de novos serviços, crescimento do tráfego, adoção de novas tecnologias e padronização. O entendimento do perfil de tráfego permite a adequação de recursos para manter a qualidade.

A vazão, ou *throughput*, representa a quantidade de dados transferidos ou processados em um determinado tempo, sendo afetada por fatores como topologia de rede, número de usuários e taxa das interfaces. A perda de pacotes ocorre quando os roteadores não conseguem armazenar pacotes infinitamente, resultando em descarte. A disponibilidade refere-se à capacidade contínua dos dispositivos e redes, enquanto a qualidade de serviço (QoS) busca utilizar recursos de forma eficaz, considerando fatores como latência, *jitter*, perda de pacotes e largura de banda disponível.

## Introdução ao VLAN Trunk Protocol

O VLAN Trunk Protocol (VTP) é essencial em redes que utilizam VLANs para segmentar o tráfego. Desenvolvido pela Cisco, o VTP é um protocolo de camada 2 que simplifica a configuração de VLANs, facilitando sua administração. VLANs, ou redes locais virtuais, permitem criar sub-redes virtuais em *switches*, de modo que cada interface pode representar uma VLAN com seu próprio domínio de broadcast.

O VTP estabelece uma estrutura cliente-servidor, em que as alterações são feitas no servidor e replicadas automaticamente para os clientes. Esse protocolo gerencia informações de configuração de VLAN, como nomes e números, propagando-as para todos os switches na rede. Isso simplifica a adição, remoção ou modificação de VLANs em vários switches, economizando tempo e reduzindo erros humanos.

Operando em modos de servidor, cliente e transparente, o VTP ajuda a evitar inconsistências na configuração de VLANs. O servidor cria e gerencia as informações de VLAN, o cliente as recebe, e o modo transparente repassa as informações sem processá-las localmente. A escolha do modo em um *switch* depende da função que ele desempenha na rede.

## Introdução ao simulador de redes Cisco Packet Tracer

O simulador de redes Cisco Packet Tracer é uma ferramenta amplamente utilizada no campo de redes de computadores. Ele permite a criação e teste de modelos virtuais de redes em um ambiente controlado, facilitando o design e a avaliação de diferentes topologias antes da implementação real. Além de economizar recursos e tempo, o Packet Tracer é valioso na educação, proporcionando aos estudantes uma experiência prática na configuração e solução de problemas em redes virtuais.

Desenvolvido pela Cisco, o Packet Tracer possui uma interface gráfica intuitiva e oferece recursos como simulação de tráfego de dados, configuração de dispositivos como roteadores e switches, e criação de topologias complexas. Ele é comumente utilizado em laboratórios de treinamento para explorar conceitos de redes, protocolos de roteamento, segurança e muito mais.

O software suporta uma variedade de dispositivos, desde roteadores até PCs, permitindo a configuração de endereços IP, máscaras de sub-rede, VLANs e outros parâmetros. Os usuários podem avaliar o desempenho da rede, identificar problemas de conectividade e praticar cenários predefinidos ou criar configurações próprias.

Uma característica essencial do Packet Tracer é sua capacidade de simular o tráfego de rede e o comportamento dos pacotes, proporcionando uma compreensão profunda do funcionamento prático dos dispositivos de rede e dos protocolos. Ele está associado ao programa Cisco Networking Academy, integrando-se ao currículo acadêmico para tornar o aprendizado mais prático e eficaz. Para utilizá-lo, os usuários podem fazer o download no site da Cisco e, se necessário, se cadastrar para obter a versão estudante.

## Construção da infraestrutura de rede no simulador

A construção da infraestrutura de rede no Cisco Packet Tracer envolve a seleção e configuração de dispositivos como roteadores, *switches* e firewalls, assim como a escolha adequada de meios de transmissão, como cabos de cobre, fibras ópticas e conexões sem fio. A topologia de rede, gestão de rede, cabeamento estruturado e conceitos modernos como virtualização e redundância são considerações essenciais.

Em simuladores, como o Cisco Packet Tracer, profissionais de redes podem aprimorar suas habilidades explorando características avançadas. Os simuladores suportam diversas topologias de rede, permitindo a configuração de parâmetros como endereços IP, máscaras de sub-rede, protocolos de roteamento e políticas de segurança. Introduzir falhas na rede, monitorar o tráfego, e analisar o desempenho são aspectos importantes da simulação.

Passos iniciais para construir uma infraestrutura de rede no Cisco Packet Tracer incluem o download e instalação do software, seleção e posicionamento de dispositivos desejados na área de trabalho, conexão dos dispositivos usando cabos disponíveis, configuração de parâmetros como endereços IP e protocolos de roteamento, e teste de conectividade usando comandos como *ping*. Recursos avançados, como configuração de NAT, ACLs e VLANs, podem ser explorados para uma compreensão mais profunda das redes.

## Configuração de serviços e protocolos no simulador

Configurar serviços e protocolos em simuladores de redes, como o Cisco Packet Tracer, tem como objetivo proporcionar treinamento e teste, sem afetar ambientes de produção. Antes das configurações, é necessário estabelecer a topologia desejada com roteadores, switches e outros equipamentos virtuais. A configuração de roteadores envolve a definição de interfaces, endereços IP e parâmetros de roteamento, incluindo protocolos como OSPF, EIGRP ou BGP. *Switches* podem ser configurados para suportar VLANs, troncos e otimizar o encaminhamento através de ajustes nas configurações de spanning tree.

Serviços de rede, como DHCP, DNS, FTP e HTTP, podem ser emulados e configurados, seguindo procedimentos semelhantes aos ambientes reais. A segurança das configurações, como firewalls e listas de controle de acesso (ACLs), também pode ser estabelecida para simular ambientes seguros e testar políticas de segurança. Simuladores oferecem recursos como monitoramento de tráfego, análise estatística de interfaces e simulação de falhas de rede.

A configuração de serviços refere-se à especificação de funcionalidades nos dispositivos de rede simulados, como a configuração de um servidor DHCP para atribuição dinâmica de endereços IP. Protocolos de comunicação, como TCP/IP, devem ser configurados para garantir a interpretação correta das informações transmitidas. No Cisco Packet Tracer, a configuração desses serviços e protocolos envolve comandos específicos para cada dispositivo, como roteadores e switches.

O processo de configuração é exemplificado com passos específicos, desde a abertura do Cisco Packet Tracer até a configuração de um roteador, switch, serviços DHCP e FTP. Testar a

conectividade e documentar a configuração são etapas finais importantes. A flexibilidade para configurar serviços e protocolos permite a criação de uma variedade de cenários, desde redes simples até ambientes complexos de larga escala. Configurações precisas são essenciais para resultados realistas na simulação.

## É Hora de Praticar!



### Este conteúdo é um vídeo!

Para assistir este conteúdo é necessário que você acesse o AVA pelo computador ou pelo aplicativo. Você pode baixar os vídeos direto no aplicativo para assistir mesmo sem conexão à internet.

Sabendo da importância do gerenciamento de redes, explique como a implementação do SNMP pode facilitar a coleta de informações sobre dispositivos e serviços em uma rede. Descreva os três princípios essenciais destacados por Kurose (2006) no gerenciamento de redes. Em seguida, explique como o SNMP (*Simple Network Information Protocol*) contribui para a coleta de dados e monitoramento de dispositivos em uma rede. Destaque também a diferença entre única gerência e sistemas de gerência.

Quanto à técnica de *sniffing*, explique como o ARP Spoofing pode ser usado para redirecionar o tráfego em uma rede e as possíveis consequências dessa prática. Explique o que é a técnica de *sniffing* e como ela pode ser utilizada para monitorar o tráfego em diferentes camadas do modelo OSI. Em seguida, aborde o ARP Spoofing, detalhando como esse ataque manipula o protocolo ARP para redirecionar o tráfego. Destaque também o papel do Wireshark na captura e análise de pacotes de rede.

Considerando a gestão de redes por meio de fluxos IP, explique a diferença entre IPFIX e NetFlow, destacando suas características e aplicações. Descreva a importância da gestão de redes por fluxos IP para o monitoramento em tempo real do tráfego. Em seguida, explique as características do IPFIX e do NetFlow, destacando como cada um contribui para a coleta de informações sobre o tráfego de rede. Apresente também situações em que essas tecnologias são essenciais, como no monitoramento de volumes de dados e na segurança de rede.

Abordando a gestão de falhas na distribuição em redes, explique a importância das medidas de segurança, como autenticação, controle de acesso, firewalls e VPNs. Detalhe a gestão de falhas na distribuição em redes, destacando a importância da segurança na garantia de conectividade e desempenho. Aborde medidas específicas, como autenticação e controle de acesso, e explique como essas medidas contribuem para a segurança na distribuição. Além disso, discuta a aplicação da criptografia na proteção da confidencialidade, integridade e autenticidade dos dados em redes.

Sobre a comunicação de dados sujeita a falhas e erros, explique a diferença entre erros de transmissão e falhas em sistemas computacionais. Descreva os diferentes tipos de erros de transmissão categorizados por Claude Shannon e explique como esses erros podem ser

detectados e corrigidos. Em seguida, discuta as falhas em sistemas computacionais, destacando fatores que podem causá-las e técnicas, como MTBF e MTTR, utilizadas para prever falhas e seu tempo de indisponibilidade.

Você pode responder a essas questões com base nas informações fornecidas no texto e em seu conhecimento sobre redes de computadores.

Discutir a técnica de *sniffing*, como o ARP Spoofing, enfatizando sua relevância para a compreensão das redes, é muito importante. Podemos pensar na reflexão sobre a necessidade de equilibrar esses conhecimentos com uma abordagem ética, evitando seu uso indevido para atividades maliciosas. A ênfase na segurança em redes, abordando medidas como criptografia e controle de acesso, suscita a reflexão sobre os desafios práticos na implementação em ambientes dinâmicos e vulneráveis a ameaças cibernéticas em constante evolução.

Como garantir a efetividade dessas medidas sem comprometer a acessibilidade e a colaboração essenciais em ambientes empresariais? Essas reflexões destacam a complexidade ética e operacional associada à gestão de redes e à segurança da informação em um contexto tecnológico em evolução constante.

Estudante, agora veja a proposta de resolução para este estudo de caso.

Os três princípios essenciais no gerenciamento de redes, conforme Kurose (2006), são: coleta de dados, análise e diagnóstico, e controle. A coleta de dados refere-se à obtenção de informações sobre o desempenho, configuração e estado dos dispositivos em uma rede. A análise e diagnóstico envolvem a interpretação desses dados para identificar padrões, tendências e possíveis problemas.

O controle refere-se à implementação de ações corretivas com base nas análises realizadas. O SNMP, por sua vez, é um protocolo amplamente utilizado para facilitar a coleta de dados em redes. Ele opera em um modelo cliente-servidor, no qual dispositivos gerenciados, como roteadores e switches, são monitorados por uma estação de gerenciamento. A estação de gerenciamento emite solicitações SNMP para os dispositivos gerenciados, que respondem com informações sobre seu estado e desempenho.

O SNMP utiliza a MIB (*Management Information Base*) para organizar e representar as informações coletadas. A diferença entre única gerência e sistemas de gerência reside no escopo e na abordagem. A única gerência utiliza ferramentas integradas para gerenciar todos os aspectos da rede de forma centralizada. Já os sistemas de gerência são ferramentas específicas para monitorar serviços, proporcionando uma abordagem mais especializada e modular.

A técnica de sniffing consiste na interceptação e registro de dados no tráfego de rede para obter informações sobre as comunicações. Ela pode ser utilizada para monitorar o tráfego em diferentes camadas do modelo OSI, destacando-se nas camadas de enlace de dados e rede. Administradores de rede utilizam programas de *sniffing*, como o Wireshark, para verificar se uma rede está operando conforme os parâmetros definidos. Esses programas são capazes de capturar e decodificar vários tipos de dados, como e-mails, logins e histórico de internet.

O ARP Spoofing é uma técnica específica de *sniffing* que manipula o protocolo de resolução de endereços (ARP). Nesse ataque, o invasor associa seu próprio endereço MAC a um endereço IP legítimo na rede, redirecionando o tráfego destinado a esse endereço para o seu. Isso pode ser usado para interceptar informações sensíveis, como senhas, antes que cheguem ao destino pretendido.

O Wireshark desempenha um papel fundamental na captura e análise de pacotes de rede. Ele permite aos administradores visualizar o tráfego em tempo real, identificar padrões, analisar protocolos específicos e detectar possíveis problemas na rede. O Wireshark é uma ferramenta poderosa tanto para administração legítima quanto para a detecção de atividades maliciosas na rede.

A gestão de redes por meio de fluxos IP é essencial para o monitoramento em tempo real do tráfego de rede, proporcionando informações valiosas para a resolução de problemas, otimização de recursos e segurança. O monitoramento de fluxos IP permite analisar o tráfego com base em informações como endereços IP, portas, protocolos e duração das conexões, proporcionando uma visão abrangente do comportamento da rede.

O IPFIX (*Internet Protocol Flow Information Export*) e o NetFlow são tecnologias fundamentais nesse contexto. O IPFIX, sendo um padrão aberto baseado no NetFlow da Cisco, é mais flexível e interoperável. Ele permite a coleta de informações de fluxo de diversos dispositivos de diferentes fabricantes, promovendo a interoperabilidade e facilitando a implementação em ambientes heterogêneos.

O NetFlow, desenvolvido pela Cisco, é implementado em roteadores e *switches* para coletar informações detalhadas sobre o tráfego IP. Ele abrange dados como endereços IP, portas, protocolos e duração das conexões, fornecendo insights valiosos para a administração da rede. Ambas as tecnologias são essenciais para o monitoramento de volumes de dados, tempo, portas, protocolos, segurança de rede e planejamento de capacidade.

A gestão de falhas na distribuição em redes é crucial para garantir conectividade e desempenho contínuo. Envolve a detecção, notificação e resolução de problemas em diversos pontos da infraestrutura de rede. Medidas específicas, como autenticação, controle de acesso, firewalls e VPNs, desempenham um papel essencial nesse processo. A autenticação e o controle de acesso garantem que apenas usuários autorizados tenham acesso aos recursos da rede, reduzindo o risco de acessos não autorizados.

Firewalls são utilizados para controlar o tráfego de entrada e saída da rede, prevenindo ameaças externas e monitorando atividades suspeitas. VPNs (redes privadas virtuais) fornecem uma camada adicional de segurança ao estabelecer conexões seguras sobre redes públicas. A criptografia desempenha um papel crucial na segurança dos dados durante a distribuição em redes. Ela protege a confidencialidade, integridade e autenticidade dos dados, aplicando algoritmos criptográficos simétricos e assimétricos.

Em protocolos como SSL/TLS e VPNs, a criptografia é fundamental para garantir que as informações transmitidas sejam seguras e não suscetíveis a interceptação ou alteração por partes não autorizadas. A gestão eficaz de chaves e a escolha adequada de algoritmos são desafios importantes na implementação bem-sucedida da criptografia.

Claude Shannon categorizou os erros de transmissão em três principais tipos: interferência, distorção e atenuação. A interferência ocorre quando sinais de diferentes fontes se misturam, causando ruídos que podem corromper os dados. A distorção é causada pela variação na intensidade do sinal, resultando em alterações na forma de onda. A atenuação refere-se à perda gradual de intensidade do sinal à medida que se propaga pelo meio de transmissão. A detecção e correção de erros de transmissão são cruciais para garantir a integridade dos dados.

Técnicas como códigos de detecção de erro, como o CRC (*Cyclic Redundancy Check*), são utilizadas para identificar a ocorrência de erros durante a transmissão. Além disso, em casos nos quais a correção é necessária, técnicas como códigos de correção de erro, como o código de Hamming, podem ser aplicadas. As falhas em sistemas computacionais são respostas

incorretas em relação ao projeto e podem ser causadas por diversos fatores, incluindo fatores humanos, meios de transmissão e componentes hardware ou software.

Técnicas como tempo médio entre falhas (MTBF) e tempo médio para reparos (MTTR) são utilizadas para prever falhas e seu tempo de indisponibilidade com base em análise estatística de dados históricos. O MTBF representa o intervalo médio entre falhas, enquanto o MTTR representa o tempo médio necessário para reparar uma falha. Essas métricas são essenciais para a gestão proativa de falhas e a maximização da disponibilidade do sistema.

## GERÊNCIA DE REDES

**1**

### GERÊNCIA DE REDES E PADRÓES

Essenciais para a manutenção eficaz; utilizam padrões como SNMP e TMN para monitoramento. O sniffing OSI e SMI analisam o tráfego. Fluxos IP, através de IPFIX e NetFlow, oferecem coleta eficiente de dados.

**2**

### GERÊNCIA DE FALHAS E SEGURANÇA

Assegura estabilidade, distribuição, armazenamento e criptografia. Falhas e erros necessitam de monitoramento contínuo, manutenção proativa e correção ágil para garantir a integridade e a segurança.

**3**

### DESEMPENHO, CONFIGURAÇÃO E CONTABILIZAÇÃO

Visam otimizar sistemas, lidando com desafios como gargalos e latência. Utilização de throughput é essencial; o VLAN Trunk Protocol facilita a configuração de redes virtuais.

**4**

### SIMULANDO REDES DE COMPUTADORES

O simulador Cisco Packet Tracer é usado para construir e configurar redes, permitindo a prática segura de serviços e protocolos. Isso facilita a aprendizagem em ambientes controlados.

KUROSE, J. F. Redes de computadores e a internet: uma abordagem top-down. 3<sup>a</sup> ed. São Paulo: Pearson, 2006.

# REDES DE COMPUTADORES

NAKAMURA, E. T. **Segurança da informação e de redes.** Londrina: Editora e Distribuidora Educacional S.A., 2016.

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

OLIVEIRA, D. B.; LUMMERTZ, R. S.; SOUZA, D. C. **Qualidade e desempenho de redes.** Porto Alegre: Sagah, 2019.

SOUZA, D. C.; *et al.* **Gerenciamento de redes de computadores.** Porto Alegre: Sagah, 2021.

TANEMBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores.** 6<sup>a</sup> ed. São Paulo: Pearson/Porto Alegre: Bookman, 2021.