



# **FACULDADE SENAC**

## **CASCABEL - PR**

# REDES DE COMPUTADORES



**Ementa:** Introdução a redes de computadores. Histórico e evolução das redes.

Classificação: redes locais e remotas. Topologias de rede. Conceitos de comunicação de dados, bases numéricas e codificação de dados. Protocolos.

Modelo de referência OSI. Modelo de referência TCP/IP. Camadas física, de enlace de dados, de rede, de transporte e de aplicação. Arquitetura de hardware e armazenamento, processamento distribuído, comunicação de dados e disponibilização de serviços. Endereços de rede, portas, sockets, datagramas.

Projeto. Modos de endereçamento, endereçamento de redes e análise de tráfego de rede TCP/IP.

A rede de computadores quebra barreiras geográficas e possibilita que informações sejam compartilhadas entre pessoas e empresas do mundo inteiro, disponibilizando informação local ou globalmente, e são úteis para a prestação de diversos serviços essenciais.



➤ exemplos de aplicações para a rede

- **Compartilhamento de arquivos:** permite compartilhar arquivos de dados por meio de uma rede;
- **Acesso e utilização de aplicativos:** permite acessar e utilizar aplicações através da rede;
- **Compartilhar hardware:** possibilita aos usuários de uma rede compartilhar dispositivos de hardware, como impressoras e discos rígidos.



## ➤ exemplos de aplicações para a rede

- **Modelo cliente-servidor:** permite que os dados sejam armazenados em servidores, onde os dispositivos do usuário final (clientes) possam acessar essas informações.
- **Voz sobre IP (VoIP):** permite aos usuários enviar dados de voz por meio de protocolos de Internet;
- **Comunicação:** pode incluir vídeo, imagens, texto e voz;
- **E-commerce:** permite aos usuários vender e comprar produtos e serviços pela internet;
- **Jogos:** permite que usuários joguem simultaneamente, mesmo estando em locais diferentes.



# EQUIPAMENTOS DE REDE

## Placa de Rede



# EQUIPAMENTOS DE REDE

Hub



# EQUIPAMENTOS DE REDE

## Switch



# EQUIPAMENTOS DE REDE

## Roteador



# EQUIPAMENTOS DE REDE

## Access Point



# EQUIPAMENTOS DE REDE

## Bridge



# O INICIO DE TUDO

Os primeiros estudos relacionados a redes de computadores ocorreram no início da década de 1960. As pesquisas foram realizadas por diferentes grupos, sendo eles:

**Leonardo Kleinrock** (1961 a 1964), por meio de seus estudos de doutorado no MIT, desenvolveu uma técnica de comutação de pacotes em rajadas.

Paul Baran (1964), deu continuidade aos estudos de Kleinrock e efetuou a transmissão segura de voz em redes militares.

- Em 1967 surge a Arpanet por meio dos estudos desenvolvidos no MIT.

Em 1969, na Universidade da Califórnia em Los Angeles (UCLA), foi instalada a primeira rede com a capacidade de transmissão de mensagens por meio de interfaces.

Em 1972 a Arpanet possuía 15 nodos (“nodos” é o termo usado para designar nós de redes) e havia desenvolvido o primeiro protocolo de comunicação em rede, chamado NCP (Network Control Protocol).

## **Surgimento de mais redes – 1972 a 1980**

Uma década após o surgimento das primeiras técnicas aplicadas em de redes de computadores, os pesquisadores ao redor do mundo tomaram conhecimento delas nos congressos e nas conferências que discutiam comunicação.

## Aumento do número de redes – 1980 a 1990

Além dos interesses militares estratégicos, o mercado vislumbrava uma potencial forma de alavancar milhares de dólares.

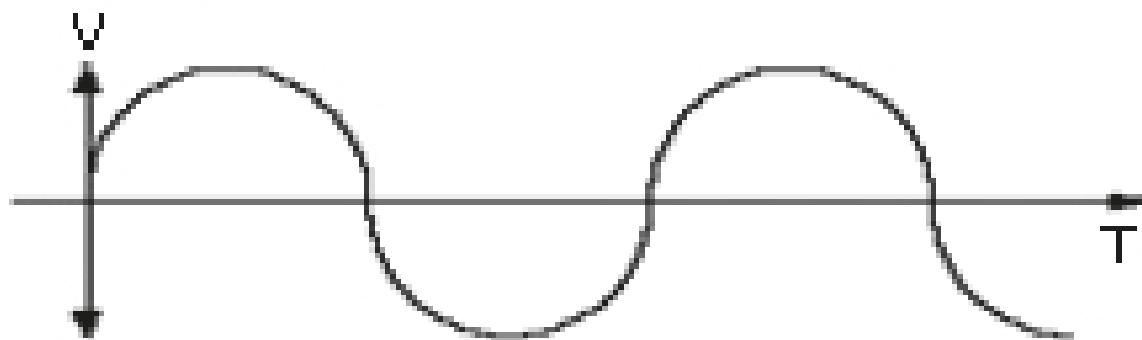
## SINAL ANALÓGICO

Segundo Tanenbaum (1997), os sinais analógicos são ondas eletromagnéticas que assumem infinitos valores ao longo do tempo.

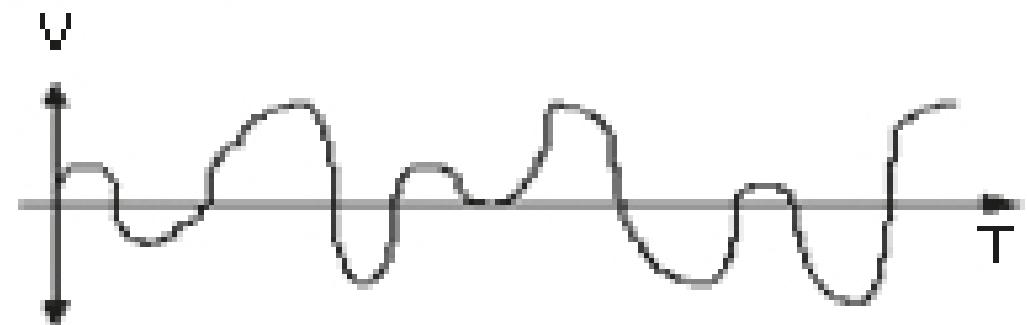
Este sinal é representado por uma onda senoidal com as seguintes características:

- **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.

**Sinal Senoidal**



**Sinal de Voz**



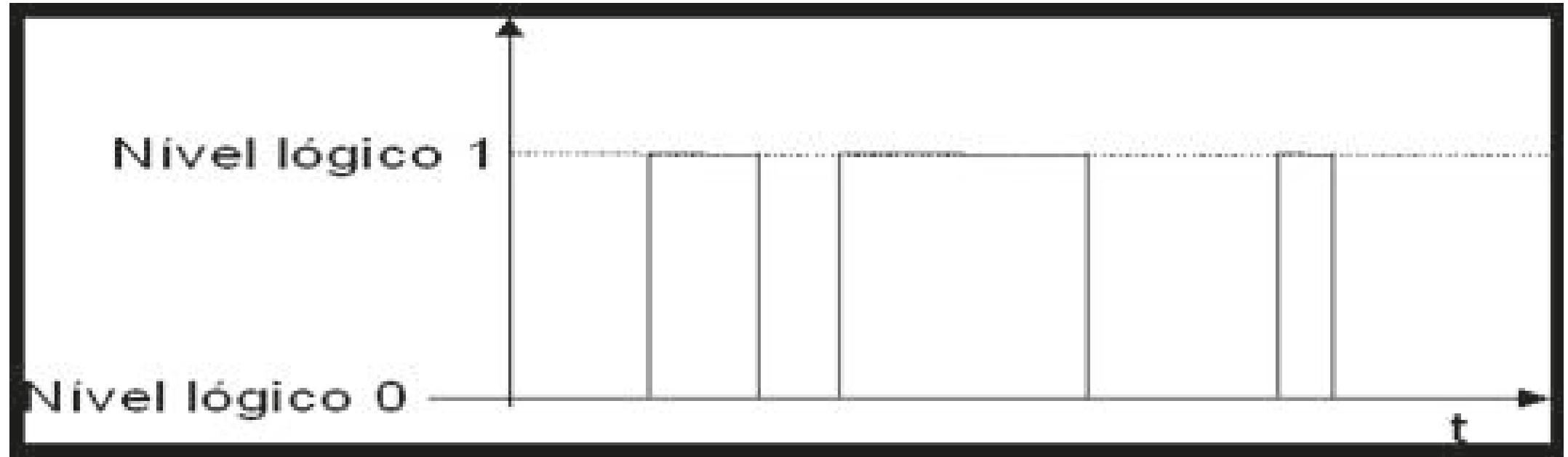
## SINAL DIGITAL

Em contrapartida, o sinal digital é representado por 0 s e 1 s, ou seja, de forma binária. A representação dos seus valores é dada como discreta ao longo do tempo e amplitude. Com isso, é possível diminuir a taxa de oscilação, fenômeno este responsável pelo aumento da qualidade de serviço.

Quando ocorre uma transmissão de dados, ocorre um processo de codificação (digitalização) desse sinal. Com isso:

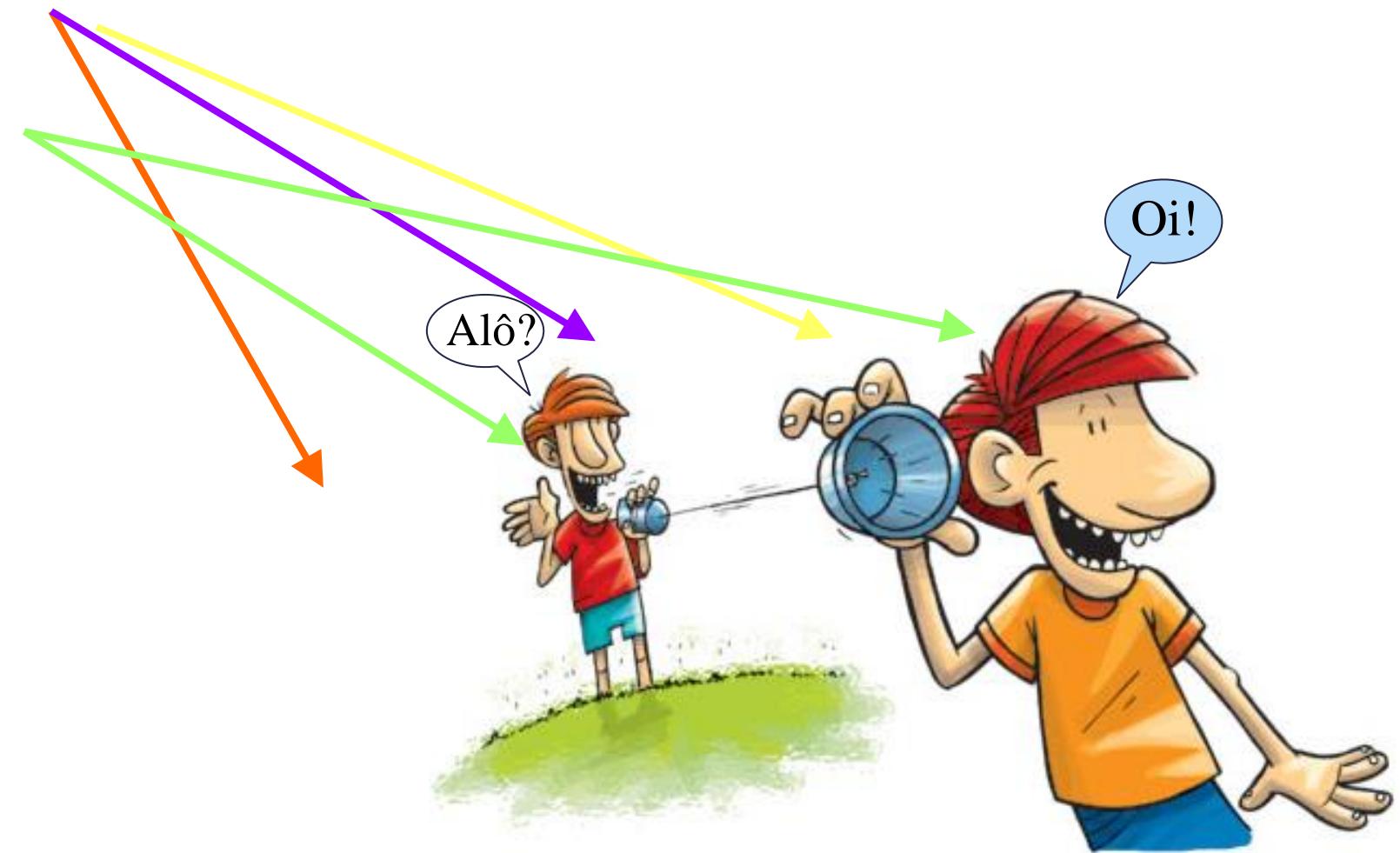
Os sinais digitais não sofrem degradação dos serviços por interferência ou ruídos.

- Pode-se transmitir maior quantidade de informações.



# Sistema Básico de Comunicação

- Transmissor
- Meio
- Mensagem
- Receptor



Ao utilizar esta tecnologia, uma série de fatores precisa ser levada em conta para garantir eficiência na comunicação. Alguns deles:

- custo
- taxas de transmissão
- facilidade de acesso
- padronização
- segurança
- portabilidade

# CONCEITOS BÁSICOS

**bit** – é a menor unidade de informação que pode ser armazenada ou transmitida. Um bit pode assumir somente dois valores: 0 ou 1

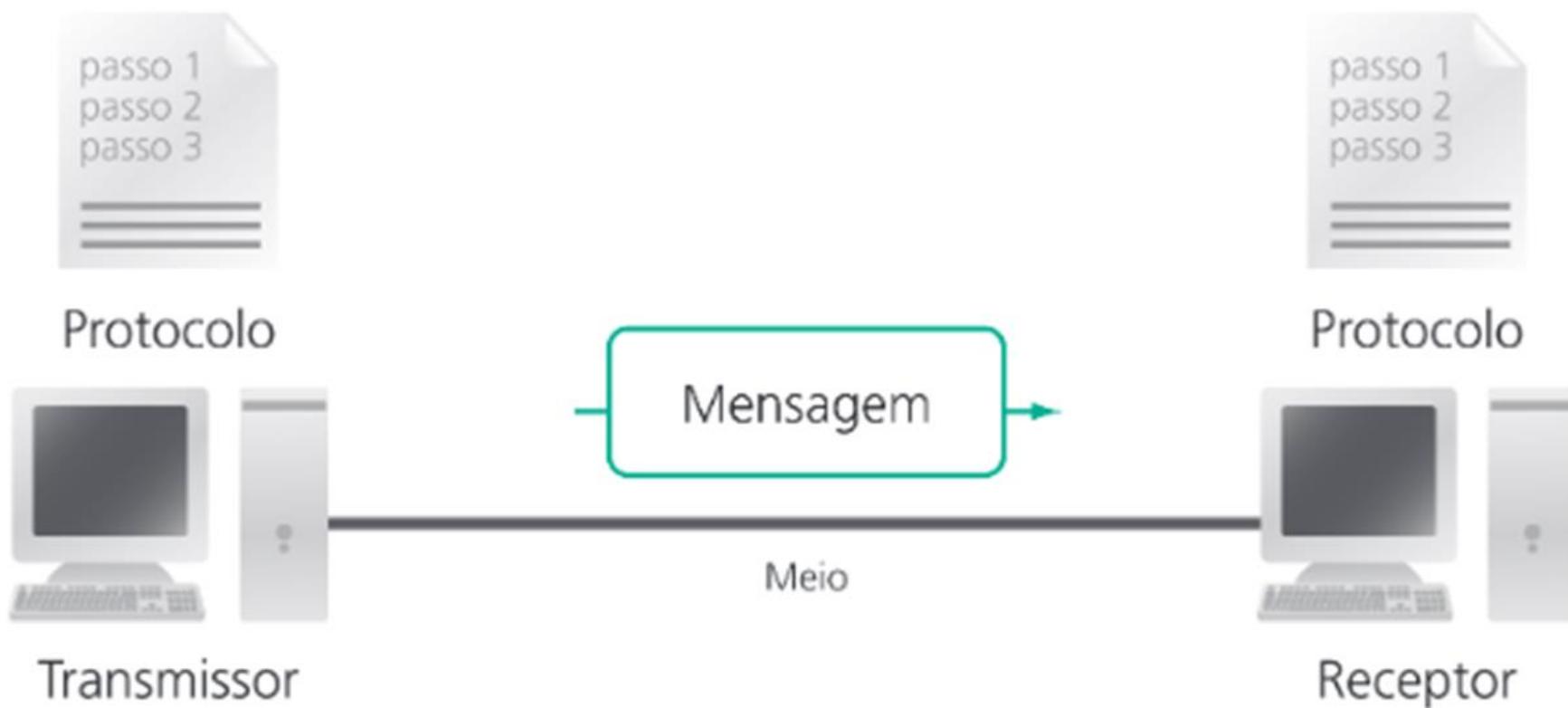
**BYTE** – um byte é composto por 8 bits

Taxa de Transmissão (Bit rate ou bitrate) – é a taxa de bits ou taxa de transferência de bits. Nas telecomunicações e na computação, o bit rate (às vezes escrito como bitrate) é o número de bits convertidos ou processados por unidade de tempo. O bit rate é medido em 'bits por segundo' (bps ou b/s), muitas vezes utilizado em conjunto com um prefixo SI (Sistema Internacional de Unidades), como kbps, Mbps, Gbps, etc...

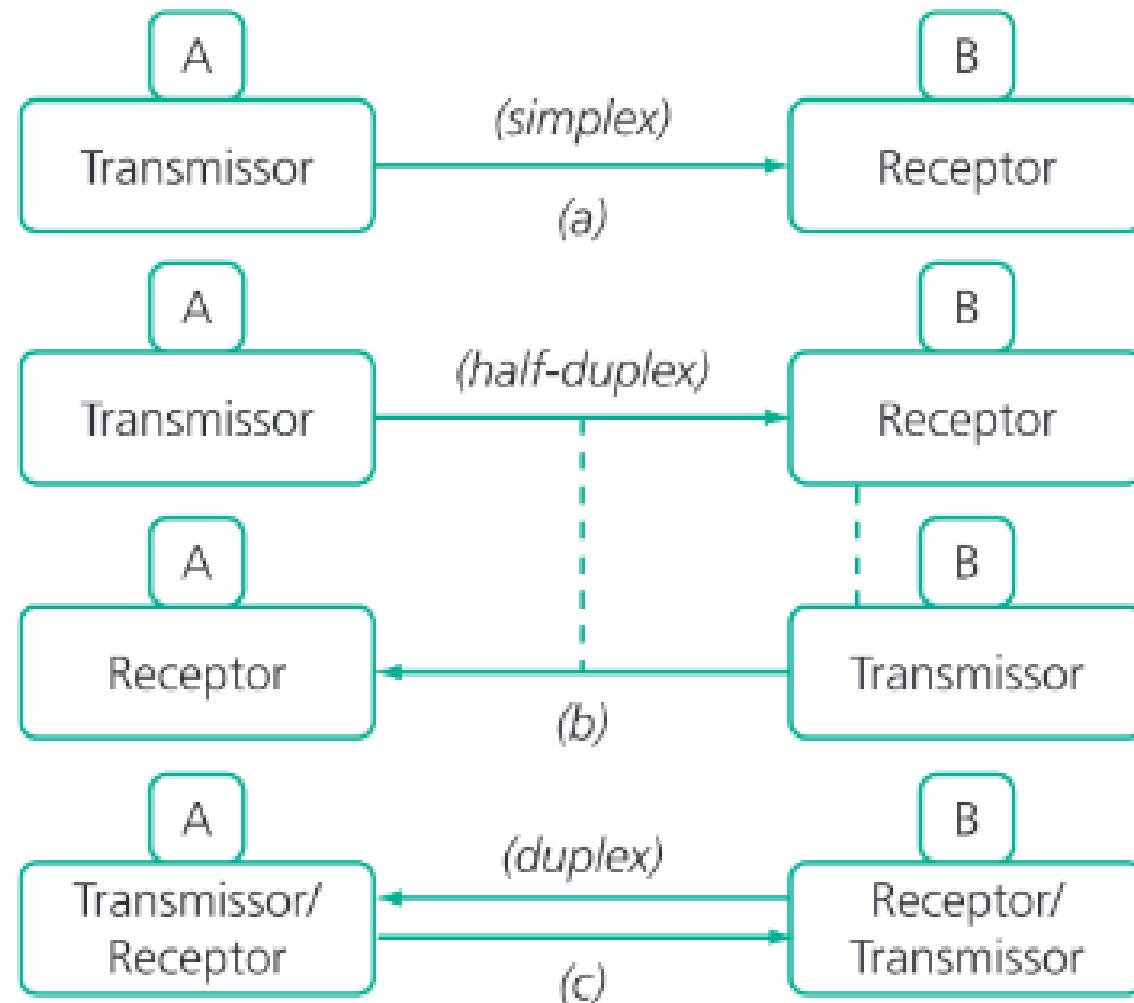
Uma rede de computadores vai muito além de uma simples conexão de cabos e placas.

Há necessidade de uma série de protocolos para regular a comunicação entre todos os níveis, desde o programa que está sendo utilizado até o tipo de cabo instalado





# TIPOS DE TRANSMISSÃO DE DADOS



# **ABRANGÊNCIA DA REDES**

## **PAN (Personal Area Network)**

Uma rede de área pessoal (PAN) conecta dispositivos eletrônicos dentro da área imediata de um usuário. O tamanho de uma PAN varia de alguns centímetros a alguns metros. Um dos exemplos mais comuns do mundo real de uma PAN é a conexão entre um fone de ouvido Bluetooth e um smartphone. PANs também podem conectar notebooks, tablets, impressoras, teclados e outros dispositivos computadorizados.

## **LAN (Local Area Network)**

É uma rede local onde os dispositivos se localizam no mesmo espaço físico.

As LANs tem três características que as distinguem de outros tipos de redes:

- (1) tamanho
- (2) tecnologia de transmissão
- (3) topologia.

As LANs tem um tamanho restrito, o que significa que o pior tempo de transmissão é limitado e conhecido com antecedência. O conhecimento desse limite permite a utilização de determinados tipos de projetos que em outras circunstâncias não seriam possíveis, além de simplificar o gerenciamento da rede.

LAN - Backbone do prédio

LAN - 2º andar



LAN - 1º andar



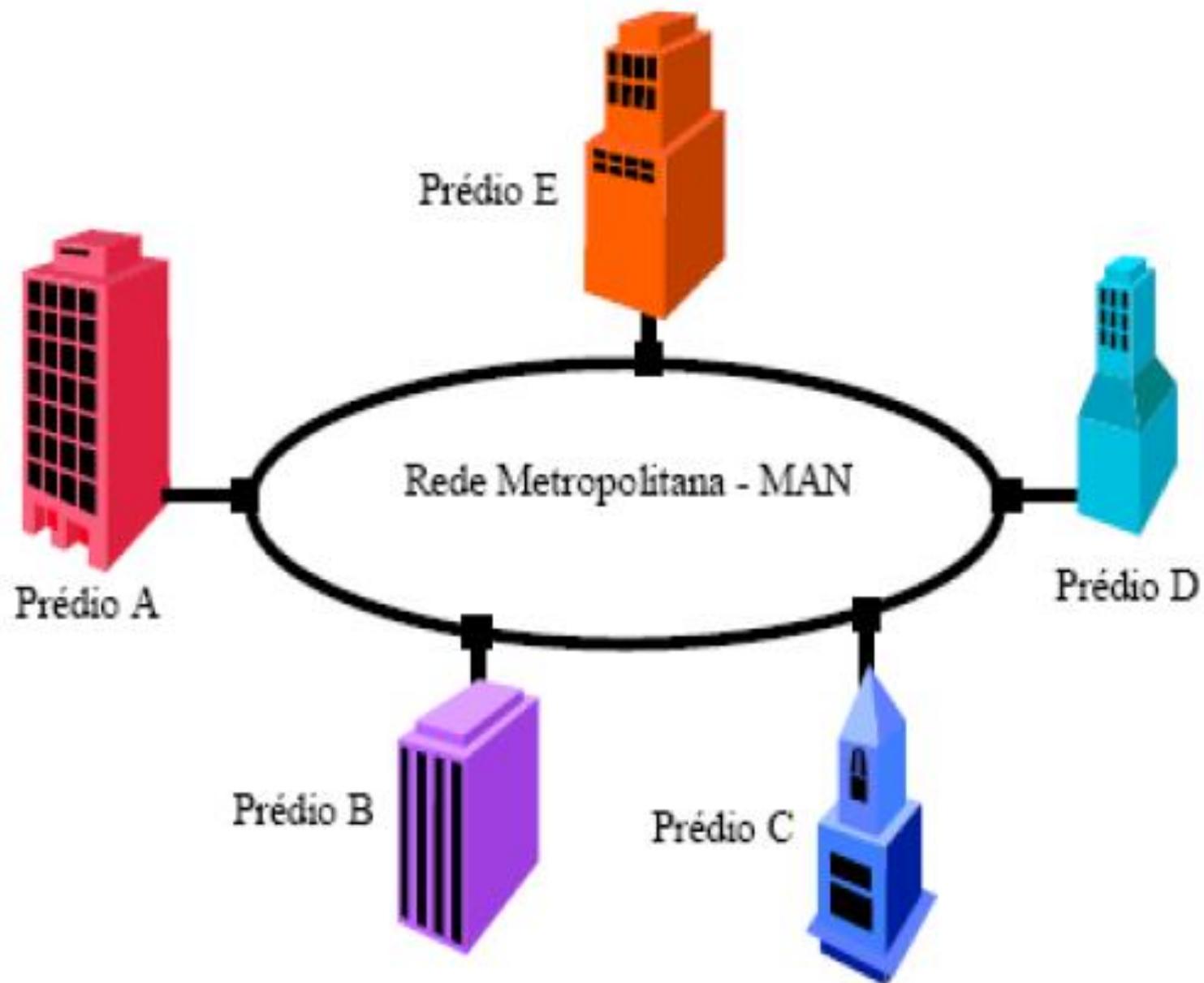
LAN - Térreo



Servidores  
corporativos

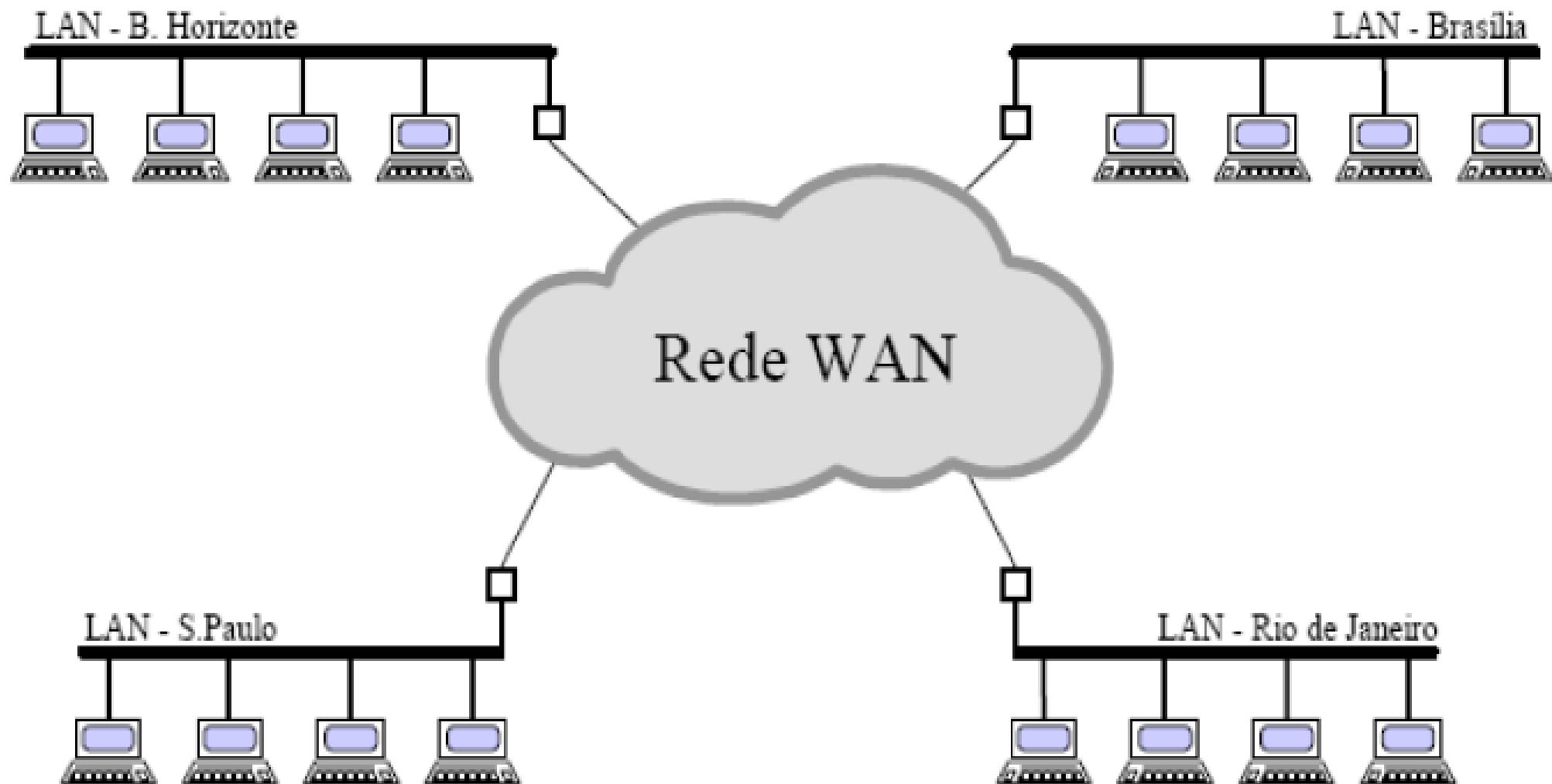
# **MAN (Metropolitan Area Network)**

É uma rede de computadores que conecta computadores dentro de uma área metropolitana, que pode ser uma única grande cidade, várias cidades e vilas, ou qualquer área com vários edifícios. Uma MAN é maior que uma rede local (LAN) mas é menor que uma rede de longa distância (WAN). As MANs não precisam estar em áreas urbanas; o termo "metropolitano" implica o tamanho da rede, não a demografia da área que ela atende.



## **WAN (Wide Area Network)**

Está é mais conhecida como a internet por ser uma grande rede que possui inúmeras sub redes,que podem estar localizada em qualquer lugar do planeta.



# **TOPOLOGIA DE REDE**

A topologia de rede diz respeito à forma como são organizados os elementos de uma rede de comunicação. O conceito é aplicado tanto de forma física, como logicamente. As topologias de rede ajudam a trazer mais organização, performance e usabilidade, qualidades cada vez mais necessárias ao implementar uma rede de computadores.

O conceito é interessante porque determina a forma como as máquinas vão se conectar entre si, considerando os hubs e switches. Muitas vezes, o conceito não é levado em consideração, o que traz uma série de problemas de sincronização de dados e erros na comunicação.

# **TOPOLOGIA DE REDE FÍSICA E LÓGICA**

# FÍSICA

A topologia de rede física diz respeito aos elementos físicos que compõem a conexão de rede. Ou seja, fala sobre a disposição de cabos e dispositivos conectados. Ao falar sobre a forma física, estamos nos referindo às estratégias de organização físicas, levando em conta a disposição das máquinas no espaço físico, bem como a conexão de cabos.

## LÓGICA

Já a representação lógica diz respeito à forma como a rede trabalha. Ou seja, aqui entendemos e aprimoramos a interface, softwares, entre outros quesitos.

O objetivo da topologia de rede lógica é conectar os nodes da rede, para trazer uma usabilidade ainda mais eficiente, ágil e intuitiva.

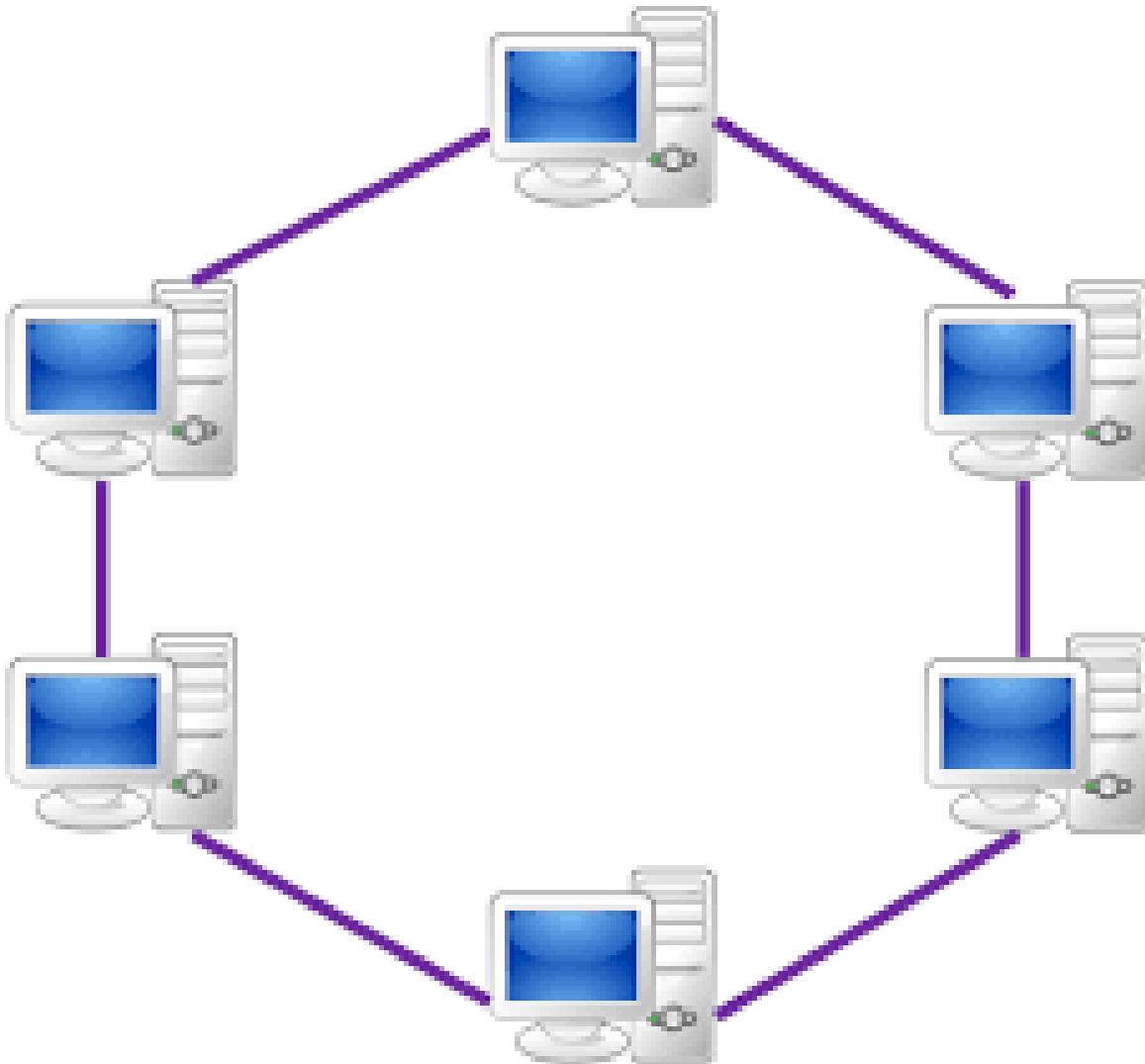
# **TIPOS DE TOPOLOGIA DE REDE**

## **ANEL**

Como o nome sugere, a topologia anel é realizada de forma circular. Isso significa que cada uma das máquinas possui duas máquinas vizinhas, pelas quais é realizada a transmissão de dados. Ou seja, é um círculo de dispositivos conectados, com fluxo de dados unidirecional e repasse por cada nó até chegar ao seu destino.

## **ANEL**

Esse tipo de topologia é bem eficiente para transmissão de dados sem erros, tem grande confiabilidade e pode ser implementada em grandes redes. Contudo, a falha de um único dispositivo pode prejudicar a estabilidade da rede inteira, o que aumenta os riscos de delay.



## **ÁRVORE**

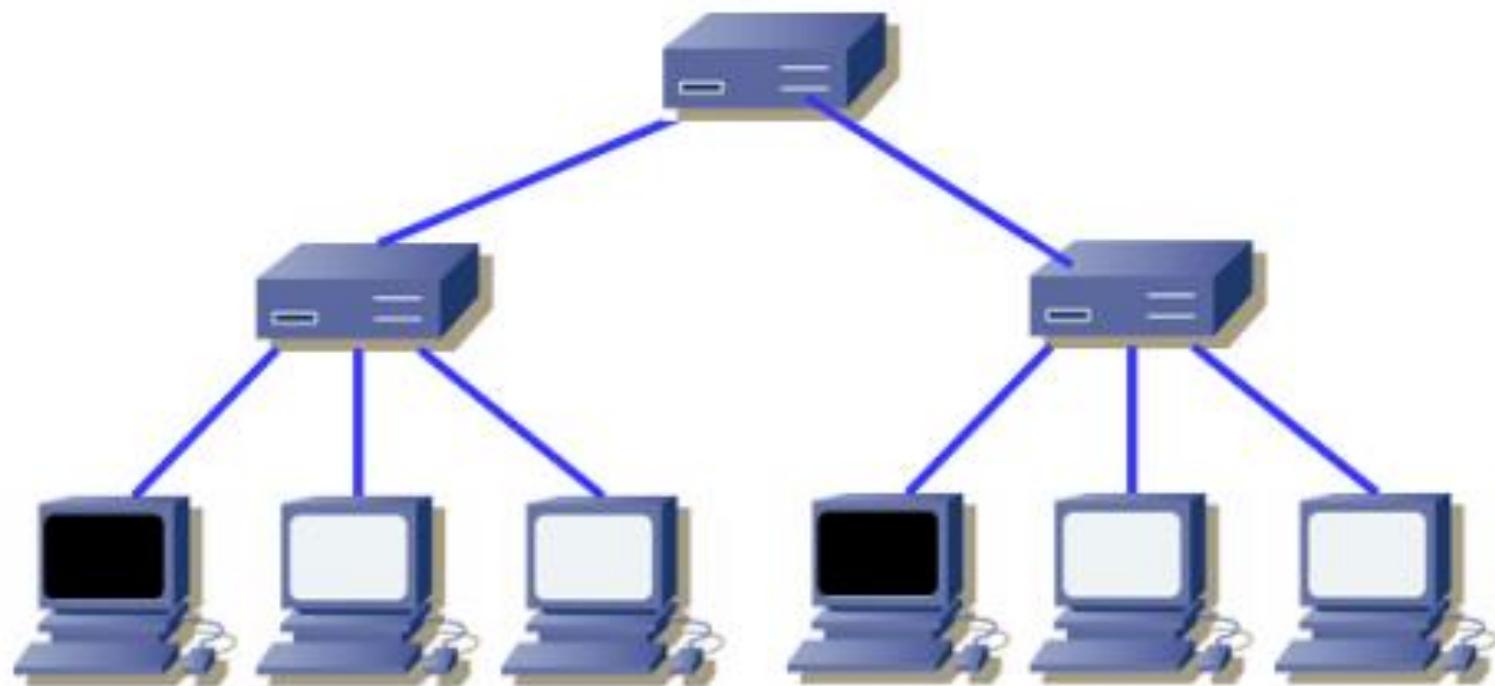
Esta topologia é baseada em switches ou dispositivos de ligações, os quais permitem uma estruturação hierárquica de várias redes ou sub-redes.

## **Vantagens:**

- Podem ser facilmente expandidas;
- Possibilidade de redundância;
- Desempenho elevado;
- Segurança aprimorada.

## **Desvantagens:**

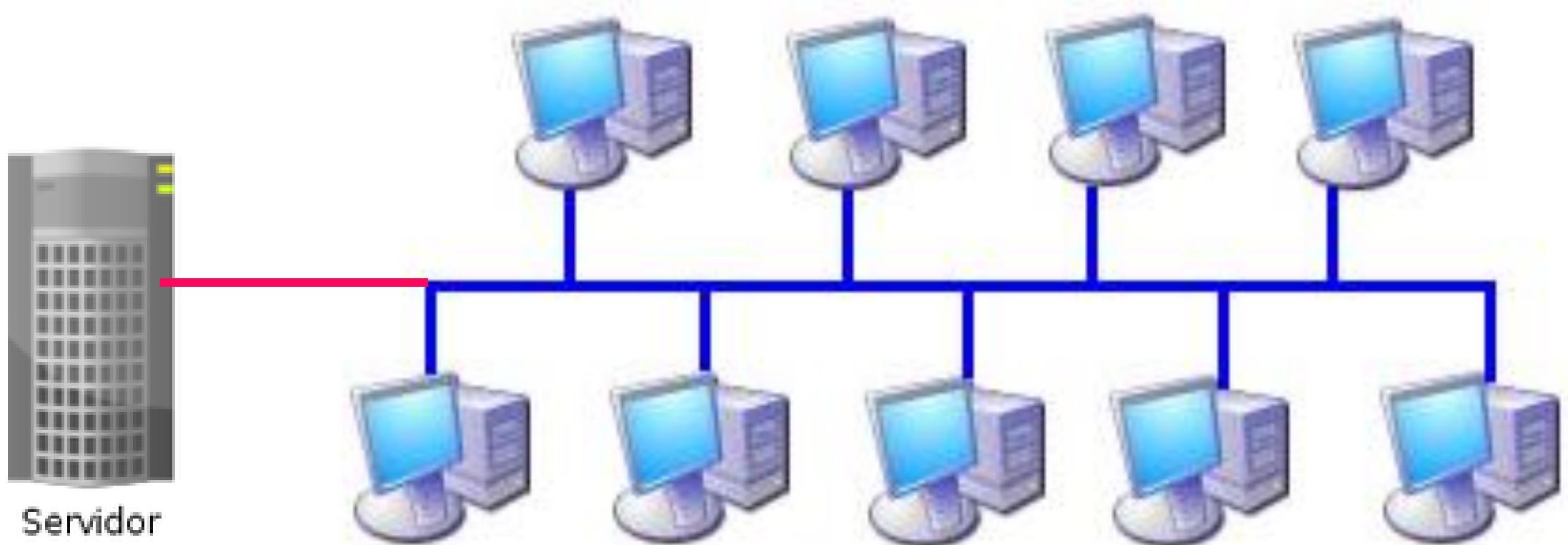
- Se o elemento centralizador falhar, o sistema fica comprometido;
- Maior custo, devido ao elevado número de concentradores



## BARRAMENTO

Um padrão que traz simplicidade e praticidade. Neste tipo, todos os dados circulam por um único cabo. A principal vantagem é que é uma estratégia econômica e versátil, com manutenção simplificada.

Contudo, sua desvantagem é similar ao tipo anel: a rede fica vulnerável diante de falhas de máquinas. Afinal, todas estão centralizadas em um único fluxo.



## **ESTRELA**

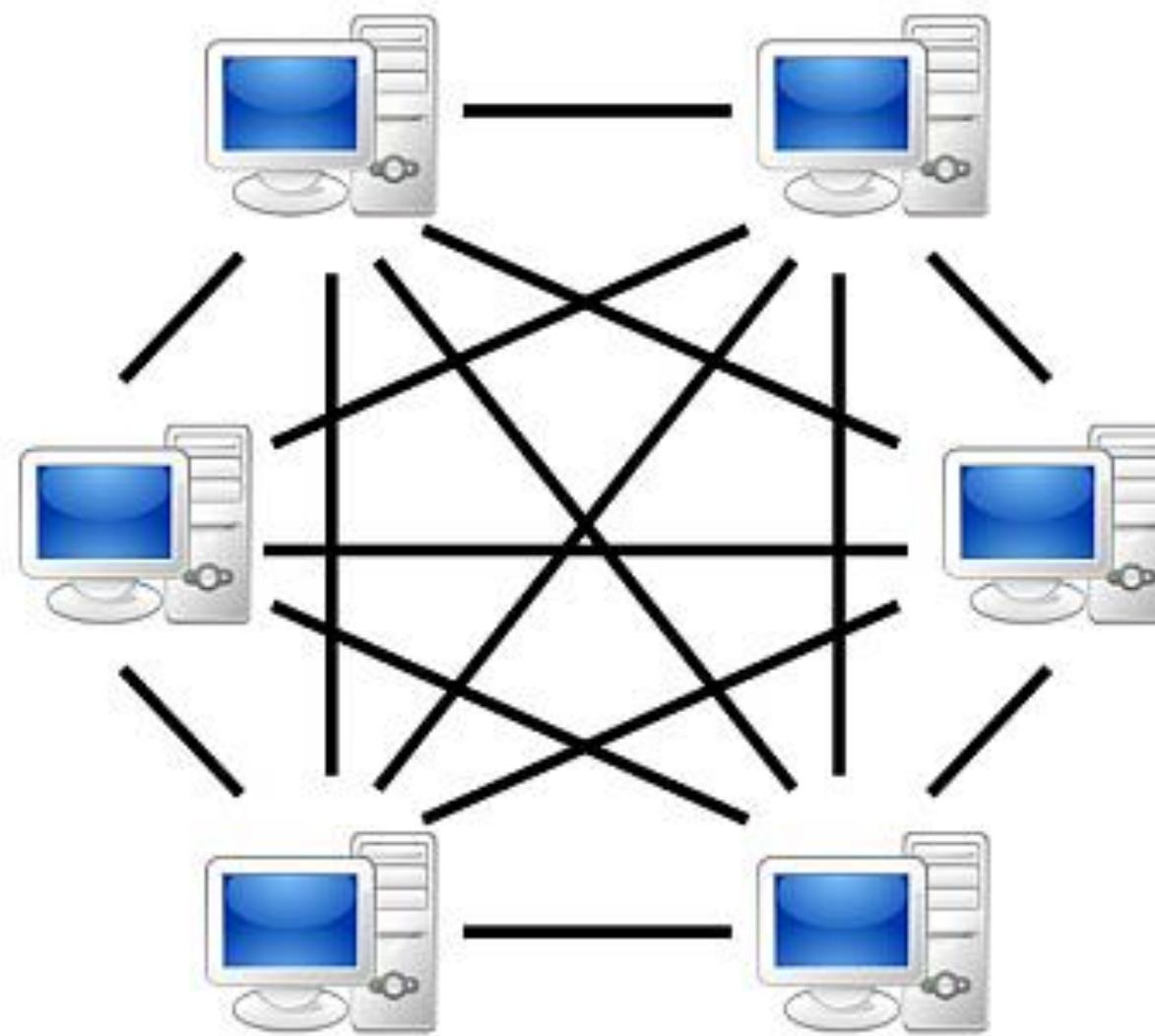
Aqui, temos braços que partem de um ponto central, em formato de estrela. A vantagem é que a falha isolada não compromete o fluxo, visto que ele parte do nó central em direção aos demais dispositivos. Mas, assim como o tipo árvore, em falhas no nó central, haverá prejuízo em todo o fluxo de dados.



## PONTO A PONTO

O tipo ponto a ponto é o que garante a maior simplicidade. Os nós todos se conectam entre si. Por conta dessa característica, é o tipo mais comum em instalações residenciais, como por exemplo, PC1 > Modem < PC2.

É ideal para estabelecer a comunicação rápida entre dois dispositivos. Sua desvantagem é que não supre as necessidades de instalações grandiosas.



## **MALHA**

Cada dispositivo possui um link dedicado aos demais dispositivos da rede.

### **Vantagens:**

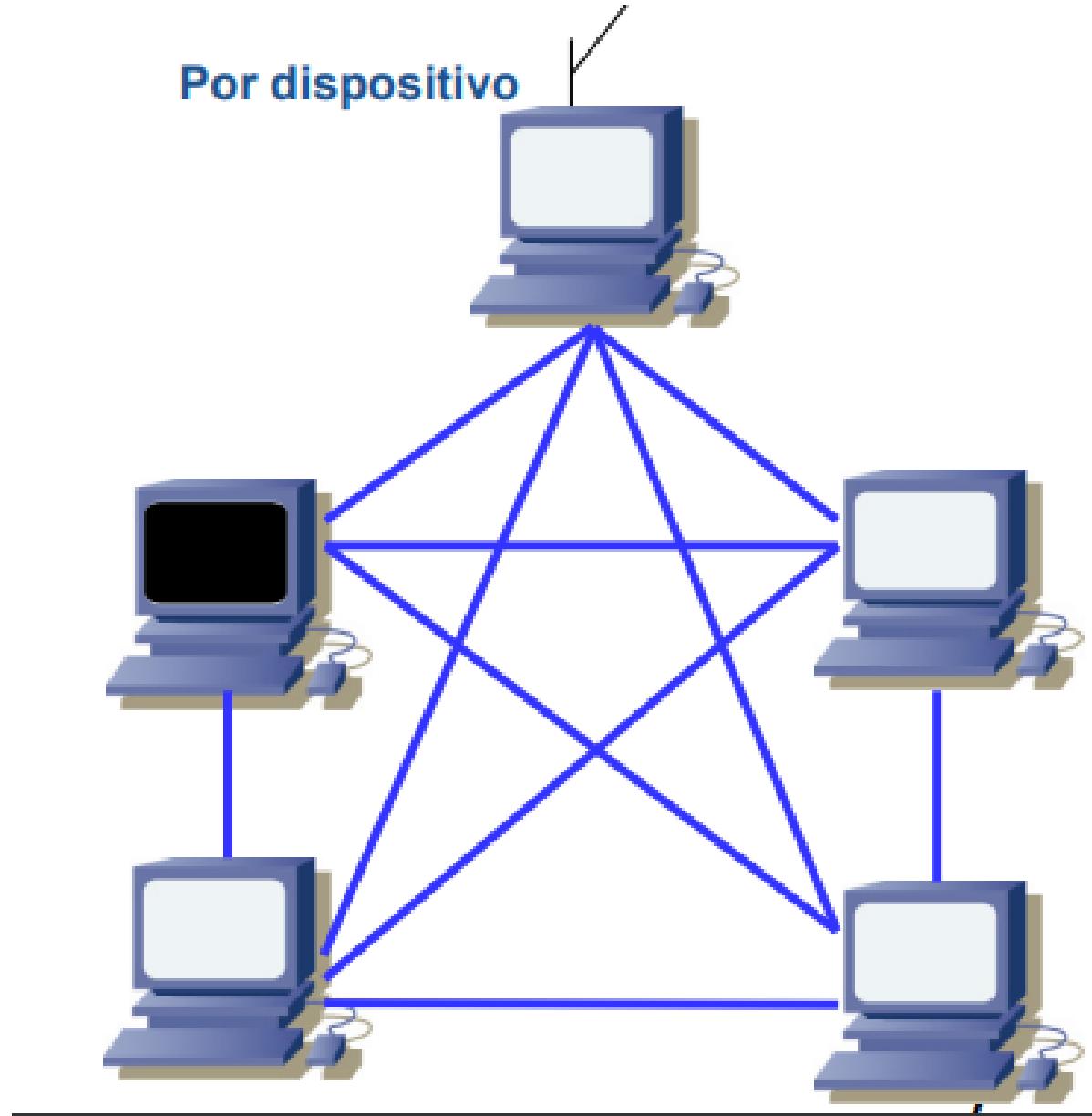
- Links dedicados;
- Privacidade e segurança;
- Robustez;
- Fácil identificação de falhas;

# **MALHA**

## **Desvantagens:**

- Cabeamento excessivo;
- Quantidade de interfaces excessiva;
- Custo do hardware.

Por dispositivo



# **MEIO FÍSICO**

**Bit:** Propaga-se entre o transmissor e o receptor

**Enlace Físico:** está entre o transmissor e o receptor

**Meios guiados:** propagam-se em meios sólidos:

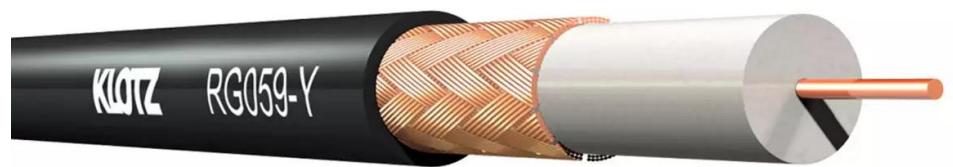
cobre, fibra, cabo coaxial

**Meios não guiados:** propagam-se livremente: rádio,

wireless.

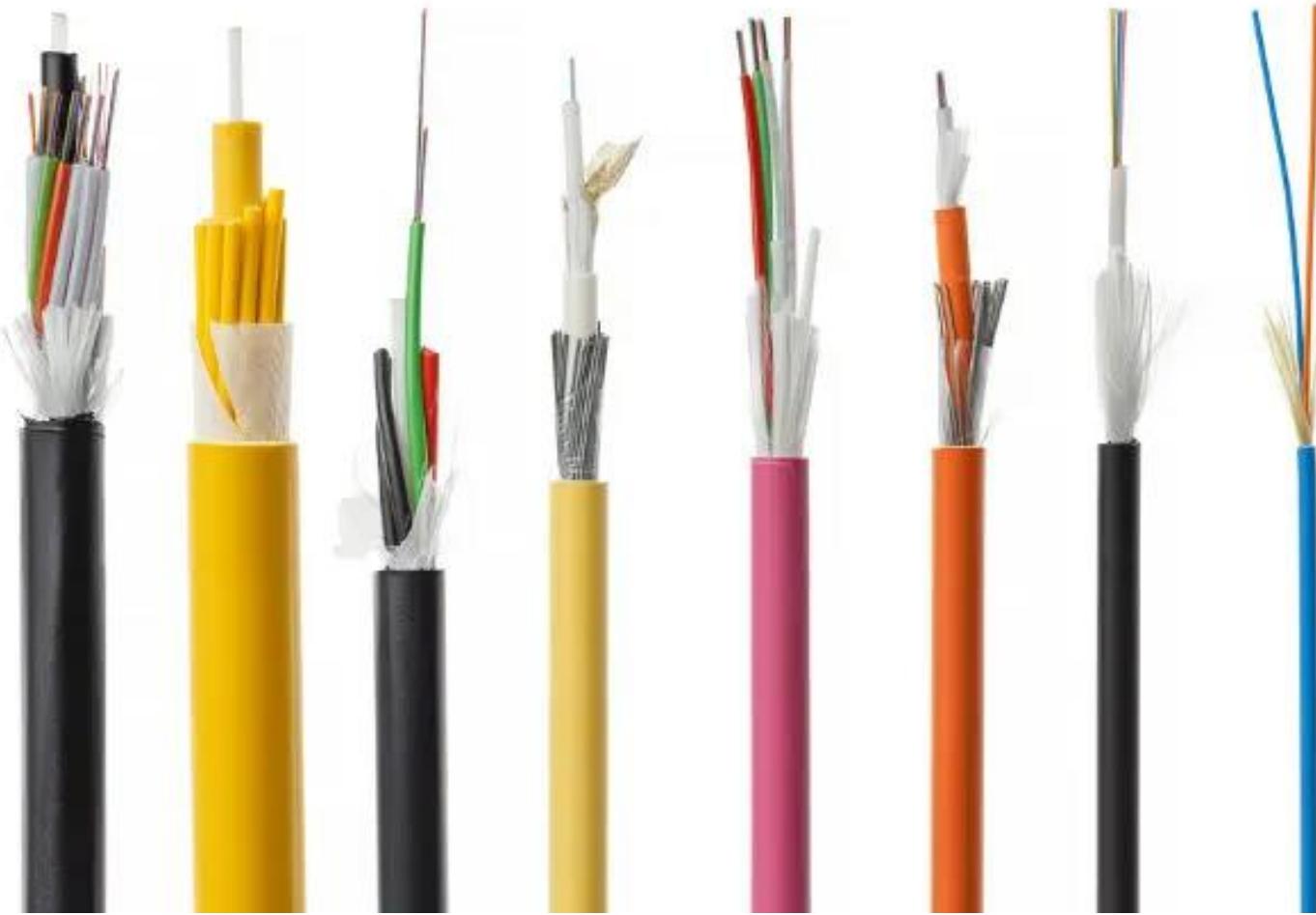
# CABO COAXIAL

- Fio (transporta o sinal) dentro de outro fio (blindagem)
- Bidirecional
- Banda Larga (broadband): Múltiplos canais num cabo



# FIBRA ÓPTICA

- Fibra de vidro que transporta pulsos de luz
- Opera em alta velocidade (até 100 Mbits por segundo)
- Banda taxa de erros
- Repedidores mais afastados
- Imune a ruído eletromagnético



# Vantagens

## Velocidade de transmissão:

A maior parte dos cabos de fibra óptica usados no mundo é capaz de transmitir 40 Gbit/s (Gigabits por segundo –  $10^9$  bits/s), entretanto, atualmente existem tecnologias que são capazes de transferir até 1 Pbit/s (Petabit por segundo –  $10^{15}$  bits/s).

# Vantagens

## Resistência a interferências eletromagnéticas:

Os cabos de fibra óptica são feitos de materiais dielétricos, e a propagação da luz no interior desses materiais não sofre interferência por ondas eletromagnéticas externas.

# Vantagens

## Baixa atenuação de sinal:

Diferentemente dos cabos condutores, as fibras ópticas conseguem transmitir informações com pequenas perdas: cerca de 0,2 dB/km (0,2 decibels – unidade de intensidade da energia carregada pela onda).

# Vantagens

## Custo:

Os cabos de fibra óptica são mais baratos que os cabos condutores de cobre.

# Vantagens

## Vida útil:

Esse tipo de cabos tem uma vida útil muito longa, estimada em mais de 100 anos de uso contínuo.

# Vantagens

**Espaço:** Em razão da sua taxa de transferência de dados, os cabos de fibra óptica ocupam espaços muito menores do que os cabos convencionais

# Desvantagens

**Aplicação:** Os cabos de fibra óptica são subterrâneos ou sempre conectados ao chão.

**Fragilidade:** Os cabos de fibra óptica são sensíveis e podem se romper mais facilmente que os cabos de cobre, além disso, não são tão maleáveis quanto cabos metálicos.

**Distâncias:** Apesar de absorverem pouca luz, os cabos de fibra óptica que cobrem grandes distâncias, como aqueles que são submarinos, precisam de muitos repetidores de sinais para reforçar as perdas da intensidade da luz

# CABO UTP

O Cabo por par trançado é um tipo de cabo que possui pares de fios entrelaçados um ao redor do outro para cancelar as interferências eletromagnéticas

# Vantagens

## Velocidade

Entre as principais vantagens dos cabos UTP, destaca-se a sua capacidade de transmitir dados em alta velocidade. Na categoria 6E, esses cabos podem transmitir dados a uma velocidade de 1Gbps, o que é extremamente veloz se comparada à velocidade média dos cabos anteriores ao UTP.

## **Qualidade da transmissão**

Além da velocidade de transmissão, a alta qualidade também é uma das vantagens dos cabos UTP. Os pares de fio de cobre trançados são cobertos por uma capa, que protege a transmissão de dados contra interferência e contra o seu rompimento acidental.

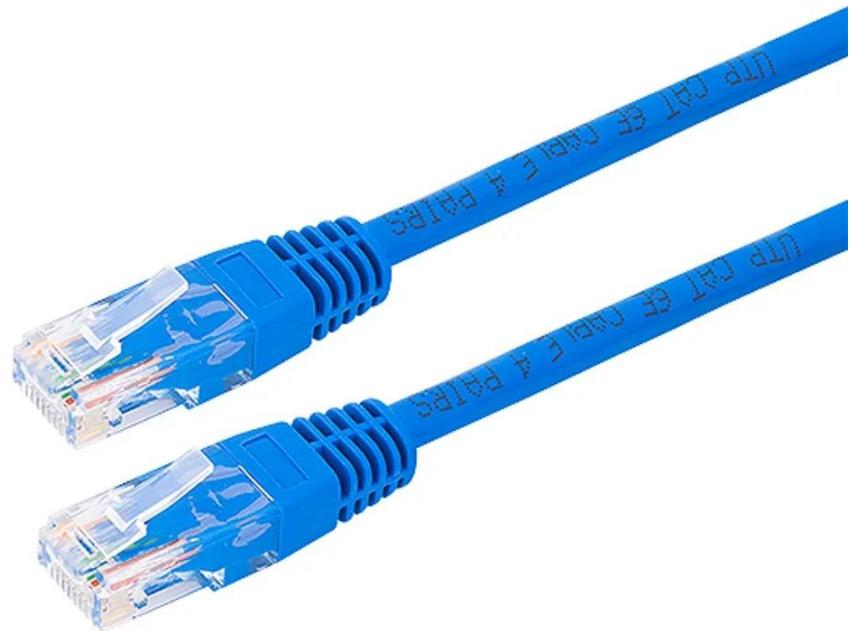
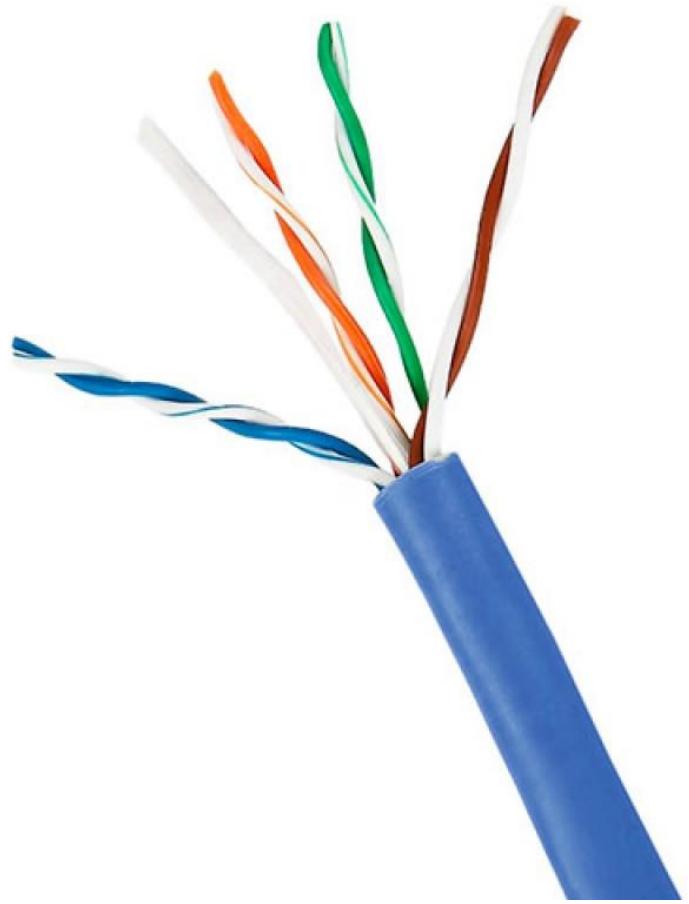
## Possibilidade de interligar em rede dispositivos afastados.

Outra vantagem do cabo UTP é a sua capacidade de manter a qualidade da transferência de dados em uma distância considerável. Os cabos da categoria 5E são capazes de transmitir dados com qualidade mesmo a uma distância de 100 metros. Isso possibilita, por exemplo, que empresas interliguem todos os seus setores em rede.

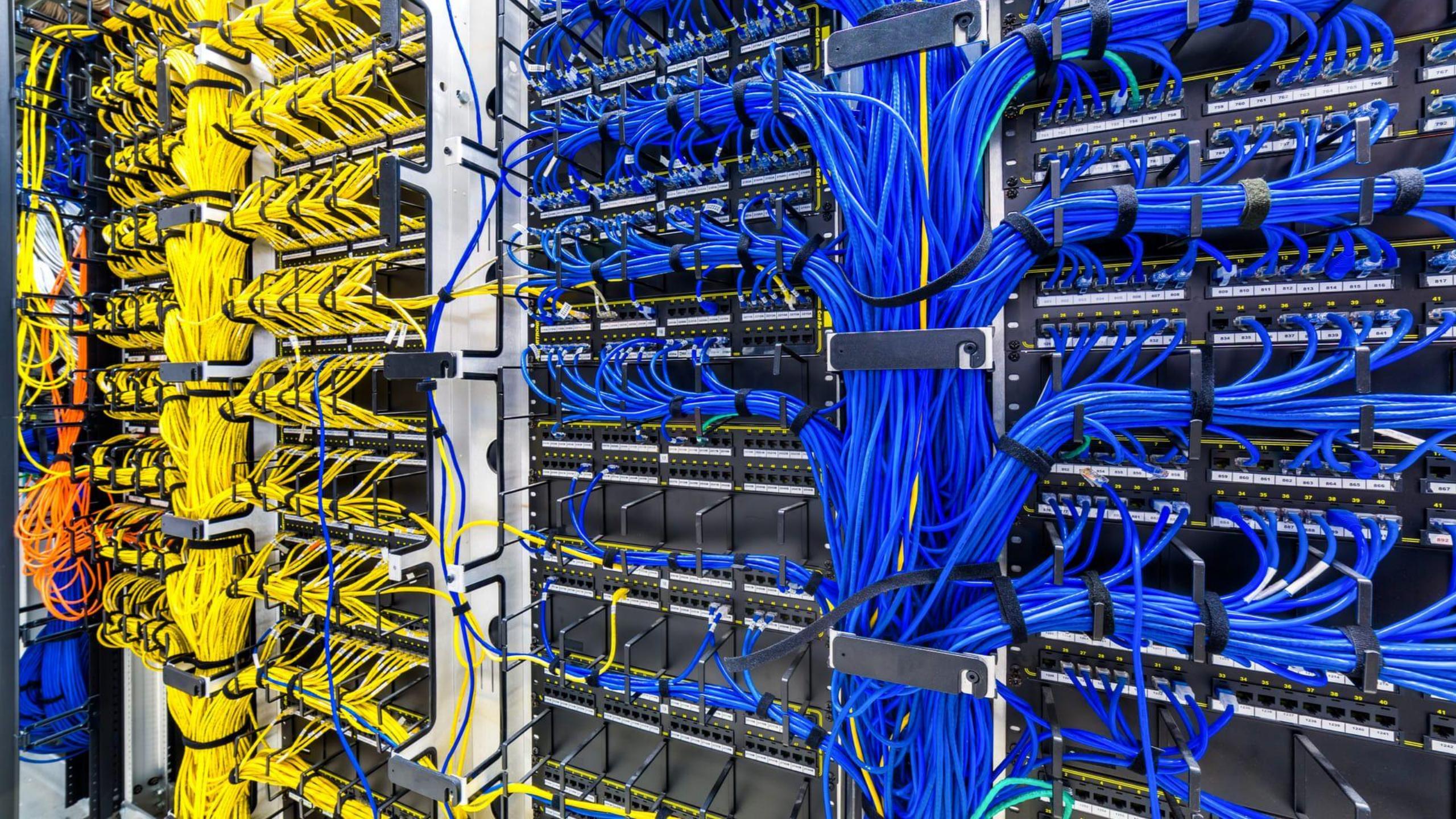
## Boa relação custo-benefício

Se comparados a outros meios de comunicação de rede, os cabos UTP podem ser considerados de baixo custo. E como a interligação em rede agrupa mais qualidade e eficiência aos dispositivos, possibilitando compartilhamento de impressoras, conexão à internet, acesso a servidores etc, o custo-benefício desses cabos é alto.

Apesar das diversas vantagens citadas anteriormente, os cabos UTP também possuem algumas desvantagens. Quando ficam muito próximos a lâmpadas fluorescentes, micro-ondas e outros tipos de emissores de ondas, os cabos ficam vulneráveis à interferência de ruídos. Outro detalhe é que os cabos UTP não são adequados a casos nos quais é preciso interligar redes em distâncias muito grandes, como 200 metros ou mais, sendo necessário o uso de um repetidor de sinal (switch, hub ou afins) a cada 100 metros.



# **TIPOS DE CABOS**

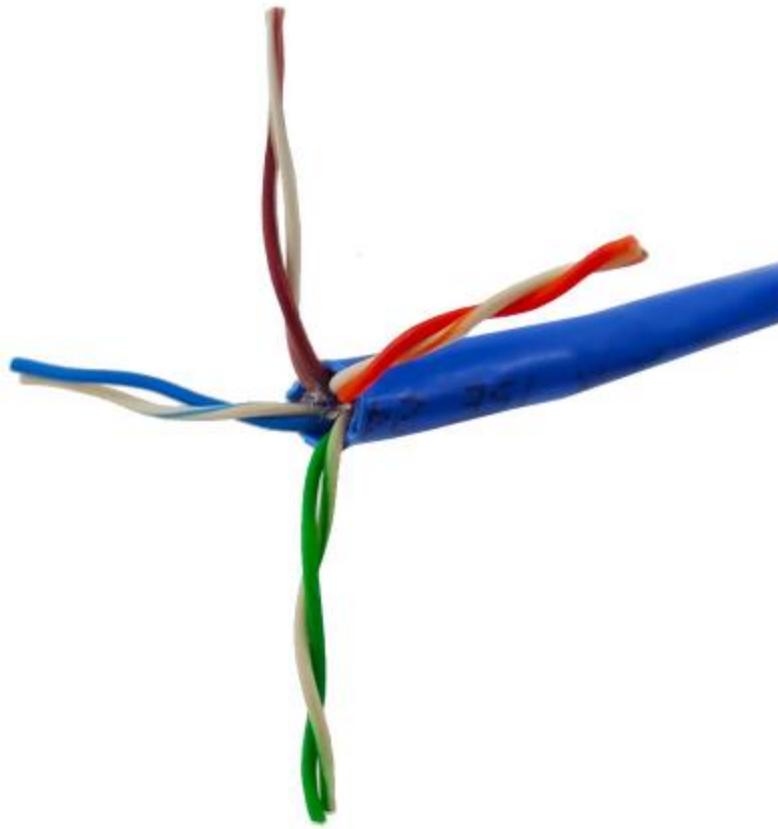


## Cat5

A versão mais básica de cabo, ele suporta taxas de transferências de até 100MBps e frequências de até 100MHz. Indicado para pequenas distâncias de comunicação. Este cabo é difícil de ser encontrado no mercado, pois foi substituído pelo Cat5e.

## Cat5e

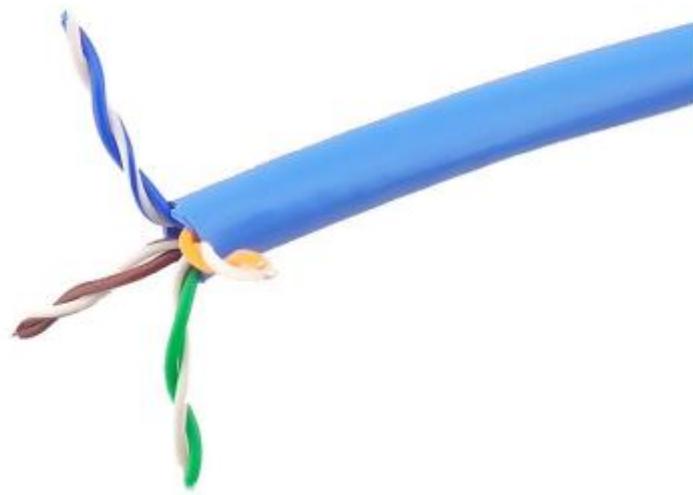
Talvez o mais popular dos cabos, o Cat5e é a versão aprimorada do modelo anterior. Novos padrões de certificação para ter menos interferência e perda de sinal. A velocidade de transmissão foi melhorada, mas a frequência se manteve igual à do modelo anterior.



## Cat6

O Cat6 é outro padrão de cabo ethernet. Ele tem a velocidade de até 10Gigabits por segundo, porém seu alcance é diminuído para manter a velocidade.

As frequências suportadas neste modelo são de até 250MHz, e isso significa menos interferência do que o modelo anterior.



## Cat6a

A atualização natural do modelo anterior, o Cat6a surge para melhorar justamente a distância que o Cat6 não tem, não perdendo a qualidade e velocidade de transferência.

Este cabo é mais grosso e menos flexível que os anteriores, por isso é importante estudar os locais onde ele deverá passar. A frequência também foi atualizada e pode suportar até 500MHz.

Essa categoria de cabo é difícil de encontrar no Brasil e seus valores são bem mais elevados que os modelos anteriores.



## Cat7

O cabo Cat7 pode suportar maiores velocidades a uma frequência de até 600MHz a uma distância considerável de até 100 metros. No entanto, há testes que indicam que o desempenho pode ser maior.

Por conta de sua construção, esse cabo é ainda mais grosso que o modelo Cat6a e mais rígido, então deve se considerar essa característica na hora da escolha.



## Cat8

Os cabos Cat8 podem ser equiparados a fibra óptica, tamanho desempenho que possuem. Mas esbarram na distância que podem ser utilizados. Por isso, se você escolher esta opção, tenha em mente que deve ser instalado em uma distância pequena.





**RJ45**

# INTERNET

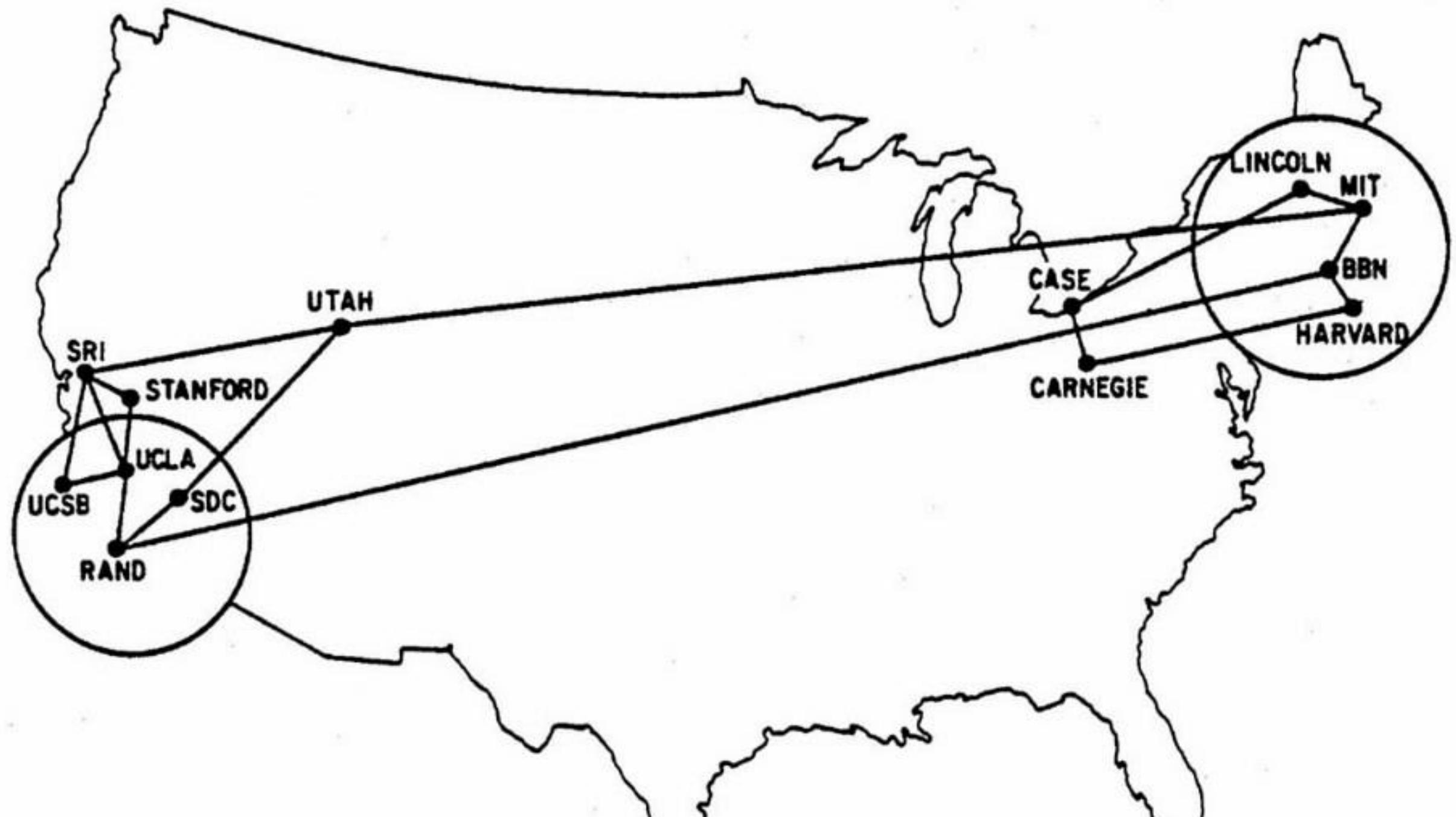


"Rede de alcance mundial";

É um sistema de documentos dispostos na Internet que permitem o acesso às informações apresentadas no formato de hipertexto.

# 1969 NASCE A ARPANET





1969 – ARPANET

1970 – O TERMO INTERNET É USADO PELA 1<sup>a</sup> VEZ

1971 – IDEALIZAÇÃO DO E-MAIL

1971 – CRIADO O 1º VÍRUS – The Creeper

1972 – @ É INCORPORADO AO E-MAIL

1973 – PRIMEIRA CONEXÃO ENTRE PAISES (Estados Unidos e Noruega)

1977 – CRIAÇÃO DO PROTOCOLO TCP/IP

1984 – O MILIONÉSIMO SERVIDOR É INSTALADO

1989 – Berners Lee PROPÕE O SISTEMA WORLD WIDE WEB (WWW)

# HOST

qualquer computador ou máquina conectado a uma rede, que conta com número de IP e nome definidos.



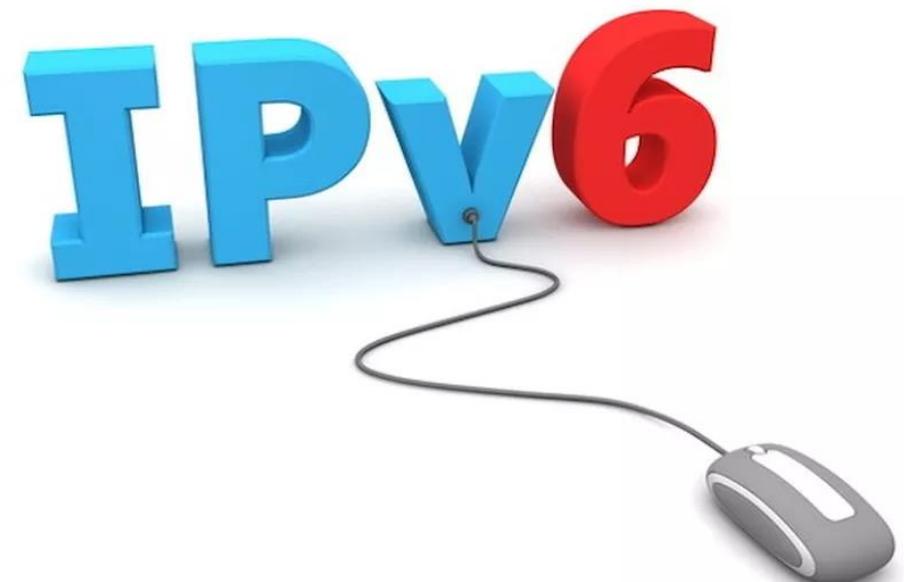
# ROTEADOR

Equipamento usado para fazer a comunicação entre diferentes redes de computadores.



# Número IP

É um endereço de um host ou de uma rede.



# SITE



# SERVIÇOS



# DOMINIO



**.mx** México

**.uk** Reino Unido

**.fr** Francia

**.at** Austria

**.es** España

**.cl** Colombia

**.pr** Puerto Rico

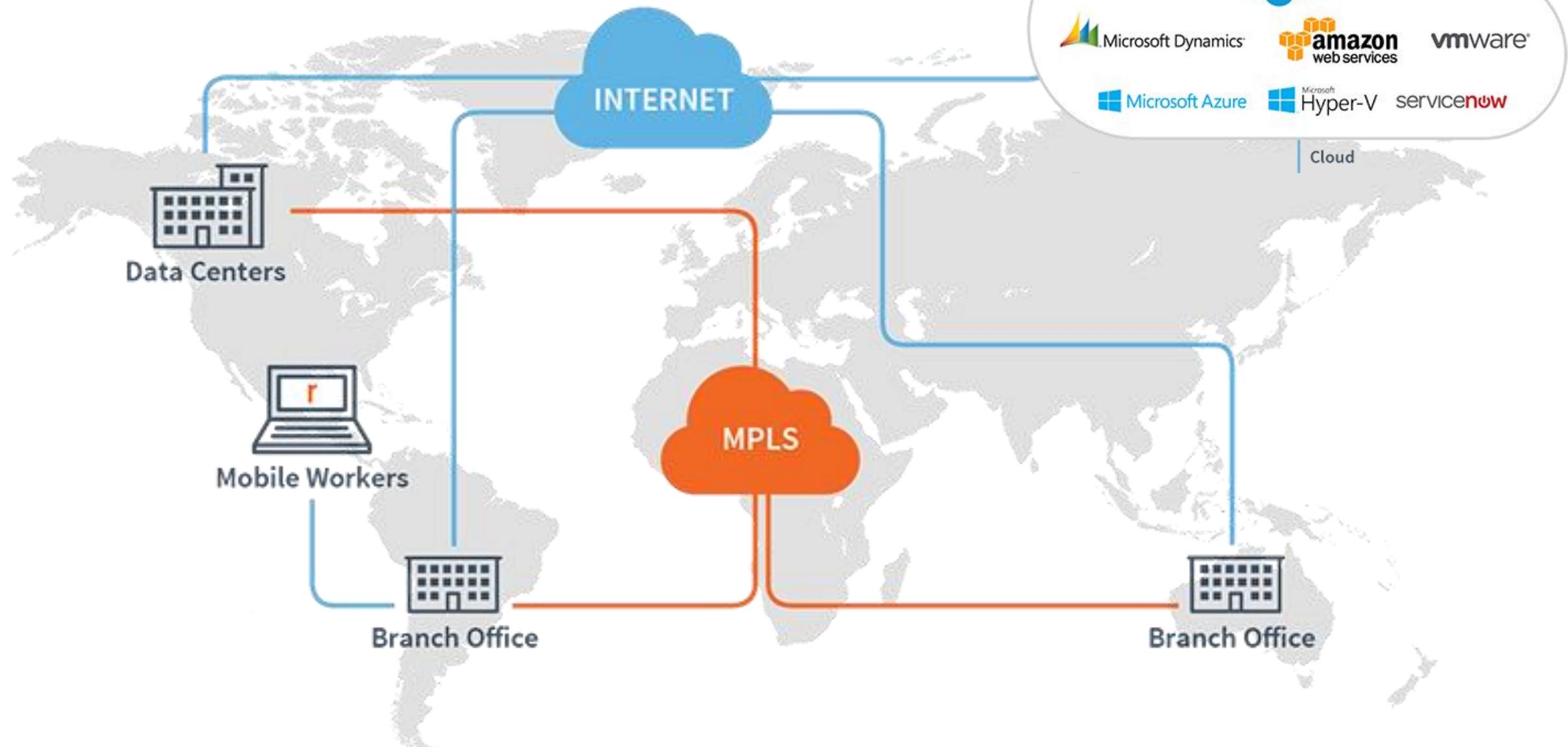
**.br** Brasil

**.ca** Canadá

**DOWNLOAD**

**UPLOAD**

# WAN



# **BACKBONE**

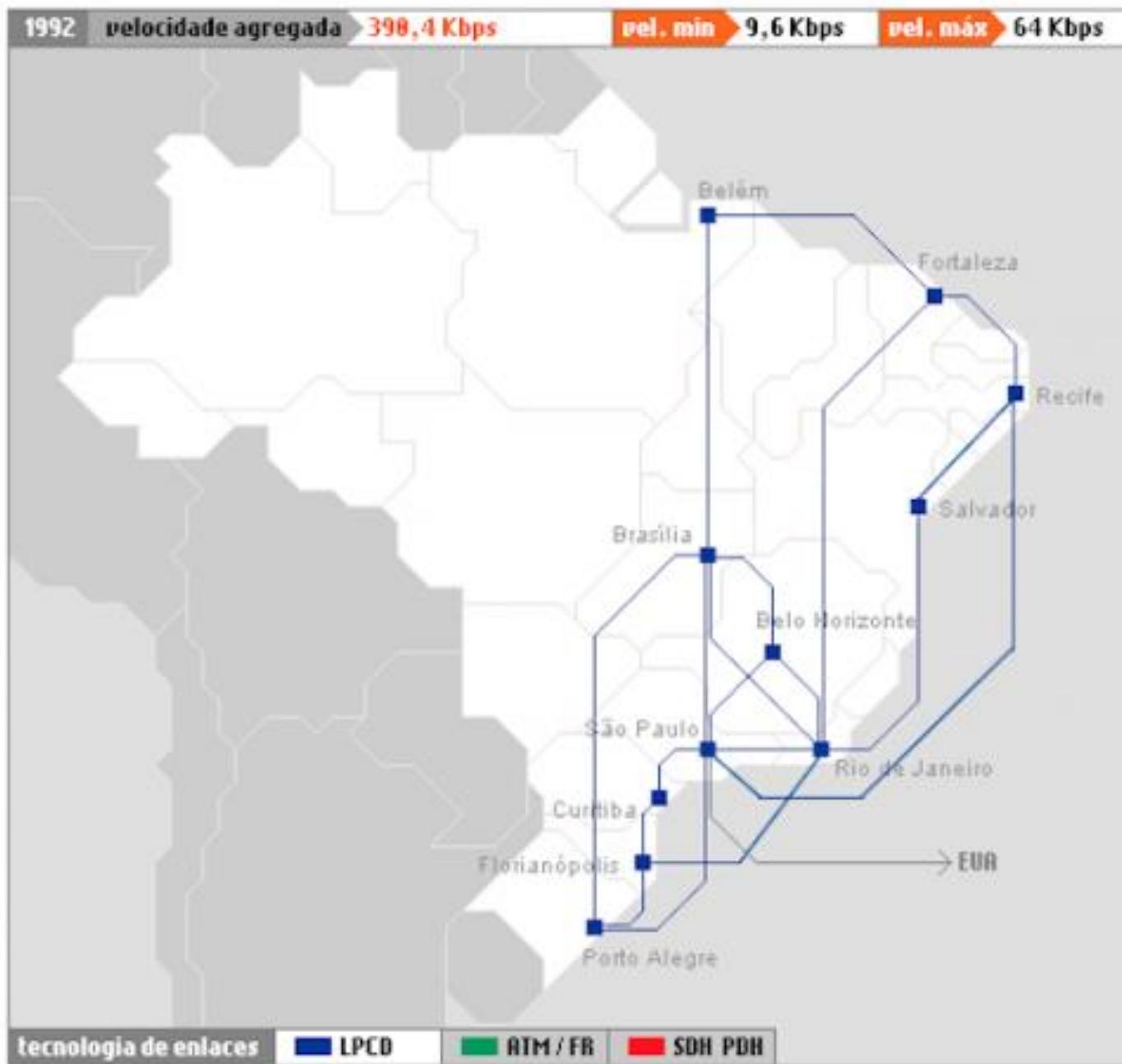
A função do backbone em telecom é conectar as centrais das operadoras de Internet aos servidores externos (nacionais ou internacionais), geralmente de forma redundante e por rotas diferentes. Em resumo, trata-se de uma malha continental.

Na prática, a estrutura é responsável pelo envio e recebimento dos dados entre diferentes computadores, dentro ou fora de um país. A rede principal (espinha dorsal) é dividida em outras para impedir que tráfego e transmissão de dados sejam lentos.

## O PRIMEIRO BACKBONE DO BRASIL

O primeiro backbone nacional nasceu em 1992 — Fase I: período de 1991 a 1993, dedicado à montagem — no ambiente acadêmico, fruto de um projeto que se iniciou pouco antes pelas mãos da Rede Nacional de Ensino e Pesquisa (RNP). Na época, interligava dez capitais brasileiras e o Distrito Federal, com capacidade de 64 kbps.

## Fase I

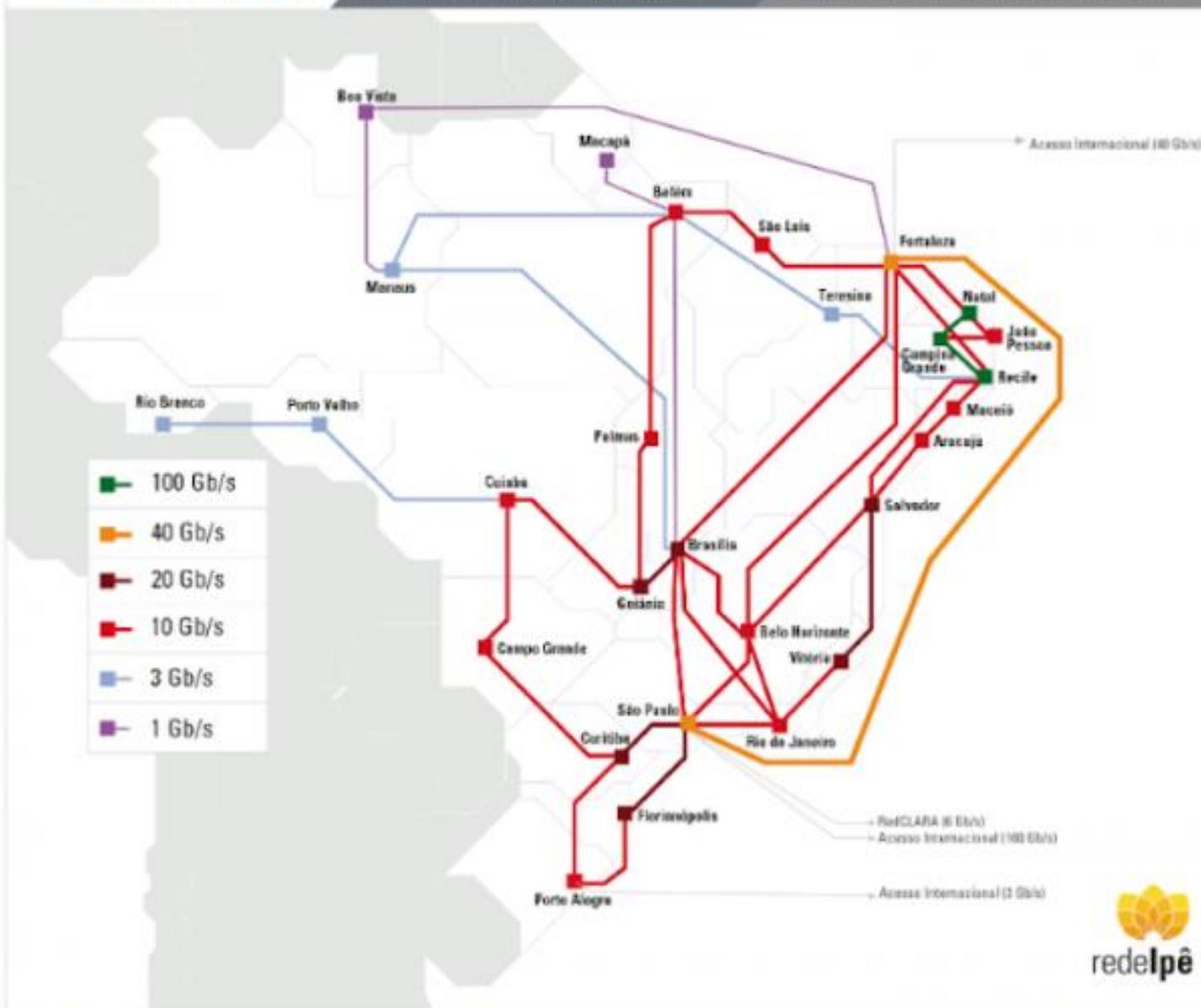


O primeiro backbone cresceu e deu origem a Rede Ipê, inaugurada em 2005, como evolução da rede inicialmente implantada em 1992 — apontada também como a primeira rede óptica nacional acadêmica a entrar em operação na América Latina.

Conexão em 2018

capacidade agregada 602 Gb/s

capacidade internacional 149 Gb/s



As redes de telecomunicações compreendem a infraestrutura necessária para atender ao usuário final, onde os sistemas de transmissão realizam a comunicação entre dois pontos, combinando os meios de transmissão com as tecnologias de transmissão.

Hierarquicamente é dividida em 3 seções, conforme a capacidade de transmissão de tráfego e também conforme as tecnologias empregadas, da seguinte forma:

**Redes Backbone**

**Redes Backhaul**

**Redes de Acesso**

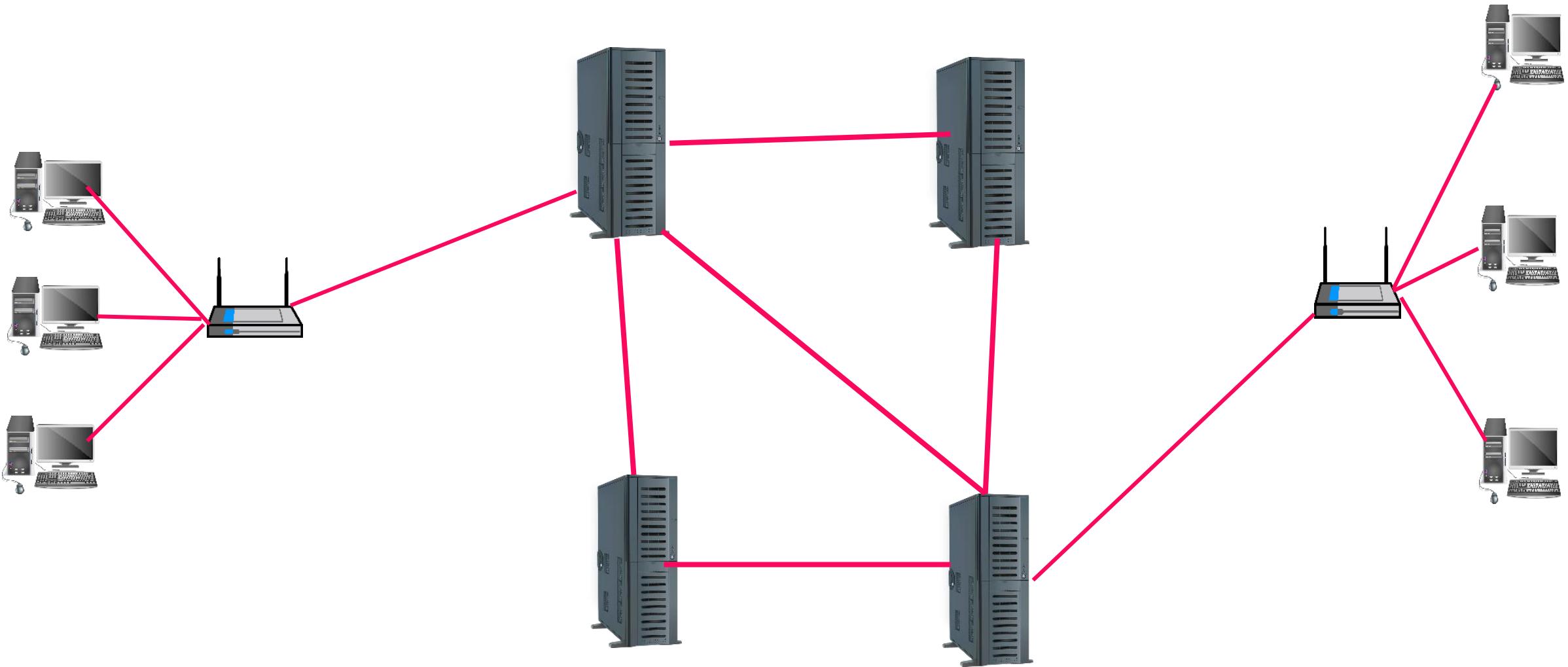
# **REDES BACKBONE**

Também chamada de “espinha dorsal”, é uma rede principal e é por essa rede que trafegam os dados dos clientes. As redes Backbone dão suporte ao tráfego de longa distância. Essa rede de telecomunicação é responsável pela transmissão, comutação, roteamento e gerenciamento de tráfego.

Comutação: É o processo de interligar dois ou mais pontos entre si.

Utilizam principalmente fibra óptica como meio de transmissão.

# REDES BACKBONE



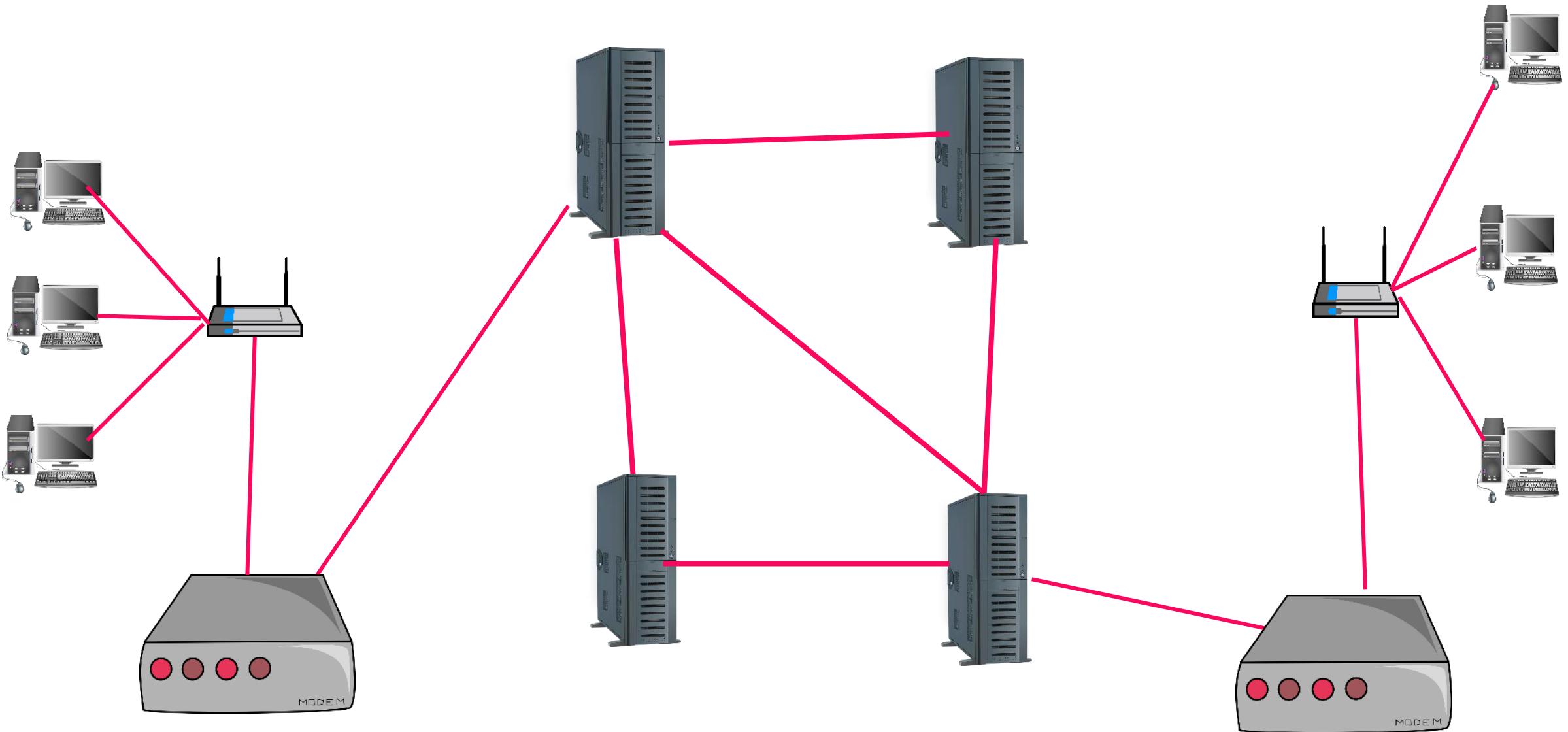
# REDES BACKHAUL

Backhaul é a porção de uma rede hierárquica de telecomunicações responsável por fazer a ligação entre o núcleo da rede, ou backbone, e as sub-redes periféricas.

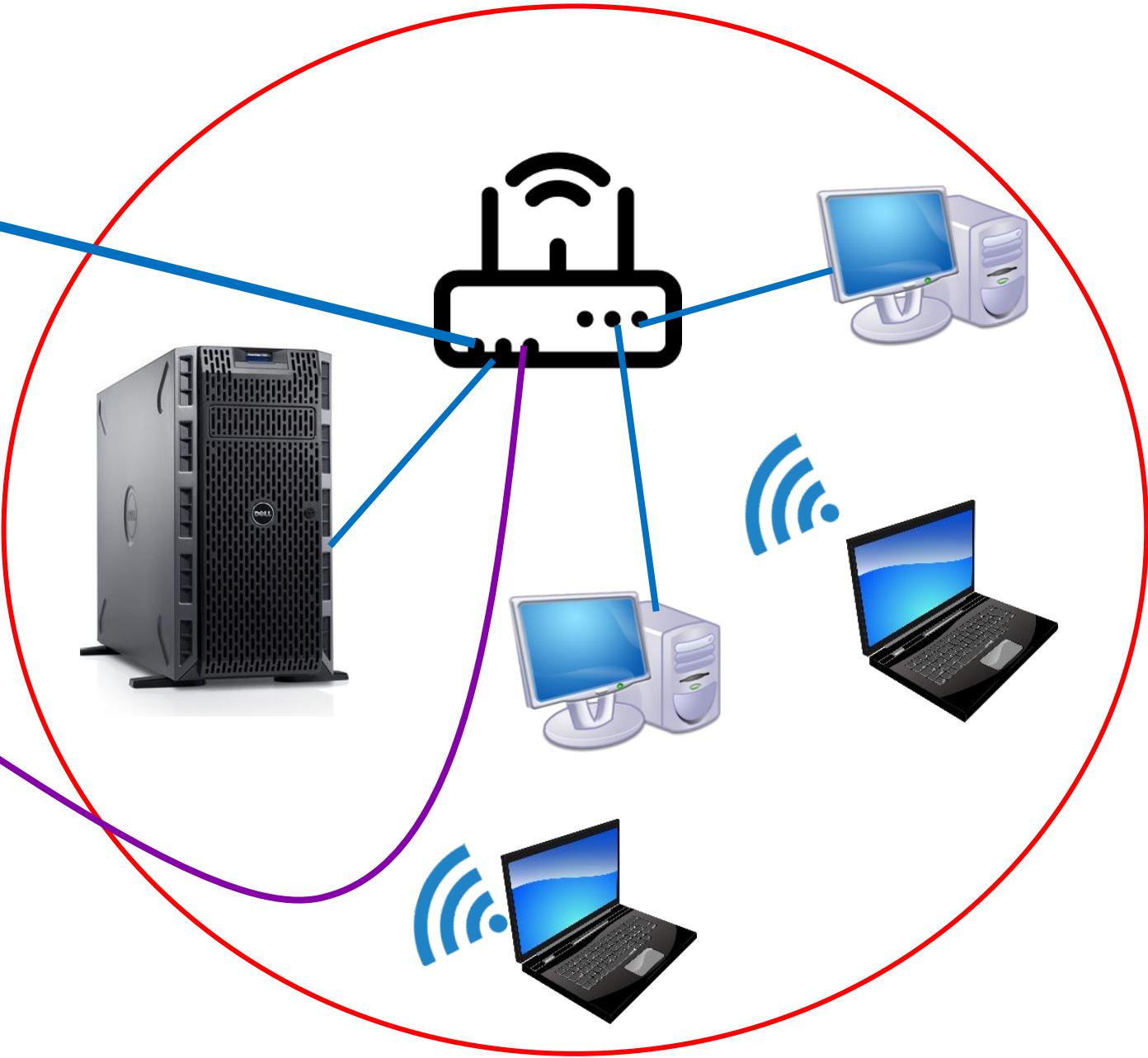
Exemplos:

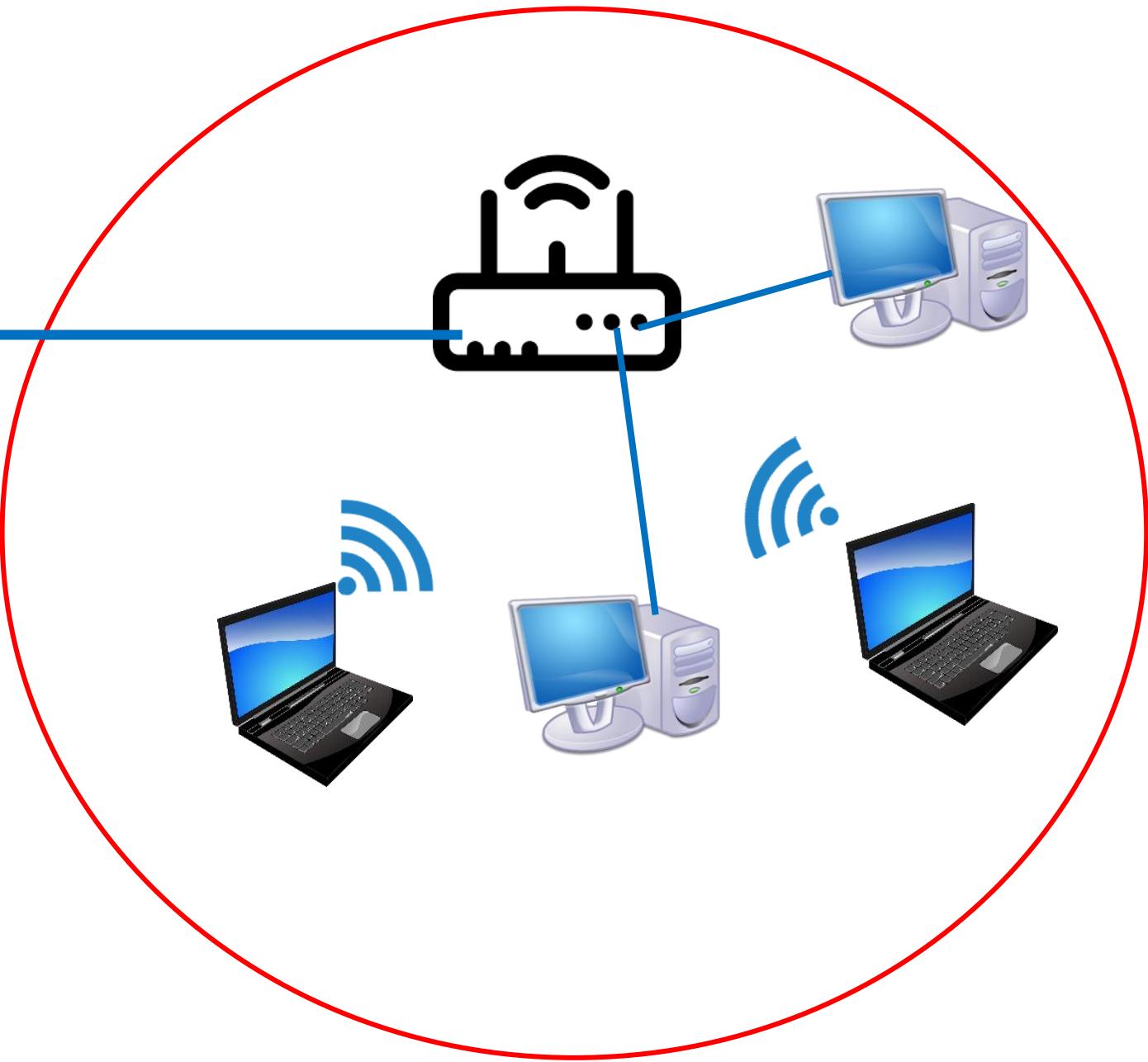
conexões entre DSLAM e nós ATM

# REDES BACKBONE



**INTRANET**





## Representações de Rede

Arquitetos e administradores de rede devem ser capazes de mostrar como suas redes serão. Eles precisam ser capazes de ver facilmente quais componentes se conectam a outros componentes, onde eles serão localizados e como eles serão conectados. Os diagramas de redes geralmente usam símbolos, como os mostrados na figura, para representar os diferentes dispositivos e conexões que compõem uma rede.

## Dispositivos finais



Computador desktop



Laptop



Impressora



Telefone IP

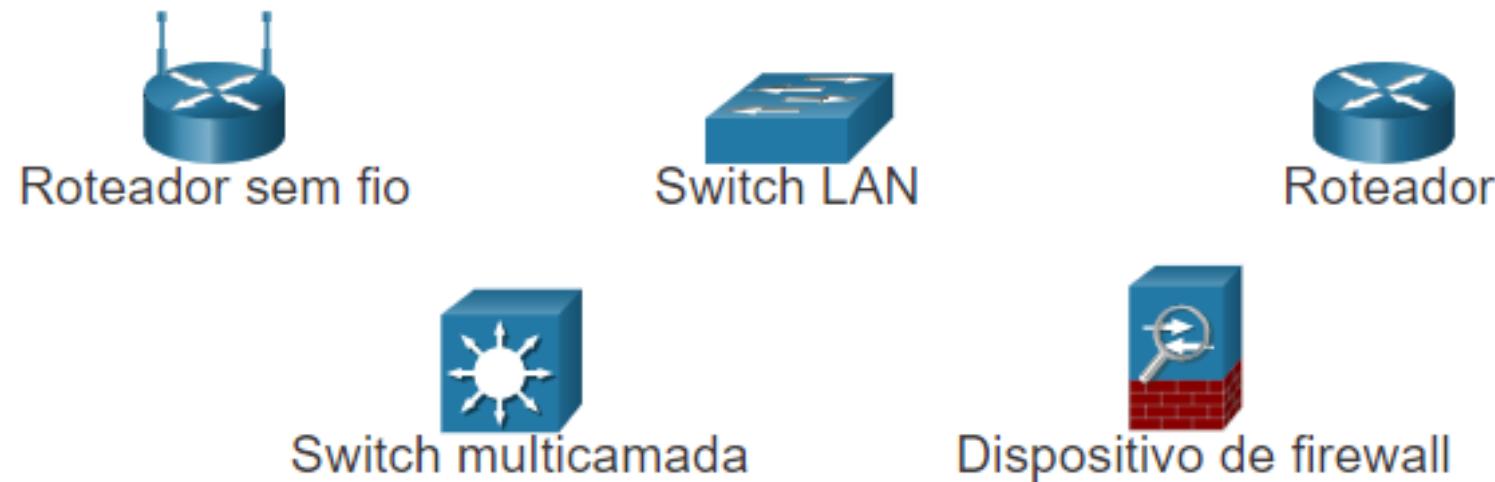


Tablet sem fio



Dispositivo final de  
TelePresença

## Dispositivos intermediários



## **Meios de rede**



Meios sem fio



Mídia LAN



Mídia WAN

## DIAGRAMAS

Um diagrama fornece uma maneira fácil de entender como os dispositivos se conectam em uma rede grande. Esse tipo de “fotografia” de uma rede é conhecido como um diagrama de topologia. A capacidade de reconhecer as representações lógicas dos componentes físicos de rede é crucial para se permitir visualizar a organização e a operação de uma rede.

Além dessas representações, é utilizada terminologia especializada para descrever como cada um desses dispositivos e mídias se conectam:

**Placa de interface de rede (NIC)** - Uma NIC conecta fisicamente o dispositivo final à rede.

**Porta física** - Um conector ou tomada em um dispositivo de rede onde a mídia se conecta a um dispositivo final ou outro dispositivo de rede.

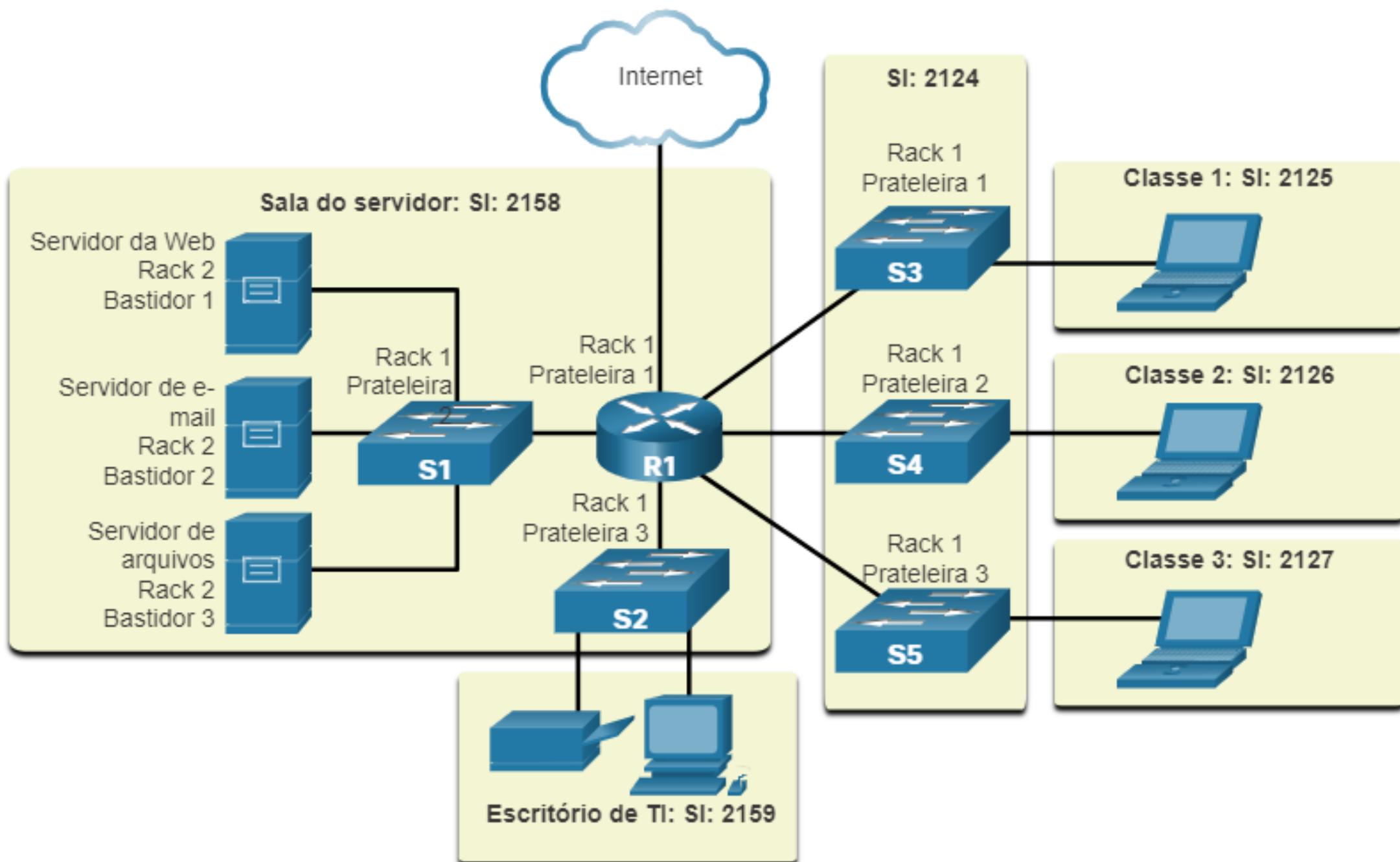
**Interface** - Portas especializadas em um dispositivo de rede que se conectam a redes individuais. Como os roteadores conectam redes, as portas em um roteador são chamadas de interfaces de rede.

# DIAGRAMAS DE TOPOLOGIA

Os diagramas de topologia são documentação obrigatória para qualquer pessoa que trabalhe com uma rede. Eles fornecem um mapa visual de como a rede está conectada. Existem dois tipos de diagramas de topologia: físicos e lógicos.

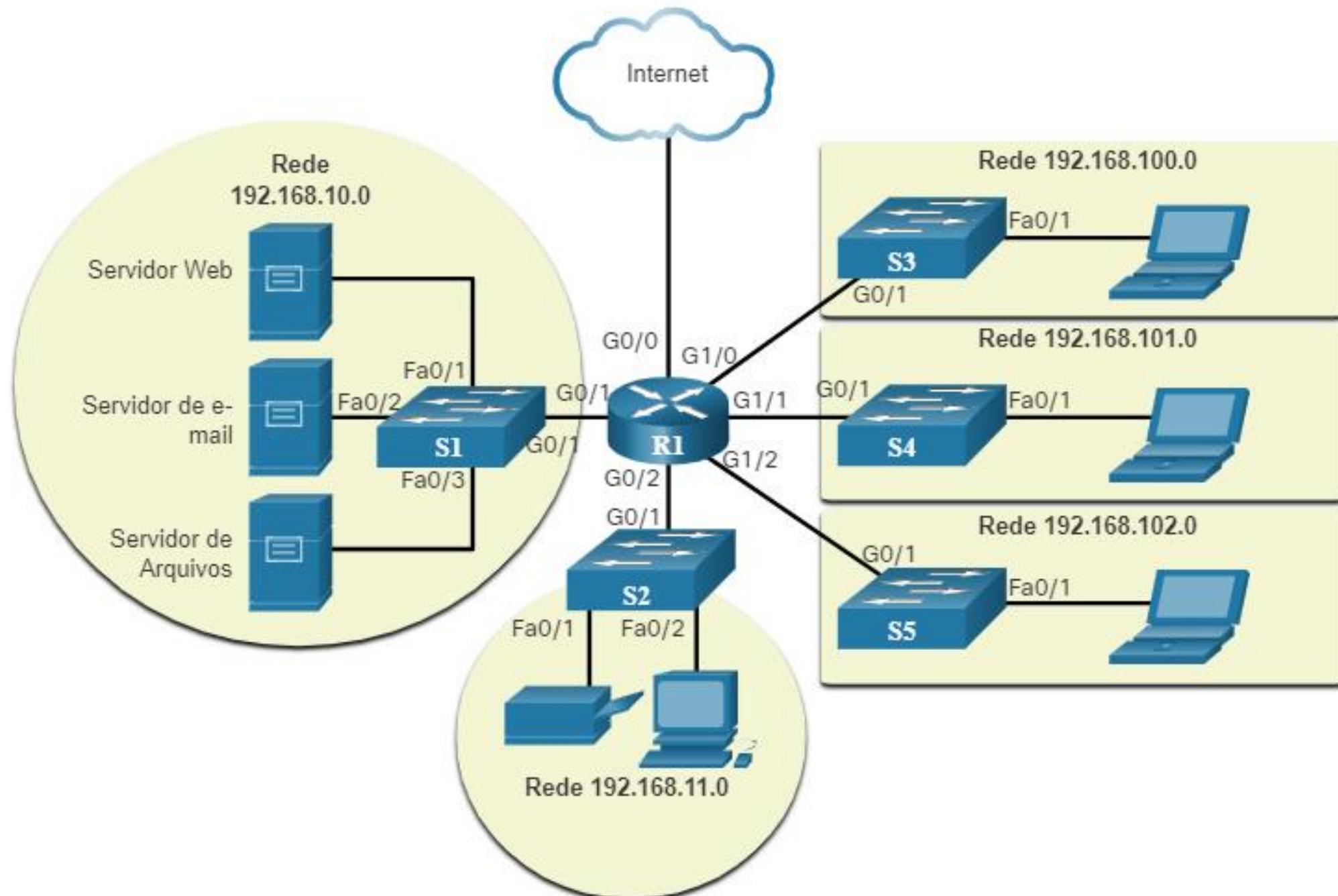
## DIAGRAMAS DE TOPOLOGIA FÍSICA

Os diagramas de topologia física ilustram a localização física dos dispositivos intermediários e a instalação dos cabos, conforme mostrado na figura. Você pode ver que as salas em que esses dispositivos estão localizados estão rotuladas nesta topologia física.



## DIAGRAMAS DE TOPOLOGIA LÓGICA

Diagramas de topologia lógica ilustram dispositivos, portas e o esquema de endereçamento da rede, conforme mostrado na figura. Você pode ver quais dispositivos finais estão conectados a quais dispositivos intermediários e que mídia está sendo usada.

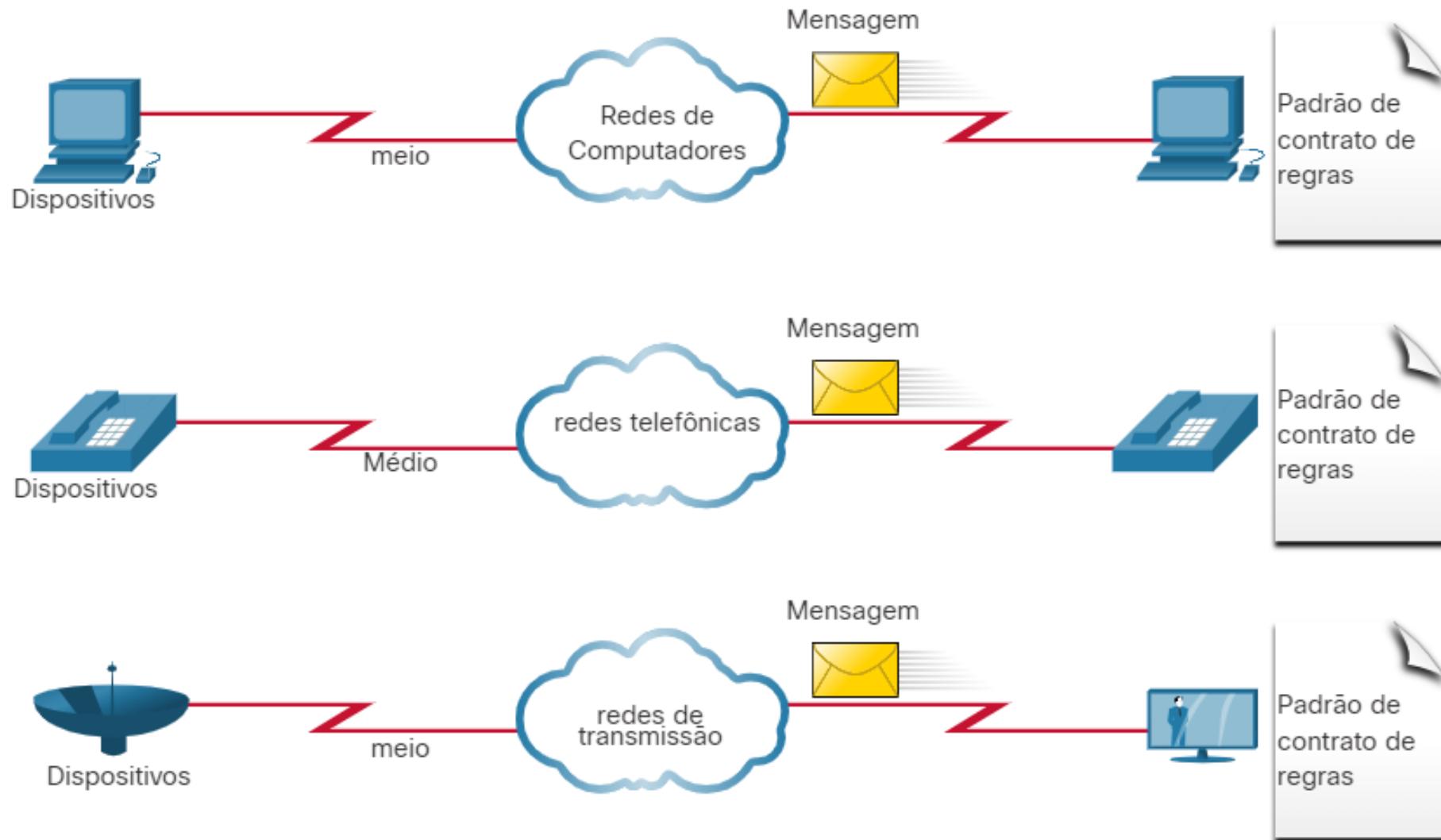


# REDE CONVERGENTE

## Redes Separadas Tradicionais

Redes separadas não podiam se comunicar. Cada rede usava tecnologias diferentes para transmitir o sinal de comunicação. Cada rede possuía seu próprio conjunto de regras e padrões para garantir uma comunicação bem-sucedida. Vários serviços são executados em várias redes.

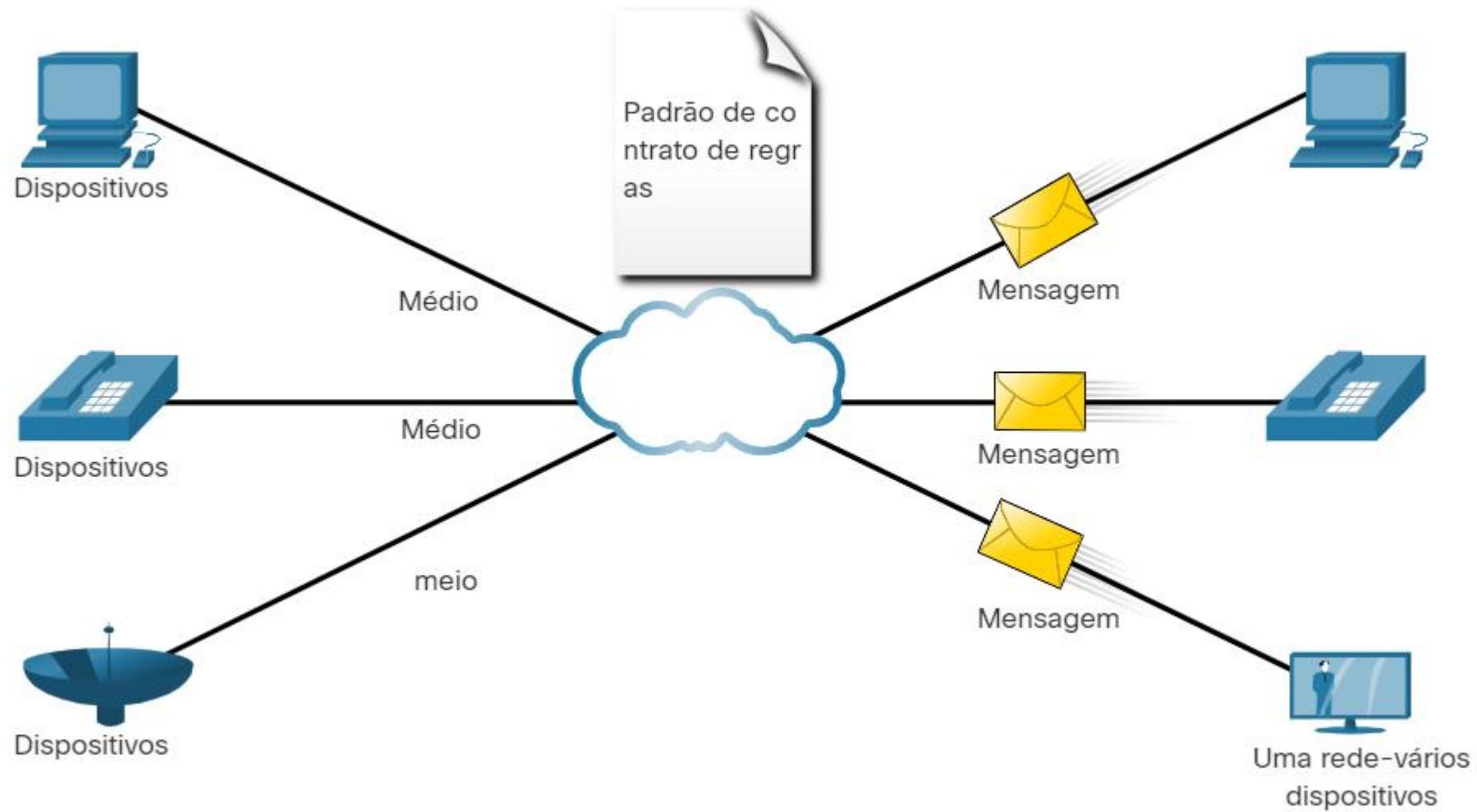
# Redes Separadas Tradicionais



## Redes Convergentes

Hoje, as redes separadas de dados, telefone e vídeo convergem. Diferentemente das redes dedicadas, as redes convergentes são capazes de fornecer dados, voz e vídeo entre muitos tipos diferentes de dispositivos na mesma infraestrutura de rede. Essa infraestrutura de rede usa o mesmo conjunto de regras, os mesmos contratos e normas de implementação. As redes de dados convergentes transportam vários serviços em uma rede.

# Redes Convergentes



# ARQUITETURA DE REDES

O papel da rede mudou de uma rede somente de dados para um sistema que permite a conexão de pessoas, dispositivos e informações em um ambiente de rede convergente rico em mídia. Para que as redes funcionem com eficiência e cresçam nesse tipo de ambiente, a rede deve ser construída sobre uma arquitetura de rede padrão.

## ARQUITETURA DE REDES

As redes também suportam uma ampla gama de aplicativos e serviços. Elas devem operar sobre muitos tipos diferentes de cabos e dispositivos, que compõem a infraestrutura física. A termo arquitetura de redes, neste contexto, refere-se às tecnologias que apoiam a infraestrutura e os serviços programados e as regras, ou protocolos, que movimentam os dados na rede.

# ARQUITETURA DE REDES

À medida que as redes evoluem, percebemos que há quatro características básicas que os arquitetos de rede devem atender às expectativas do usuário:

- Tolerância a falhas;
- Escalabilidade;
- Qualidade de serviço (QoS);
- Segurança.

## Tolerância a Falhas

Uma rede tolerante a falhas é aquela que limita o número de dispositivos dependentes durante uma falha. Ela foi desenvolvida para permitir uma recuperação rápida quando ocorre uma falha. Essas redes dependem de vários caminhos entre a origem e o destino de uma mensagem.

## Tolerância a Falhas

Se um caminho falhar, as mensagens serão enviadas instantaneamente por um link diferente. Ter vários caminhos para um destino é conhecido como redundância.

## Tolerância a Falhas

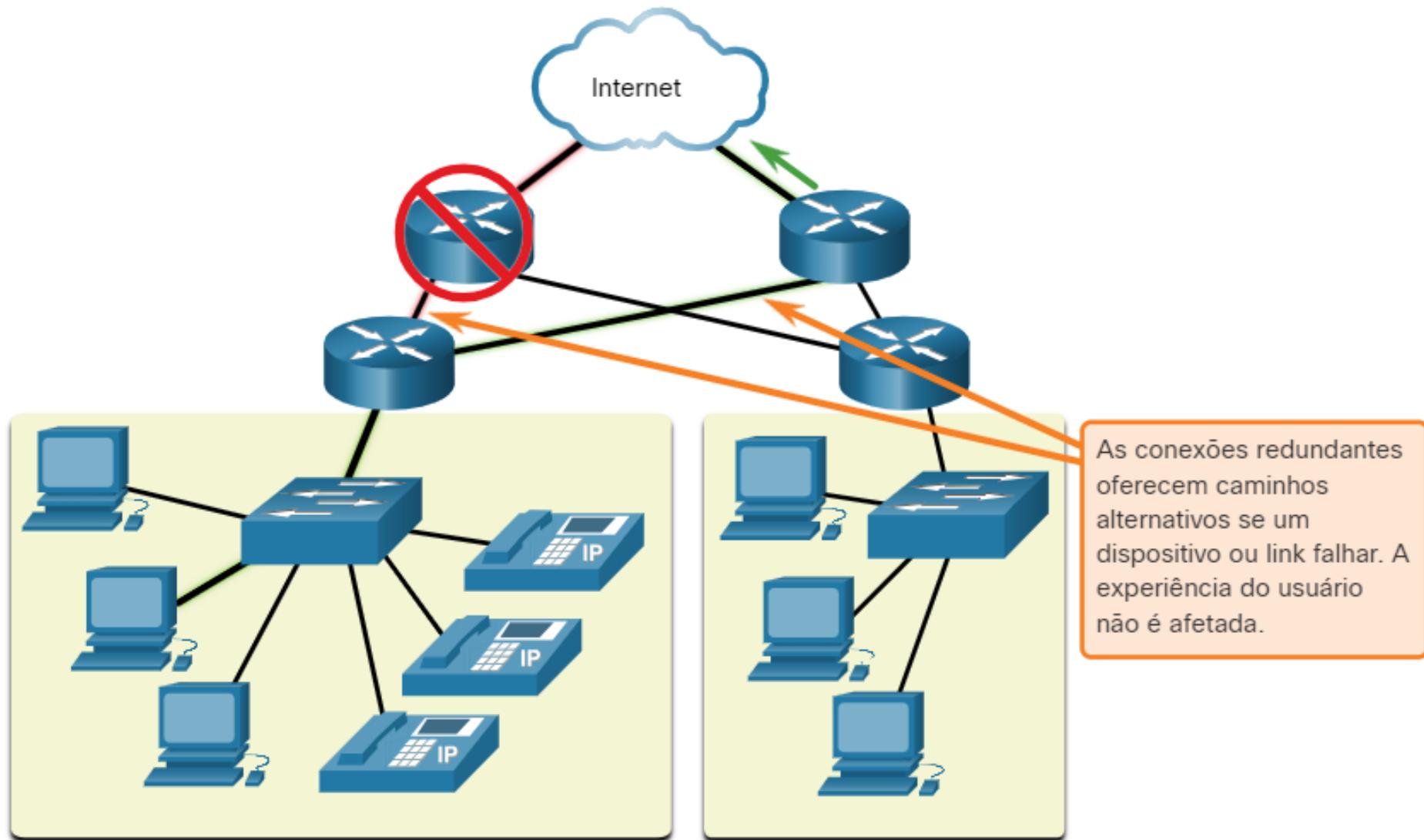
Se um caminho falhar, as mensagens serão enviadas instantaneamente por um link diferente. Ter vários caminhos para um destino é conhecido como redundância.

## Tolerância a Falhas

A implementação de uma rede comutada por pacotes é uma das maneiras pelas quais redes confiáveis fornecem redundância. A comutação de pacotes divide os dados do tráfego em pacotes que são roteados por uma rede compartilhada. Uma única mensagem, como um e-mail ou stream de vídeo, é dividido em vários blocos, chamados pacotes.

## Tolerância a Falhas

Cada pacote tem as informações de endereço necessárias da origem e do destino da mensagem. Os roteadores na rede alternam os pacotes com base na condição da rede no momento. Isso significa que todos os pacotes em uma única mensagem podem seguir caminhos muito diferentes para o mesmo destino. Na figura, o usuário desconhece e não é afetado pelo roteador que está alterando dinamicamente a rota quando um link falha.

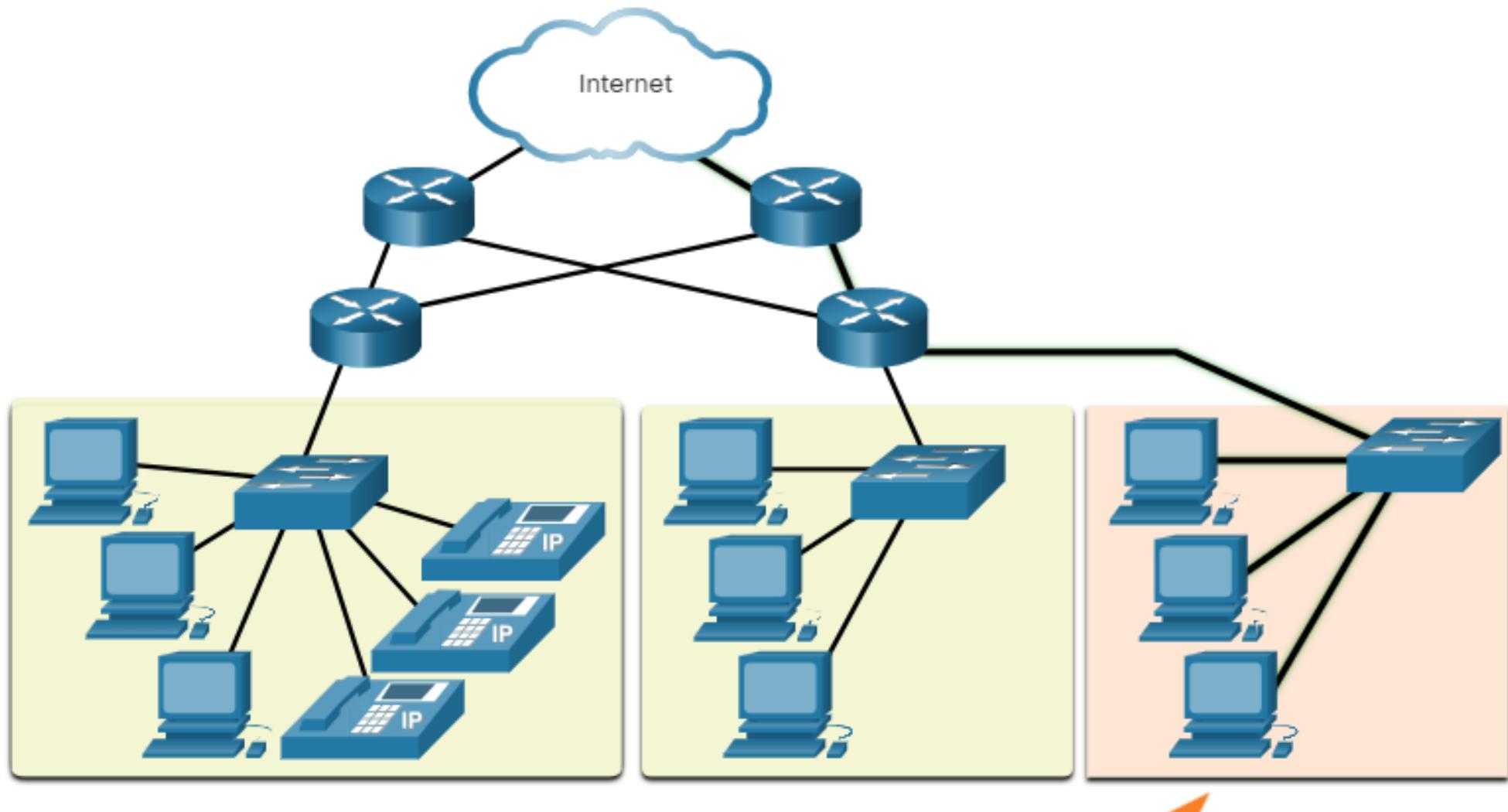


## Escalabilidade

Uma rede escalável se expande rapidamente para oferecer suporte a novos usuários e aplicativos. Ele faz isso sem degradar o desempenho dos serviços que estão sendo acessados por usuários existentes. A figura mostra como uma nova rede é facilmente adicionada a uma rede existente.

## Escalabilidade

Essas redes são escaláveis porque os projetistas seguem padrões e protocolos aceitos. Isso permite que os fornecedores de software e hardware se concentrem em melhorar produtos e serviços sem precisar criar um novo conjunto de regras para operar na rede.



Usuários adicionais e redes inteiras podem ser conectados à Internet sem reduzir o desempenho para usuários atuais.

## Qualidade do Serviço

A qualidade do serviço (QoS) é um requisito crescente das redes atualmente. Novos aplicativos disponíveis para usuários em redes, como transmissões de voz e vídeo ao vivo, criam expectativas mais altas em relação à qualidade dos serviços entregues. Conforme o conteúdo de vídeo, voz e dados continua a convergir na mesma rede, o QoS se torna um mecanismo essencial para gerenciar os congestionamentos e garantir a entrega confiável do conteúdo para todos os usuários.

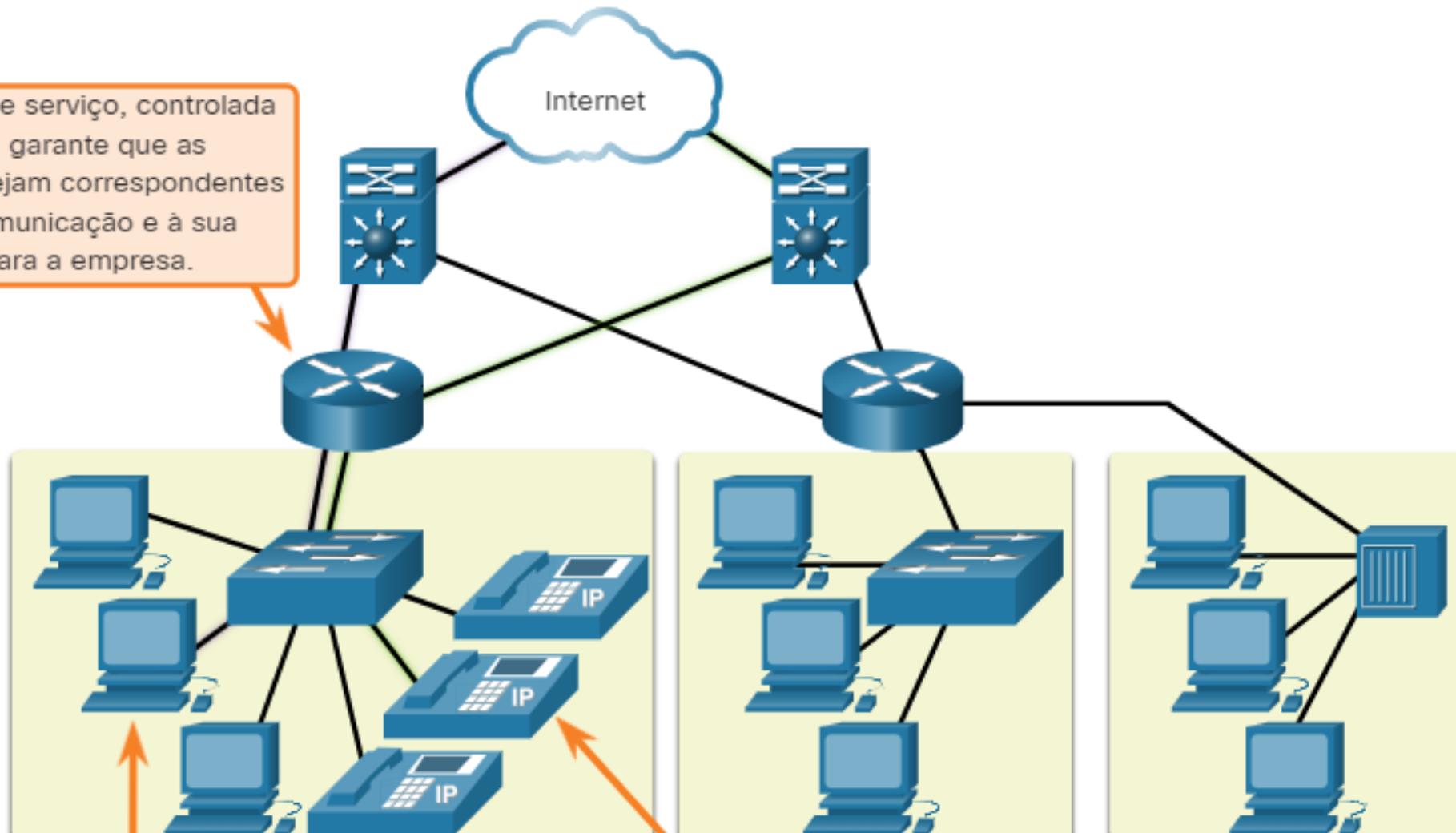
## Qualidade do Serviço

O congestionamento acontece quando a demanda por largura de banda excede a quantidade disponível. A largura de banda é medida pelo número de bits que podem ser transmitidos em um único segundo, ou bits por segundo (bps). Ao tentar uma comunicação simultânea pela rede, a demanda pela largura de banda pode exceder sua disponibilidade, criando um congestionamento na rede.

## Qualidade do Serviço

Quando o volume de tráfego é maior do que o que pode ser transportado pela rede, os dispositivos retêm os pacotes na memória até que os recursos estejam disponíveis para transmiti-los. Na figura, um usuário está solicitando uma página da Web e outro está em uma ligação. Com uma política de QoS configurada, o roteador é capaz de gerenciar o fluxo do tráfego de voz e de dados, priorizando as comunicações por voz se a rede ficar congestionada.

A qualidade de serviço, controlada pelo roteador, garante que as prioridades sejam correspondentes ao tipo de comunicação e à sua importância para a empresa.



Geralmente, as páginas Web podem receber uma prioridade mais baixa.

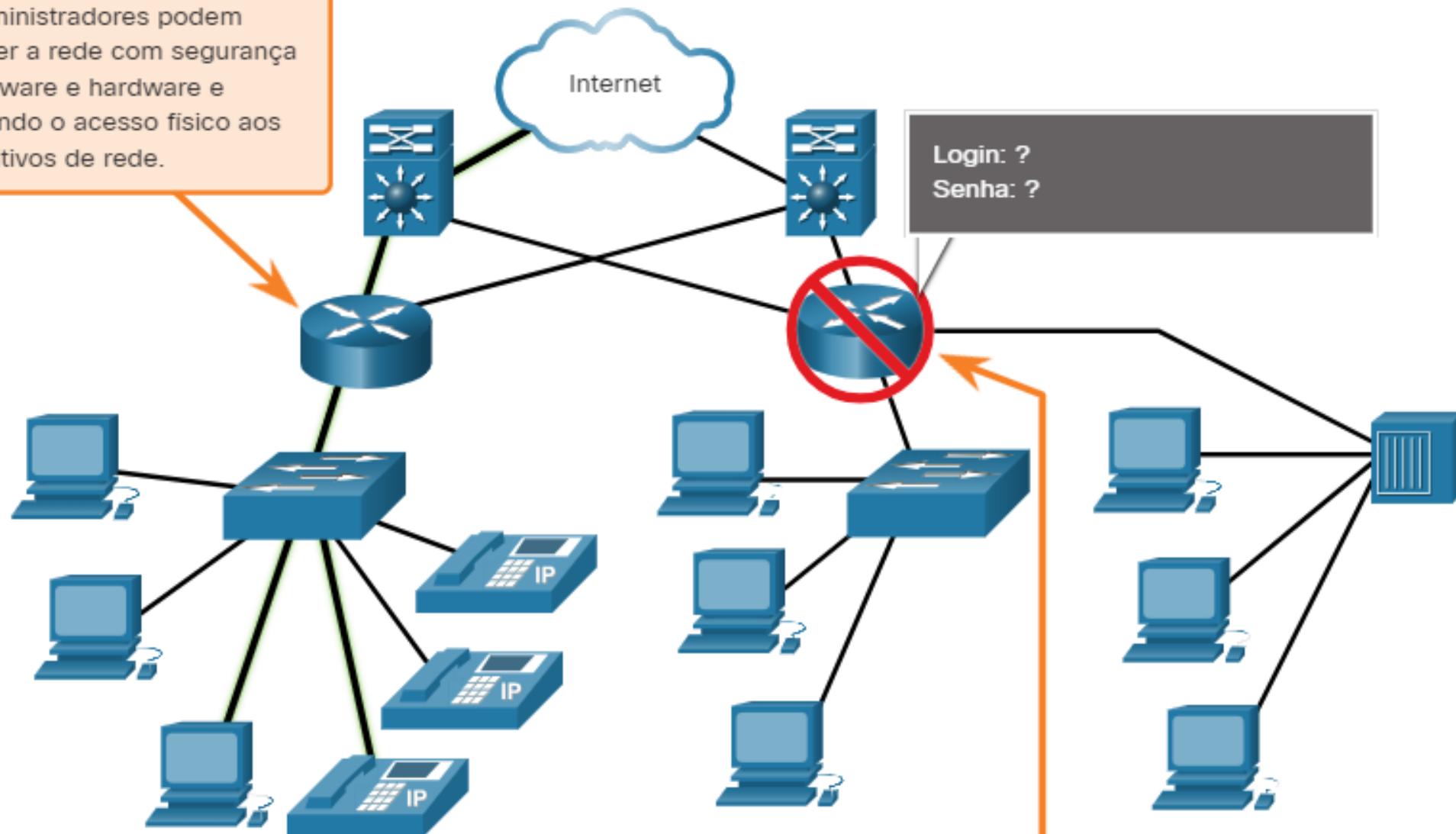
Uma chamada de voz sobre IP (VoIP) precisará de prioridade para manter uma experiência suave e ininterrupta do usuário.

## Segurança da rede

A infraestrutura da rede, os serviços e os dados contidos nos dispositivos conectados à rede são recursos pessoais e comerciais críticos. Os administradores de rede devem abordar dois tipos de preocupações de segurança de rede: segurança da infraestrutura de rede e segurança da informação.

Proteger a infraestrutura de rede inclui proteger fisicamente os dispositivos que fornecem conectividade de rede e impedir o acesso não autorizado ao software de gerenciamento que reside neles.

Os administradores podem proteger a rede com segurança de software e hardware e impedindo o acesso físico aos dispositivos de rede.



Medidas de segurança protegem a rede de acessos não autorizados.

## Segurança da rede

Os administradores de rede também devem proteger as informações contidas nos pacotes transmitidos pela rede e as informações armazenadas nos dispositivos conectados à rede. Para atingir os objetivos de segurança de rede, existem três requisitos principais.

# Segurança da rede

**Confidencialidade** - Confidencialidade dos dados significa que apenas os destinatários pretendidos e autorizados podem acessar e ler dados.

**Integridade** - A integridade dos dados garante aos usuários que as informações não foram alteradas na transmissão, da origem ao destino.

**Disponibilidade** - A disponibilidade de dados garante aos usuários acesso oportuno e confiável aos serviços de dados para usuários autorizados.

## Tendências recentes

As redes, como todo o resto, continuam a mudar.

À medida que novas tecnologias e dispositivos do usuário final chegam ao mercado, as empresas e os consumidores devem continuar se ajustando a esse ambiente em constante mudança. Existem várias tendências de rede que afetam organizações e consumidores:

- BYOD (Bring Your Own Device);
- Colaboração on-line;
- Comunicação por vídeo;
- Computação em nuvem.

## **Traga seu próprio dispositivo (BYOD)**

BYOD significa o uso de qualquer dispositivo, de qualquer propriedade e em qualquer lugar.

O conceito de qualquer dispositivo, para qualquer conteúdo, de qualquer maneira, é uma grande tendência global que requer mudanças significativas na maneira como usamos os dispositivos e os conectamos com segurança às redes. Isso se chama Traga seu próprio dispositivo (BYOD).

O BYOD permite aos usuários finais a liberdade de usar ferramentas pessoais para acessar informações e se comunicar através de uma rede comercial ou do campus. Com o crescimento de dispositivos de consumo e a queda de custo relacionada, funcionários e estudantes podem ter dispositivos avançados de computação e rede para uso pessoal. Isso inclui laptops, notebooks, tablets, smartphones e e-readers. Estes podem ser adquiridos pela empresa ou escola, adquiridos pelo indivíduo ou por ambos.

## Colaboração On-line

As pessoas querem se conectar à rede não só para acessar as aplicações de dados, mas também para colaborar com outras pessoas. A colaboração é definida como “ato de trabalho com outro ou outros em um projeto em parceria”. As ferramentas de colaboração, como o Cisco WebEx, mostrado na figura, oferecem aos funcionários, alunos, professores, clientes e parceiros uma maneira de conectar, interagir e alcançar instantaneamente seus objetivos.

## Comunicações em vídeo

Outra faceta da rede crítica para o esforço de comunicação e colaboração é o vídeo. O vídeo é usado para comunicação, colaboração e entretenimento. Chamadas de vídeo são feitas de e para qualquer pessoa com uma conexão à Internet, independentemente de onde elas estão localizadas.

A videoconferência é uma ferramenta poderosa para se comunicar com outras pessoas, local e globalmente. O vídeo está se tornando um requisito fundamental para a colaboração efetiva à medida que as empresas se expandem pelos limites geográficos e culturais.

## Computação em nuvem

A computação em nuvem é uma das maneiras pelas quais acessamos e armazenamos dados. A computação em nuvem nos permite armazenar arquivos pessoais, até fazer backup de uma unidade inteira em servidores pela Internet. Aplicativos como processamento de texto e edição de fotos podem ser acessados usando a nuvem.

## Computação em nuvem

Para as empresas, a computação em nuvem amplia os recursos de TI sem exigir investimento em nova infraestrutura, treinamento de novas equipes ou licenciamento de novo software. Esses serviços estão disponíveis sob demanda e são entregues economicamente a qualquer dispositivo que esteja em qualquer lugar do mundo, sem comprometer a segurança ou a função.

## Computação em nuvem

A computação em nuvem é possível devido aos data centers. Os data centers são instalações usadas para hospedar sistemas de computador e componentes associados. Um data center pode ocupar uma sala de um edifício, um ou mais andares ou todo um prédio do tamanho de um armazém. Os data centers normalmente são muito caros de construir e manter.

## Computação em nuvem

Por esse motivo, apenas as grandes empresas usam data centers construídos de forma privada para abrigar os dados e fornecer serviços aos usuários. Empresas de pequeno porte que não podem arcar com a manutenção de seu próprio data center podem reduzir os custos gerais de propriedade ao alugar um servidor e armazenar serviços em uma empresa de data center maior na nuvem.

## Computação em nuvem

Para segurança, confiabilidade e tolerância a falhas, os provedores de nuvem geralmente armazenam dados em data centers distribuídos. Em vez de armazenar todos os dados de uma pessoa ou uma organização em um data center, eles são armazenados em vários data centers em locais diferentes.

Existem quatro tipos principais de nuvens: nuvens públicas, nuvens privadas, nuvens híbridas e nuvens da comunidade

## **Nuvens públicas**

Aplicativos e serviços baseados em nuvem oferecidos em uma nuvem pública são criados disponível para a população em geral. Os serviços podem ser gratuitos ou são oferecidos em um modelo de pagamento por uso, como pagar por armazenamento on-line. A nuvem pública usa a internet para fornecer serviços.

## Nuvens privadas

Os aplicativos e serviços baseados em nuvem oferecidos em uma nuvem privada são destinado a uma organização ou entidade específica, como um governo. A nuvem privada pode ser configurada usando o rede, embora isso possa ser caro para construir e manter. Uma nuvem privada também pode ser gerenciada por uma organização externa com acesso estrito segurança.

## **Nuvens híbridas**

Uma nuvem híbrida é composta de duas ou mais nuvens (exemplo: parte privada, parte pública), onde cada parte permanece um objeto distinto, mas ambos são conectados usando uma única arquitetura. Indivíduos em uma nuvem híbrida seria capaz de ter graus de acesso a vários serviços com base em direitos de acesso do usuário.

Nuvens comunitárias      Uma nuvem de comunidade é criada para uso exclusivo por entidades ou organizações específicas. As diferenças entre nuvens públicas e nuvens da comunidade são as necessidades funcionais que foram personalizadas para a comunidade. Por exemplo, organizações de saúde devem manter a conformidade com políticas e leis (por exemplo, HIPAA) que exigem confidencialidade e autenticação especial.

As nuvens comunitárias são usadas por várias organizações que têm necessidades e preocupações semelhantes. As nuvens comunitárias são semelhantes a um ambiente de nuvem pública, mas com níveis definidos de segurança, privacidade e até mesmo conformidade normativa de uma nuvem privada.

## Tendências Tecnológicas em Casa

As tendências de rede não estão apenas afetando a maneira como nos comunicamos no trabalho e na escola, mas também mudando muitos aspectos da casa. As mais novas tendências para casas incluem a “tecnologia residencial inteligente”.



## Rede Powerline

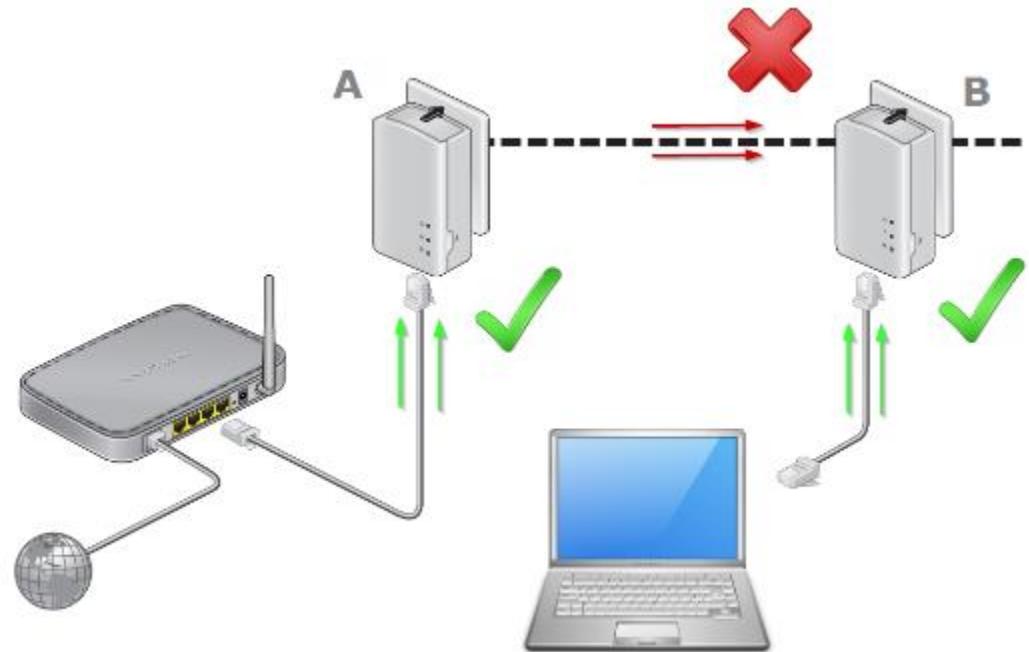
Um powerline nada mais é do que um dispositivo que funciona como um repetidor de sinal da sua internet dentro de casa. Ao conectar um cabo Ethernet ao roteador, o sinal é transmitido via banda larga adicionando um sinal modulado aos sistemas de fiação da rede elétrica.

A energia é transmitida em uma faixa que varia entre 50 Hz e 60 Hz, enquanto os dados são transmitidos em uma faixa que varia entre 1 Hz e 30 Hz. É por essa razão que as duas coisas podem correr pela fiação de forma simultânea.

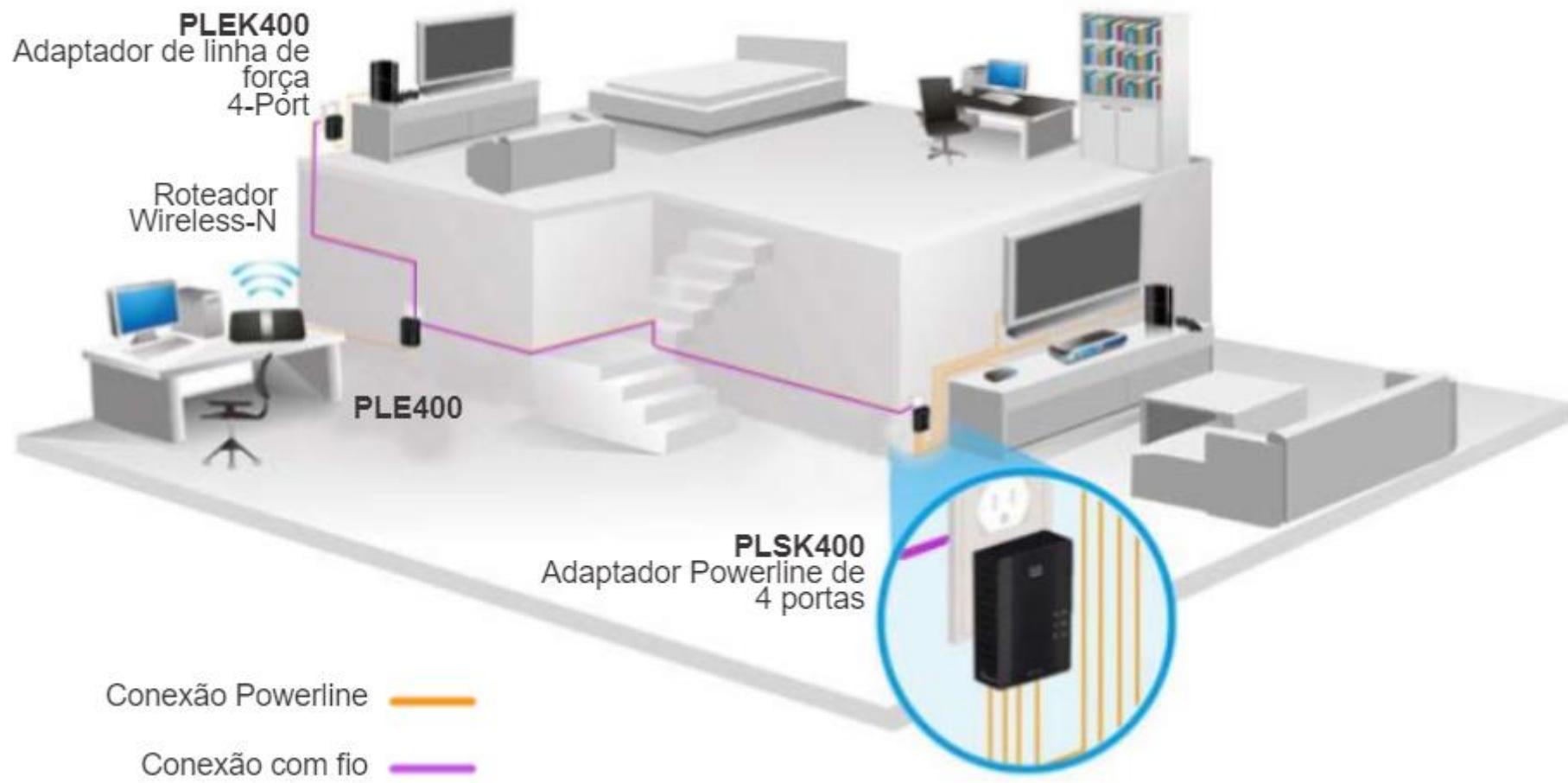
O segredo consiste em transformar as tomadas da casa em pontos de acesso à internet. Tudo o que você precisa fazer é colocar uma ponta do adaptador no seu roteador e a outra em uma tomada distante dele. Dessa forma, ele amplifica o sinal recebido a partir do ponto em questão.

## **Powerline é diferente de um repetidor?**

Sim. Embora suas funções sejam bastante similares, o modo de operação é completamente diferente. Os repetidores Wi-Fi se conectam ao roteador por meio de uma rede sem fio e, por essa razão, eles requerem proximidade da base, sendo indicados para lugares menores do que 100 metros quadrados.



Já o powerline se liga ao roteador por meio de um cabo Ethernet e, como a transferência é feita por meio da rede elétrica, as distâncias que o sinal percorre podem ser maiores, chegando a cobrir áreas de até 400 metros quadrados. É por essa razão que eles são um pouco mais caros do que os repetidores, além de mais eficientes.



## Ameaças à Segurança

A segurança da rede é parte integrante da rede de computadores, independentemente de a rede estar em uma casa com uma única conexão à Internet ou se é uma corporação com milhares de usuários. A segurança da rede deve considerar o ambiente, bem como as ferramentas e os requisitos da rede. Ele deve poder proteger os dados e, ao mesmo tempo, permitir a qualidade do serviço que os usuários esperam da rede.

A proteção de uma rede envolve protocolos, tecnologias, dispositivos, ferramentas e técnicas para proteger dados e mitigar ameaças. Vetores de ameaça podem ser internos ou externos. Hoje, muitas ameaças à segurança de rede externa se originam da Internet.

Existem várias ameaças externas comuns às redes:

**Vírus, worms e cavalos de Tróia** - Eles contêm software ou código malicioso em execução no dispositivo do usuário.

**Spyware e adware** - Estes são tipos de software que são instalados no dispositivo de um usuário. O software, em seguida, coleta secretamente informações sobre o usuário.

**Ataques de dia zero** - Também chamados de ataques de hora zero, ocorrem no primeiro dia em que uma vulnerabilidade se torna conhecida.

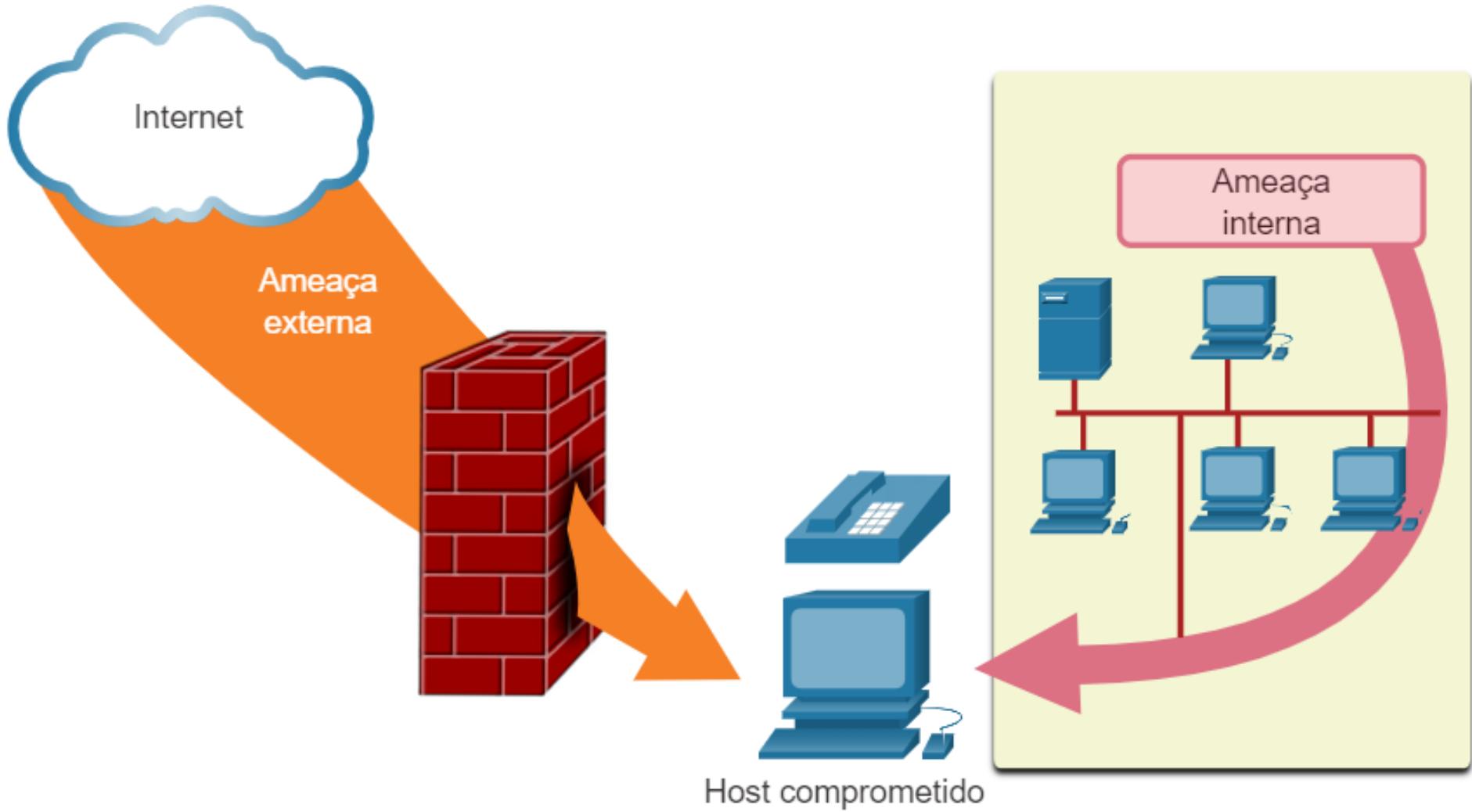
**Ataques de ator de ameaça** - Uma pessoa mal-intencionada ataca dispositivos de usuário ou recursos de rede.

**Ataques de negação de serviço** - Esses ataques atrasam ou travam aplicativos e processos em um dispositivo de rede.

**Interceptação de dados e roubo** - Esse ataque captura informações privadas da rede de uma organização.

**Roubo de identidade** - Esse ataque rouba as credenciais de login de um usuário para acessar informações privadas.

Também é importante considerar ameaças internas. Há muitos estudos que mostram que as violações mais comuns ocorrem por causa de usuários internos da rede. Isso pode ser atribuído a dispositivos perdidos ou roubados, mau uso acidental por parte dos funcionários e, no ambiente comercial, até mesmo funcionários mal-intencionados. Com as estratégias BYOD em evolução, os dados corporativos ficam muito mais vulneráveis. Portanto, ao desenvolver uma política de segurança, é importante abordar ameaças de segurança externas e internas.



## Soluções de Segurança

Nenhuma solução única pode proteger a rede da variedade de ameaças existentes. Por esse motivo, a segurança deve ser implementada em várias camadas, com uso de mais de uma solução. Se um componente de segurança falhar na identificação e proteção da rede, outros poderão ter êxito.

Uma implementação de segurança para redes domésticas é normalmente bastante básica. Normalmente, você o implementa nos dispositivos finais, bem como no ponto de conexão com a Internet, e pode até confiar nos serviços contratados pelo ISP.

Estes são os componentes básicos de segurança para uma rede doméstica ou de pequeno escritório:

**Antivírus e antispyware** - Esses aplicativos ajudam a proteger os dispositivos finais contra a infecção por software malicioso.

**Filtragem por firewall** - A filtragem por firewall bloqueia o acesso não autorizado dentro e fora da rede. Isso pode incluir um sistema de firewall baseado em host que impede o acesso não autorizado ao dispositivo final ou um serviço básico de filtragem no roteador doméstico para impedir o acesso não autorizado do mundo externo à rede.

Em contrapartida, a implementação de segurança para uma rede corporativa geralmente consiste em vários componentes incorporados à rede para monitorar e filtrar o tráfego. Idealmente, todos os componentes trabalham juntos, o que minimiza a manutenção e melhora a segurança. Redes maiores e redes corporativas usam antivírus, antispyware e filtragem por firewall, mas também têm outros requisitos de segurança:

**Sistemas de firewall dedicados** - Eles fornecem recursos de firewall mais avançados que podem filtrar grandes quantidades de tráfego com mais granularidade.

**Listas de controle de acesso (ACL)** - Eles filtram ainda mais o acesso e o encaminhamento de tráfego com base em endereços e aplicativos IP.

**Sistemas de prevenção de intrusões (IPS)** - Identificam ameaças de rápida disseminação, como ataques de dia zero ou hora zero.

**Redes privadas virtuais (VPN)** - fornecem acesso seguro a uma organização para trabalhadores remotos.

Os requisitos de segurança de rede devem considerar o ambiente, os vários aplicativos e os requisitos de computação. Ambientes domésticos e comerciais devem poder proteger seus dados e, ao mesmo tempo, permitir a qualidade do serviço que os usuários esperam de cada tecnologia. Além disso, as soluções de segurança implementadas devem ser adaptáveis às tendências de crescimento e variáveis da rede.

O estudo das ameaças à rede e de técnicas de mitigação é iniciado com um claro entendimento da infraestrutura de roteamento e de comutação usada para organizar serviços de rede.

# CONFIGURAÇÃO BÁSICA DE DISPOSITIVOS

## Nomes de Dispositivo

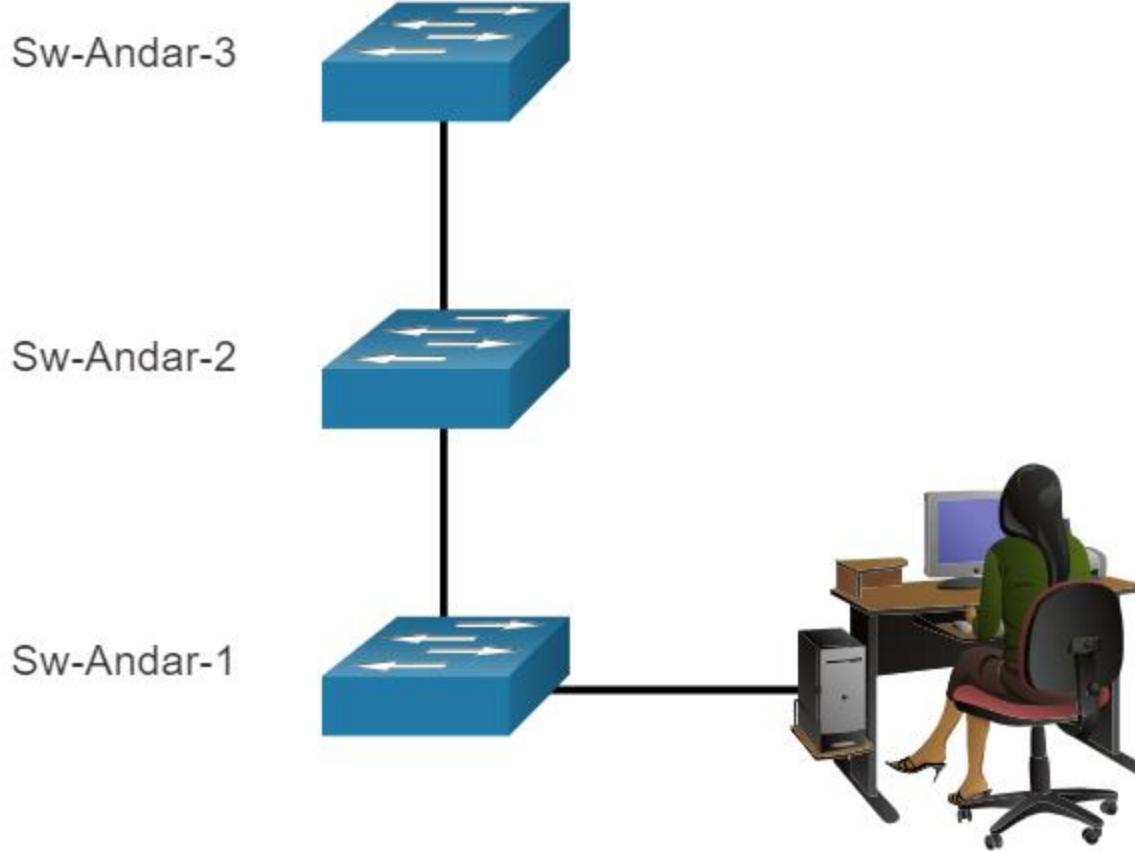
O primeiro comando de configuração em qualquer dispositivo deve ser dar a ele um nome de dispositivo exclusivo ou nome de host.

Com uma escolha sábia de nomes, é mais fácil lembrar, documentar e identificar dispositivos de rede. Aqui estão algumas diretrizes de nomenclatura importantes para hosts:

- Começar com uma letra;
- Não conter espaços;
- Terminar com uma letra ou dígito;
- Usar somente letras, números e traços;
- Ter menos de 64 caracteres.

Uma organização deve escolher uma convenção de nomenclatura que torne fácil e intuitivo identificar um dispositivo específico. Os nomes de host usados no IOS do dispositivo preservam os caracteres em maiúsculas e minúsculas. Por exemplo, a figura mostra que três comutadores, abrangendo três andares diferentes, estão interconectados em uma rede.

A convenção de nomenclatura usada incorporou o local e a finalidade de cada dispositivo. A documentação de rede deve explicar como esses nomes foram escolhidos, de modo que outros dispositivos possam receber nomes apropriados.



# **PROTOCOLOS DE REDE**

Os protocolos usados nas comunicações de rede compartilham muitas dessas características fundamentais. Além de identificar a origem e o destino, os protocolos de computadores e de redes definem os detalhes sobre como uma mensagem é transmitida por uma rede. Protocolos de computador comuns incluem os seguintes requisitos:

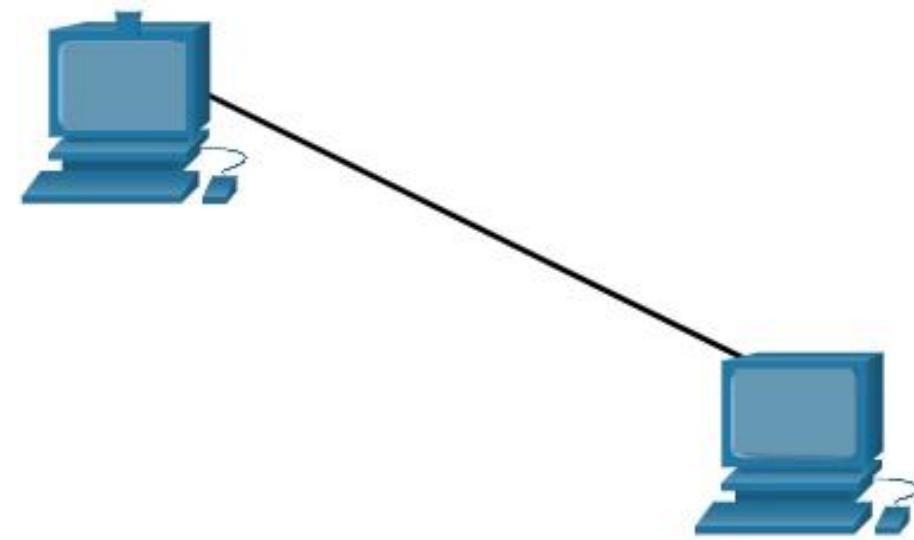
- Codificação de mensagens;
- Formatação e encapsulamento de mensagens;
- Tamanho da mensagem;
- Tempo da mensagem;
- Opções de envio de mensagem.

# Codificação de Mensagens

Uma das primeiras etapas para enviar uma mensagem é codificá-la. A codificação é o processo de conversão de informações em outra forma aceitável para a transmissão. A decodificação reverte esse processo para interpretar as informações.

A codificação entre hosts deve estar em um formato adequado para o meio físico. As mensagens enviadas pela rede são convertidas primeiramente em bits pelo host emissor. Cada bit é codificado em um padrão de tensões em fios de cobre, luz infravermelha em fibras ópticas ou microondas para sistemas sem fio. O host de destino recebe e decodifica os sinais para interpretar a mensagem.

Mensagem Sinal Mensagem



# Formatação e Encapsulamento de Mensagens

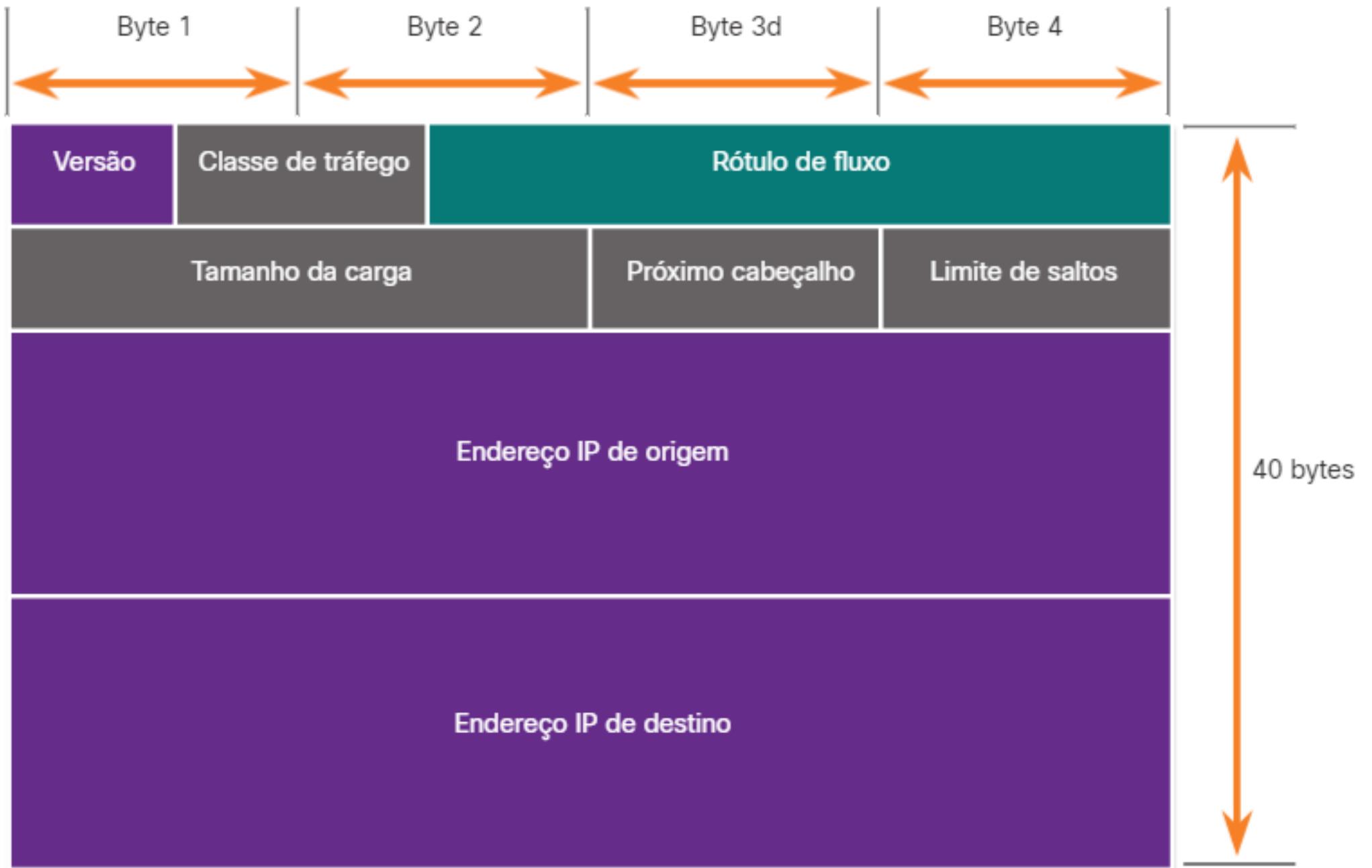
Quando uma mensagem é enviada da origem para o destino, deve usar um formato ou uma estrutura específica. Os formatos da mensagem dependem do tipo de mensagem e do canal usado para entregá-la.

## **Rede**

Semelhante ao envio de uma carta, uma mensagem enviada por uma rede de computadores segue regras específicas de formato para que ela seja entregue e processada.

## Rede

Internet Protocol (IP) é um protocolo com uma função semelhante ao exemplo de envelope. Na figura, os campos do pacote IPv6 (Internet Protocol versão 6) identificam a origem do pacote e seu destino. IP é responsável por enviar uma mensagem da origem da mensagem para o destino através de uma ou mais redes.

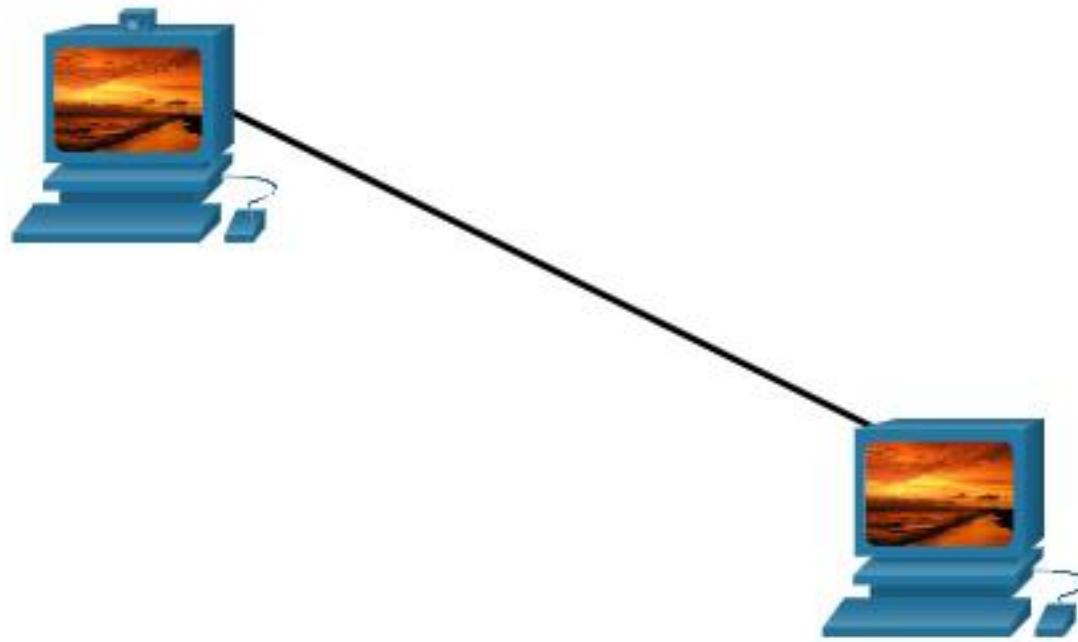


# Tamanho da Mensagem

Outra regra de comunicação é o tamanho da mensagem.

Do mesmo modo, quando uma mensagem longa é enviada de um host a outro em uma rede, é necessário dividir a mensagem em partes menores. As regras que regem o tamanho das partes, ou quadros, transmitidos pela rede são muito rígidas. Também podem diferir, dependendo do canal usado. Os quadros que são muito longos ou muito curtos não são entregues.

As restrições de tamanho dos quadros exigem que o host origem divida uma mensagem longa em pedaços individuais que atendam aos requisitos de tamanho mínimo e máximo. A mensagem longa será enviada em quadros separados, e cada um contém uma parte da mensagem original. Cada quadro também terá suas próprias informações de endereço. No host destino, as partes individuais da mensagem são reconstruídas na mensagem original.



Os protocolos usados nas comunicações de rede compartilham muitas dessas características fundamentais. Além de identificar a origem e o destino, os protocolos de computadores e de redes definem os detalhes sobre como uma mensagem é transmitida por uma rede. Protocolos de computador comuns incluem os seguintes requisitos:

# Temporização de Mensagem

O tempo de mensagens também é muito importante nas comunicações de rede. A temporização da mensagem inclui o seguinte:

# Temporização de Mensagem

**Controle de Fluxo** - Este é o processo de gerenciamento da taxa de transmissão de dados. O controle de fluxo define quanta informação pode ser enviada e a velocidade com que pode ser entregue. Por exemplo, se uma pessoa fala muito rapidamente, pode ser difícil para o receptor ouvir e entender a mensagem. Na comunicação de rede, existem protocolos de rede usados pelos dispositivos de origem e destino para negociar e gerenciar o fluxo de informações.

# Temporização de Mensagem

**Tempo limite da resposta** - se uma pessoa fizer uma pergunta e não ouvir uma resposta dentro de um período de tempo aceitável, ela assume que nenhuma resposta está chegando e reage de acordo. A pessoa pode repetir a pergunta ou prosseguir com a conversa. Os hosts da rede usam protocolos de rede que especificam quanto tempo esperar pelas respostas e que ação executar se ocorrer um tempo limite de resposta.

# Temporização de Mensagem

**Método de acesso** - determinar quando alguém pode enviar uma mensagem.

# Opções de Envio de Mensagem

Uma mensagem pode ser entregue de maneiras diferentes.

As comunicações em rede têm opções de entrega semelhantes para se comunicar. Como mostrado na figura, existem três tipos de comunicações de dados que incluem:

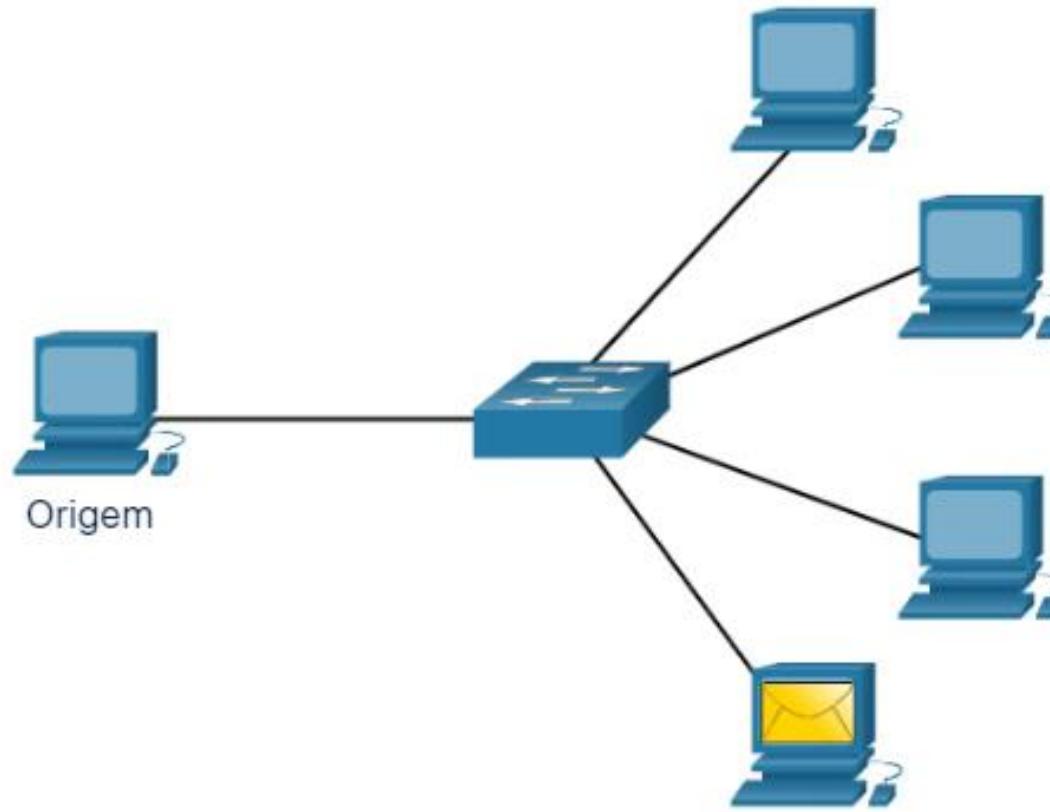
# Opções de Envio de Mensagem

**Unicast** - As informações estão sendo transmitidas para um único dispositivo final.

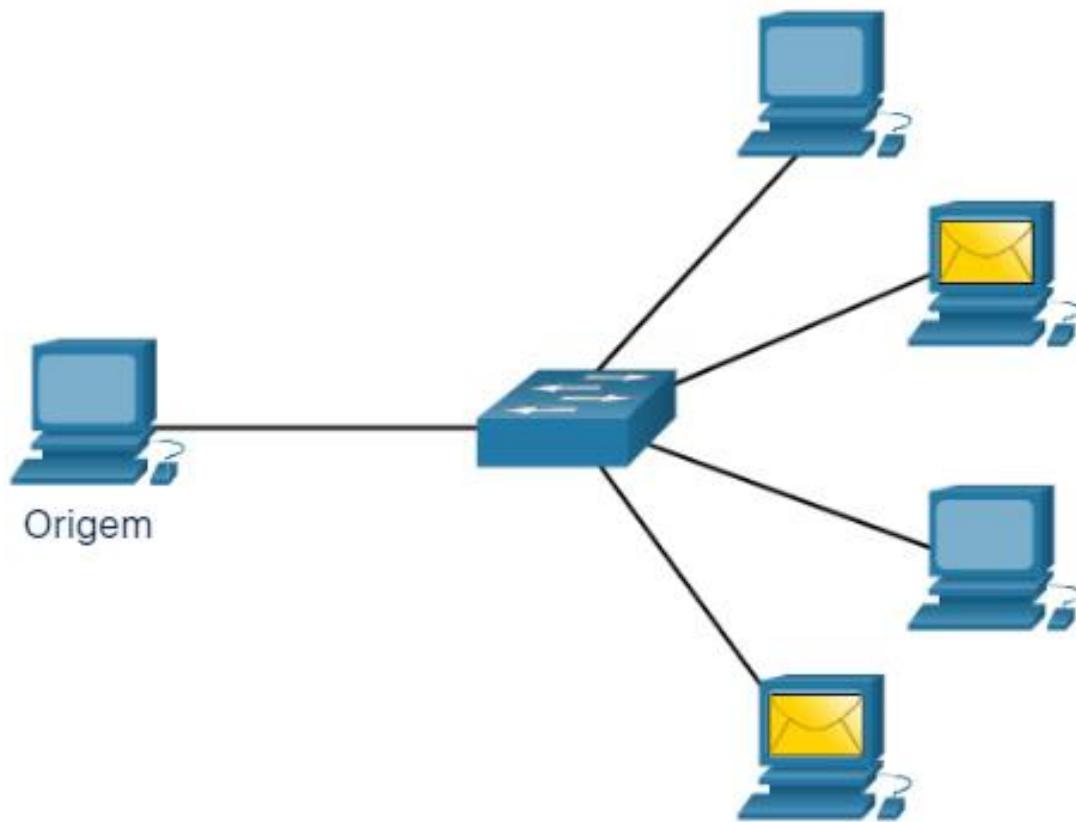
**Multicast** - Informações estão sendo transmitidas para um ou mais dispositivos finais.

**Broadcast** - Informações estão sendo transmitidas para todos os dispositivos finais.

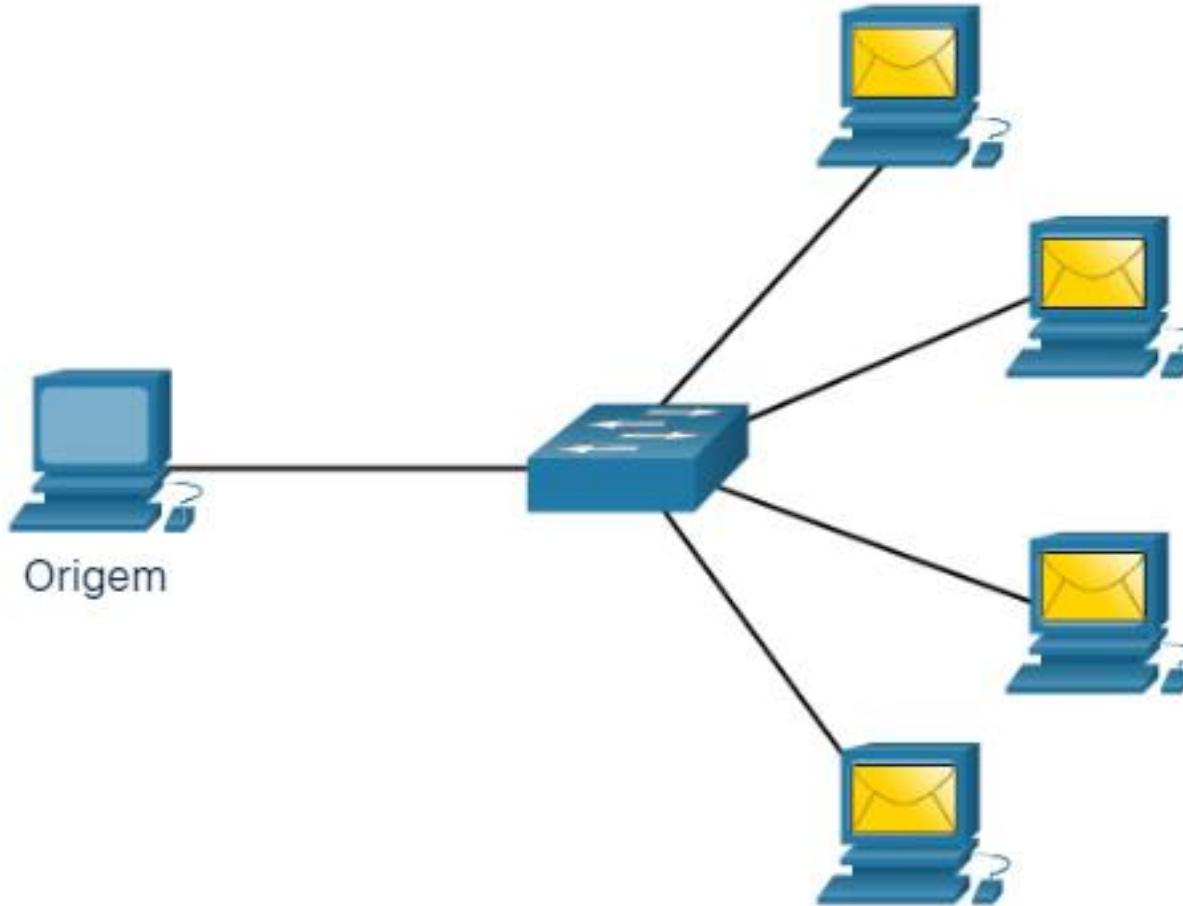
# UNICAST



# MULTICAST



# BRODCAST



# PROTOCOLO DE REDE

Os dispositivos finais possam se comunicar através de uma rede, cada dispositivo deve cumprir o mesmo conjunto de regras. Essas regras são chamadas de protocolos e elas têm muitas funções em uma rede.

# PROTOCOLO DE REDE

Os protocolos de rede definem um formato comum e um conjunto de regras para a troca de mensagens entre dispositivos. Os protocolos são implementados por dispositivos preliminares e intermediários em software, hardware ou ambos. Cada protocolo de rede tem sua própria função, formato e regras para comunicações.

# PROTOCOLO DE REDE

TIPO DE PROTOCOLO	DESCRIÇÃO
<b>Protocolos de comunicação em rede</b>	Os protocolos permitem que dois ou mais dispositivos se comuniquem através de uma ou mais redes. A família de tecnologias Ethernet envolve uma variedade de protocolos como IP, Transmission Control Protocol (TCP), HyperText Protocol de download (HTTP) e muito mais.

# PROTOCOLO DE REDE

TIPO DE PROTOCOLO	DESCRIÇÃO
<b>Protocolos de segurança de rede</b>	Protocolos protegem os dados para fornecer autenticação, integridade dos dados e criptografia de dados. Exemplos de protocolos de seguro incluem o Secure Shell (SSH), SSL (Secure Sockets Layer) e TLS (Transport Layer Security).

# PROTOCOLO DE REDE

TIPO DE PROTOCOLO	DESCRIÇÃO
<b>Protocolos de roteamento</b>	Os protocolos permitem que os roteadores troquem informações de rota, compare o caminho e, em seguida, selecione o melhor caminho para o destino remoto. Exemplos de protocolos de roteamento incluem Open Shortest Path First (OSPF) e Border Gateway Protocol (BGP).

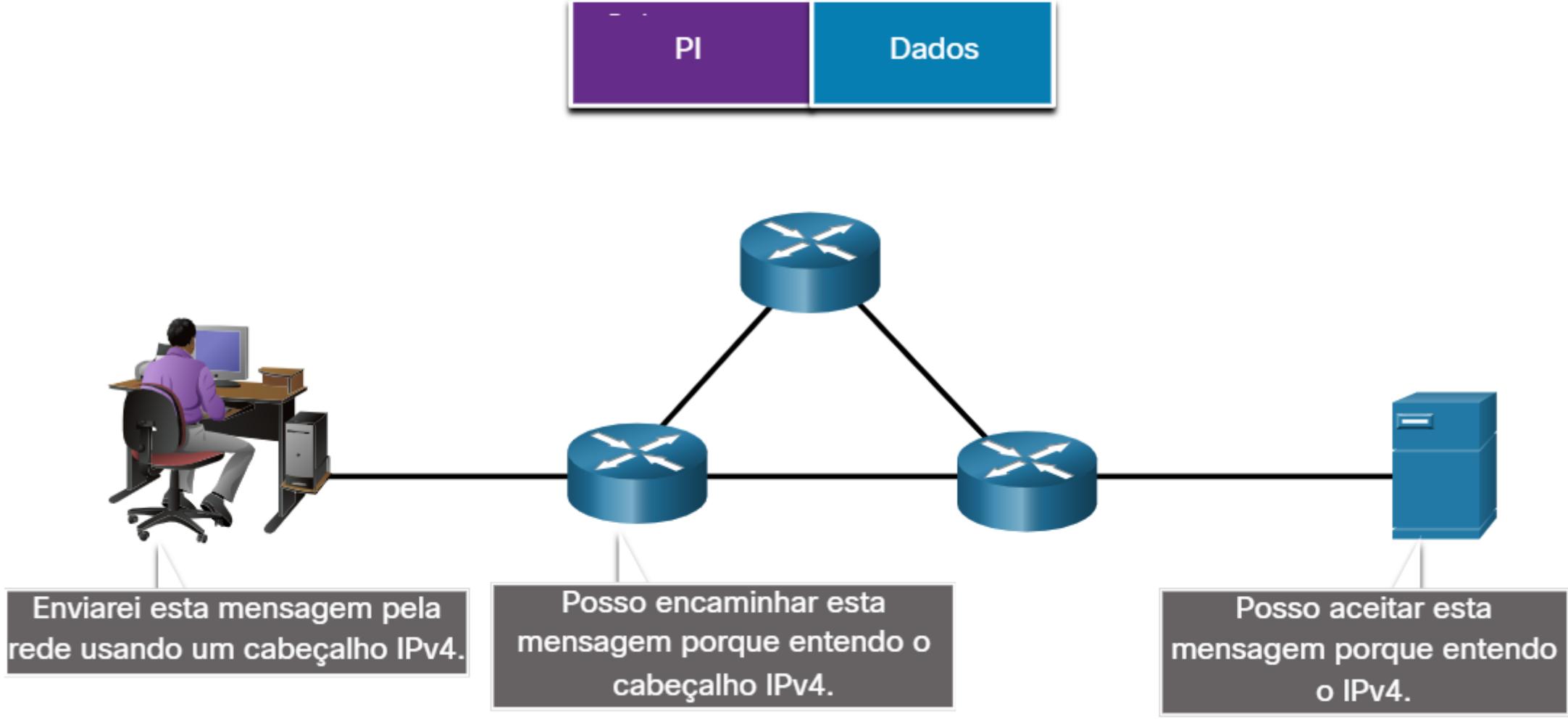
# PROTOCOLO DE REDE

TIPO DE PROTOCOLO	DESCRIÇÃO
<b>Protocolos de descoberta de serviço</b>	Protocolos são usados para detecção automática de dispositivos ou serviços. Exemplos de protocolos de detecção de serviços incluem Host dinâmico Protocolo de Configuração (DHCP) que detecta serviços para alocação de endereço IP e Sistema de Nomes de Domínio (DNS) que é usado para executar conversão de nome para endereço IP.

# Funções de protocolo de rede

Os protocolos de comunicação de rede são responsáveis por uma variedade de funções necessárias para comunicações de rede entre dispositivos finais.

# Funções de protocolo de rede

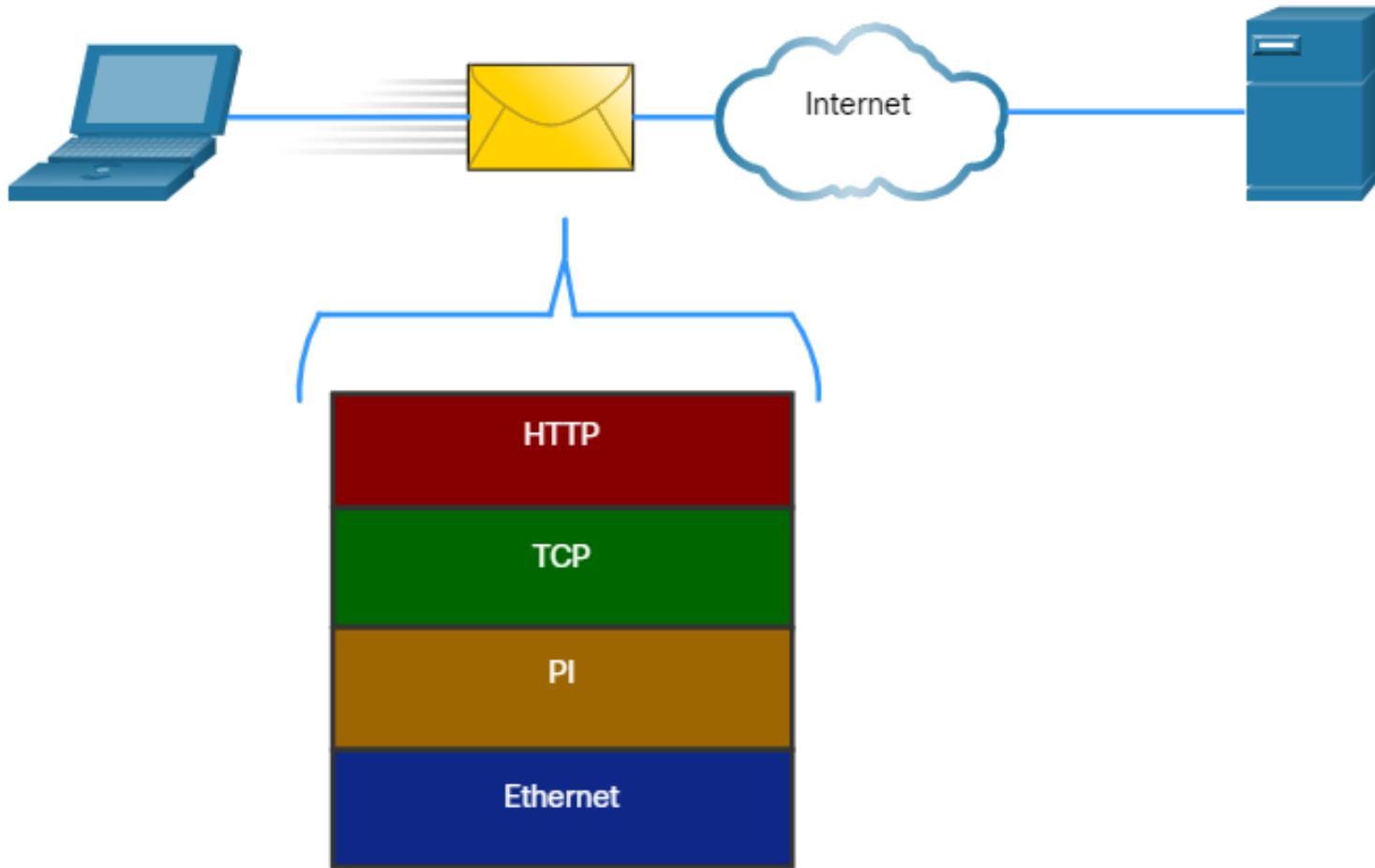


FUNÇÃO	DESCRIÇÃO
<b>Endereçamento</b>	Identificar o remetente e o destinatário da mensagem usando um esquema de endereçamento definido. Exemplos de protocolos fornecidos incluem Ethernet, IPv4 e IPv6.
<b>Confiabilidade</b>	Esta função fornece mecanismos de entrega garantidos em caso de mensagens perdidas ou prejudicadas no trânsito. O TCP fornece entrega garantida.

FUNÇÃO	DESCRIÇÃO
<b>Sequenciamento</b>	Esta função rotula exclusivamente cada segmento de dados transmitidos. A usa como informações de sequenciamento para remontar as informações corretamente. Isso é útil se os segmentos de dados forem perdidos, atrasados ou recebidos fora de ordem. O TCP fornece serviços de sequenciamento.
<b>Detecção de erros</b>	Esta função é usada para determinar se os dados foram interrompidos durante a transmissão. Vários protocolos que fornecem detecção de erros incluem Ethernet, IPv4, IPv6 e TCP.
<b>Interface de aplicação</b>	Esta função contém informações usadas para processar a comunicação entre aplicações de rede. Por exemplo, ao acessar uma página da Web, os protocolos HTTP ou HTTPS são usados para se comunicar entre os processos da Web do cliente e do servidor.

# Interação de Protocolos

Uma mensagem enviada através de uma rede de computadores normalmente requer o uso de vários protocolos, cada um com suas próprias funções e formato. A figura mostra alguns protocolos de rede comuns que são usados quando um dispositivo envia uma solicitação para um servidor Web para sua página da Web.



Os protocolos na figura são descritos da seguinte forma:

- **Protocolo de transferência de hipertexto (HTTP)** - Este protocolo controla a mesma maneira que um servidor da web e um cliente de interação web. O HTTP define o conteúdo e a formatação das conexões e respostas trocadas entre o cliente e o servidor. Tanto o software do cliente quanto o servidor Web implementam HTTP como parte da aplicação. O HTTP conta com outros protocolos para controlar o modo como as mensagens são transportadas entre cliente e servidor.
- **Transmission Control Protocol (TCP)** - Este protocolo gerencia as conversas individuais. A TCP é responsável por garantir a entrega confiável das informações e gerenciar o controle de fluxo entre os dispositivos finais.
- **Protocolo Internet (IP)** - Este protocolo é responsável por entregar mensagens do remetente para o receptor. IP é usado por roteadores para encaminhar mensagens em várias redes.
- **Ethernet** - Este protocolo é responsável pela entrega de mensagens de uma NIC para outra NIC na mesma rede local (LAN) Ethernet.

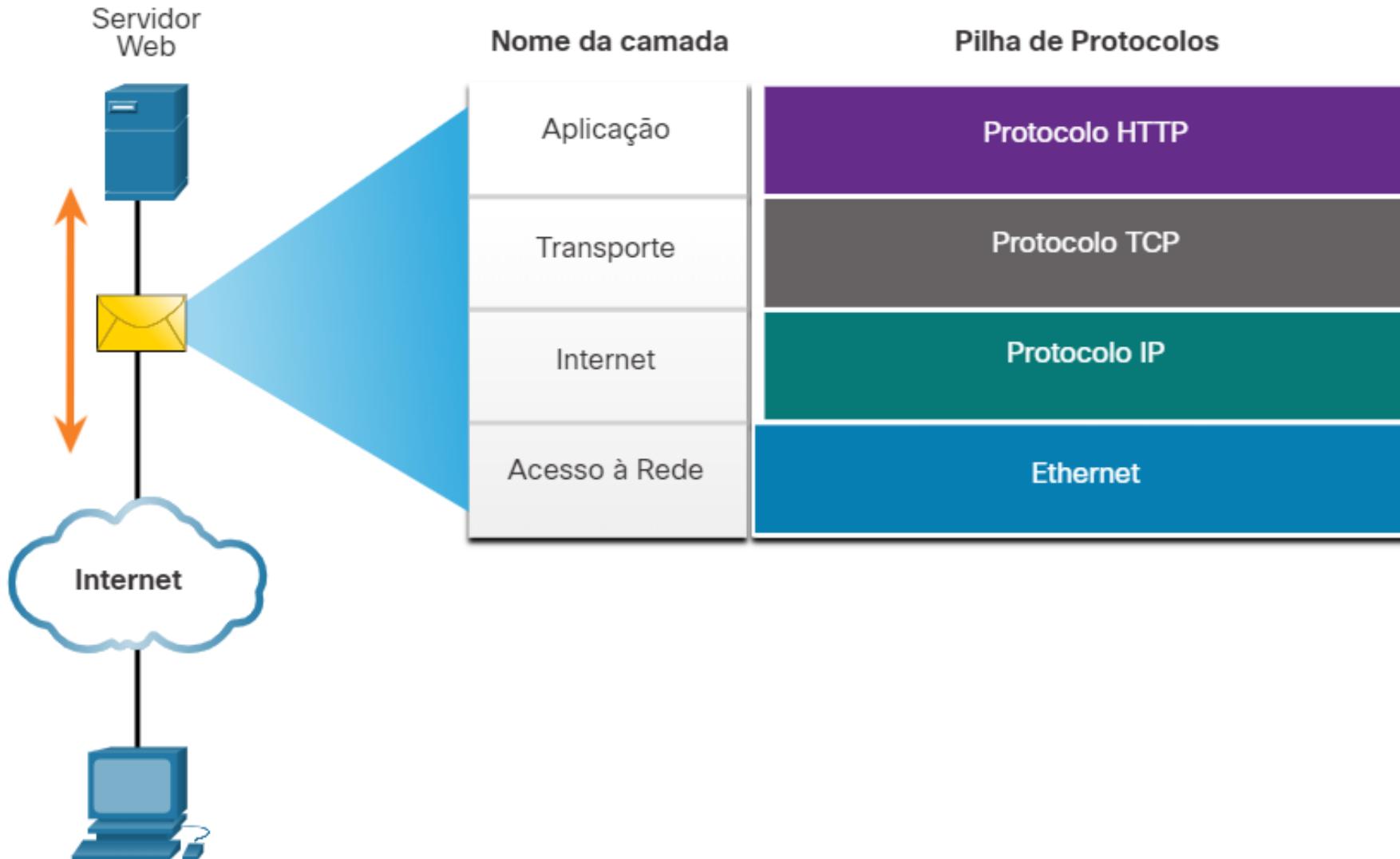
# CONJUNTOS DE PROTOCOLOS

Nome da camada TCP/IP	TCP/IP	ISO	Apple Talk	Novell Netware
Aplicação	HTTP DNS DHCP FTP	ACSE ROSA TRSE SESE	AFP	NDS
Transporte	TCP/UDP –	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Acesso à Rede		WLAN Ethernet ARP		

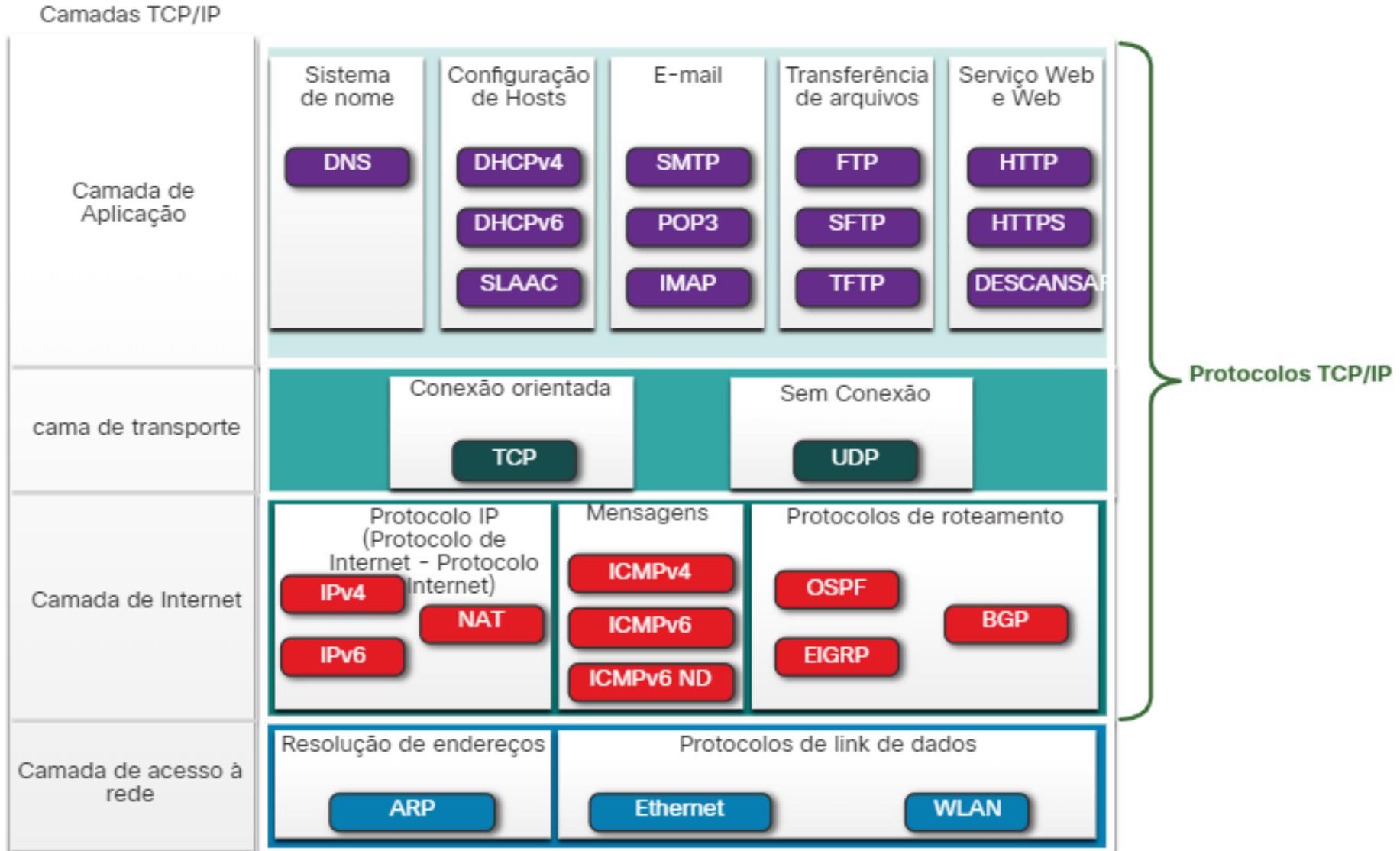
# Exemplo de Protocolo TCP/IP

Os protocolos TCP/IP estão disponíveis para as camadas de aplicativo, transporte e Internet. Não há protocolos TCP/IP na camada de acesso à rede. Os protocolos LAN da camada de acesso à rede mais comum são os protocolos Ethernet e WLAN (LAN sem fio). Os protocolos da camada de acesso à rede são responsáveis por fornecer o pacote IP pela mídia física.

# Exemplo de Protocolo TCP/IP



# Suíte de Protocolos TCP/IP



TCP/IP é o conjunto de protocolos usado pela internet e pelas redes de hoje. O TCP/IP tem dois aspectos importantes para fornecedores e fabricantes:

- **Conjunto de protocolos padrão aberto** - Isso significa que está disponível gratuitamente ao público e pode ser usado por qualquer fornecedor em seu hardware ou software.
- **Conjunto de protocolos com base em padrões** - isso significa que foi endossado pela indústria de rede e aprovado por uma organização de padrões. Isso garante que produtos de diferentes fabricantes possam interoperar com sucesso.

# CAMADA DE APLICAÇÃO

## Sistema de nomes

DNS - Sistema de nomes de domínio. Converter nomes de domínio, como cisco.com, em endereços IP.

# CAMADA DE APLICAÇÃO

## Configuração de hosts

DHCPv4 - Protocolo de configuração de host dinâmico para IPv4. Um servidor DHCPv4 atribui dinamicamente informações de endereçamento IPv4 aos clientes DHCPv4 na inicialização e permite que os endereços sejam reutilizados quando não forem mais necessários.

DHCPv6 - Protocolo de Configuração do Host Dinâmico para IPv6. DHCPv6 é semelhante ao DHCPv4. Um servidor DHCPv6 atribui dinamicamente informações de endereçamento IPv6 aos clientes DHCPv6 na inicialização.

# CAMADA DE APLICAÇÃO

## E-mail

SMTP -Protocolo de transferência de correio simples. Permite que os clientes enviem e-mails para um servidor de e-mail e permite que os servidores enviem e-mails para outros servidores.

# CAMADA DE APLICAÇÃO

## E-mail

**POP3** - Post Office Protocol versão 3. Permite que os clientes recuperem e-mails de um servidor de e-mail e baixem o e-mail para o aplicativo de e-mail local do cliente.

**IMAP** - Protocolo de Acesso à Mensagem na Internet. Permite que os clientes acessem o e-mail armazenado em um servidor de e-mail e também mantenham o e-mail no servidor.

# CAMADA DE APLICAÇÃO

## Transferência de arquivos

- **FTP**

Protocolo de transferência de arquivos. Define as regras que permitem que um usuário em um host acesse e transfira arquivos para e de outro host em uma rede. O FTP é um protocolo de entrega de arquivos confiáveis, orientado a conexão e reconhecido.

# CAMADA DE APLICAÇÃO

## Web e serviço Web

- **HTTP** - Protocolo de transferência de hipertexto. Um conjunto de regras para a troca de texto, imagens gráficas, som, vídeo e outros arquivos multimídia na World Wide Web.
- **HTTPS** - HTTP seguro. Uma forma segura de HTTP que criptografa os dados que são trocados pela World Wide Web.

# CAMADA DE TRANSPORTE

## Conexão orientada

**TCP** - Protocolo de controle de transmissão. Permite a comunicação confiável entre processos executados em hosts separados e fornecidos supervisionados e reconhecidos que confirmam a entrega bem-sucedida.

## Sem Conexão

**UDP** - Protocolo de datagrama do usuário. Permite que um processo em execução em um host envie pacotes para um processo em execução em outro host. No entanto, o UDP não confirmou a transmissão bem-sucedida do datagrama.

# CAMADA DE INTERNET

## Protocolo IP (Internet Protocol)

- **IPv4** - Protocolo da Internet 4. Recebe segmentos de mensagem da camada de transporte, embalados mensagens em pacotes e endereça pacotes versão para entrega de ponta a ponta através de uma rede. O IPv4 usa um endereço de 32 bits.
- **IPv6** - IP versão 6. semelhante ao IPv4, mas usa um endereço de 128 bits.

# CAMADA DE ACESSO A REDE

## Resolução de endereços

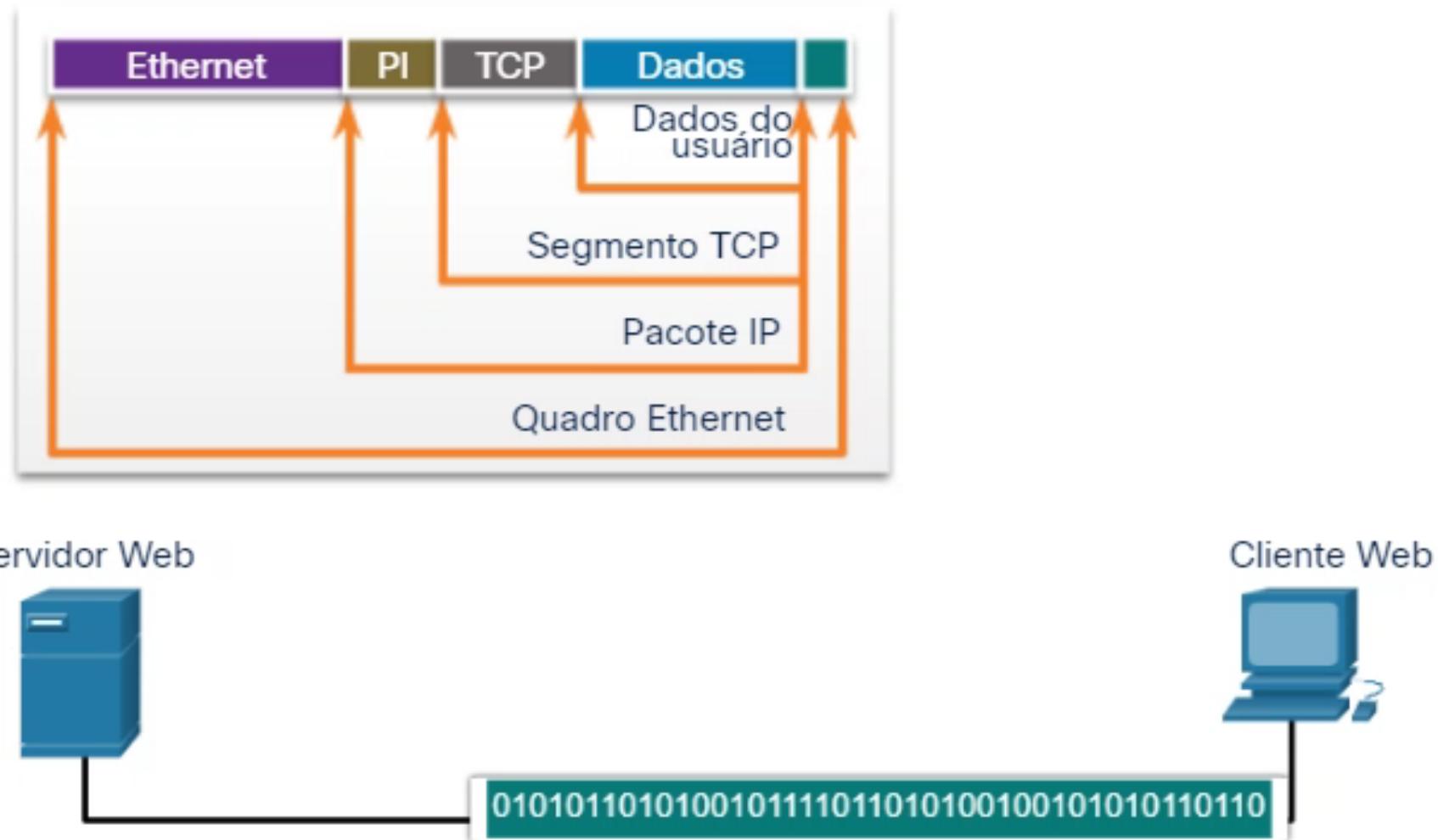
- **ARP** - Protocolo de Resolução de Endereço. mapeamento fornecido de endereço dinâmico entre um endereço IPv4 e um endereço de hardware.
- **Observação** : O ARP opera na camada de Acesso à Rede (OSI Camada 2) porque o seu objetivo principal é descobrir o endereço MAC do destino. Um endereço MAC é um endereço da camada 2.

# CAMADA DE ACESSO A REDE

## Protocolos de link de dados

- **Ethernet** - define como regras para os padrões de iluminação e sinalização da camada de acesso à rede.
- **WLAN** - Rede local sem fio. Definir como regras para sinalização sem fio nas frequências de rádio de 2,4 GHz e 5 GHz.

# Processo de Comunicação TCP/IP



# Processo de Comunicação TCP/IP



# EMPRESAS DE PADRÕES

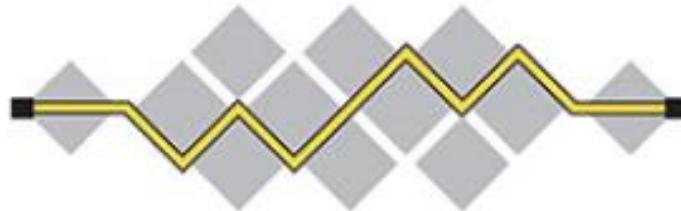
## PADRÕES ABERTOS

Como existem muitos fabricantes diferentes de componentes de rede, todos eles devem usar os mesmos padrões. Em redes, os padrões são desenvolvidos por organizações internacionais de padrões.

Os padrões abertos incentivam a interoperabilidade, a concorrência e a inovação. Eles também garantem que o produto de nenhuma empresa possa monopolizar o mercado ou ter uma vantagem injusta sobre a concorrência.

Um bom exemplo disso é a compra de um roteador de rede sem fio para residências. Existem muitas opções diferentes disponíveis em uma variedade de fornecedores, todas incorporando protocolos padrão, como IPv4, IPv6, DHCP, SLAAC, Ethernet e LAN sem fio 802.11. Esses padrões abertos também permitem que um cliente executando o sistema operacional Apple OS X baixe uma página da Web de um servidor Web executando o sistema operacional Linux. Isso porque ambos os sistemas operacionais implementam os protocolos de padrão aberto, como aqueles da suíte de protocolos TCP/IP.

As organizações padronizadoras geralmente são organizações sem fins lucrativos e independentes de fornecedores condicionais para desenvolver e promover o conceito de padrões abertos. Essas organizações são importantes na manutenção de uma Internet aberta, com especificações e protocolos acessíveis gratuitamente, que podem ser implementados por qualquer fornecedor.



The Internet Corporation for Assigned Names and Numbers



## PADRÕES DA INTERNET

Várias organizações têm responsabilidades diferentes para promover e criar padrões para a Internet e o protocolo TCP/IP.



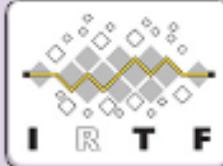
Sociedade da Internet (ISOC)



Conselho de Arquitetura da Internet (IAB)



Força-Tarefa de Engenharia  
da Internet (IETF)



Força-Tarefa de Pesquisa na  
Internet (IRTF)

Grupo Diretor de Engenharia da Internet  
(IESG)

Grupo Diretor de Pesquisa da Internet  
(IRSG)

Grupo trabalho nº  
de 1

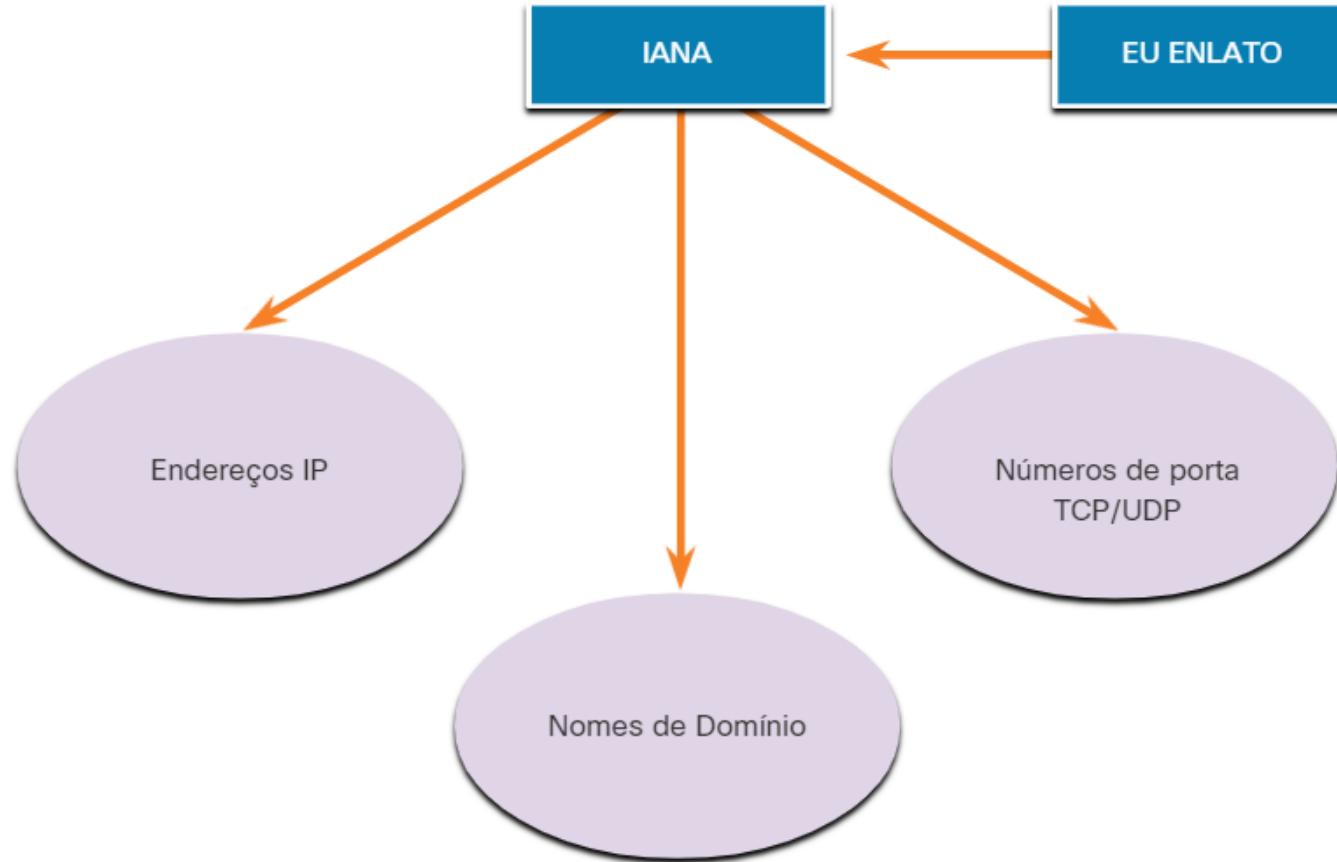
Grupo trabalho nº  
de 2

Grupo pesquisa  
de nº 1

Grupo pesquisa  
de nº 2

- **Internet Society (ISOC)** - Responsável por promover o desenvolvimento aberto e a evolução do uso da Internet em todo o mundo.
- **Internet Architecture Board (IAB)** - Responsável pelo gerenciamento e desenvolvimento geral dos padrões da Internet.
- **Força-tarefa de Engenharia da Internet (IETF)** - Desenvolver, atualizar e manter as tecnologias de Internet e TCP/IP. Isso inclui o processo e os documentos para o desenvolvimento de novos protocolos e a atualização de protocolos existentes, conhecidos como documentos RFC (Request for Comments).
- **Força-Tarefa de Pesquisa na Internet (IRTF)** - Focada em pesquisas de longo prazo relacionadas à Internet e aos protocolos TCP/IP, como o Grupo de Pesquisa Anti-Spam (ASRG), o Grupo de Pesquisa do Fórum Criptografado (CFRG) e o Ponto a Ponto Grupo de Pesquisa (P2PRG).

A próxima figura mostra as organizações de padrões envolvidas no desenvolvimento e suporte do TCP/IP e incluem a IANA e a ICANN.



- **Corporação da Internet para Nomes e Números (ICANN)** - sediada nos Estados Unidos, a ICANN coordena a alocação de endereços IP, o gerenciamento de nomes de domínio e a atribuição de outras informações usadas nos protocolos TCP/IP.
- **Autoridade para atribuição de números da Internet (IANA)** - Responsável pela supervisão e gerenciamento da alocação de endereços IP, gerenciamento de nomes de domínio e identificadores de protocolo da ICANN.

# Padrões eletrônicos e de comunicações

Outras organizações de padrões têm a responsabilidade de promover e criar os padrões eletrônicos e de comunicação usados para entregar os pacotes IP como sinais eletrônicos em um meio com ou sem fio.

Essas organizações padrão incluem o seguinte:

**Instituto de Engenheiros Elétricos e Eletrônicos ( IEEE ) – Organização padronizadora de engenharia elétrica e eletrônica que se dedica ao progresso da inovação tecnológica e à criação de padrões em vários setores, inclusive força e energia, saúde, telecomunicações e redes. Os padrões de rede IEEE importantes incluem os padrões 802.3 Ethernet e 802.11 WLAN. Executado na Internet para outros padrões de rede IEEE.**



**Aliança das Indústrias Eletrônicas (EIA)** - A organização é mais conhecida por seus padrões relacionados a módulos elétricos, conectores e racks de 19 polegadas usados para montar equipamentos de rede.

**Associação da Indústria de Telecomunicações (TIA)** - Organização responsável pelo desenvolvimento de padrões de comunicação em uma variedade de áreas, incluindo equipamentos de rádio, torres celulares, dispositivos de Voz sobre IP (VoIP), comunicações via satélite e muito mais. A figura mostra um exemplo de um cabo Ethernet certificado que foi desenvolvido cooperativamente pela TIA e pela EIA.



**Setor de Normalização das Telecomunicações da União Internacional de Telecomunicações (ITU-T)** - Uma das maiores e mais antigas organizações de padrões de comunicação. A ITU-T define padrões para compactação de vídeo, televisão por IP (IPTV) e comunicações de banda larga, como DSL.





- 
- The diagram illustrates the 7 layers of the OSI model, each represented by a yellow box containing a number and a layer name, connected by a blue rounded rectangle. To the right of each layer is a red arrow pointing to its corresponding function.
- 7 Aplicação** → Processos de rede para aplicações
  - 6 Apresentação** → Representação de dados
  - 5 Sessão** → Comunicação entre hosts
  - 4 Transporte** → Conexões ponto a ponto
  - 3 Rede** → Endereço e melhor caminho
  - 2 Enlace** → Acesso aos meios
  - 1 Física** → Transmissão binária

O termo “protocolo OSI” refere-se ao Modelo de Referência OSI (Open Systems Interconnection), também conhecido como Modelo OSI. Ele é um modelo conceitual usado para entender e descrever as funcionalidades e interações entre os diferentes protocolos de rede em um sistema de comunicação de dados.

# CAMADA FÍSICA

Seja na conexão com uma impressora local em casa ou em um site em outro país, antes que ocorra qualquer comunicação em rede, é necessário estabelecer uma conexão física com uma rede local. Uma conexão física pode ser uma conexão com fio usando um cabo ou uma conexão sem fio usando ondas de rádio.

A camada física do modelo OSI fornece os meios para transportar os bits que formam um quadro da camada de enlace de dados no meio físico de rede. Essa camada aceita um quadro completo da camada de enlace de dados e o codifica como uma série de sinais que são transmitidos à mídia local. Os bits codificados que formam um quadro são recebidos por um dispositivo final ou por um dispositivo intermediário.

A camada física codifica os quadros e cria os sinais de onda elétrica, óptica ou de rádio que representam os bits em cada quadro. Esses sinais são então enviados pela mídia, um de cada vez.

A camada física do nó destino recupera esses sinais individuais do meio físico, restaura-os às suas representações de bits e passa os bits para a camada de enlace de dados como um quadro completo.

# **Padrões da Camada Física**

A camada física consiste em circuitos eletrônicos, meios físicos e conectores desenvolvidos pelos engenheiros. Portanto, é aconselhável que os padrões que regem esse hardware sejam definidos pelas organizações de engenharia de comunicações e elétrica relevantes.

Há muitas organizações nacionais e internacionais diferentes, organizações reguladoras de governo e empresas privadas envolvidas no estabelecimento e na manutenção de padrões da camada física. Por exemplo, os padrões de hardware, mídia, codificação e sinalização da camada física são definidos e governados por essas organizações de padrões:

- International Organization for Standardization (ISO)
- Telecommunications Industry Association/Electronic Industries Association (TIA/EIA)
- União Internacional de Telecomunicações (ITU)
- Instituto Nacional de Padronização Americano (ANSI)
- Institute of Electrical and Electronics Engineers (IEEE)
- Autoridades reguladoras de telecomunicações nacionais, incluem Federal Communication Commission (FCC) nos EUA e European Telecommunications Standards Institute (ETSI)



Os padrões TCP/IP são implementados em software e orientados pela IETF.

Os padrões da camada física são implementados em hardware e orientados por muitas organizações, inclusive:

- ISO
- EIA/TIA
- ITU-T
- ANSI
- IEEE

# **Componentes Físicos**

Os padrões da camada física abordam três áreas funcionais:

- Componentes Físicos;
- Codificação;
- Sinalização.

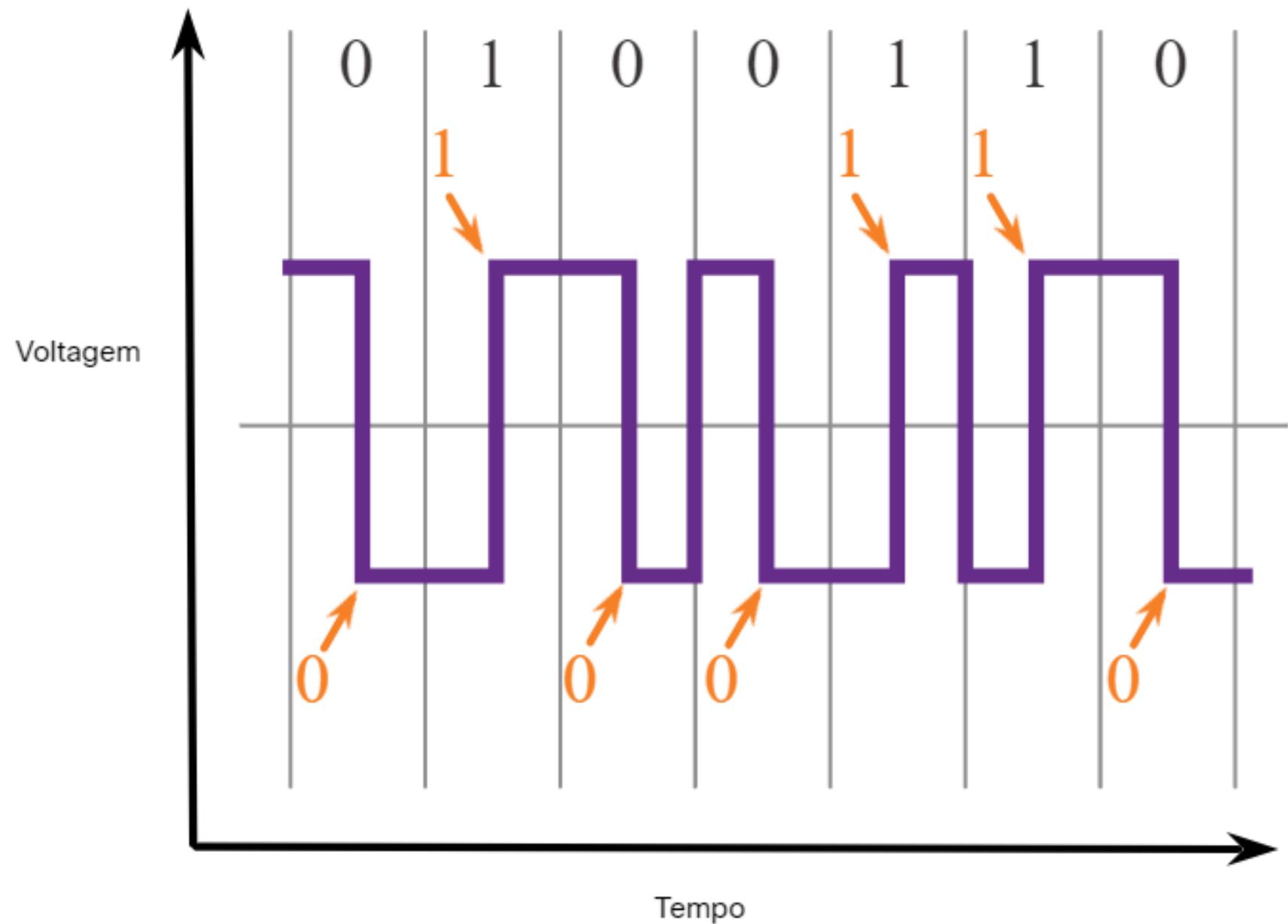
# **Componentes Físicos**

Os componentes físicos são os dispositivos de hardware eletrônico, mídia e outros conectores que transmitem os sinais que representam os bits. Os componentes de hardware, como NICs, interfaces e conectores, materiais de cabo e projetos de cabo são especificados nos padrões associados à camada física.

# Codificação

A codificação ou codificação de linha é um método para converter um fluxo de bits de dados em um "código" predefinido. Os códigos são agrupamentos de bits usados para fornecer um padrão previsível que pode ser reconhecido tanto pelo emissor quanto pelo receptor. Em outras palavras, a codificação é o método ou o padrão usado para representar as informações digitais. É semelhante a como o código Morse codifica uma mensagem usando uma série de pontos e traços.

Por exemplo, a codificação Manchester representa um bit 0 por uma transição de alta para baixa voltagem, e um bit 1 é representado como uma transição de baixa para alta voltagem. Um exemplo de codificação Manchester é ilustrado na figura. A transição ocorre no meio de cada período de bit. Esse tipo de codificação é usado na Ethernet de 10 Mbps. Taxas de dados mais rápidas exigem uma codificação mais complexa. A codificação Manchester é usada em padrões Ethernet mais antigos, como o 10BASE-T. A Ethernet 100BASE-TX usa codificação 4B / 5B e 1000BASE-T usa codificação 8B / 10B.

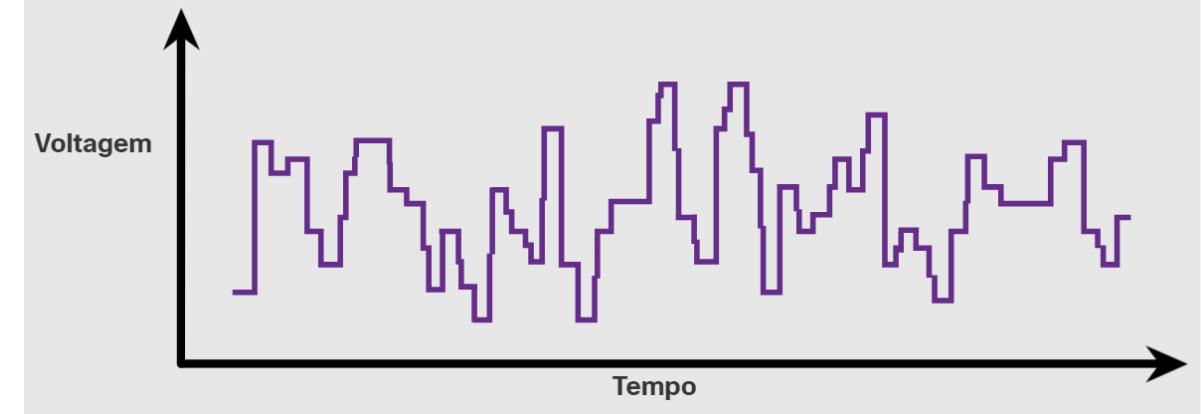


# Sinalização

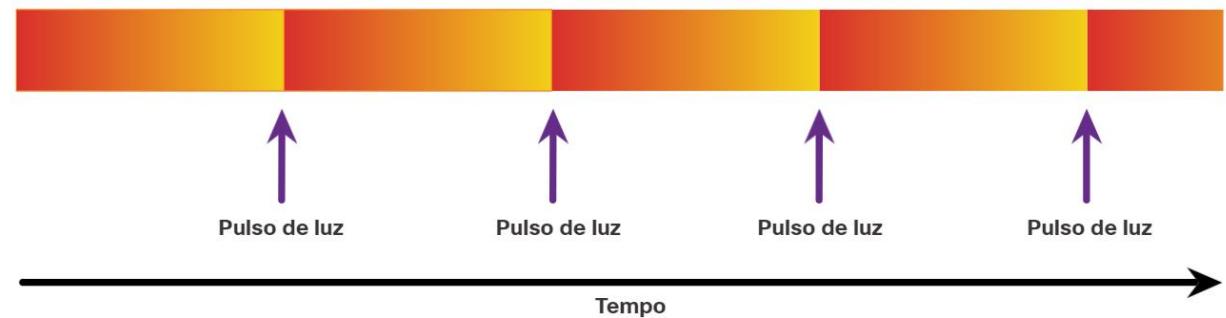
A camada física deve gerar os sinais elétricos, ópticos ou sem fio que representam os valores “1” e “0” no meio físico. A maneira como os bits são representados é chamada de método de sinalização. Os padrões de camada física devem definir que tipo de sinal representa o valor “1” e que tipo de sinal representa o valor “0”. Isso pode ser tão simples quanto uma alteração no nível de um sinal elétrico ou de um pulso óptico. Por exemplo, um pulso longo pode representar um 1, enquanto um pulso curto pode representar um 0.

Isso é semelhante ao método de sinalização usado no código Morse, que pode usar uma série de tons de ligar e desligar, luzes ou cliques para enviar o texto por fios telefônicos ou entre as embarcações no mar.

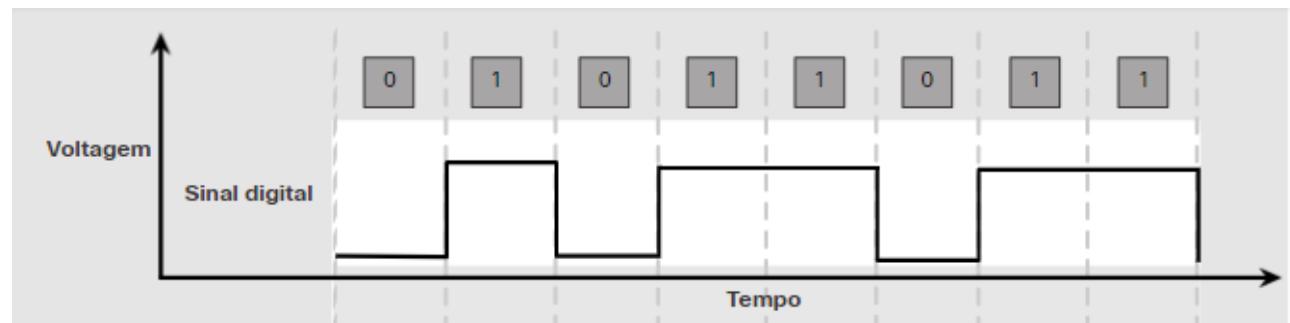
## Cabo de cobre



## Cabo de fibra ótica



## Midia sem fio



# Largura de Banda

Meios físicos diferentes aceitam a transferência de bits a taxas diferentes. A transferência de dados é geralmente discutida em termos de largura de banda. Largura de banda é a capacidade na qual um meio pode transportar dados.

# Largura de Banda

A largura de banda digital mede a quantidade de dados que podem fluir de um lugar para outro durante um determinado tempo. A largura de banda é normalmente medida em kilobits por segundo (kbps), megabits por segundo (Mbps) ou gigabits por segundo (Gbps). Às vezes, a largura de banda é pensada como a velocidade em que os bits viajam, no entanto, isso não é preciso. Por exemplo, na Ethernet de 10 Mbps e 100 Mbps, os bits são enviados na velocidade da eletricidade. A diferença é o número de bits que são transmitidos por segundo.

Uma combinação de fatores determina a largura de banda prática de uma rede:

- ✓ **As propriedades do meio físico**
- ✓ **As tecnologias escolhidas para sinalização e detecção de sinais de rede.**

As propriedades do meio físico, as tecnologias atuais e as leis da física desempenham sua função na determinação da largura de banda disponível.

Unidades de Largura de Banda	Sigla	Equivalência
Bits por segundo	bps	1 bps = unidade fundamental de largura de banda
Quilobits por segundo	Kbps	1 Kbps = 1,000 bps = $10^3$ bps
Megabits por segundo	Mbps	1 Mbps = 1,000,000 bps = $10^6$ bps
Gigabits por segundo	Gbps	1 Gbps = 1,000,000,000 bps = $10^9$ bps
Terabits por segundo	Tbps	1 Tbps = 1,000,000,000,000 bps = $10^{12}$ bps

# **Terminologia de largura de banda**

Os termos usados para medir a qualidade da largura de banda incluem:

- **Latência;**
- **Rendimento;**
- **Dados úteis.**

# **Latência**

O termo latência se refere ao tempo necessário para os dados viajarem de um ponto a outro, incluindo atrasos.

# Latência

Em uma internetwork ou em uma rede com vários segmentos, a taxa de transferência não pode ser mais rápida que o link mais lento no caminho da origem ao destino. Mesmo que todos ou a maioria dos segmentos tenham alta largura de banda, será necessário apenas um segmento no caminho com baixa taxa de transferência para criar um gargalo na taxa de transferência de toda a rede.

# Taxa de transferência

Taxa de transferência é a medida da transferência de bits através da mídia durante um determinado período.

Devido a alguns fatores, geralmente a taxa de transferência não corresponde à largura de banda especificada nas implementações da camada física. A taxa de transferência geralmente é menor que a largura de banda. Existem muitos fatores que influenciam a taxa de transferência:

# Taxa de transferência

- A quantidade de tráfego;
- O tipo de tráfego;
- A latência criada pelo número de dispositivos de rede encontrados entre a origem e o destino.

Existem muitos testes de velocidade on-line que podem revelar a taxa de transferência de uma conexão com a Internet. A figura fornece exemplos de resultados de um teste de velocidade.

## Dados úteis

Há uma terceira medida para avaliar a transferência de dados utilizáveis; é conhecido como goodput. Goodput é a medida de dados usáveis transferidos em um determinado período. Goodput é a taxa de transferência menos a sobrecarga de tráfego para estabelecer sessões, reconhecimentos, encapsulamento e bits retransmitidos. O goodput é sempre menor que a taxa de transferência, que geralmente é menor do que a largura de banda.

Velocidade de Transferência

 **80.78** Mbps

Velocidade de upload

 **8.78** Mbps



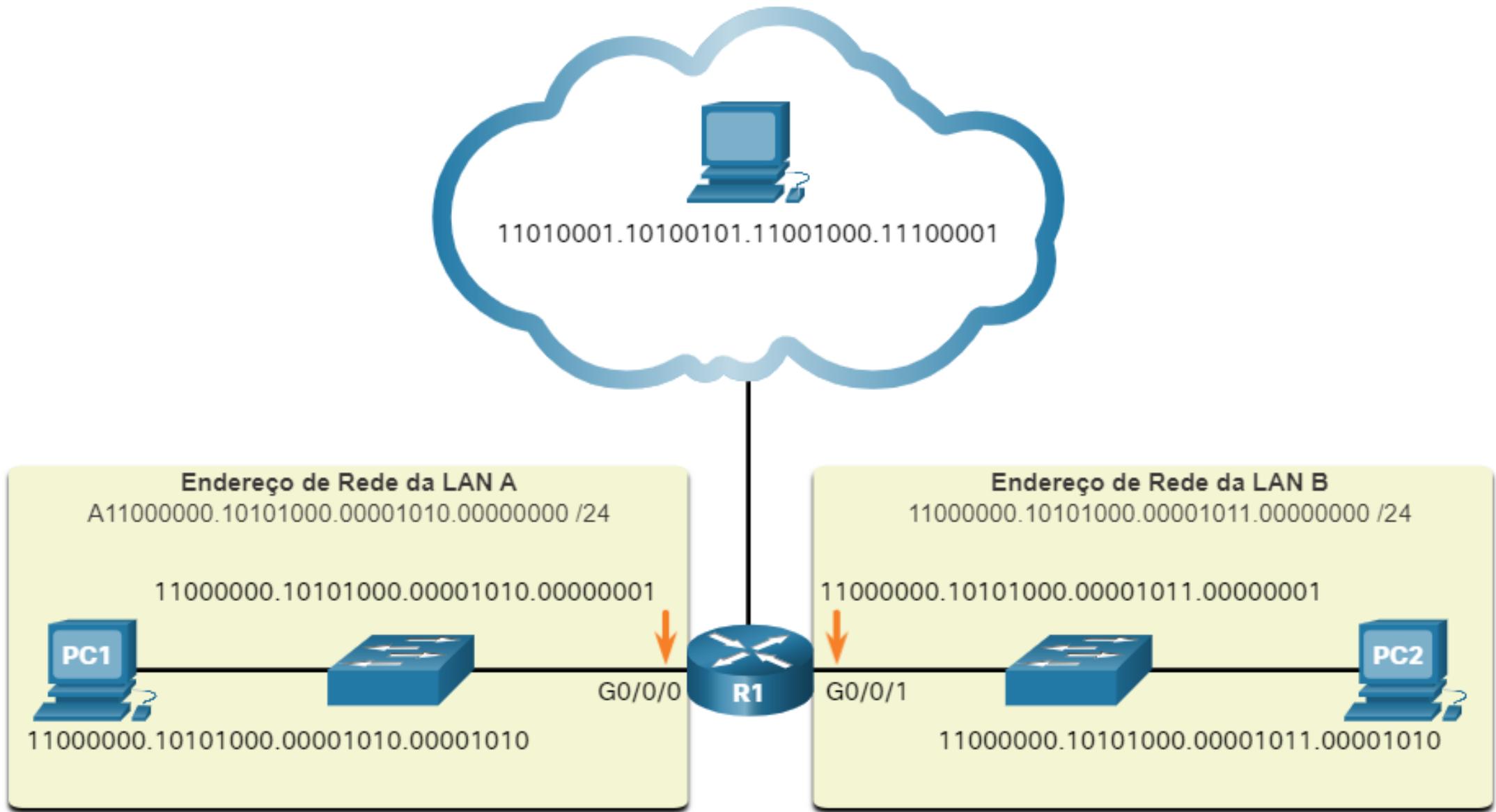
# **SISTEMA DE NUMERAÇÃO BINÁRIO**

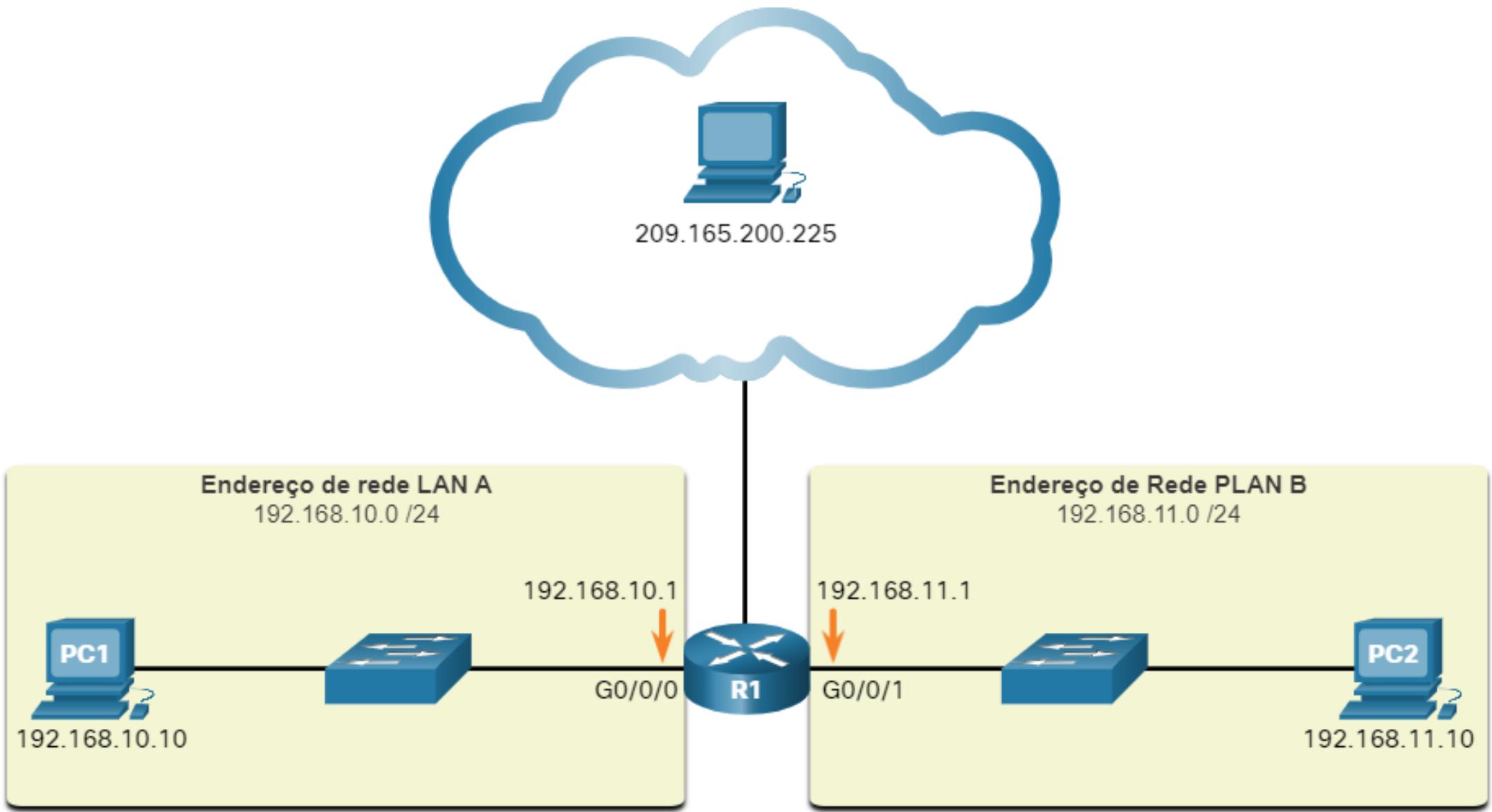
# Endereços Binários e IPv4

Os endereços IPv4 começam como binários, uma série de apenas 1s e 0s. Eles são difíceis de gerenciar, portanto, os administradores de rede devem convertê-los em decimal. Este tópico mostra algumas maneiras de fazer isso.

Binário é um sistema de numeração que consiste nos dígitos 0 e 1 chamados bits. Por outro lado, o sistema de numeração decimal consiste em 10 dígitos, consistindo nos dígitos de 0 a 9.

É importante compreender o binário porque hosts, servidores e dispositivos de rede usam esse tipo de endereçamento. Especificamente, eles usam endereços IPv4 binários, como mostrado na figura, para se identificar.





# **ENDEREÇOS DECIMAL e IPv4**

<b>128</b>	<b>64</b>	<b>32</b>	<b>16</b>	<b>8</b>	<b>4</b>	<b>2</b>	<b>1</b>

# **ENDEREÇOS HEXADECIMAIS e IPv6**

Assim como decimal é um sistema numérico de base dez, hexadecimal é um sistema de dezesseis bases. O sistema numérico de dezesseis base usa os dígitos 0 a 9 e as letras A a F.

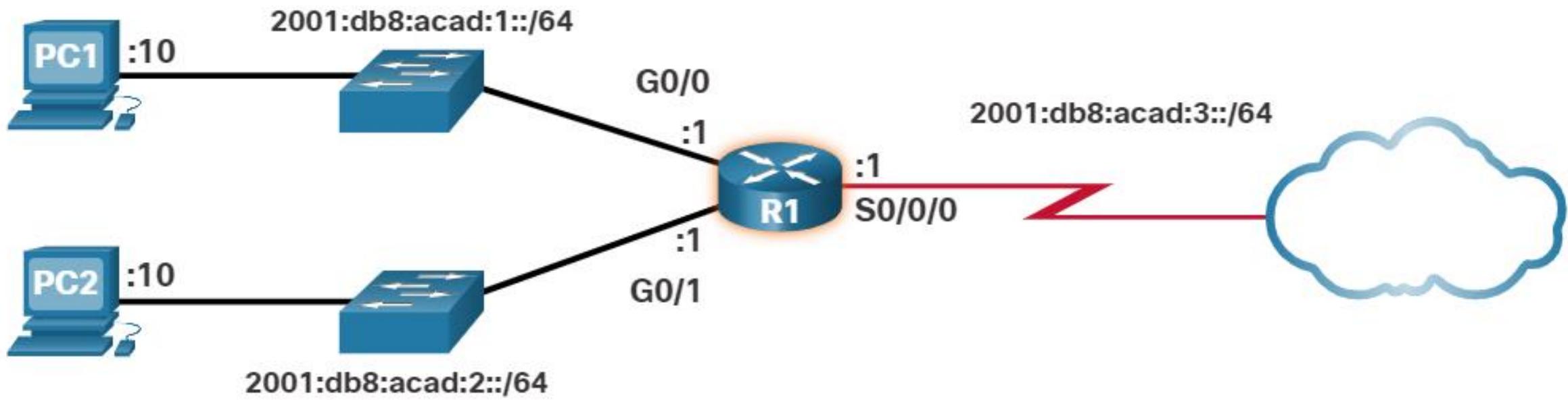
O sistema de numeração hexadecimal é usado em rede para representar endereços IP versão 6 e endereços MAC Ethernet.

Os endereços IPv6 têm 128 bits de comprimento e a cada 4 bits é representado por um único dígito hexadecimal; para um total de 32 valores hexadecimais.

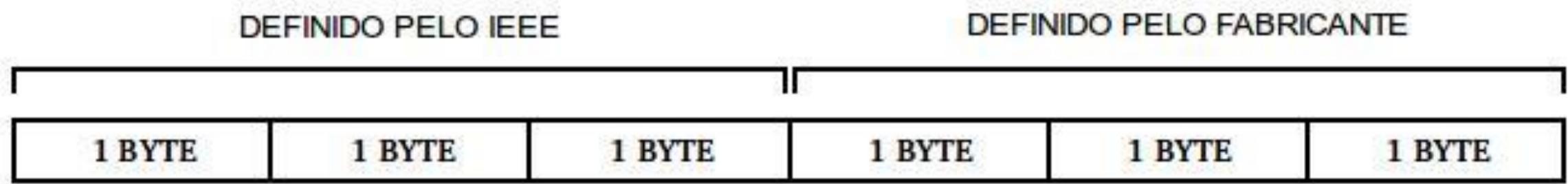
**Os endereços IPv6 não diferenciam maiúsculas e minúsculas e podem ser escritos tanto em minúsculas como em maiúsculas.**

O formato preferido para escrever um endereço IPv6 é **x:x:x:x:x:x:x**, com cada "x" consistindo em quatro valores hexadecimais. Quando falamos de 8 bits de um endereço IPv4, usamos o termo octeto. No IPv6, hextet é o termo não oficial usado para se referir a um segmento de 16 bits ou quatro valores hexadecimais. Cada "x" é um único hextet, 16 bits ou quatro dígitos hexadecimais.

Decimal	Binário	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F



O endereço MAC é formado por um conjunto de 6 bytes separados por dois pontos (“：“) ou hífen (“-”), sendo cada byte representado por dois algarismos na forma hexadecimal, como por exemplo: "00:19:B9:FB:E2:58". Cada algarismo em hexadecimal corresponde a uma palavra binária de quatro bits, desta forma, os 12 algarismos que formam o endereço totalizam 48 bits.





- 
- The diagram illustrates the 7 layers of the OSI model, each represented by a yellow box containing a number and a layer name, connected by a blue rounded rectangle. To the right of each layer is a red arrow pointing to its corresponding function.
- 7 Aplicação** → Processos de rede para aplicações
  - 6 Apresentação** → Representação de dados
  - 5 Sessão** → Comunicação entre hosts
  - 4 Transporte** → Conexões ponto a ponto
  - 3 Rede** → Endereço e melhor caminho
  - 2 Enlace** → Acesso aos meios
  - 1 Física** → Transmissão binária

CAMADA REDE

A camada de rede é responsável por endereçar e permitir a transferência de dados da origem até o destino de uma comunicação por meio das diversas redes que podem existir nesse caminho.

Nos modelos de referência definidos para a comunicação entre equipamentos há uma camada primordial para o perfeito funcionamento de comunicações por meios das redes, que é a camada de rede.

**Endereçamento:** é o processo de definir endereços para os dispositivos existentes em uma rede que permite a comunicação de dados.

**Encapsulamento:** é o processo de empacotar, moldar, segmentar o fluxo de dados a ser transmitido pela rede dentro do PDU do protocolo da camada de rede utilizado.

**Roteamento:** é o processo que consiste na tarefa de diferenciar estes pacotes montados no processo de encapsulamento, por meio da rede de dados.

**Desencapsulamento:** é o processo de desempacotar, retirar o conteúdo de dados constante no pacote recebido e entregar a camada superior do modelo de referência OSI(Transporte).

Protocolos implementados para atender as funções básicas desta camada:

- **IPv4**
- **IPv6**
- **IPX**
- **Appletalk**

Protocolos que tem a função de auxiliar o protocolo principal:

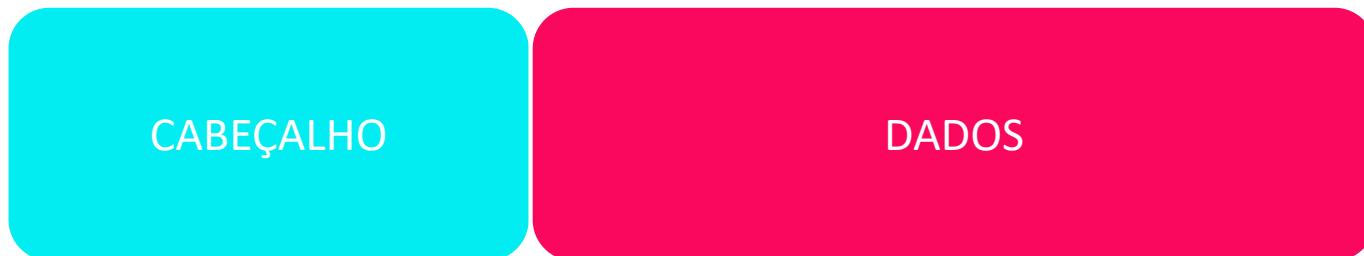
- **ICMP**
- **ARP**

# **IPV4**

Uma das grandes características deste protocolo é permitir a sua utilização em qualquer tipo de rede física, permitindo com isso, uma interoperabilidade perfeita entre as diversas tecnologias.

## PACOTE IP

Também chamado de datagrama é a unidade básica de transferência da camada de rede. É ele que define o layout dos pacotes a serem transferidos.



**Cabeçalho:** é o conjunto de campos que definem diversas propriedades do pacote.

**Dados:** é o conjunto de dados recebidos da camada superior para a rede, no caso, o segmento da camada de transporte.

## **Endereçamento IPv4**

32 bits divididos em 4 octetos de 8 bits mas sendo representados em formato decimal chamado notação decimal.

## Classe de endereços IP

Os endereços IPs foram separados por classes criadas(A, B, C, D e E), acomodando todo os IPs possíveis.

**A B C:** Usadas comercialmente na atribuição de endereços IPs aos dispositivos de uma rede.

**D:** Endereçamento multicast.

**E:** para fins experimentais pela IANA.

## **ENDEREÇOS PÚBLICOS E ENDEREÇOS PRIVADOS.**

<b>CLASSE</b>	<b>INTERVALO DE ENDEREÇOS INTERNOS RFC 1918</b>
A	10.0.0.0 até 10.255.255.255
B	172.16.0 até 172.31.255.255
C	192.168.0.0 até 192.168.255.255

# **IPv6**

Com a evolução das redes dos novos dispositivos móveis das populações de todos os países tendo á acesso a internet houve a necessidade de muitos endereços de redes para permitir o endereçamento de todos esses equipamentos.

# **IPv6**

Foi criado o IPv6 com as seguintes características:

- Maior espaço de endereçamento;
- Mobilidade;
- Segurança;
- Auto configuração.

## O pacote IPv6

Também chamado de datagrama é composto por duas partes: o cabeçalho e os dados. Um das grandes diferenças entre as versões do protocolo IP é o cabeçalho do pacote.

## **Endereçamento IPv6**

A representação do endereço é feita por meio do agrupamento de 16 em 16 bits separados por “：“.

Estes grupos de 16 bits são representados utilizando a notação hexadecimal sendo que cada digito hexadecimal representa 4 bits separados.

O endereçamento Ipv6 especifica 3 tipos de endereços possíveis:

- Unicast;
- Anycast;
- Multicast.

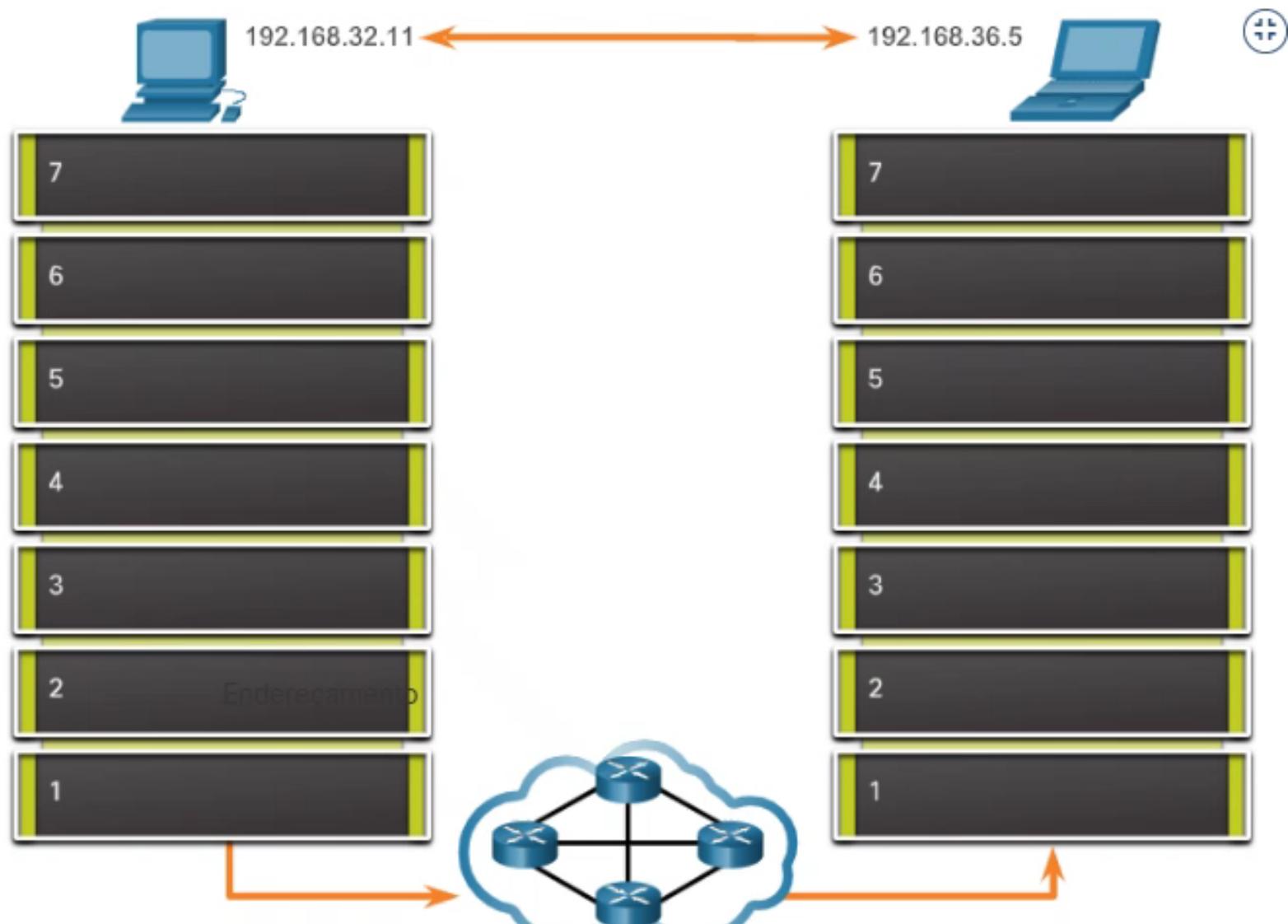
## **ICMP**

É um protocolo que também opera na camada 3 do modelo OSI, porém não é utilizado para a transmissão de dados, mas sim, como protocolo de controle, auxiliando o perfeito funcionamento do protocolo IP.

ICMP tem como funcionalidade permitir que roteadores interligados em redes possam informar erros ou problemas inesperados ocorridos durante a transmissão de pacotes.

## **ARP**

A RFC 826 apresenta o protocolo ARP que implementa uma funcionalidade que permite aos equipamentos na rede conseguirem mapear endereços lógico e físico.



Protocolos de camada de rede encaminham PDUs de camada de transporte entre hosts.

Toda vez que uma mensagem é enviada para um dispositivo que não se encontra no mesmo local, ela pode percorrer vários caminhos distintos.

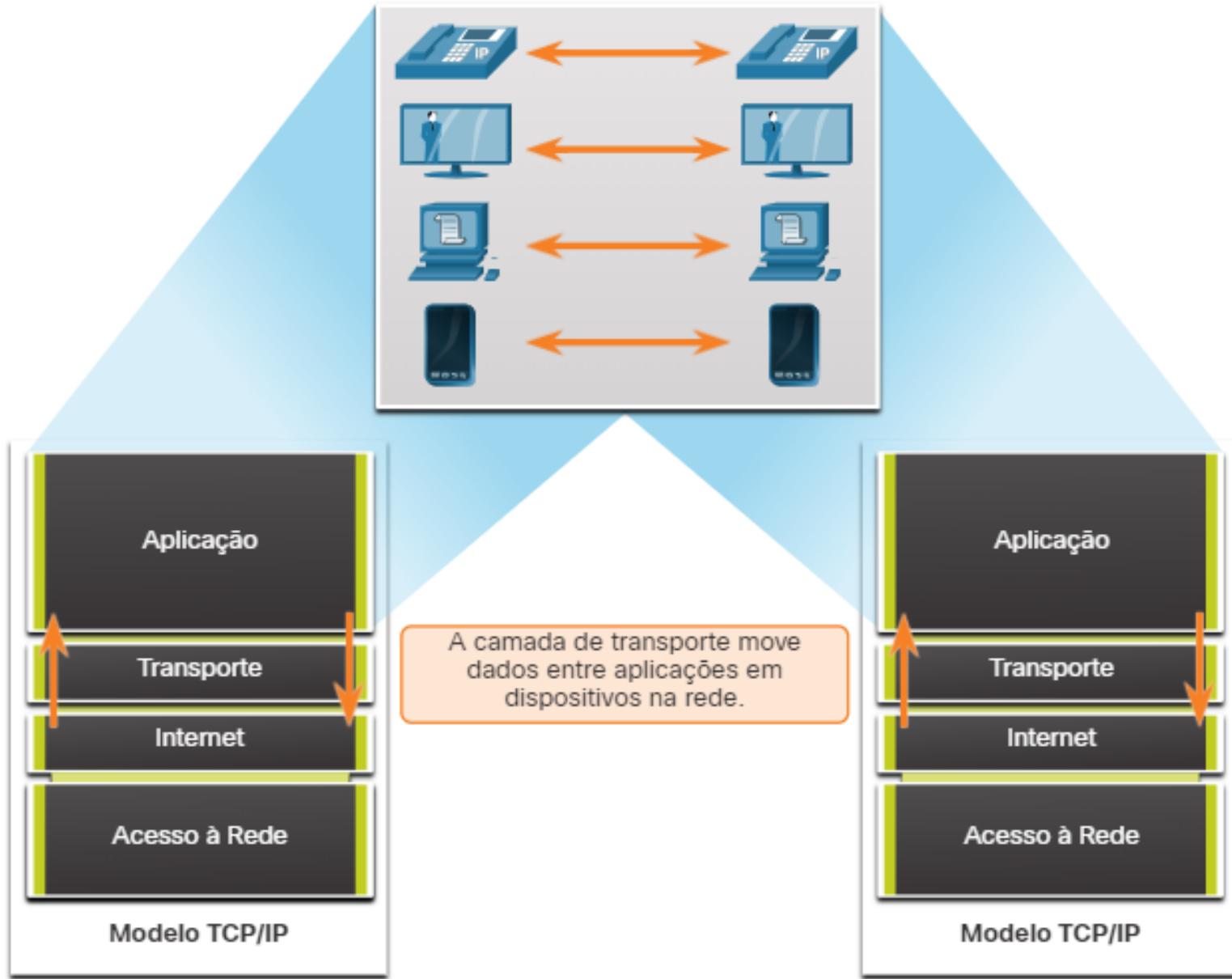
Para entender esse conceito, faça os seguintes passos.

1. Abra o Prompt de Comando (cmd).
2. Digite: tracert google.com.br (no Linux traceroute)

Observe que ao efetuar esse comando uma solicitação é feita ao servidor do Google, e esta mensagem passa por vários nodos que são identificados na medição.

CAMADA  
DE  
TRANSPORTE

Os programas da camada de aplicação geram dados que devem ser trocados entre os hosts de origem e de destino. A camada de transporte é responsável pela comunicação lógica entre aplicativos executados em hosts diferentes. Isso pode incluir serviços como o estabelecimento de uma sessão temporária entre dois hosts e a transmissão de informações confiáveis para um aplicativo.



A camada de transporte não tem conhecimento do tipo de host de destino, do tipo de mídia pela qual os dados devem percorrer, do caminho percorrido pelos dados, do congestionamento em um link ou do tamanho da rede.

A camada de transporte inclui dois protocolos:

Protocolo TCP (Protocolo de Controle de Transmissão)

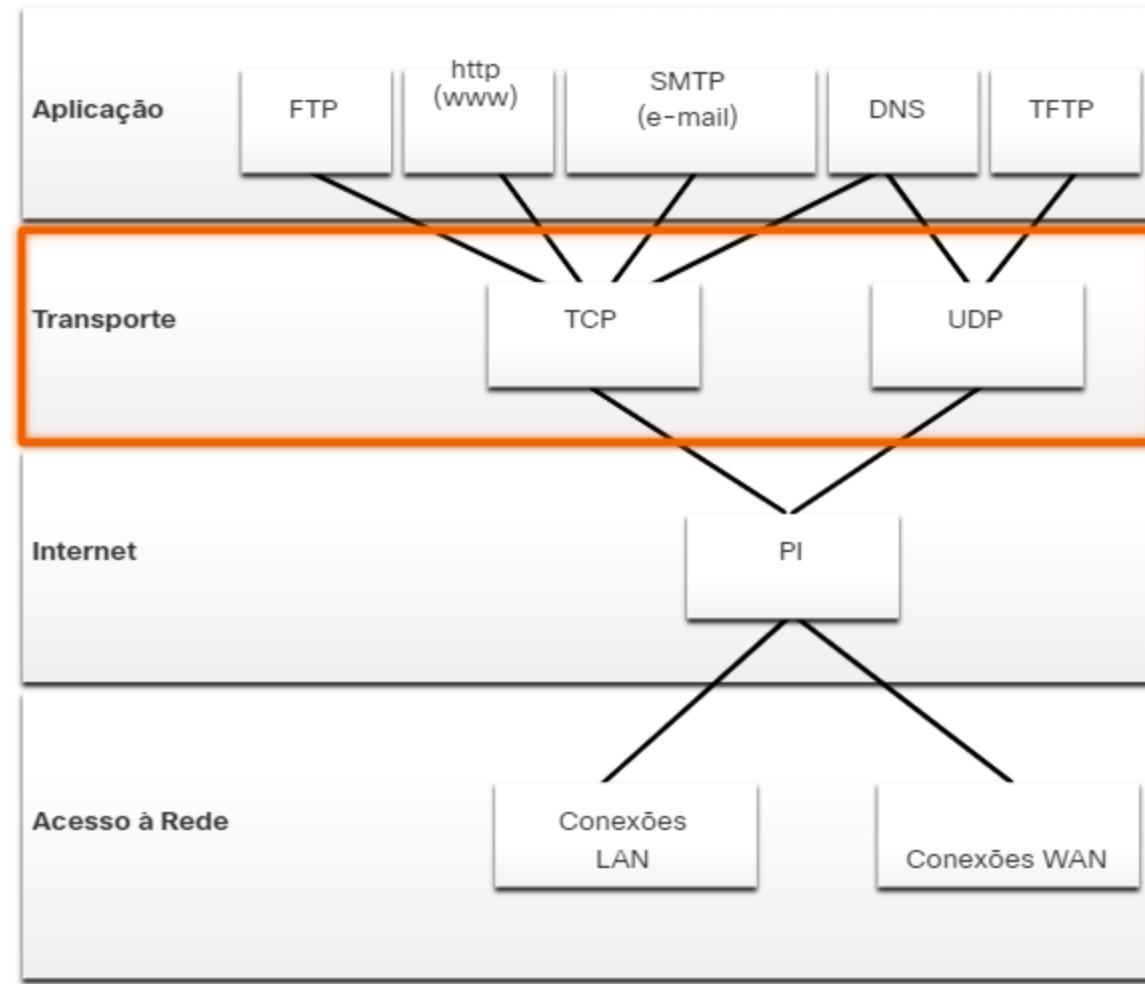
Protocolo UDP (Protocolo de Datagrama do Usuário)

# **PROTOCOLOS DA CAMADA DE TRANSPORTE**

O IP está preocupado apenas com a estrutura, endereçamento e roteamento de pacotes. O IP não especifica como a entrega ou o transporte dos pacotes incluídos.

Os protocolos de camada de transporte especificam como transferir mensagens entre hosts e são responsáveis pelo gerenciamento dos requisitos de confiabilidade de uma conversa. A camada de transporte inclui os protocolos TCP e UDP.

As aplicações têm diferentes necessidades de confiabilidade diferente de transporte. Portanto, o TCP/IP fornece dois protocolos de camada de transporte



# **Protocolo TCP (Protocolo de Controle de Transmissão)**

O TCP é considerado um protocolo de camada de transporte confiável, completo, que garante que todos os dados cheguem ao destino. O TCP inclui campos que garantem a entrega dos dados do aplicativo. Esses campos estão bloqueados no processamento adicional pelos hosts de envio e coleta.

O TCP fornece confiabilidade e controle de fluxo usando estas operações básicas:

Número e rastreamento de segmentos de dados transmitidos para um host específico a partir de um aplicativo específico;  
Confirmar dados recebidos;

Retransmitir todos os dados não confirmados após um determinado período de tempo

Dados de sequência que podem chegar em ordem errada

Enviar dados a uma taxa eficiente que seja aceitável pelo receptor.

O UDP é um protocolo de camada de transporte mais simples que o TCP. Ele não fornece confiabilidade e controle de fluxo, o que significa que requer menos campos de cabeçalho. Como o envio e os processos do receptor UDP não precisam de gerenciamento de confiabilidade e controle de fluxo, isso significa que os datagramas UDP podem ser processados mais rapidamente dos segmentos TCP. A UDP fornece as funções básicas para fornecer datagramas entre as aplicações protetoras, com muita pouca sobrecarga e verificação de dados.

UDP é um protocolo sem conexão. Como o UDP não fornece confiabilidade ou controle de fluxo, ele não requer uma conexão estabelecida. Como o UDP não controla informações enviadas ou recebidas entre o cliente e o servidor, o UDP também é conhecido como um protocolo sem estado.

O UDP também é conhecido como um protocolo de entrega de melhor esforço porque não há confirmação de que os dados são recebidos no destino. Com o UDP, não há processo de camada de transporte que informe ao envio se a entrega foi bem-sucedida.

# O PROTOCOLO DE CAMADA DE TRANSPORTE CERTO PARA A APLICAÇÃO CERTA

Alguns aplicativos toleram a perda de dados durante a transmissão pela rede, mas podem atrasos na transmissão são inaceitáveis. Para esses aplicativos, o UDP é a melhor escolha, pois requer menos sobrecarga da rede. O UDP é preferível para aplicativos como Voz sobre IP (VoIP). Confirmações e retransmissão atrasariam a entrega e tornariam a conversa por voz inaceitável.

Para outras aplicações, é importante que todos os dados cheguem e que possam ser processados em sua sequência adequada. Para esses tipos de aplicativos, o TCP é usado como o protocolo de transporte. Por exemplo, aplicações como bancos de dados, navegadores e clientes de e-mail bloqueiam que todos os dados enviados cheguem ao destino em seu estado original. Quaisquer dados ausentes podem corromper uma comunicação, tornando-a incompleta ou ilegível. Por exemplo, é importante ao acessar informações bancárias pela web certificar-se de que todas as informações são enviadas e recebidas corretamente.

Vídeo e voz em tempo real geralmente usam UDP, mas também podem usar TCP, ou UDP e TCP. Um aplicativo de videoconferência pode usar UDP por padrão, mas como muitos firewalls bloqueiam UDP, o aplicativo também pode ser enviado por TCP.

Os aplicativos que transmitem áudio e vídeo armazenados usam TCP. Por exemplo, se sua rede, de repente, não comportar a largura de banda necessária para a transmissão de um filme sob demanda, a aplicação interrompeu a reprodução. Durante essa interrupção, você deverá ver uma mensagem de “buffering...”, enquanto o TCP será para restabelecer a transmissão. Quando todos os segmentos estão em ordem e um nível mínimo de largura de banda é restaurado, a sessão TCP é retomada e o filme retorna à reprodução.

## UDP



VoIP  
(telefonia IP)



DNS  
(resolução de nomes de domínio)

## TCP



SMTP/IMAP  
(E-mail)



HTTP/HTTPS  
(World Wide Web)

Propriedades permitidas para escolha do protocolo:

- Rápido
- Baixa sobrecarga
- Não exige confirmações
- Não reenvia dados perdidos
- Entrega dos dados assim que chegam

Propriedades permitidas para escolha do protocolo:

- Confiável
- Confirmação da chegada dos dados
- Reenviar dados perdidos
- Entrega dos dados em sequência



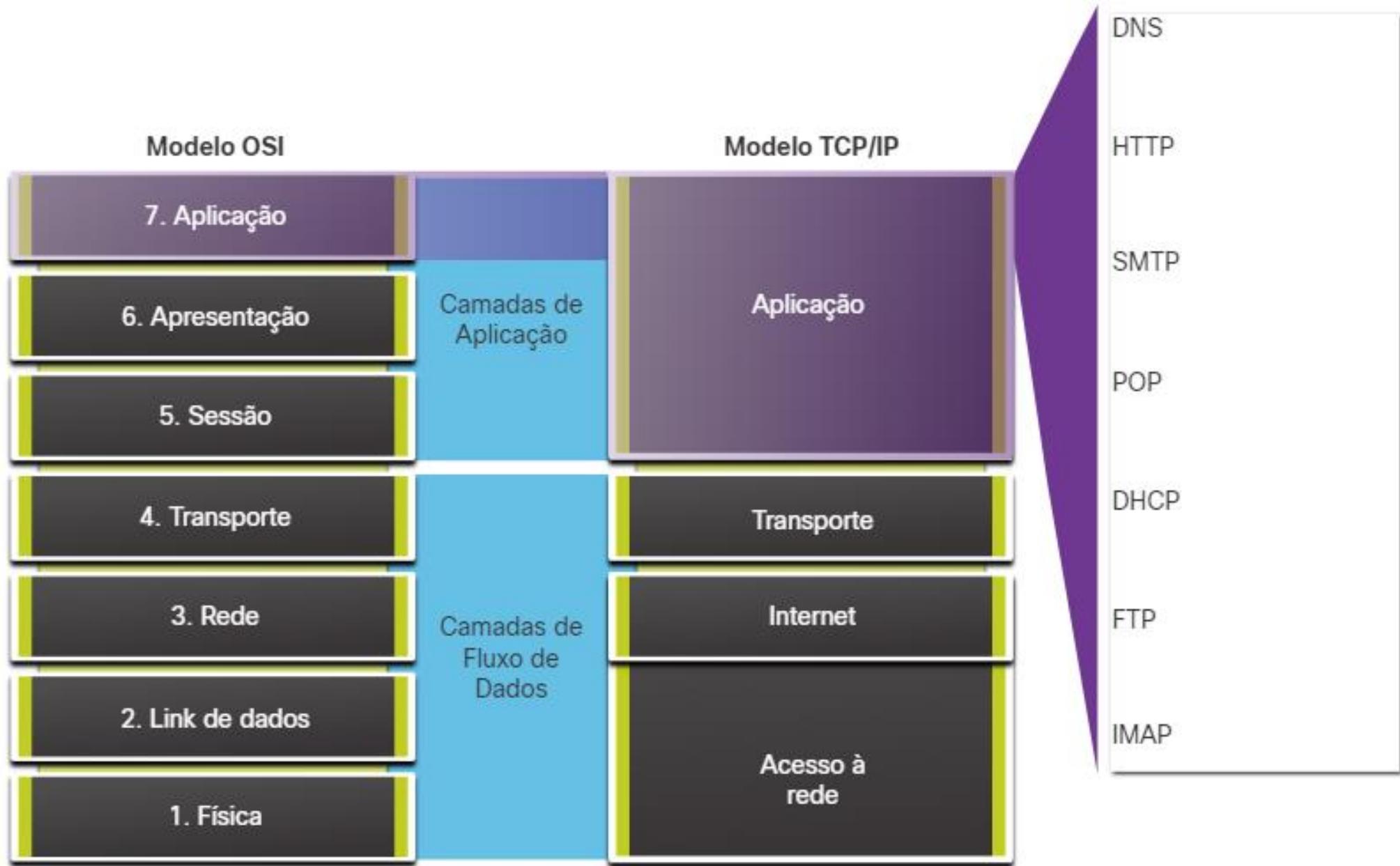
- 
- The diagram illustrates the 7 layers of the OSI model, each represented by a yellow box containing a number and a layer name, connected by a blue rounded rectangle. To the right of each layer is a red arrow pointing to its corresponding function.
- 7 Aplicação** → Processos de rede para aplicações
  - 6 Apresentação** → Representação de dados
  - 5 Sessão** → Comunicação entre hosts
  - 4 Transporte** → Conexões ponto a ponto
  - 3 Rede** → Endereço e melhor caminho
  - 2 Enlace** → Acesso aos meios
  - 1 Física** → Transmissão binária

APLICAÇÃO

APRESENTAÇÃO

SESSÃO

Nos modelos OSI e TCP/IP, a camada de aplicativo é a camada mais próxima do usuário final, é a camada que fornece a interface entre os aplicativos usados para se comunicar e a rede subjacente pela qual as mensagens são transmitidas. Os protocolos de camada de aplicação são usados para troca de dados entre programas executados em hosts de origem e destino.

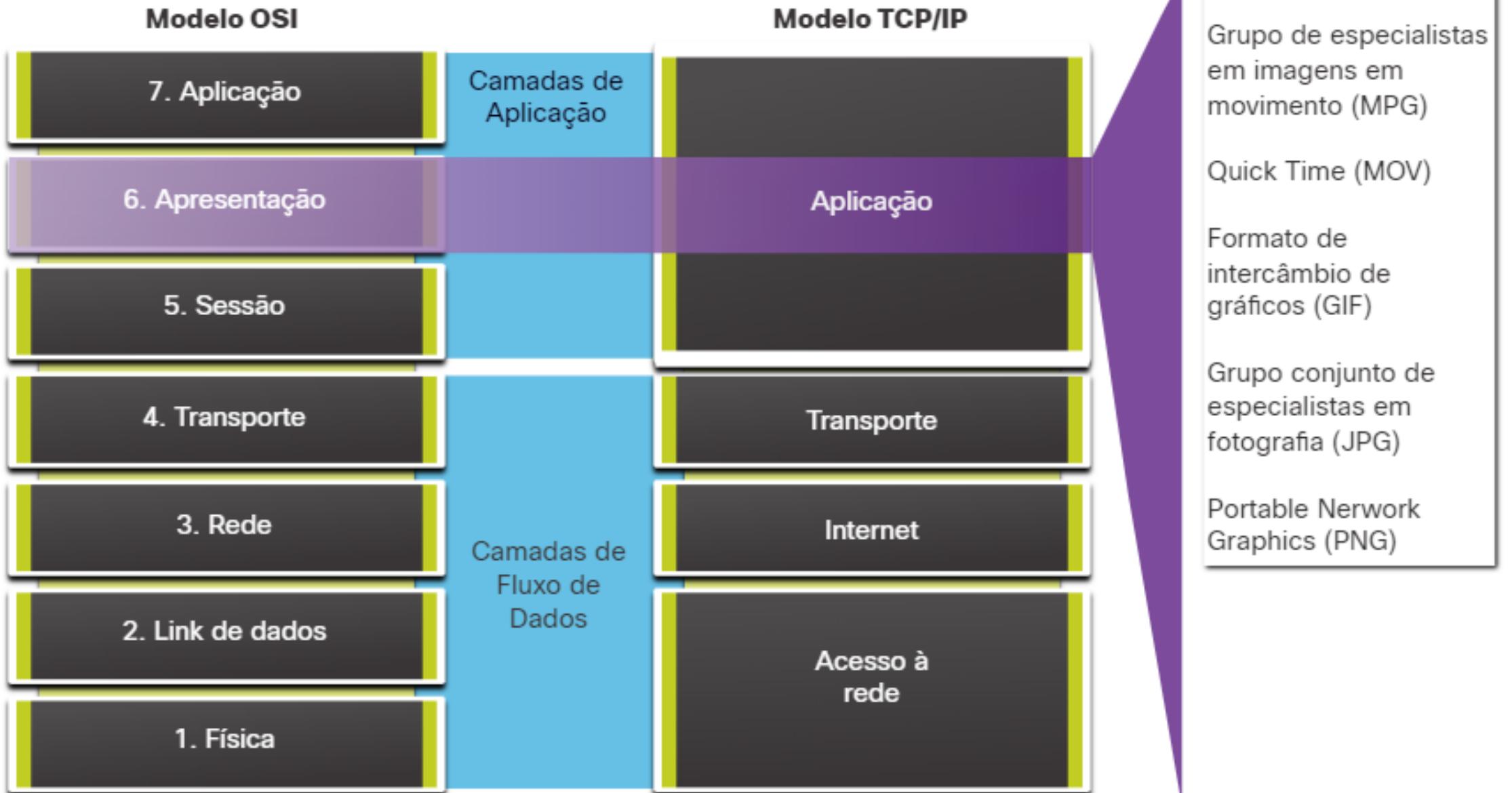


Com base no modelo TCP/IP, as três camadas superiores do modelo OSI (aplicativo, apresentação e sessão) definem funções da camada de aplicativo TCP/IP.

Há muitos protocolos de camada de aplicação e outros novos estão em constante desenvolvimento. Alguns dos protocolos da camada de aplicação mais conhecidos incluem o HTTP (Hypertext Transfer Protocol), o FTP (File Transfer Protocol), o TFTP (Trivial File Transfer Protocol), o IMAP (Internet Message Access Protocol) e o DNS (Domain Name System) .

- Camada de apresentação
- A camada de apresentação tem três funções principais:
- Formatar ou apresentar dados no dispositivo de origem em um formato compatível para coleta de destino.
- Comprimir dados de uma maneira que o dispositivo possa ser descompactado pelo destino.

- Camada de apresentação
- A camada de apresentação tem três funções principais:
- Formatar ou apresentar dados no dispositivo de origem em um formato compatível para coleta de destino.
- Comprimir dados de uma maneira que o dispositivo possa ser descompactado pelo destino.



# **PROTOCOLOS TCP/IP DA CAMADA DE APLICAÇÃO**

Os protocolos de aplicativos TCP/IP especificam o formato e as informações de controle permitidas para muitas funções comuns de comunicação da Internet. Os protocolos de camada de aplicação são usados pelos dispositivos de origem e destino durante uma sessão de comunicação. Para que as comunicações sejam bem concluídas, os protocolos da camada de aplicativo implementados no host de origem e destino devem ser compatíveis.

## **SISTEMA DE NOMES**

- DNS - Sistema de Nomes de Domínio (ou Serviço)
- TCP, cliente UDP 53
- Converta nomes de domínio, como cisco.com, em endereços IP.



## Transferência de arquivo

### FTP - Protocolo de Transferência de Arquivos

- Define as regras que permitem que um usuário em um host acesse e transfira arquivos de e para outro host em uma rede
- O FTP é um protocolo de entrega de arquivos confiável, orientado à conexão e reconhecido

### TFTP - Protocolo de Transferência de Arquivos Trivial

- **HTTP** - Protocolo de transferência de hipertexto
  - Um conjunto de regras para a troca de texto, imagens gráficas, som, vídeo e outros arquivos multimídia na World Wide Web
- 
- **HTTPS - HTTP seguro**
  - O navegador usa criptografia para proteger conversas HTTP
  - Autentica o site ao qual você conecta seu navegador

# IVIOAEIO Cliente-Servidor

Este es un sistema de cliente-servidor que se divide en tres partes principales:

1. Servidor: Se encarga de manejar las solicitudes de los clientes y proporcionarles los datos requeridos.

2. Cliente: Se encarga de enviar las solicitudes al servidor y recibir los datos en respuesta.

3. Base de datos: Almacena la información que se muestra en el cliente.

El sistema se implementó utilizando Python como lenguaje de programación y MySQL como base de datos.

Los datos se almacenan en una sola tabla llamada "empleados" con las siguientes columnas:

Nombre, Apellido, DNI, Edad, Salario, Departamento, Fecha de contratación.

El sistema permite realizar consultas y actualizaciones a través de una interfaz gráfica.

Algunas de las funcionalidades del sistema incluyen:

1. Consulta de empleados: Permite buscar empleados por nombre, apellido o DNI.

2. Actualización de empleados: Permite modificar datos de un empleado existente.

3. Eliminación de empleados: Permite eliminar un empleado de la base de datos.

4. Consulta de estadísticas: Permite obtener estadísticas sobre los empleados, como el promedio de edad o salario.

5. Consulta de departamentos: Permite obtener información sobre los departamentos y sus empleados.

6. Consulta de empleados por departamento: Permite buscar empleados dentro de un departamento específico.

7. Consulta de empleados por rango de edad: Permite buscar empleados dentro de un rango de edad específico.

8. Consulta de empleados por rango de salario: Permite buscar empleados dentro de un rango de salario específico.

9. Consulta de empleados por fecha de contratación: Permite buscar empleados dentro de una fecha de contratación específica.

10. Consulta de empleados por nombre y apellido: Permite buscar empleados dentro de un nombre y apellido específico.

11. Consulta de empleados por DNI: Permite buscar empleados dentro de un DNI específico.

12. Consulta de empleados por departamento y rango de edad: Permite buscar empleados dentro de un departamento y rango de edad específico.

13. Consulta de empleados por departamento y rango de salario: Permite buscar empleados dentro de un departamento y rango de salario específico.

14. Consulta de empleados por departamento y fecha de contratación: Permite buscar empleados dentro de un departamento y fecha de contratación específica.

15. Consulta de empleados por nombre, apellido y DNI: Permite buscar empleados dentro de un nombre, apellido y DNI específico.

# IVIOAEIO Cliente-Servidor

Este es un sistema de cliente-servidor que se divide en tres partes principales:

- El cliente (el dispositivo que hace la solicitud).

- El servidor (el dispositivo que responde a las solicitudes).

- La red (el medio por el cual el cliente y el servidor se comunican).

El sistema se basa en la transferencia de datos entre el cliente y el servidor.

El cliente envía una solicitud al servidor, el servidor responde con los datos solicitados y el cliente los recibe.

Este sistema es muy útil para la transferencia de datos entre dispositivos.

Algunos ejemplos de sistemas de cliente-servidor incluyen:

- El sistema de correo electrónico.

- El sistema de gestión de bases de datos.

- El sistema de gestión de contenido.

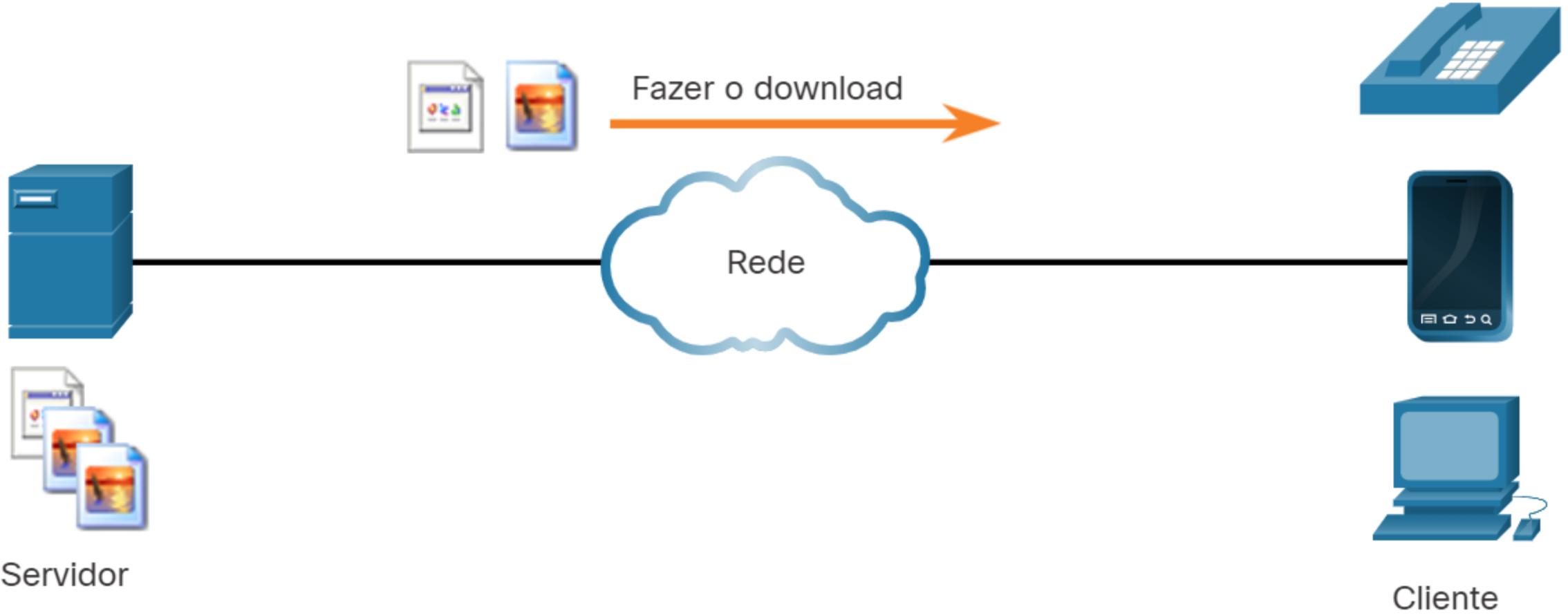
- El sistema de gestión de la cadena de suministro.

- El sistema de gestión de la calidad.

- El sistema de gestión de la producción.

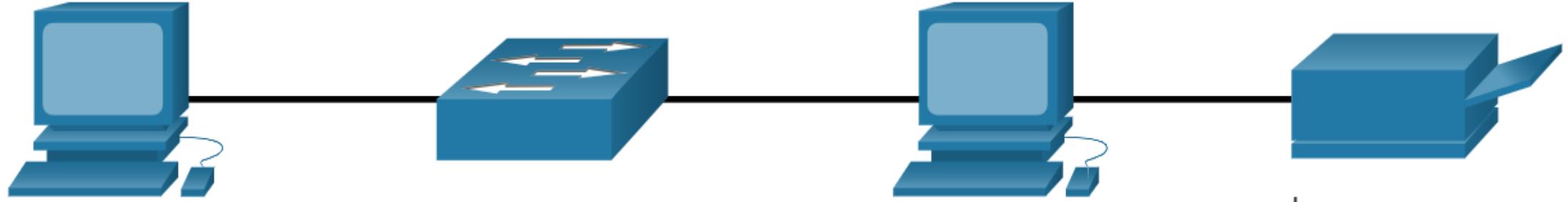
Considere que os processos de cliente e servidor estão na camada de aplicação. O cliente começa a troca ao solicitar dados do servidor, que responde enviando uma ou mais sequências de dados ao cliente. Os protocolos da camada de aplicação descrevem o formato das requisições e respostas entre clientes e servidores. Além da transferência real de dados, essa troca de informações também pode exigir informações de autenticação de usuário e identificação de um arquivo de dados a ser transferido.

Um exemplo de rede cliente / servidor é usar o serviço de e-mail de um ISP para enviar, receber e armazenar e-mail. O cliente de e-mail em um computador doméstico emite uma solicitação ao servidor de e-mail do ISP para qualquer e-mail não lido. O servidor responde enviando o e-mail solicitado ao cliente. A transferência de dados de um cliente para um servidor é chamada de upload e os dados de um servidor para um cliente como um download.





- Em uma rede P2P, dois ou mais computadores são conectados via rede e podem compartilhar recursos (como impressoras e arquivos) sem ter um servidor exclusivo. Cada dispositivo conectado final (conhecido como peer) pode funcionar como cliente ou servidor. Um computador pode assumir a função de servidor para uma transação ao mesmo tempo em que é o cliente de outro. As funções de cliente e servidor são definidas de acordo com a requisição.
- Além de compartilhar arquivos, uma rede como essa permitiria aos usuários ativar jogos na rede ou compartilhar uma conexão com a Internet.



Ponto 1

Ponto 2

Impressora

Servidor de  
arquivos do cliente  
de impressão

Cliente de arquivo  
do servidor de  
impressão

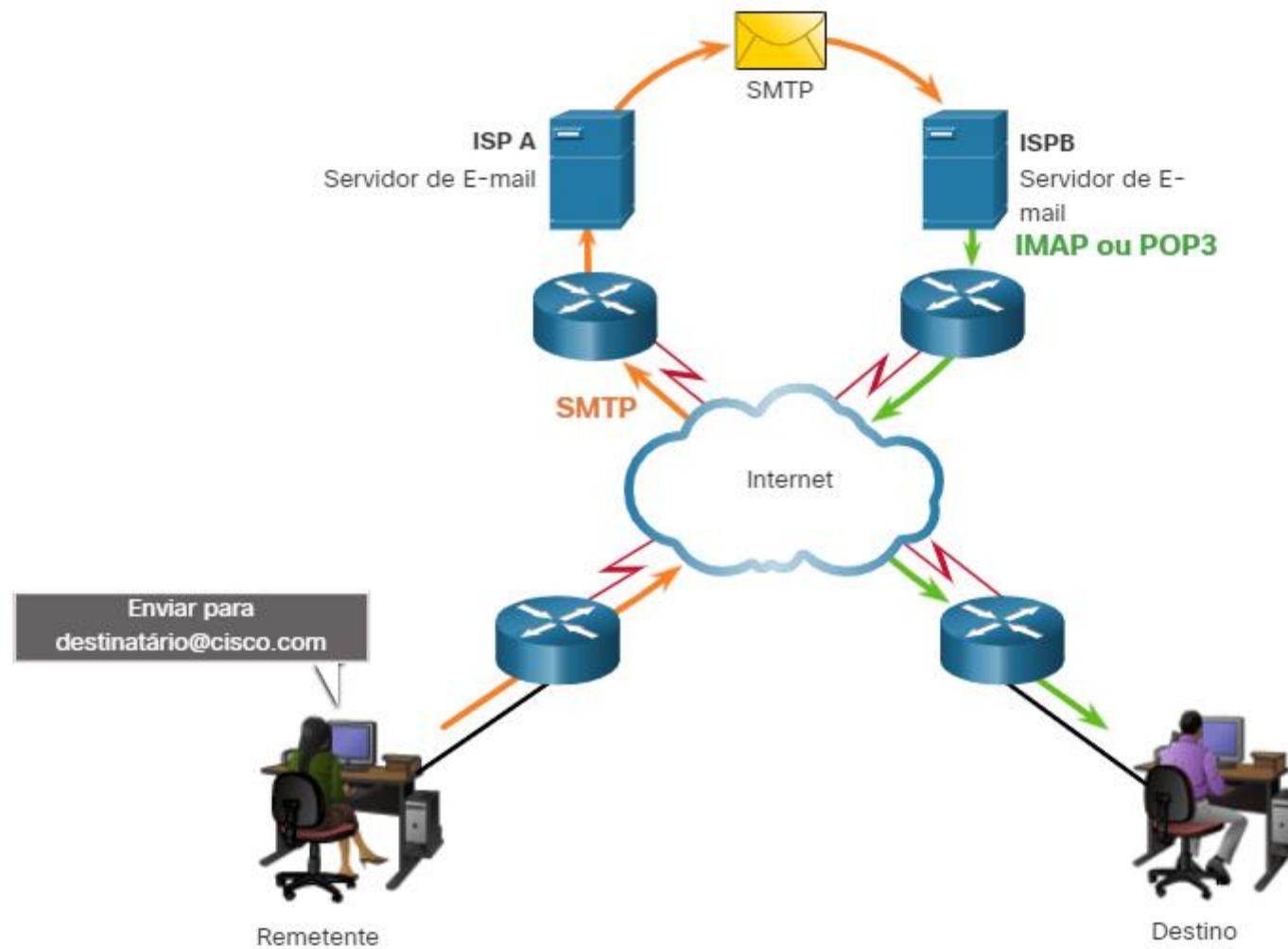
Impressora  
conectada  
diretamente

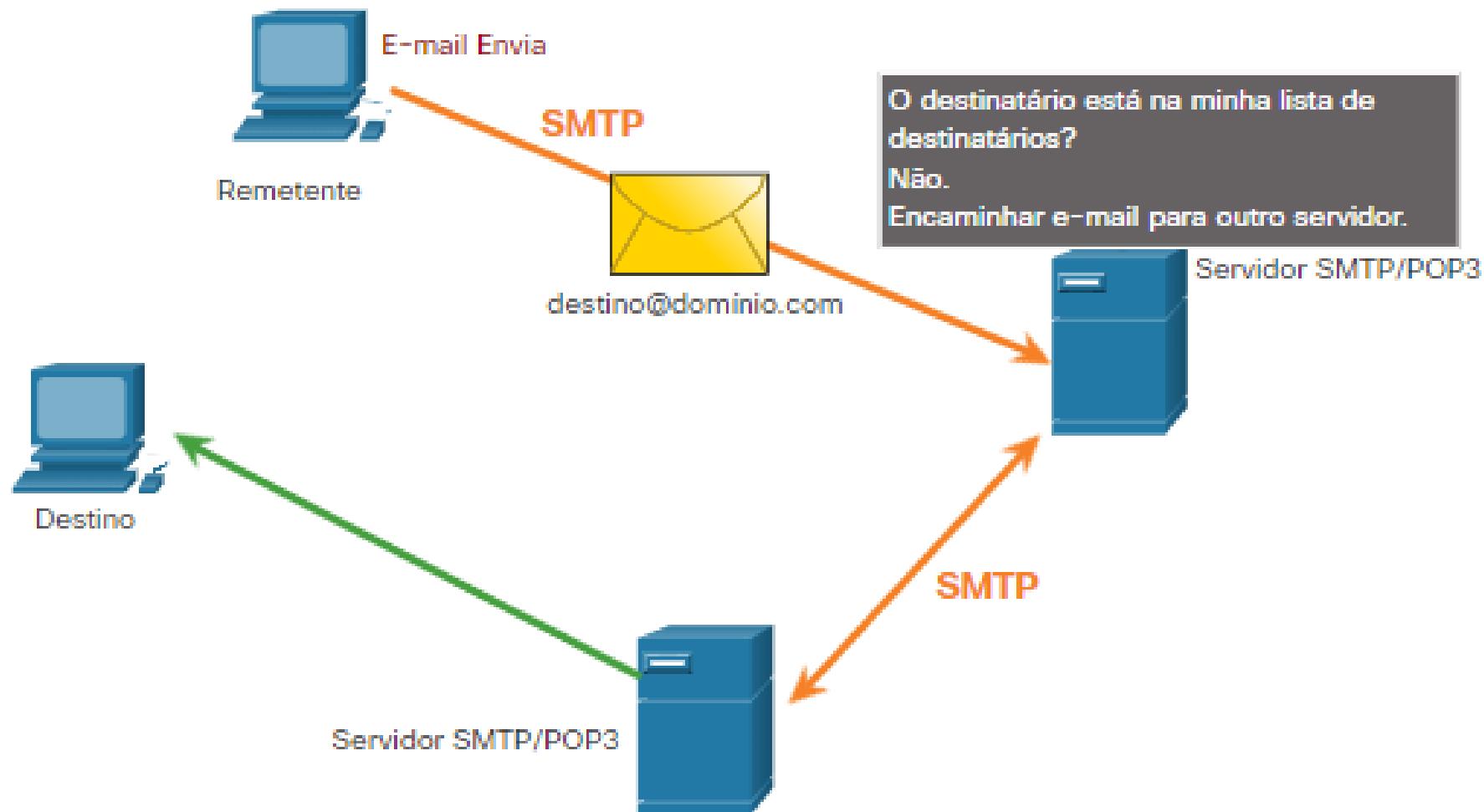
- **Protocolos de E-mail e Web**
- HTTP e HTML
- Existem protocolos específicos da camada do aplicativo que são específicos para usos comuns, como navegação na Web e e-mail. O primeiro tópico lhe deu uma visão geral desses protocolos. Este tópico entra em mais detalhes.

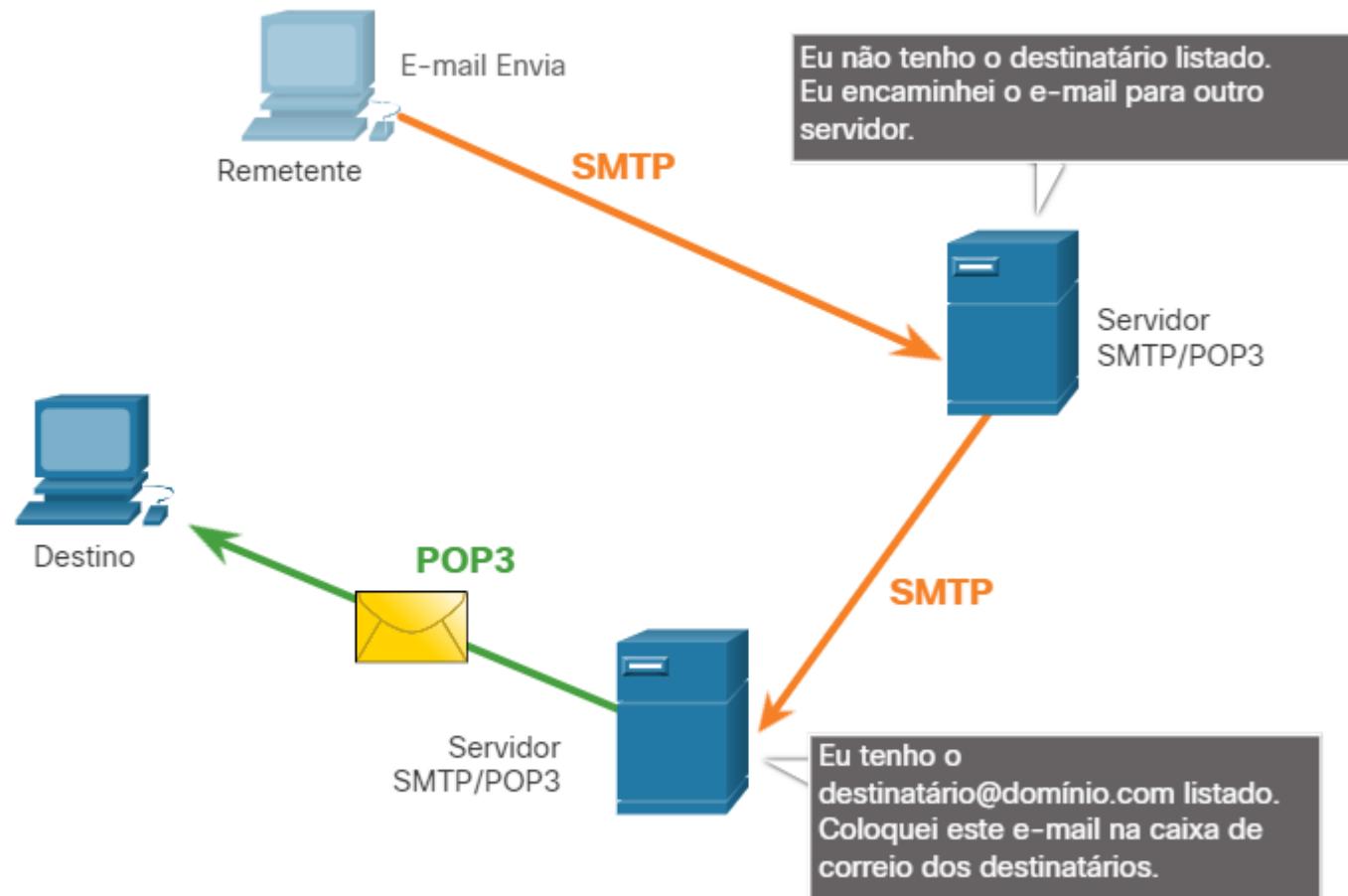
- **Protocolos de E-mail e Web**
- Quando um endereço da Web ou URL (URL) é digitado em um navegador da Web, ele estabelece uma conexão com o serviço da Web. O serviço Web está em execução no servidor que utiliza o protocolo HTTP. URLs e URIs (Uniform Resource Identifiers) são os nomes que a maioria das pessoas associa aos endereços da Web.

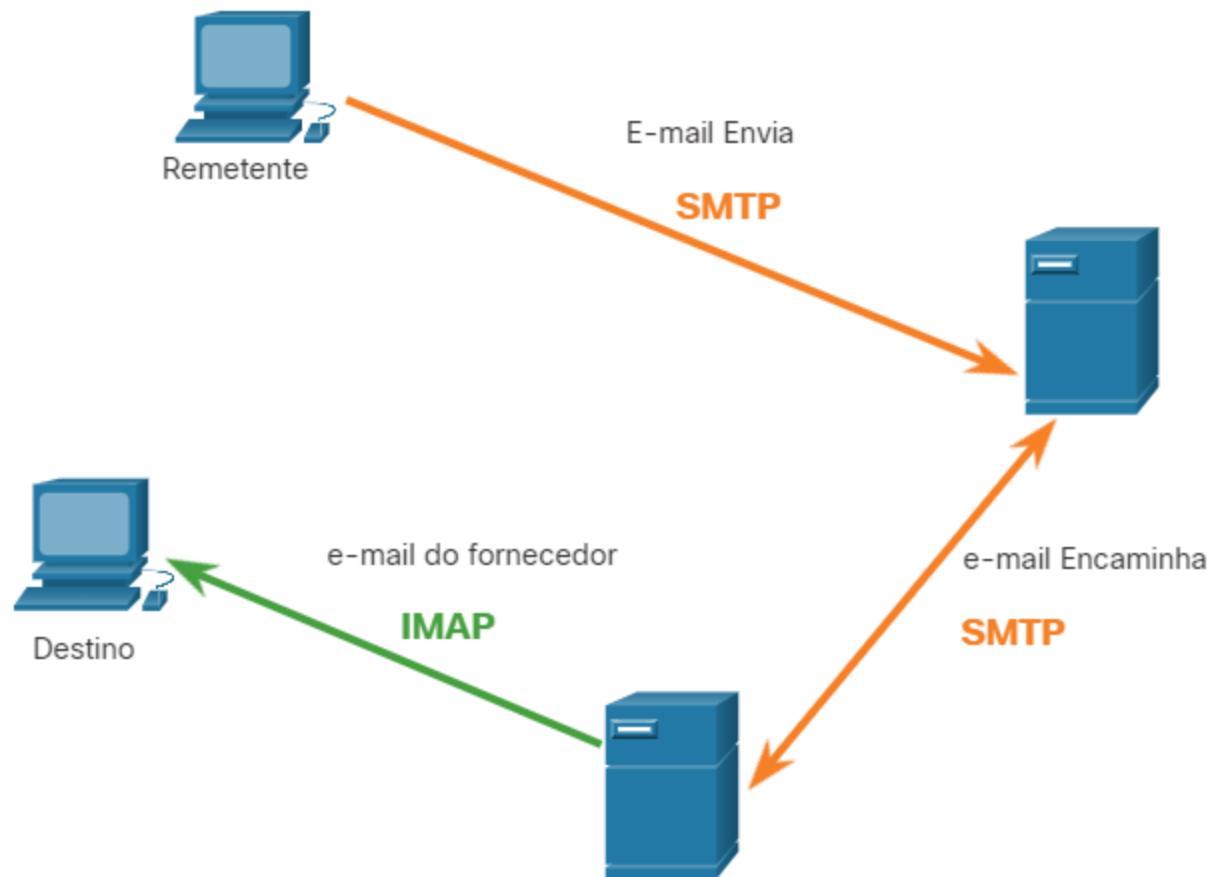
# Protocolos de e-mail

Um dos serviços básicos oferecidos por um ISP é a hospedagem de e-mails. Para ser executado em um computador ou outro dispositivo final, o e-mail precisa de várias aplicações e serviços, como mostra a figura. O e-mail é um método de armazenar e encaminhar, de enviar e de recuperar mensagens eletrônicas em uma rede. Mensagens de e-mail são armazenadas em bancos de dados em servidores de e-mail.











# **FACULDADE SENAC**

## **CASCAVEL - PR**

**1º SEMESTRE 2024**