

# Redes de Computadores

# Autor: Gabriel Felippe

**Website:** [akiradev.netlify.app](https://akiradev.netlify.app)

# Introdução

- Uma rede de computadores é um grupo de computadores que usa um conjunto de protocolos de comunicação comuns em interconexões digitais com o objetivo de compartilhar recursos localizados ou fornecidos pelos nós da rede.
- As interconexões entre os nós são formadas a partir de um amplo espectro de tecnologias de rede de telecomunicações, conectados fisicamente através de fios, óptico e métodos de radiofrequência sem fio que podem ser organizados em uma variedade de topologias de rede.

# Nós de uma Rede

- Os nós de uma rede de computadores podem incluir computadores pessoais, servidores, hardware de rede ou outros hosts especializados ou de uso geral.

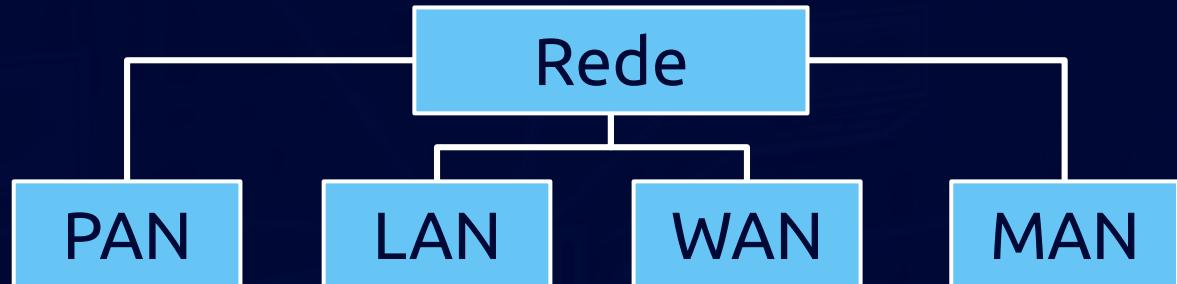


# Nós de uma Rede

- Em uma rede de comunicações, um nó de rede é um ponto de conexão que pode receber, criar, armazenar ou enviar dados ao longo de rotas de rede distribuídas. Cada nó da rede - seja um ponto final para transmissões de dados ou um ponto de redistribuição - tem uma capacidade programada ou projetada para reconhecer, processar e encaminhar as transmissões para outros nós da rede.
- Os nós são identificados por **hostnames** e **endereços de rede**.
- Os hostnames servem como rótulos memoráveis para os nós, raramente alterados após a atribuição inicial.
- Os endereços de rede servem para localizar e identificar os nós por protocolos de comunicação, como o **Internet Protocol (IP)**.

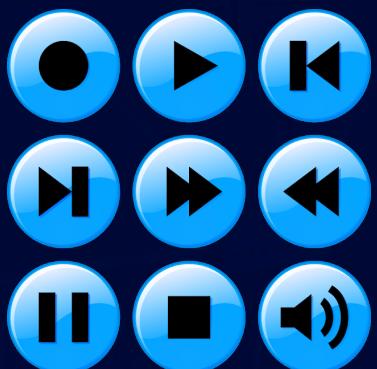
# Classificação de uma Rede

- As redes de computadores podem ser classificadas por vários critérios, incluindo o meio de transmissão usado para transportar sinais, largura de banda, protocolos de comunicação para organizar o tráfego da rede, o **tamanho da rede**, a topologia, o mecanismo de controle de tráfego e a intenção organizacional.



# Aplicações

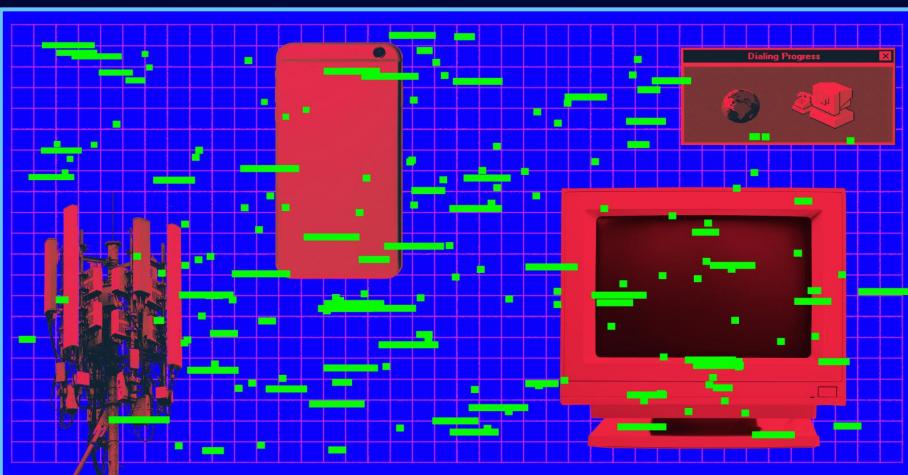
- As redes de computadores oferecem suporte a muitas aplicações e serviços, como acesso à World Wide Web, vídeo digital, áudio digital, uso compartilhado de aplicativos e servidores de armazenamento, impressoras e aparelhos de fax e uso de aplicativos de e-mail e mensagens instantâneas.



# Breve Histórico

- Redes de computadores pode ser considerado um ramo da ciência da computação, engenharia da computação e telecomunicações, uma vez que depende da aplicação teórica e prática das disciplinas relacionadas.

As redes de computadores foram influenciadas por uma ampla gama de desenvolvimentos tecnológicos e marcos históricos.



# Breve Histórico

- No final da década de 1950, as primeiras redes de computadores incluíam o sistema de radar militar dos Estados Unidos da América: **Semi-Automatic Ground Environment** (SAGE).
- Em 1959, **Christopher Strachey** entrou com um pedido de patente para *time-sharing* e **John McCarthy** iniciou o primeiro projeto para implementar time-sharing de programas de usuário no MIT. Stratchey passou o conceito para J. C. R. Licklider na Conferência de Processamento de Informação da UNESCO inaugural em Paris naquele ano. McCarthy foi fundamental na criação de três dos primeiros sistemas de time-sharing (Compatible Time-Sharing System em 1961, BBN Time-Sharing System em 1962 e Dartmouth Time Sharing System em 1963).

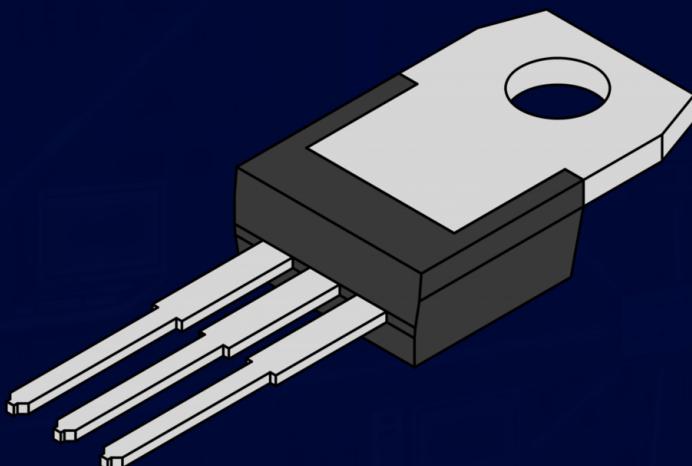
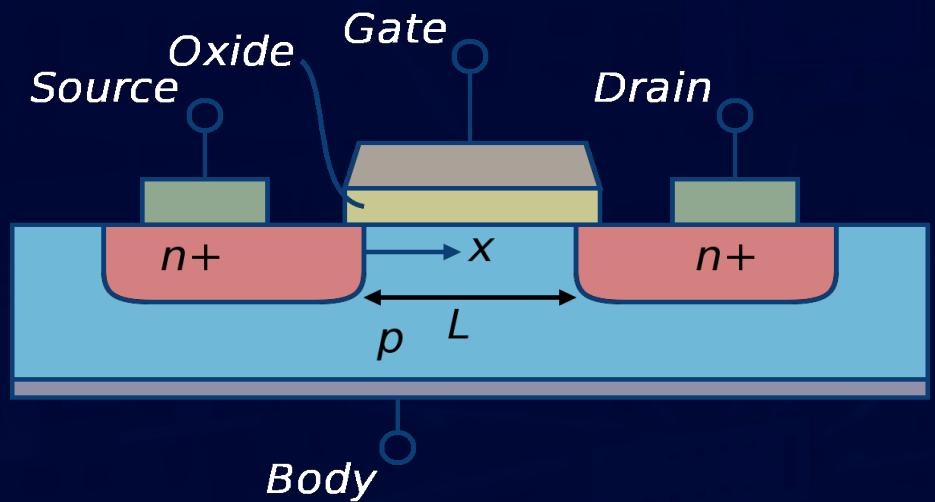
# Breve Histórico

- Em 1959, Anatolii Ivanovich Kitov propôs ao Comitê Central do Partido Comunista da União Soviética um plano detalhado para a reorganização do controle das forças armadas soviéticas e da economia soviética com base em uma rede de centros de computação, o OGAS.



# Breve Histórico

- Em 1959, o transistor MOS foi inventado por Mohamed Atalla e Dawon Kahng no Bell Labs. Mais tarde, tornou-se um dos blocos básicos de construção de virtualmente qualquer elemento da infraestrutura de comunicações.



# Breve Histórico

- Em 1960, o sistema de reservas de linhas aéreas comerciais conhecido como *semi-automatic business research environment* (SABRE) entrou em operação com dois mainframes conectados.
- Em 1963, J. C. R. Licklider enviou um memorando para colegas de escritório discutindo o conceito de "Rede Intergalática de Computadores", uma rede de computadores destinada a permitir comunicações gerais entre usuários de computador.

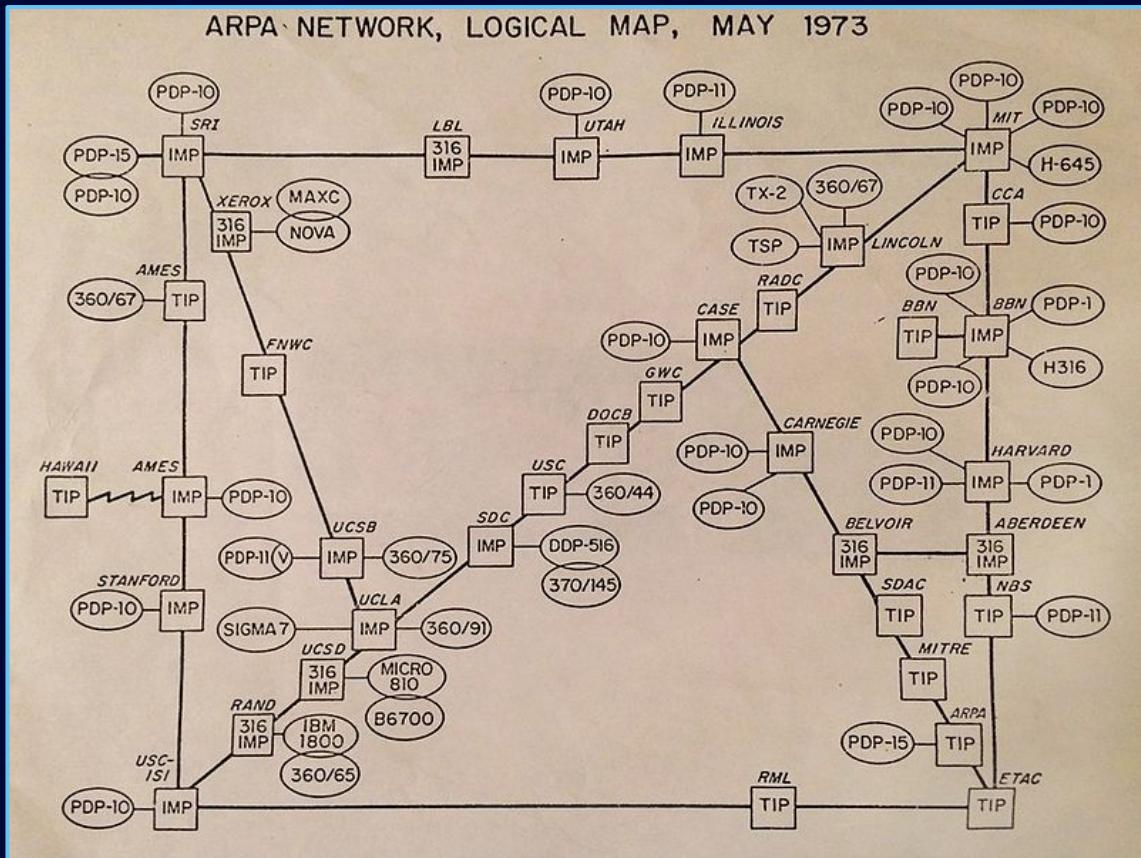
# Breve Histórico

- Ao longo da década de 1960, Paul Baran e Donald Davies desenvolveram independentemente o conceito de *packet switching* para transferir informações entre computadores em uma rede. Davies foi o pioneiro na implementação do conceito com a [rede NPL](#), uma rede de área local no National Physical Laboratory (Reino Unido) usando uma velocidade de linha de 768 kbit/s.
- Em 1965, a Western Electric introduziu a primeira central telefônica amplamente usada que implementou o controle de computador.

# Breve Histórico

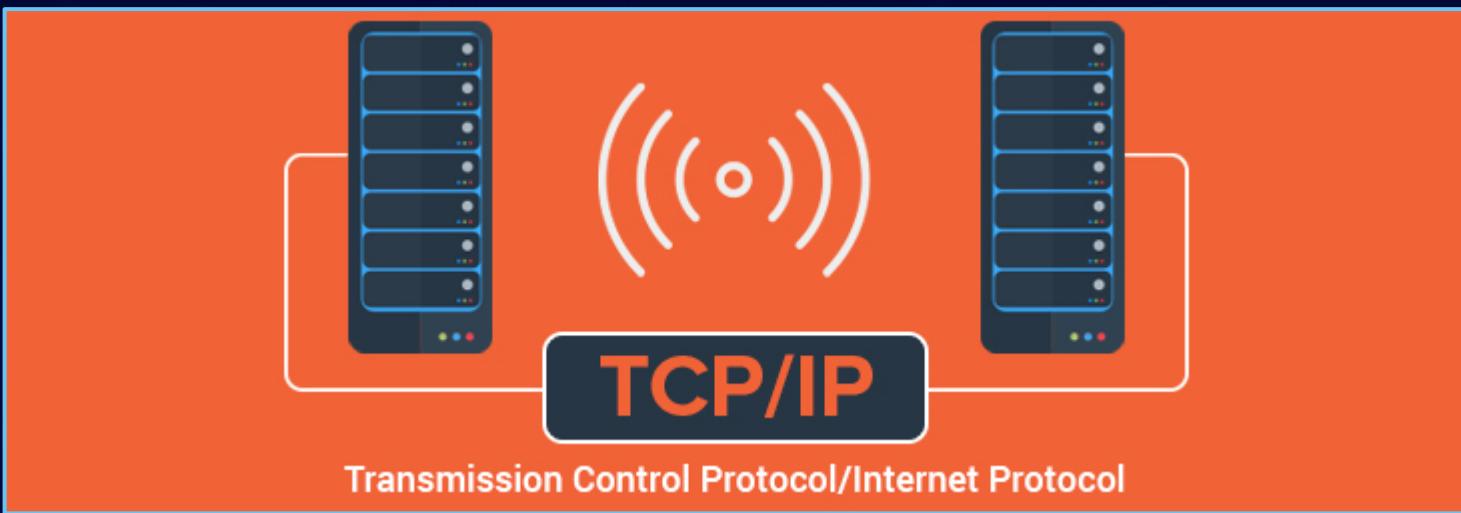
- Em 1969, os primeiros quatro nodes da ARPANET foram conectados usando circuitos de 50 kbit/s entre a University of California em Los Angeles, o Stanford Research Institute, a University of California em Santa Barbara e a University of Utah. Na década de 1970, Leonard Kleinrock realizou um trabalho matemático para modelar o desempenho de *packet-switched networks*, que sustentou o desenvolvimento da ARPANET. Seu trabalho teórico sobre roteamento hierárquico no final dos anos 1970 com o estudante Farouk Kamoun continua sendo crítico para a operação da Internet hoje.

# Mapa da ARPANET (1973)



# Breve Histórico

- Em 1972, serviços comerciais usando X.25 foram implantados e mais tarde usados como uma infraestrutura subjacente para expandir redes TCP/IP.



# Breve Histórico

- Em 1973, a rede francesa CYCLADES foi a primeira a responsabilizar os hosts pela entrega confiável de dados, ao invés de ser um serviço centralizado da própria rede.
- Em 1973, Robert Metcalfe escreveu um memorando formal no Xerox PARC descrevendo a Ethernet, um sistema de rede baseado na rede Aloha, desenvolvido na década de 1960 por Norman Abramson e colegas da Universidade do Havaí. Em julho de 1976, Robert Metcalfe e David Boggs publicaram seu artigo "Ethernet: Distributed Packet Switching for Local Computer Networks" e colaboraram em várias patentes recebidas em 1977 e 1978.

# Breve Histórico

- Em 1974, Vint Cerf, Yogen Dalal e Carl Sunshine publicaram a especificação do Protocolo de Controle de Transmissão (TCP), RFC 675, cunhando o termo Internet como uma abreviação para internetworking.
- Em 1976, John Murphy da Datapoint Corporation criou a ARCNET, uma rede de passagem de tokens usada pela primeira vez para compartilhar dispositivos de armazenamento.
- Em 1977, a primeira rede de fibra de longa distância foi implantada pela GTE em Long Beach, Califórnia.

# Breve Histórico

- Em 1977, a Xerox Network Systems (XNS) foi desenvolvida por Robert Metcalfe e Yogen Dalal na Xerox.
- Em 1979, Robert Metcalfe buscou tornar a Ethernet um padrão aberto.
- Em 1980, a Ethernet foi atualizada do protocolo original de 2,94 Mbit/s para o protocolo de 10 Mbit/s, que foi desenvolvido por Ron Crane, Bob Garner, Roy Ogas e Yogen Dalal.

# Breve Histórico



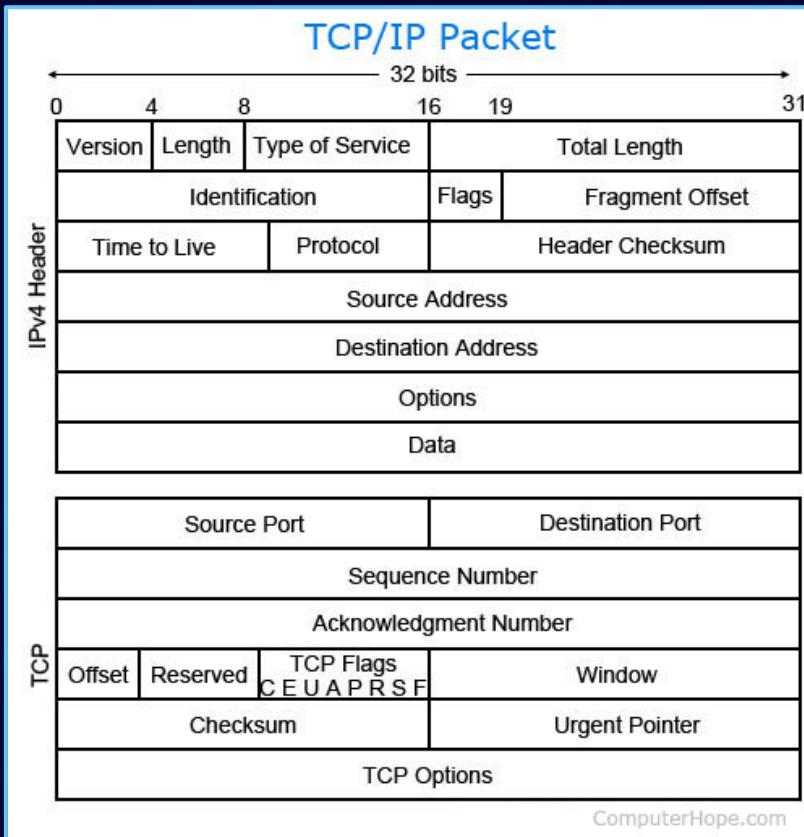
- Em 1995, a capacidade de velocidade de transmissão para Ethernet aumentou de 10 Mbit/s para 100 Mbit/s.
- Em 1998, a Ethernet suportava velocidades de transmissão de Gigabit. Posteriormente, velocidades mais altas de até 400 Gbit/s foram adicionadas (a partir de 2018).
- O dimensionamento da Ethernet tem contribuído para seu uso contínuo.

# Uso das Redes

- Uma rede de computadores é capaz então de estender as comunicações interpessoais por meio eletrônico com várias tecnologias, como e-mail, mensagens instantâneas, chat online, chamadas de voz e vídeo e videoconferência.
- Uma rede permite o compartilhamento de recursos de rede e de computação.
- Os usuários podem acessar e usar recursos fornecidos por dispositivos na rede, como imprimir um documento em uma impressora de rede compartilhada ou usar um dispositivo de armazenamento compartilhado.
- Uma rede permite o compartilhamento de arquivos, dados e outros tipos de informações, dando aos usuários autorizados a capacidade de acessar informações armazenadas em outros computadores da rede.
- A computação distribuída usa recursos de computação em uma rede para realizar tarefas.

# Pacote de Rede

- A maioria das redes de computadores modernas usa protocolos baseados na transmissão em modo de pacote.
- Um **pacote de rede** é uma unidade formatada de dados transportada por uma **rede comutada por pacotes**.
- As tecnologias de link físico da rede de pacotes normalmente limitam o tamanho dos pacotes a uma determinada **maximum transmission unit (MTU)**.



# Pacote de Rede

- Uma mensagem mais longa é fragmentada antes de ser transferida e, uma vez que os pacotes chegam, eles são remontados para construir a mensagem original.
- Os pacotes consistem em dois tipos de dados: **informações de controle** e **dados do usuário** (payload).
- As **informações de controle** fornecem os dados de que a rede precisa para entregar os dados do usuário, por exemplo, endereços de rede de origem e destino, códigos de detecção de erros e informações de sequenciamento.

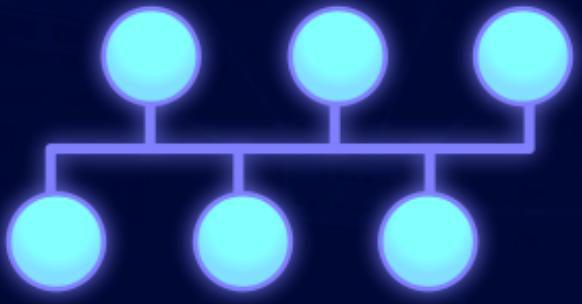
# Pacote de Rede

- Normalmente, as informações de controle são encontradas em headers e trailers de pacotes, com dados de payload entre eles.
- Na **comutação de pacotes**, a largura de banda do **meio de transmissão** é compartilhada entre várias sessões de comunicação, em contraste com a **comutação de circuitos**, na qual os circuitos são pré-alocados para a duração de uma sessão e os dados são normalmente transmitidos como um **bit stream** contínuo.
- Quando um usuário não está enviando pacotes, o link pode ser preenchido com pacotes de outros usuários e, portanto, o custo pode ser compartilhado, com relativamente pouca interferência, desde que o link não seja usado em demasia. Freqüentemente, a rota que um pacote precisa seguir através de uma rede não está imediatamente disponível. Nesse caso, o pacote é **enfileirado** e espera até que um link esteja livre.

# Topologia de Rede

- Topologia de rede é o layout, padrão ou hierarquia organizacional da interconexão de hosts de rede, em contraste com sua localização física ou geográfica.
- Normalmente, a maioria dos diagramas que descrevem redes são organizados por sua topologia.
- A topologia da rede pode afetar o rendimento, mas a confiabilidade costuma ser mais crítica.
- Com muitas tecnologias, como redes de barramento ou estrela, uma única falha pode fazer com que a rede falhe totalmente.

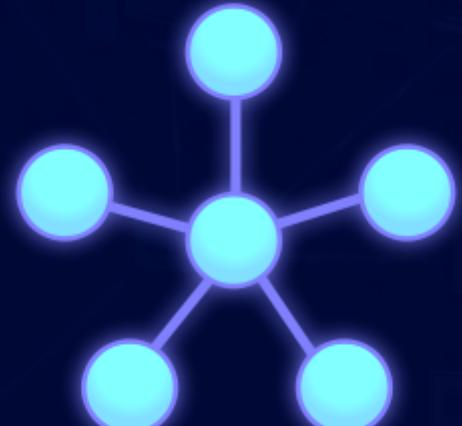
# Layouts Comuns



Bus

- **Rede de barramento:** todos os nós estão conectados a um meio comum ao longo deste meio. Esse era o layout usado na Ethernet original, chamado 10BASE5 e 10BASE2. Essa ainda é uma topologia comum na camada de enlace, embora as variantes modernas da camada física usem links ponto a ponto.

# Layouts Comuns



**Star**

- **Rede estrela:** todos os nós são conectados a um nó central especial. Este é o layout típico encontrado em uma LAN sem fio, onde cada cliente sem fio se conecta ao ponto de acesso sem fio central.

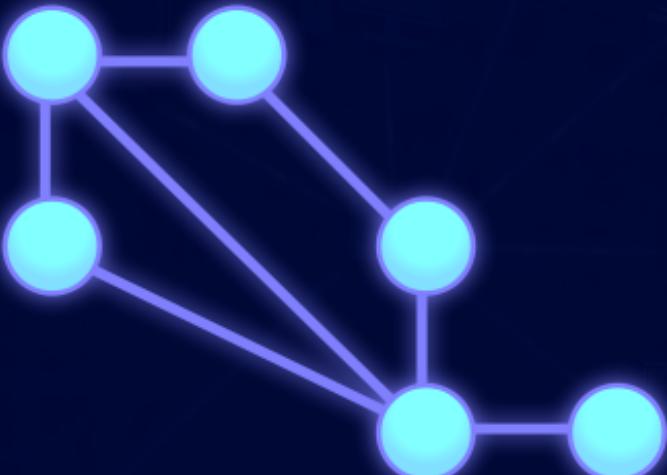
# Layouts Comuns



Ring

- **Rede em anel:** cada nó é conectado a seu nó vizinho esquerdo e direito, de modo que todos os nós estejam conectados e que cada nó possa alcançar um outro nó atravessando os nós para a esquerda ou para a direita. A **Interface de Dados Distribuídos de Fibra (FDDI)** fez uso dessa topologia.

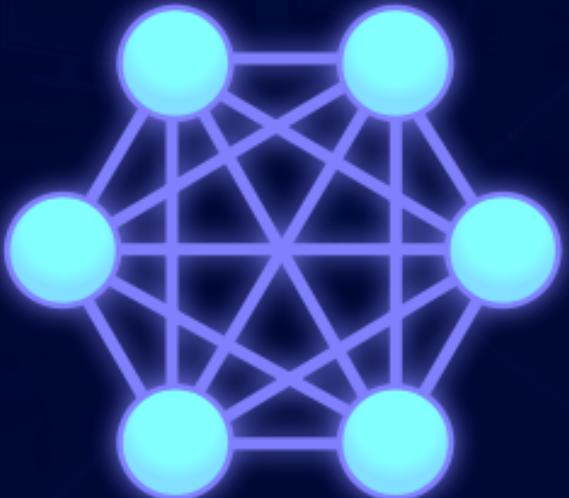
# Layouts Comuns



Mesh

- **Rede mesh:** cada nó é conectado a um número arbitrário de vizinhos de tal forma que haja pelo menos uma passagem de qualquer nó para outro.

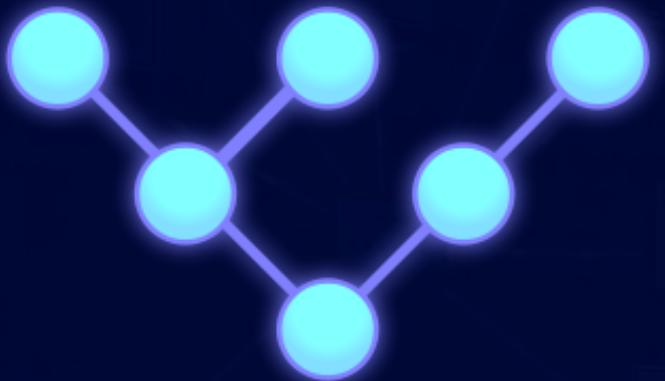
# Layouts Comuns



**Fully Connected**

- **Rede totalmente conectada:** cada nó está conectado a todos os outros nós da rede.

# Layouts Comuns



Tree

- **Rede em árvore:** os nós são organizados hierarquicamente.

# Layout Físico

- O layout físico dos nós em uma rede pode não refletir necessariamente a topologia da rede. Por exemplo, com o **FDDI**, a topologia da rede é um anel, mas a topologia física geralmente é uma estrela, porque todas as conexões vizinhas podem ser roteadas por meio de um local físico central.
- O layout físico não é completamente irrelevante, uma vez que, como dutos comuns e locais de equipamentos podem representar pontos únicos de falha devido a problemas como incêndios, falhas de energia e inundações.

# Overlay Network



- Uma overlay network é uma rede virtual construída sobre outra rede. Os nós na overlay network são conectados por links virtuais ou lógicos. Cada link corresponde a um caminho, talvez por meio de muitos links físicos, na rede subjacente.

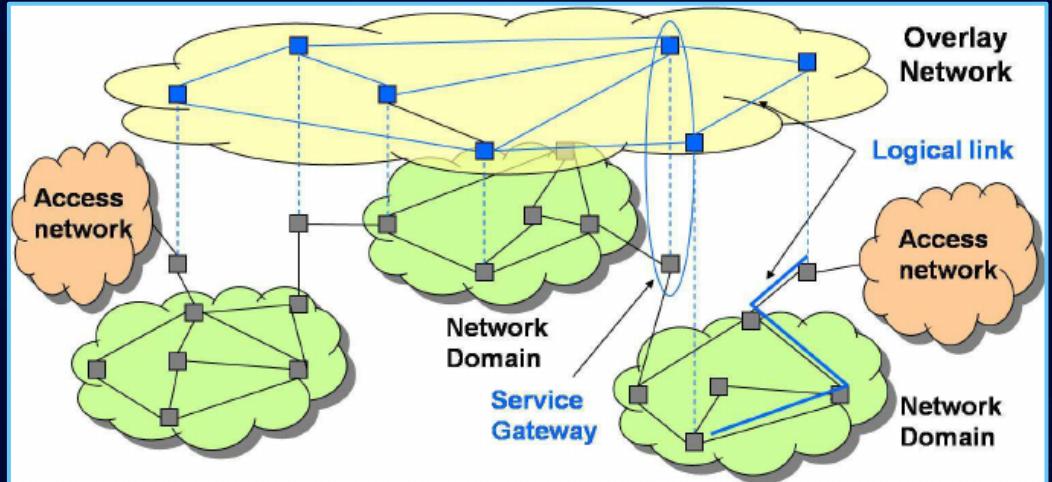
# Overlay Network

- A topologia da overlay network pode (e geralmente é) diferir daquela subjacente. Por exemplo, muitas redes ponto a ponto são overlay networks. Eles são organizados como nós de um sistema virtual de links que rodam no topo da Internet.
- As overlay networks existem desde a invenção das redes, quando os sistemas de computador eram conectados por linhas telefônicas usando **modems**, antes que qualquer rede de dados existisse.

# Overlay Network

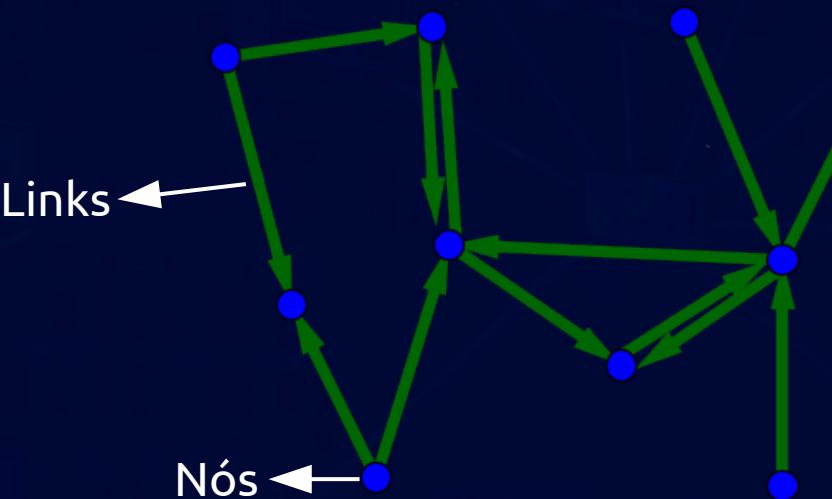
- O exemplo mais marcante de uma overlay network é a própria Internet.
- A própria Internet foi inicialmente construída como uma sobreposição na rede telefônica.
- Mesmo hoje, cada nó da Internet pode se comunicar com praticamente qualquer outro por meio de uma malha subjacente de sub-redes de topologias e tecnologias totalmente diferentes.
- A resolução de endereço e o roteamento são os meios que permitem o mapeamento de uma IP overlay network totalmente conectada à sua rede subjacente.

# Overlay Network



- Outro exemplo de overlay network é uma tabela **hash distribuída**, que mapeia chaves para nós na rede. Nesse caso, a rede subjacente é uma rede IP e a overlay network é uma tabela (na verdade, um mapa) indexado por chaves.

# Links de Rede

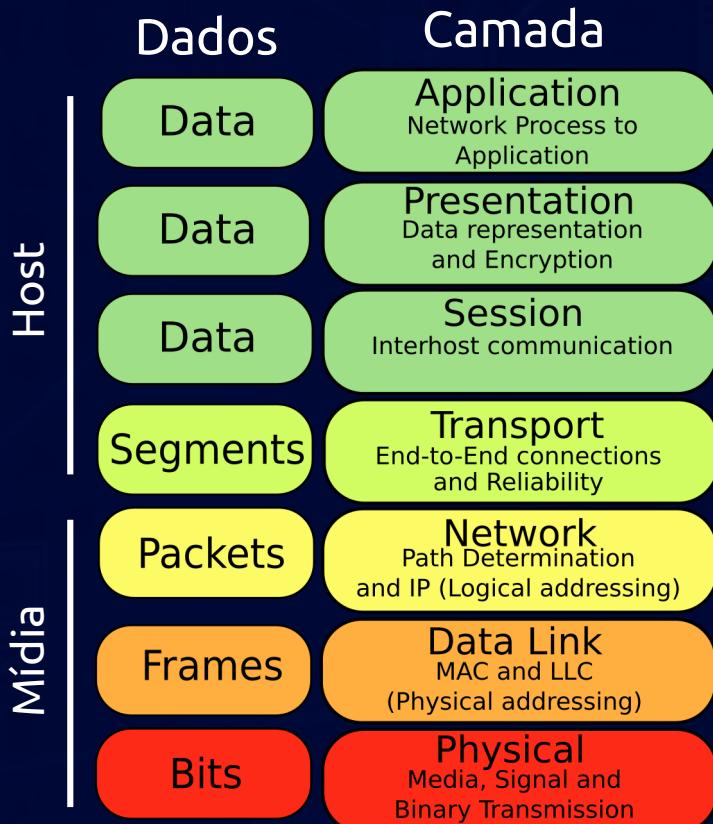


- Os meios de transmissão (frequentemente referidos na literatura como o meio físico) usados para conectar dispositivos para formar uma rede de computadores incluem cabo elétrico, fibra óptica e espaço livre.

# Links de Rede

- No **modelo OSI**, o software para lidar com a mídia é definido nas camadas 1 e 2 - a **camada física** e a **camada de enlace de dados**.

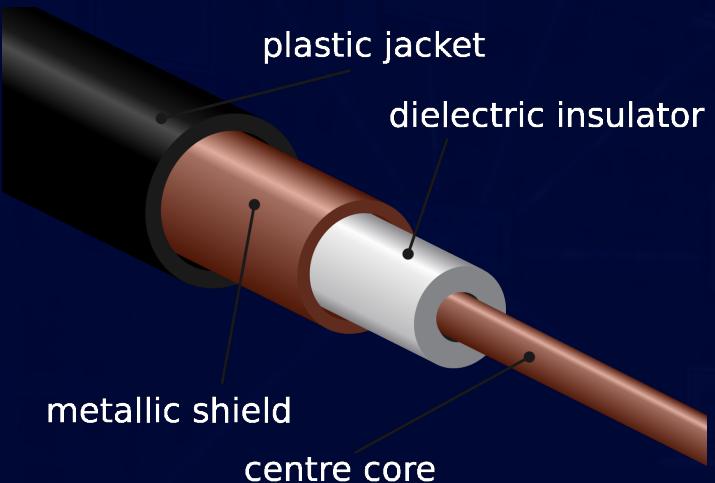
Modelo OSI



# Links de Rede

- Uma família amplamente adotada que usa mídia de cobre e fibra na tecnologia de rede local (LAN) é conhecida coletivamente como Ethernet.
- Os padrões de mídia e protocolo que permitem a comunicação entre dispositivos em rede pela Ethernet são definidos pelo IEEE 802.3.
- Os padrões de LAN sem fio (wireless) usam ondas de rádio, outros usam sinais infravermelhos como meio de transmissão.
- A comunicação por linha de energia usa o cabeamento elétrico de um prédio para transmitir dados.

# Tecnologias com Fio

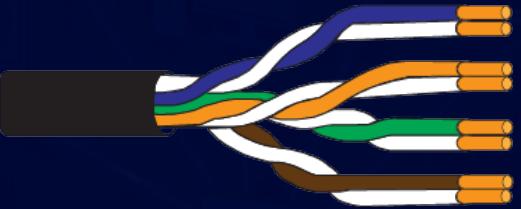


- O cabo coaxial é amplamente utilizado para sistemas de televisão a cabo, edifícios de escritórios e outros locais de trabalho para redes locais. A velocidade de transmissão varia de 200 milhões de bits por segundo a mais de 500 milhões de bits por segundo.

# Tecnologias com Fio

- A tecnologia ITU-T G.hn usa fiação doméstica existente (cabo coaxial, linhas telefônicas e linhas de energia) para criar uma rede local de alta velocidade.

# Tecnologias com Fio



- O cabeamento de par trançado é usado para Ethernet com fio e outros padrões. Normalmente consiste em 4 pares de cabos de cobre que podem ser utilizados para transmissão de voz e dados. O uso de dois fios trançados ajuda a reduzir a diafonia e a indução eletromagnética.
- A velocidade de transmissão varia de 2 Mbit/s a 10 Gbit/s. O cabeamento de par trançado vem em duas formas: par trançado não blindado (UTP) e par trançado blindado (STP). Cada formulário vem em várias classificações de categoria, projetadas para uso em vários cenários.

# Tecnologias com Fio

- Uma **fibra óptica** é uma fibra de vidro. Ele carrega pulsos de luz que representam dados por meio de lasers e amplificadores ópticos.
- Algumas vantagens das fibras ópticas em relação aos fios de metal são a perda de transmissão muito baixa e a imunidade à interferência elétrica.
- Usando a **dense wave division multiplexing**, as fibras ópticas podem transportar simultaneamente vários fluxos de dados em diferentes comprimentos de onda de luz, o que aumenta muito a taxa com que os dados podem ser enviados para até trilhões de bits por segundo.
- As fibras ópticas podem ser usadas para longas extensões de cabo transportando taxas de dados muito altas e são usadas para cabos submarinos para interconectar continentes.

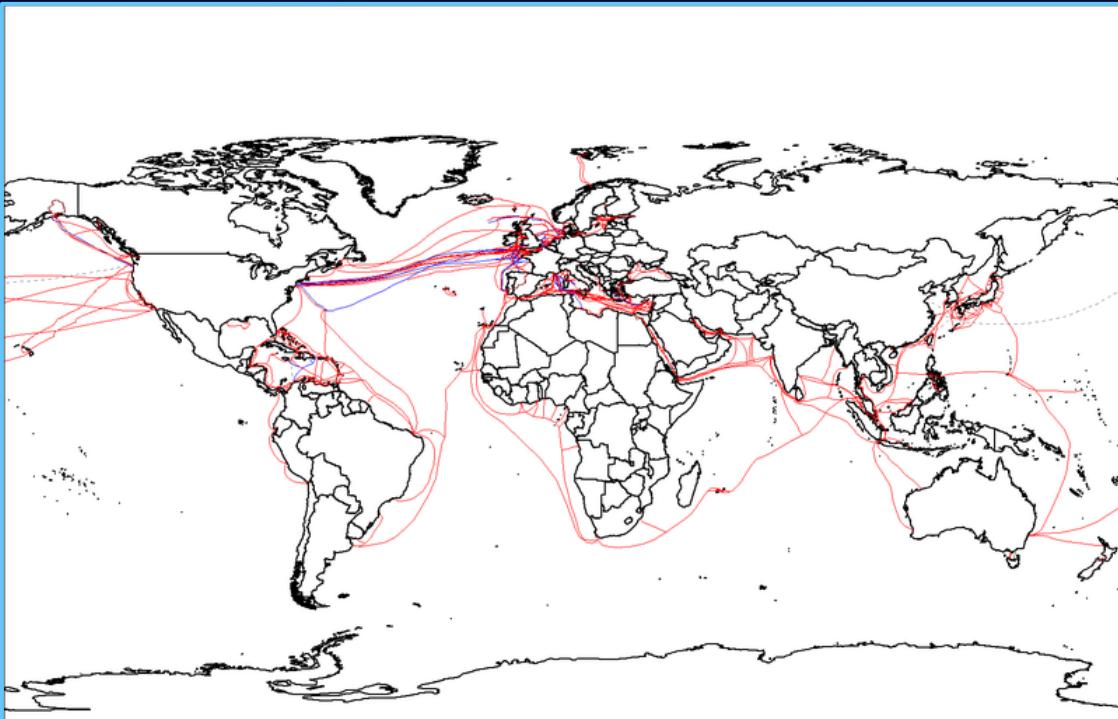
# Tecnologias com Fio



- Existem dois tipos básicos de fibra ótica, **single-mode optical fiber (SMF)** e **multi-mode optical fiber (MMF)**.
- A Single-mode fiber tem a vantagem de ser capaz de sustentar um sinal coerente por dezenas ou até cem quilômetros.
- A Multimode fiber é mais barata, mas está limitada a algumas centenas ou mesmo apenas algumas dezenas de metros, dependendo da taxa de dados e do grau do cabo.

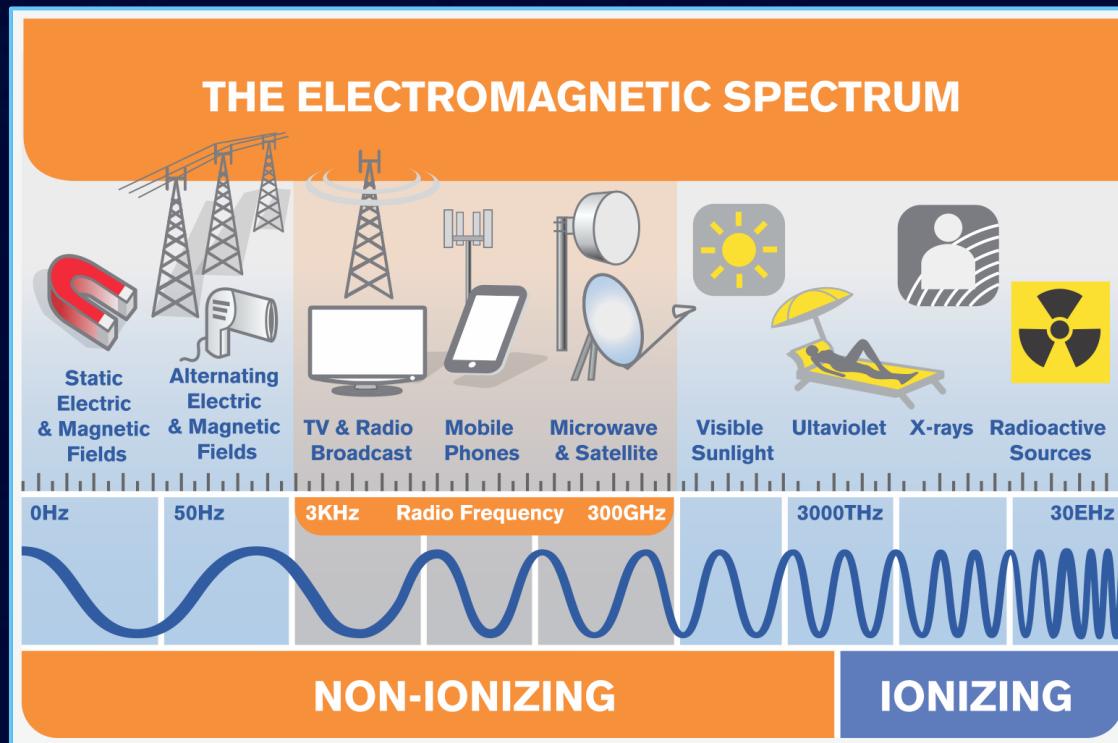
# Mapa

- Mapa de 2007 mostrando cabos de telecomunicações de fibra óptica submarinos em todo o mundo.



# Tecnologias sem Fio

- As conexões de rede podem ser estabelecidas sem fio usando rádio ou outro meio **eletromagnético** de comunicação.



# Tecnologias sem Fio



- Micro-ondas terrestres: a comunicação por micro-ondas terrestres usa transmissores e receptores baseados na Terra, semelhantes a antenas parabólicas. As microondas terrestres estão na faixa de baixo gigahertz, o que limita todas as comunicações à linha de visão. As estações retransmissoras estão espaçadas aproximadamente 40 milhas (64 km) uma da outra.

# Tecnologias sem Fio



- **Satélites de comunicação:** Os satélites também se comunicam por microondas. Os satélites estão estacionados no espaço, normalmente em órbita geossíncrona 35.400 km (22.000 milhas) acima do equador. Esses sistemas em órbita terrestre são capazes de receber e retransmitir voz, dados e sinais de TV.

# Tecnologias sem Fio



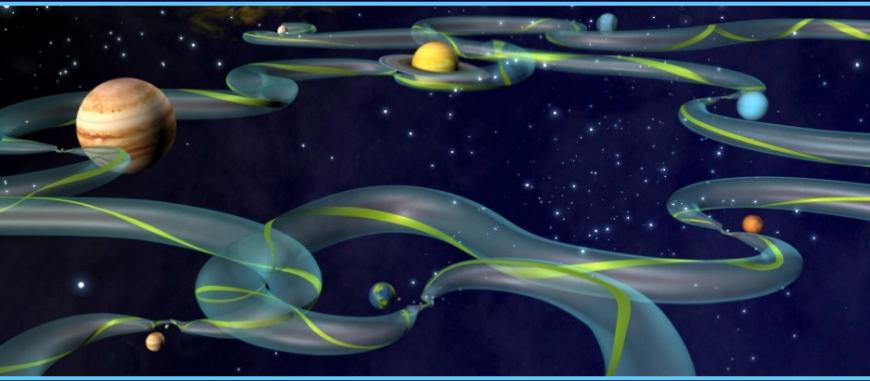
- As **redes de celulares** usam várias tecnologias de comunicação de rádio. Os sistemas dividem a região coberta em várias áreas geográficas. Cada área é servida por um **transceptor** de baixa potência.

# Tecnologias sem Fio



- As *redes de celulares* usam várias tecnologias de comunicação de rádioTecnologias de rádio e *spread spectrum*  
- LANs sem fio usam uma tecnologia de rádio de alta frequência semelhante ao celular digital. As LANs sem fio usam tecnologia de espalhamento espectral para permitir a comunicação entre vários dispositivos em uma área limitada. O IEEE *802.11* define um tipo comum de tecnologia de ondas de rádio sem fio de padrões abertos conhecido como *Wi-Fi*.

# Tecnologias sem Fio



- A **Free-space optical communication** usa luz visível ou invisível para as comunicações. Na maioria dos casos, a propagação em linha de visão é usada, o que limita o posicionamento físico dos dispositivos de comunicação.
- Estendendo a Internet para dimensões interplanetárias por meio de ondas de rádio e meios ópticos, a **Internet Interplanetária**.

# Nós de Rede



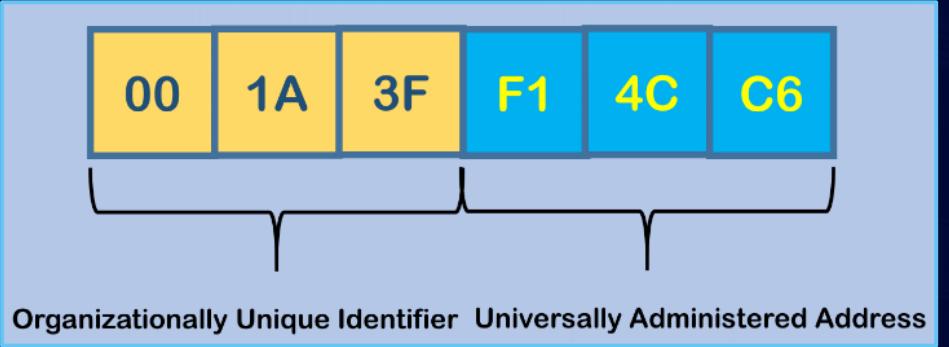
- Além de qualquer mídia de transmissão física, as redes são construídas a partir de blocos de construção básicos adicionais do sistema, como network interface controllers (NICs), repetidores, hubs, bridges, switches, roteadores, modems e firewalls.
- Qualquer peça específica de equipamento, freqüentemente, contém vários blocos de construção e, portanto, pode executar várias funções.

# Network Interface Controller



- Um **network interface controller** (NIC) é um hardware de computador que conecta o computador à mídia de rede e tem a capacidade de processar informações de rede de baixo nível.
- Por exemplo, o NIC pode ter um conector para aceitar um cabo ou uma antena para transmissão e recepção sem fio e o circuito associado.

# Endereço MAC



- Em redes Ethernet, cada controlador de interface de rede possui um endereço MAC (Media Access Control) exclusivo, geralmente armazenado na memória permanente do controlador.
- Para evitar conflitos de endereço entre dispositivos de rede, o Institute of Electrical and Electronics Engineers (IEEE) mantém e administra a exclusividade do endereço MAC.
- O tamanho de um endereço MAC Ethernet é de seis octetos.
- Os três octetos mais significativos são reservados para identificar os fabricantes de NIC.

# Repetidores



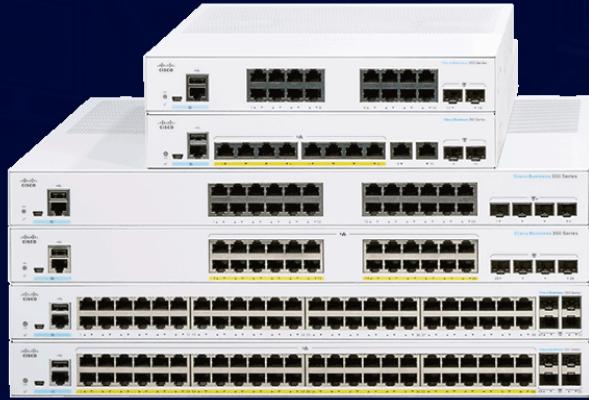
- Um **repetidor** é um dispositivo eletrônico que recebe um sinal de rede, limpa-o de ruídos desnecessários e o regenera.
- O sinal é retransmitido em um nível de potência mais alto ou para o outro lado da obstrução, de forma que o sinal possa cobrir distâncias maiores sem degradação.
- Na maioria das configurações Ethernet de par trançado, os repetidores são necessários para cabos com mais de 100 metros. Com fibra óptica, os repetidores podem estar separados por dezenas ou até centenas de quilômetros.

# Hub



- Um repetidor Ethernet com várias portas é conhecido como **hub** Ethernet.
- Além de recondicionar e distribuir sinais de rede, um hub repetidor auxilia na detecção de colisões e isolamento de falhas para a rede.
- Hubs e repetidores em LANs tornaram-se amplamente obsoletos pelos **switches** de rede modernos.

# Bridges e Switches



- As **bridges** e os **switches** de rede são diferentes de um hub, pois encaminham apenas **frames** para as portas envolvidas na comunicação, enquanto um hub encaminha para todas as portas.
- As bridges têm apenas duas portas, mas um switch pode ser considerado uma ponte com várias portas. Os switches normalmente têm várias portas, facilitando uma topologia em estrela para dispositivos e para switches adicionais em cascata.

# Bridges e Switches

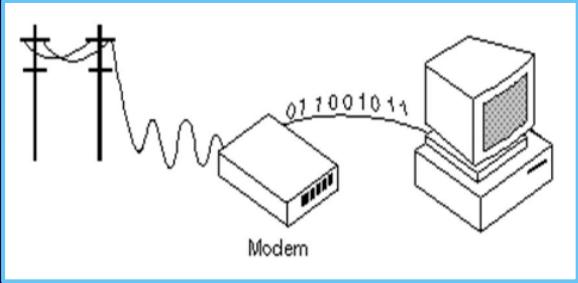
- Bridges e switches operam na camada de enlace de dados (camada 2) do modelo OSI e fazem a ponte de tráfego entre dois ou mais segmentos de rede para formar uma única rede local.
- Ambos são dispositivos que encaminham frames de dados entre portas com base no endereço MAC de destino em cada frame.
- Eles aprendem a associação de portas físicas a endereços MAC, examinando os endereços de origem dos frames recebidos e apenas encaminham o frame quando necessário.
- Se um MAC de destino desconhecido for direcionado, o dispositivo transmite a solicitação para todas as portas, exceto a origem, e descobre a localização na resposta.
- Bridges e switches dividem o domínio de colisão da rede, mas mantêm um único domínio de broadcast. A segmentação da rede por meio de bridging e switching ajuda a quebrar uma rede grande e congestionada em uma agregação de redes menores e mais eficientes.

# Roteadores



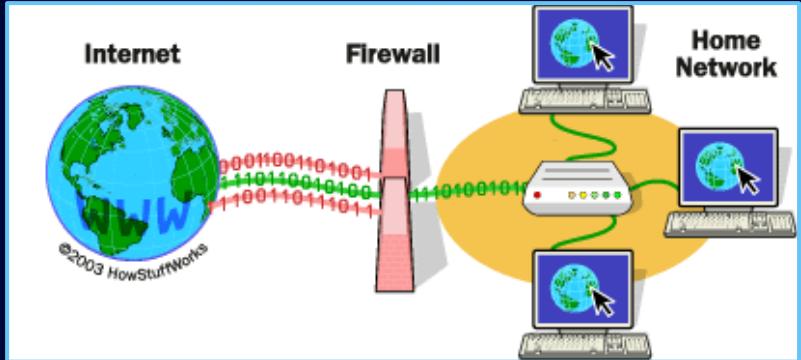
- Um **roteador** é um dispositivo de internetworking que encaminha pacotes entre redes processando as informações de endereçamento ou roteamento incluídas no pacote.
- As informações de roteamento geralmente são processadas em conjunto com a **tabela de roteamento**.
- Um roteador usa sua tabela de roteamento para determinar para onde encaminhar os pacotes e não requer pacotes de transmissão, o que é ineficiente para redes muito grandes.

# Modems



- Modems (**modulador-demodulador**) são usados para conectar nós de rede por meio de fios não projetados originalmente para tráfego de rede digital ou sem fio.
- Para fazer isso, um ou mais sinais de portadora são modulados pelo **sinal digital** para produzir um **sinal analógico** que pode ser adaptado para fornecer as propriedades necessárias para a transmissão.
- Os primeiros modems modulavam os sinais de áudio enviados por uma linha telefônica de voz padrão.
- Os modems ainda são comumente usados para linhas telefônicas, usando uma tecnologia de *digital subscriber line* e sistemas de televisão a cabo usando a tecnologia **DOCSIS**.

# Firewalls

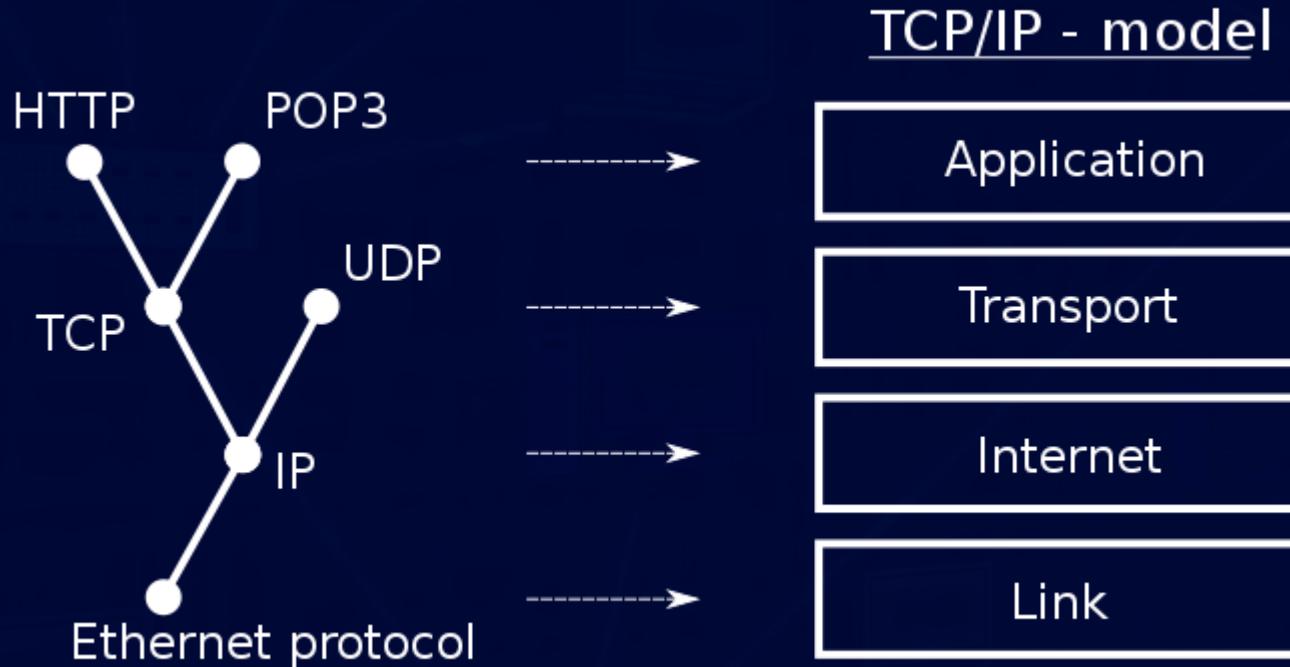


- Um **firewall** é um dispositivo de rede ou software para controlar a segurança da rede e as regras de acesso.
- Os **firewalls** são inseridos em conexões entre redes internas seguras e redes externas potencialmente inseguras, como a Internet.
- Normalmente, os **firewalls** são configurados para rejeitar solicitações de acesso de fontes não reconhecidas, permitindo ações de fontes reconhecidas.
- O papel vital que os **firewalls** desempenham na segurança da rede cresce paralelamente ao aumento constante dos **ataques cibernéticos**.

# Protocolos de Comunicação

- Um **protocolo de comunicação** é um conjunto de regras para troca de informações em uma rede.
- Em uma **protocol stack** (por exemplo: o **modelo OSI**), o protocolo é dividido em **camadas**, onde cada camada de protocolo alavanca os serviços da camada de protocolo abaixo dela até que a camada inferior controle o hardware que envia informações pela mídia.

# Protocolos de Comunicação



- Acima temos o **modelo TCP/IP** e sua relação com os protocolos comuns usados em diferentes camadas do modelo.

# Protocolos de Comunicação

- Atualmente, o uso de camadas de protocolo é omnipresente no campo das redes de computadores.
- Um exemplo importante de protocol stack é **HTTP** (o protocolo da World Wide Web) rodando sobre **TCP** sobre **IP** (os protocolos da Internet) sobre **IEEE 802.11** (o protocolo Wi-Fi).
- Esta stack é usada entre o roteador sem fio e o computador pessoal do usuário doméstico quando o usuário está navegando na web.
- Os protocolos de comunicação têm várias características. Eles podem ser **connection-oriented** ou **connectionless**, podem usar **circuit mode** ou **packet switching**, e podem usar endereçamento hierárquico ou endereçamento simples.

# Internet Protocol Suite

- O Internet Protocol Suite, também chamado de TCP/IP, é a base de todas as redes modernas.
- Ele oferece serviços connection-less e connection-oriented em uma rede inherentemente não confiável, atravessada por transmissão de datagrama no nível do Internet protocol (IP).
- Em seu núcleo, o conjunto de protocolos define as especificações de endereçamento, identificação e roteamento para o Internet Protocol Version 4 (IPv4) e para o IPv6, a próxima geração do protocolo com uma capacidade de endereçamento muito maior.
- O Internet Protocol Suite é o conjunto definidor de protocolos para a Internet. Embora muitos computadores se comuniquem pela Internet, na verdade ela é uma rede de redes, conforme elaborado por Andrew Tannenbaum.

# O Protocolo TCP

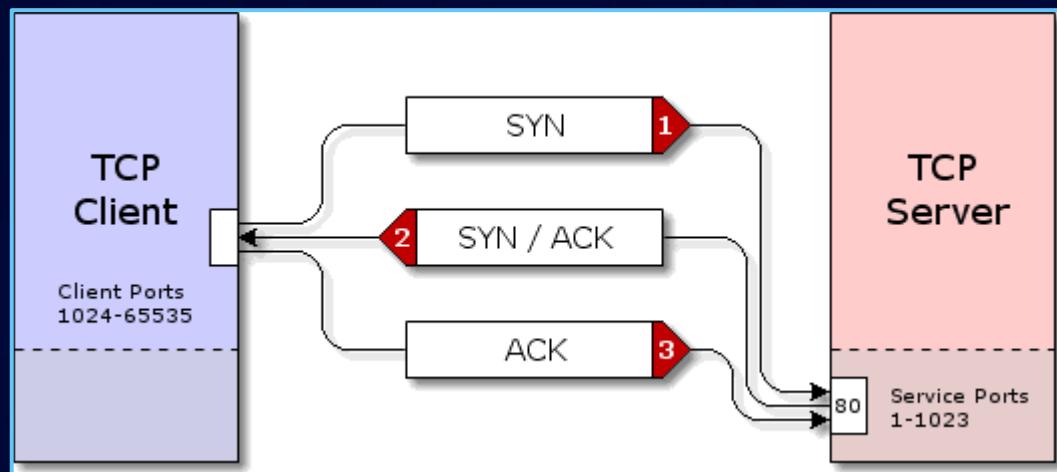
- **Transmission Control Protocol (TCP)**: É um dos principais protocolos do conjunto de protocolos da Internet.
- O TCP fornece entrega confiável, ordenada e com verificação de erros de um fluxo de octetos (bytes) entre aplicações em execução em hosts que se comunicam por meio de uma rede IP.
- As principais aplicações da Internet, como a World Wide Web, e-mail, administração remota e transferência de arquivos, dependem do TCP, que faz parte da **camada de transporte** do conjunto TCP/IP.
- **SSL/TLS** geralmente é executado em cima do TCP.

# O Protocolo TCP

- O TCP é **connection-oriented** e uma conexão entre o **cliente** e o **servidor** é estabelecida antes que os dados possam ser enviados.
- O servidor deve estar ouvindo (passive open) para solicitações de conexão de clientes antes que uma conexão seja estabelecida.
- O **three-way handshake** (active open), a retransmissão e a detecção de erros aumentam a confiabilidade, mas aumentam a latência.
- Aplicações que não exigem um serviço de fluxo de dados confiável podem usar o **User Datagram Protocol (UDP)**, que fornece um serviço de datagrama **connectionless** que prioriza o tempo em relação à confiabilidade.

# TCP Handshake

- O TCP usa um three-way handshake para estabelecer uma conexão confiável. A conexão é full duplex e ambos os lados sincronizam (SYN) e reconhecem (ACK) um ao outro.
- A troca desses quatro sinalizadores é realizada em três etapas: SYN, SYN-ACK e ACK, apresentadas na figura abaixo:



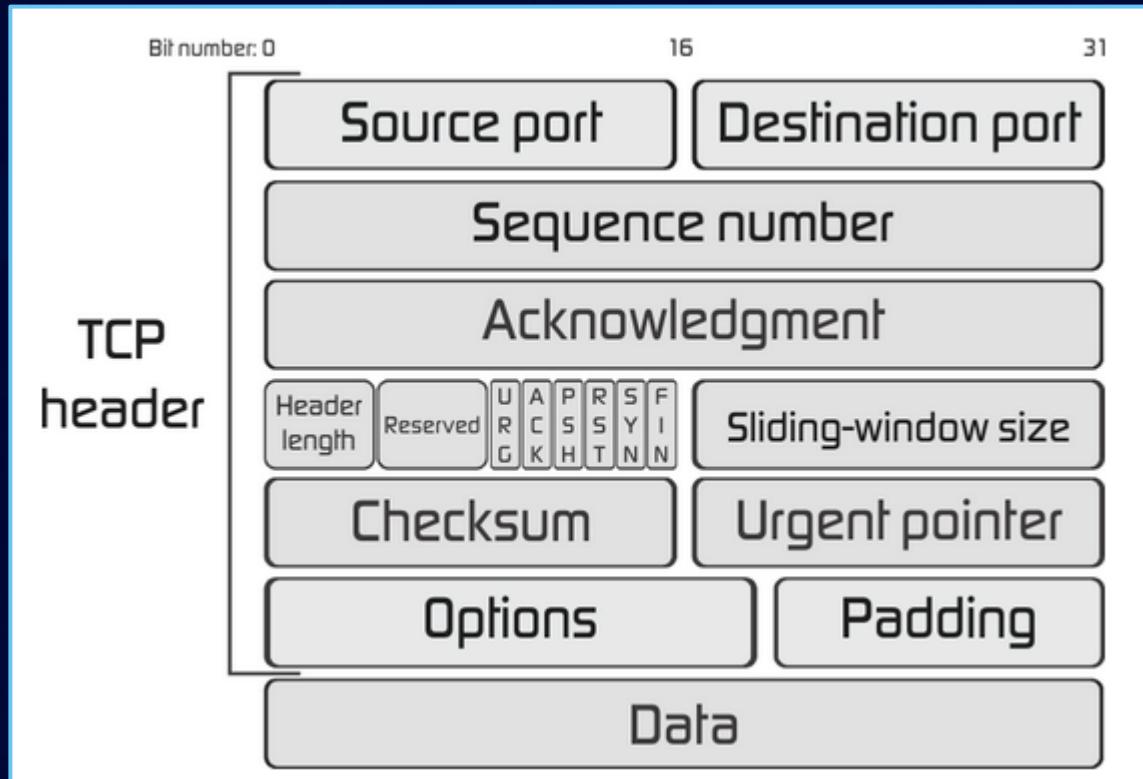
# TCP Handshake

- 1 (SYN): Na primeira etapa, o cliente deseja estabelecer uma conexão com o servidor, então envia um segmento com SYN (Sincronizar número de sequência) que informa ao servidor que o cliente provavelmente iniciará a comunicação e com qual número de sequência iniciará os segmentos com.
- 2 (SYN + ACK): O servidor responde à solicitação do cliente com bits de sinal SYN-ACK definidos. Reconhecimento (ACK) significa a resposta do segmento recebido e SYN significa com qual número de sequência é provável que os segmentos sejam iniciados.
- 3 (ACK): Na parte final, o cliente reconhece a resposta do servidor e ambos estabelecem uma conexão confiável com a qual iniciarão a transferência de dados real.
- As etapas 1 e 2 estabelecem o parâmetro de conexão (número de sequência) para uma direção e é confirmado. As etapas 2, 3 estabelecem o parâmetro de conexão (número de sequência) para a outra direção e é confirmado. Com eles, uma comunicação **full-duplex** é estabelecida.

# Estrutura do Segmento TCP

- O Transmission Control Protocol aceita dados de um fluxo de dados, divide-os em blocos e adiciona um **TCP header** criando um **segmento TCP**.
- O segmento TCP é então encapsulado em um datagrama do Internet Protocol (IP) e trocado com os pares.
- Um segmento TCP consiste em um **header** de segmento e uma **seção de dados**. O header do segmento contém 10 campos obrigatórios e um campo de extensão opcional (Options).
- A seção de dados segue o header e são os dados de *payload* transportados para o aplicação.

# Estrutura do Segmento TCP



[https://en.wikipedia.org/wiki/Transmission\\_Control\\_Protocol#TCP\\_segment\\_structure](https://en.wikipedia.org/wiki/Transmission_Control_Protocol#TCP_segment_structure)

# Internet Protocol (IP)

- O Internet Protocol (IP) é o principal protocolo de comunicação no conjunto de protocolos da Internet para retransmissão de datagramas através dos limites da rede.
- Sua função de roteamento permite a internetworking e, essencialmente, estabelece a Internet.
- O IP tem a tarefa de entregar pacotes do host de origem ao host de destino, exclusivamente com base nos endereços IP nos headers dos pacotes.
- Para isso, o IP define estruturas de pacotes que encapsulam os dados a serem entregues.
- Ele também define métodos de endereçamento que são usados para rotular o datagrama com informações de origem e destino.

# Internet Protocol (IP)

- Historicamente, o IP era o serviço de datagrama **connectionless** no **Transmission Control Program** original introduzido por Vint Cerf e Bob Kahn em 1974, que foi complementado por um serviço **connection-oriented** que se tornou a base para o Transmission Control Protocol (TCP).
- O conjunto de protocolos da Internet é, portanto, frequentemente referido como **TCP/IP**.
- A primeira versão principal do IP, **Internet Protocol Version 4 (IPv4)**, é o protocolo dominante da Internet. Seu sucessor é o **Internet Protocol versão 6 (IPv6)**, que tem aumentado sua implantação na Internet pública desde 2006.

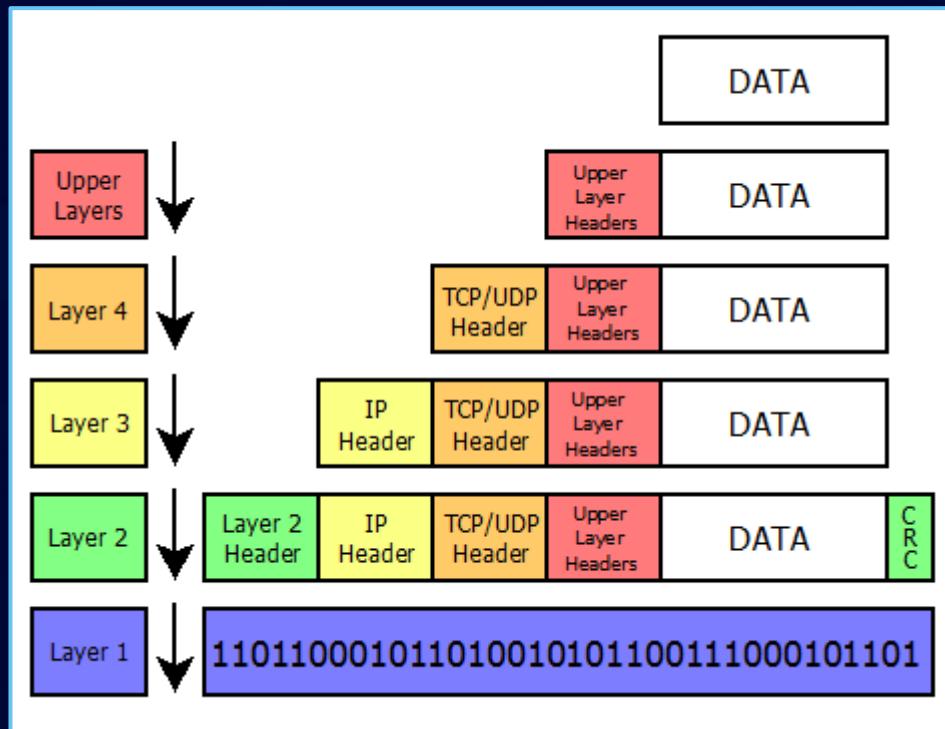
# Função do Internet Protocol

- O Internet Protocol é responsável por endereçar interfaces de host, **encapsular** dados em datagramas (incluindo **fragmentação** e **remontagem**) e rotear datagramas de uma interface de host de origem para uma interface de host de destino em uma ou mais redes IP.
- Para esses fins, o protocolo da Internet define o formato dos pacotes e fornece um sistema de endereçamento.
- Cada datagrama possui dois componentes: um **header** e um **payload**.
- O IP header inclui o endereço IP de origem, o endereço IP de destino e outros metadados necessários para rotear e entregar o datagrama.
- O payload são os dados transportados. Este método de aninhar o payload de dados em um pacote com um header é chamado de **encapsulamento**.

# Função do Internet Protocol

- O endereçamento IP envolve a atribuição de endereços IP e parâmetros associados às interfaces do host.
- O espaço de endereço é dividido em sub-redes, envolvendo a designação de prefixos de rede.
- O roteamento IP é executado por todos os hosts, bem como roteadores, cuja função principal é transportar pacotes através dos limites da rede.
- Os roteadores se comunicam entre si por meio de protocolos de roteamento especialmente projetados.

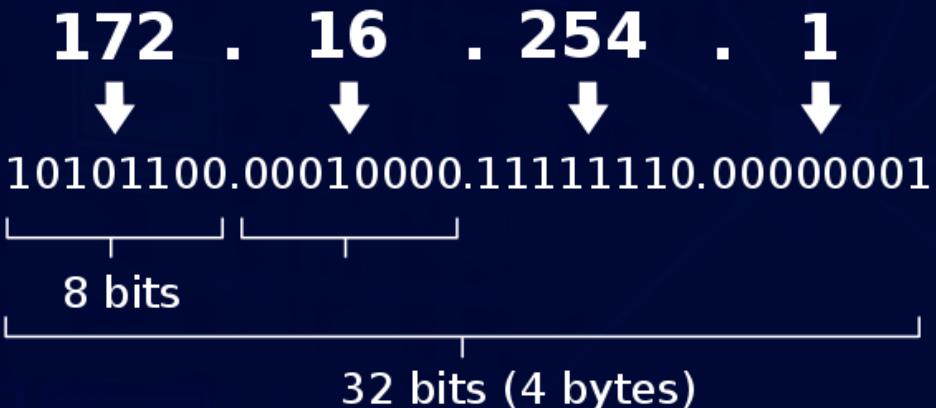
# Encapsulamento



Conforme o pacote viaja pela stack de protocolos TCP/IP, os protocolos em cada camada adicionam ou removem campos do header básico. Quando um protocolo no host de envio adiciona dados ao cabeçalho do pacote, o processo é chamado de **encapsulamento** de dados.

# Endereço IP

## IPv4 address in dotted-decimal notation



- Um endereço de Internet Protocol (endereço IP) é uma etiqueta numérica atribuída a cada dispositivo conectado a uma rede de computadores que usa o protocolo da Internet para comunicação.
  - Um endereço IP tem duas funções principais: identificação de host ou interface de rede e endereçamento de localização.

# Endereço IP

- O Internet Protocol version 4 (IPv4) define um endereço IP como um número de 32 bits.
- No entanto, devido ao crescimento da Internet e ao esgotamento dos endereços IPv4 disponíveis, uma nova versão do IP (IPv6), usando 128 bits para o endereço IP, foi padronizada em 1998.
- Os endereços IP são gravados e exibidos em notações legíveis por humanos, como 172.16.254.1 no IPv4 e 2001:db8:0:1234:0:567:8:1 no IPv6.
- O tamanho do prefixo de roteamento do endereço é designado em notação CIDR sufixando o endereço com o número de bits significativos, por exemplo, 192.168.1.15/24, que é equivalente à máscara de sub-rede usada historicamente 255.255.255.0.
- Os administradores de rede atribuem um endereço IP a cada dispositivo conectado a uma rede. Essas atribuições podem ser estáticas (fixas ou permanentes) ou dinâmicas, dependendo das práticas da rede e dos recursos do software.

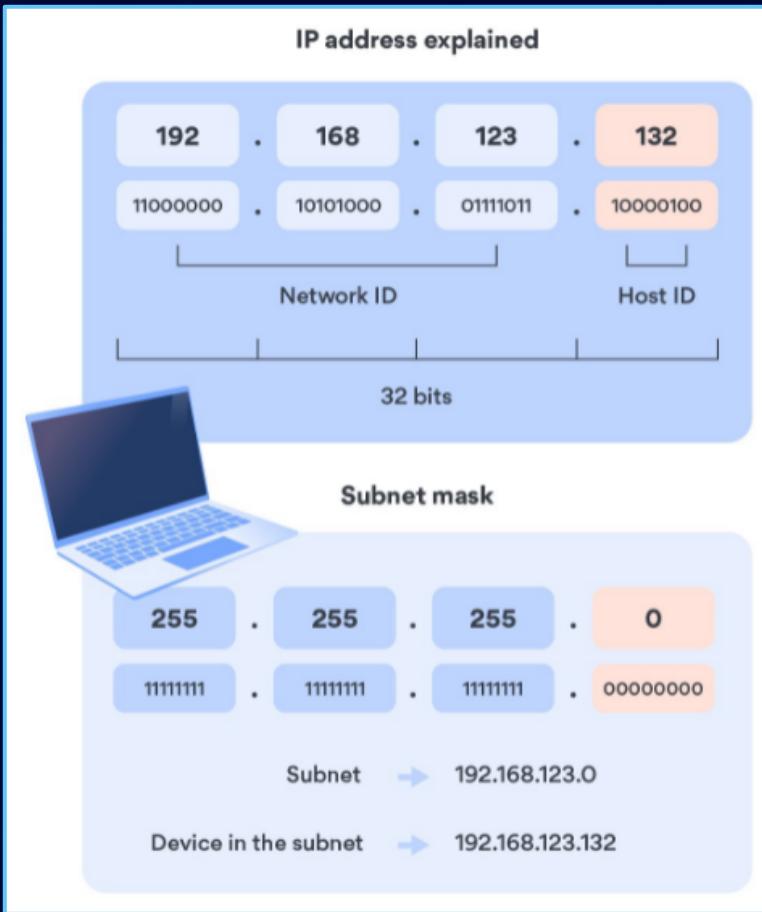
# Sub-redes

- As redes IP podem ser divididas em sub-redes em IPv4 e IPv6.
- Para este propósito, um endereço IP é reconhecido como consistindo em duas partes: o prefixo de rede nos bits de ordem superior e os bits restantes chamados de **rest field**, **identificador de host** ou **identificador de interface** (IPv6), usado para numeração de host em uma rede .
- A **máscara de sub-rede** ou notação CIDR determina como o endereço IP é dividido em partes de rede e host.

# Máscara de Sub-rede

- O termo máscara de sub-rede é usado apenas no IPv4.
- Ambas as versões de IP, entretanto, usam o conceito e a notação CIDR.
- Nele, o endereço IP é seguido por uma barra e o número (em decimal) dos bits usados para a parte da rede, também chamado de prefixo de roteamento.
- Por exemplo, um endereço IPv4 e sua máscara de sub-rede podem ser 192.0.2.1 e 255.255.255.0, respectivamente. A notação CIDR para o mesmo endereço IP e sub-rede é 192.0.2.1/24, porque os primeiros 24 bits do endereço IP indicam a rede e a sub-rede.

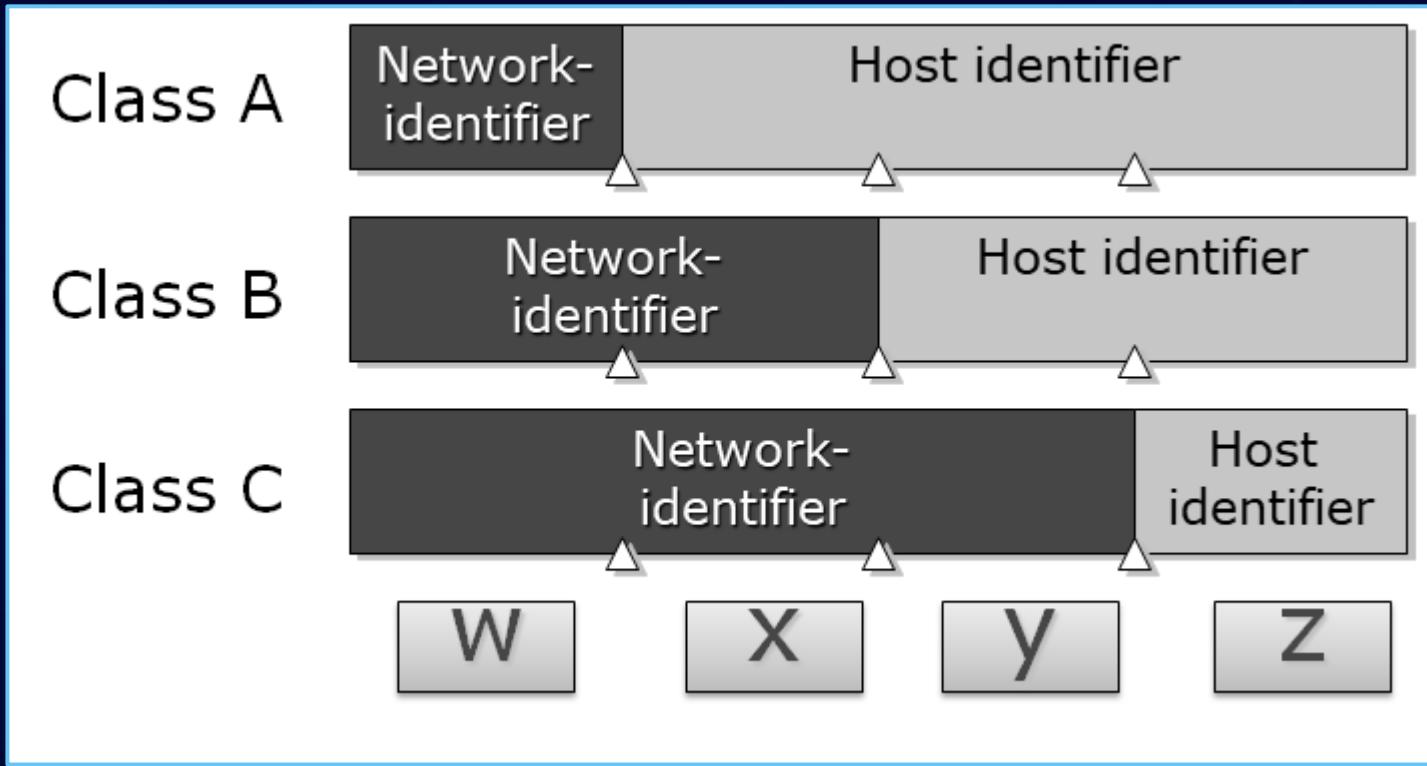
# Máscara de Sub-rede



# Classes de Rede

- Os endereços da Internet são alocados pelo InterNIC, a organização que administra a Internet. Esses endereços IP são divididos em classes.
- Os mais comuns são as classes A, B e C.
- As classes D e E existem, mas não são usadas pelos usuários finais.
- Cada uma das classes de endereço possui uma máscara de sub-rede padrão diferente.
- Você pode identificar a classe de um endereço IP observando seu primeiro octeto.

# Classes de Rede



# Classe A

- As redes Classe A usam uma máscara de sub-rede padrão de 255.0.0.0 e têm 0-127 como seu primeiro octeto. O endereço 10.52.36.11 é um endereço de classe A. Seu primeiro octeto é 10, que está entre 1 e 126, inclusive.

# Classe B

- As redes Classe B usam uma máscara de sub-rede padrão de 255.255.0.0 e têm 128-191 como seu primeiro octeto. O endereço 172.16.52.63 é um endereço de classe B. Seu primeiro octeto é 172, que está entre 128 e 191, inclusive.

# Classe C

- Redes de classe C usam uma máscara de sub-rede padrão de 255.255.255.0 e têm 192-223 como seu primeiro octeto. O endereço 192.168.123.132 é um endereço de classe C. Seu primeiro octeto é 192, que está entre 192 e 223, inclusive.

# Subnetting

- Uma rede TCP/IP Classe A, B ou C pode ser dividida posteriormente, ou “subnetted”, por um administrador de sistemas.
- Isso se torna necessário à medida que você reconcilia o esquema de endereço lógico da Internet (o mundo abstrato de endereços IP e sub-redes) com as redes físicas em uso pelo mundo real.
- Um administrador de sistema que está alocado a um bloco de endereços IP pode estar administrando redes que não estão organizadas de uma forma que se ajuste facilmente a esses endereços.

# Subnetting

- Por exemplo, você tem uma **wide area network** com 150 hosts em três redes (em cidades diferentes) que são conectadas por um roteador TCP/IP.
- Cada uma dessas três redes possui 50 hosts. Você está alocado na rede de classe C **192.168.123.0**. (Para ilustração, este endereço é, na verdade, de um intervalo que não está alocado na Internet.)
- Isso significa que você pode usar os endereços **192.168.123.1** a **192.168.123.254** para seus **150 hosts**.

# Subnetting

- Dois endereços que não podem ser usados em seu exemplo são **192.168.123.0** e **192.168.123.255** porque os endereços binários com uma parte do host de todos os zeros e uns são inválidos.
- O endereço zero é inválido porque é usado para especificar uma rede sem especificar um host.
- O endereço 255 (em notação binária, um endereço de host de todos uns) é usado para transmitir uma mensagem a cada host em uma rede (broadcast).
- Lembre-se de que o primeiro e o último endereço em qualquer rede ou sub-rede não podem ser atribuídos a nenhum host individual.

# Subnetting

- Agora você deve ser capaz de fornecer endereços IP a 254 hosts.
- Funciona bem se todos os 150 computadores estiverem em uma única rede.
- No entanto, seus 150 computadores estão em três redes físicas separadas.
- Em vez de solicitar mais blocos de endereço para cada rede, você divide sua rede em sub-redes que permitem usar um bloco de endereços em várias redes físicas.
- Nesse caso, você divide sua rede em quatro sub-redes usando uma máscara de sub-rede que torna o endereço de rede maior e o intervalo possível de endereços de host menor.

# Subnetting

- Em outras palavras, você está 'pegando emprestado' alguns dos bits usados para o endereço do host e os está usando para a parte da rede do endereço.
- A máscara de sub-rede 255.255.255.192 oferece quatro redes de 62 hosts cada. Funciona porque na notação binária, 255.255.255.192 é o mesmo que 1111111.1111111.1111111.1100000.
- Os primeiros dois dígitos do último octeto tornam-se endereços de rede, então você obtém as redes adicionais 0000000 (0), 01000000 (64), 10000000 (128) e 11000000 (192).
- Alguns administradores usarão apenas duas das sub-redes usando 255.255.255.192 como máscara de sub-rede.
- Para obter mais informações sobre este tópico, consulte [RFC 1878](#).

# Subnetting

- Nessas quatro redes, os últimos seis dígitos binários podem ser usados para endereços de host.
- Usando uma máscara de sub-rede de 255.255.255.192, sua rede 192.168.123.0 então se torna as quatro redes 192.168.123.0, 192.168.123.64, 192.168.123.128 e 192.168.123.192.
- Essas quatro redes teriam como endereços de host válidos:  
192.168.123.1-62      192.168.123.65-126      192.168.123.129-190  
192.168.123.193-254.
- Lembre-se, novamente, de que os endereços de host binários com apenas uns ou zeros são inválidos, portanto, você não pode usar endereços com o último octeto de 0, 63, 64, 127, 128, 191, 192 ou 255.

# Subnetting

Mais detalhes em:

<https://www.dnsstuff.com/subnet-ip-subnetting-guide>

<https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

<http://jodies.de/ipcalc>

- Você pode ver como funciona observando dois endereços de host, 192.168.123.71 e 192.168.123.133.
- Se você usou a máscara de sub-rede Classe C padrão de 255.255.255.0, ambos os endereços estão na rede 192.168.123.0.
- Entretanto, se você usar a máscara de sub-rede 255.255.255.192, eles estarão em redes diferentes; 192.168.123.71 está na rede 192.168.123.64, 192.168.123.133 está na rede 192.168.123.128.

# Default Gateways

- Se um computador TCP/IP precisar se comunicar com um host em outra rede, ele geralmente se comunicará por meio de um dispositivo chamado **roteador**.
- Em termos de TCP/IP, um roteador especificado em um host, que vincula a sub-rede do host a outras redes, é chamado de **default gateway**.
- Quando um host tenta se comunicar com outro dispositivo usando TCP/IP, ele executa um processo de comparação usando a máscara de sub-rede definida e o endereço IP de destino versus a máscara de sub-rede e seu próprio endereço IP.

# Default Gateways

- O resultado dessa comparação informa ao computador se o destino é um host local ou remoto.
- Se o resultado desse processo determinar que o destino é um host local, o computador enviará o pacote na sub-rede local.
- Se o resultado da comparação determinar que o destino é um host remoto, o computador encaminhará o pacote para o default gateway definido em suas propriedades TCP/IP.
- É então responsabilidade do roteador encaminhar o pacote para a sub-rede correta.

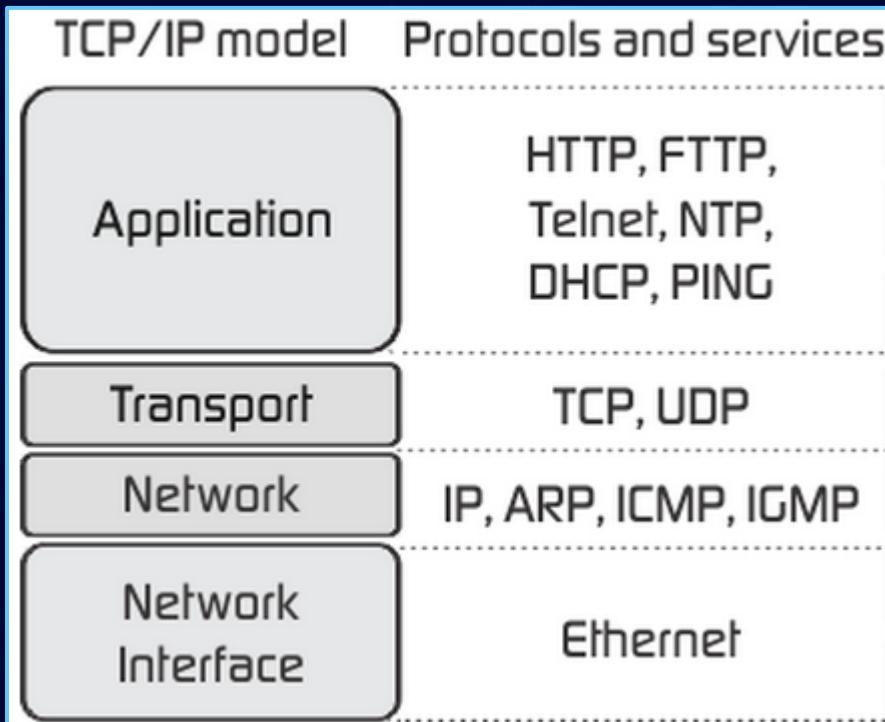
# O Modelo TCP/IP

- O Internet protocol suite é o modelo conceitual e o conjunto de protocolos de comunicação usados na Internet e em redes de computadores semelhantes.
- É comumente conhecido como TCP/IP porque os protocolos básicos do conjunto são o Transmission Control Protocol (TCP) e o Internet Protocol (IP).
- Durante seu desenvolvimento, as versões dele eram conhecidas como o modelo do Department of Defense (DoD) porque o desenvolvimento do método de rede foi financiado pelo Departamento de Defesa dos Estados Unidos por meio da DARPA.
- Sua implementação é uma protocol stack.

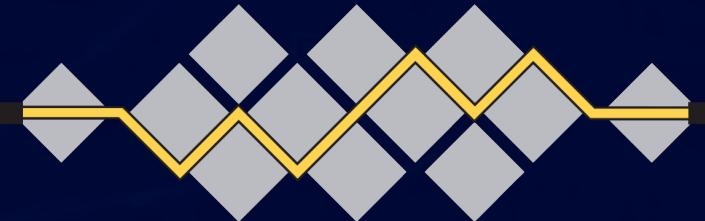
# O Modelo TCP/IP

- O **Internet protocol suite** fornece comunicação de dados ponta a ponta (end-to-end), especificando como os dados devem ser empacotados, endereçados, transmitidos, roteados e recebidos.
- Essa funcionalidade é organizada em quatro **camadas de abstração**, que classificam todos os protocolos relacionados de acordo com o escopo da rede envolvida.
- Do mais baixo ao mais alto, as camadas são a **camada de enlace**, contendo métodos de comunicação para dados que permanecem em um único segmento de rede (enlace); a **camada de internet**, fornecendo internetworking entre redes independentes; a **camada de transporte**, lidando com a comunicação host-a-host; e a **camada de aplicação**, fornecendo troca de dados processo a processo para aplicações.

# O Modelo TCP/IP



# O Modelo TCP/IP



I E T F®

- Os padrões técnicos subjacentes ao conjunto de protocolos da Internet e seus protocolos constituintes são mantidos pela Internet Engineering Task Force (IETF).
- O Internet protocol suite é anterior ao modelo OSI, uma estrutura de referência mais abrangente para sistemas de rede em geral.

# Princípios Arquitetônicos TCP/IP

- O princípio de ponta a ponta evoluiu ao longo do tempo. Sua expressão original colocava a manutenção do estado e da inteligência geral nas edges, e pressupunha que a Internet que conectava as edges não retinha nenhum estado e se concentrava na velocidade e na simplicidade.
- As necessidades reais de firewalls, tradutores de endereço de rede, caches de conteúdo da web e similares forçaram mudanças neste princípio.
- O princípio de robustez declara: "Em geral, uma implementação deve ser conservadora em seu comportamento de envio e liberal em seu comportamento de recebimento.
- Ou seja, deve-se ter o cuidado de enviar datagramas bem formados, mas deve-se aceitar qualquer datagrama que possa interpretar (por exemplo, não se opor a erros técnicos onde o significado ainda é claro)."

# Princípios Arquitetônicos TCP/IP

- "A segunda parte do princípio é quase tão importante: o software em outros hosts pode conter deficiências que tornam imprudente explorar recursos de protocolo legais, mas obscuros."
- O **encapsulamento** é usado para fornecer abstração de protocolos e serviços. O encapsulamento é geralmente alinhado com a divisão do conjunto de protocolos em camadas de funcionalidade geral.
- Em geral, uma aplicação (o nível mais alto do modelo) usa um conjunto de protocolos para enviar seus dados pelas camadas. Os dados são posteriormente encapsulados em cada nível.
- Um dos primeiros documentos arquitetônicos, **RFC 1122**, enfatiza os princípios arquitetônicos sobre as camadas. **RFC 1122**, intitulado **Host Requirements**, é estruturado em parágrafos que se referem a camadas. Ele define vagamente um modelo de **quatro camadas**, com as camadas tendo nomes, não números.

# Camada de Aplicação

- A camada de aplicação é o escopo dentro do qual aplicações, ou processos, criam dados do usuário e comunicam esses dados a outras aplicações em outro ou no mesmo host.
- As aplicações fazem uso dos serviços fornecidos pelas camadas inferiores subjacentes, especialmente a camada de transporte, que fornece canais confiáveis ou não confiáveis para outros processos.
- Os parceiros de comunicação são caracterizados pela arquitetura da aplicação, como o modelo cliente-servidor e rede ponto a ponto (**peer-to-peer**).
- Esta é a camada em que operam todos os protocolos de aplicação, como **SMTP, FTP, SSH, HTTP**.
- Os processos são endereçados por meio de portas que representam essencialmente serviços.

# Camada de Transporte

- A camada de transporte realiza comunicações host-a-host na rede local ou em redes remotas separadas por roteadores.
- Ele fornece um canal para as necessidades de comunicação das aplicações. UDP é o protocolo básico da camada de transporte, fornecendo um serviço de datagrama sem conexão confiável.
- O Transmission Control Protocol (TCP) fornece controle de fluxo, estabelecimento de conexão e transmissão confiável de dados.

# Camada de Internet

- A camada da Internet troca datagramas através dos limites da rede.
- Ele fornece uma interface de rede uniforme que oculta a topologia (layout) real das conexões de rede subjacentes.
- Portanto, é também a camada que estabelece a internetworking. Na verdade, ele define e estabelece a Internet.
- Essa camada define as estruturas de **endereçamento** e **roteamento** usadas para o conjunto de protocolos TCP/IP.
- O protocolo principal neste escopo é o **Internet Protocol**, que define os endereços IP. Sua função no roteamento é transportar datagramas para o próximo host, funcionando como um roteador IP, que possui a conectividade com uma rede mais próxima do destino final dos dados.

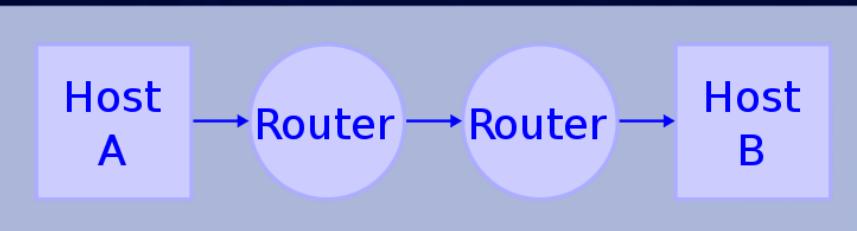
# Camada de Enlace

- Também chamada de **camada de link**, ela define os métodos de rede dentro do escopo do link de rede local em que os hosts se comunicam sem roteadores intervenientes.
- Essa camada inclui os protocolos usados para descrever a topologia da rede local e as interfaces necessárias para afetar a transmissão dos datagramas da camada da Internet para os hosts vizinhos do próximo.

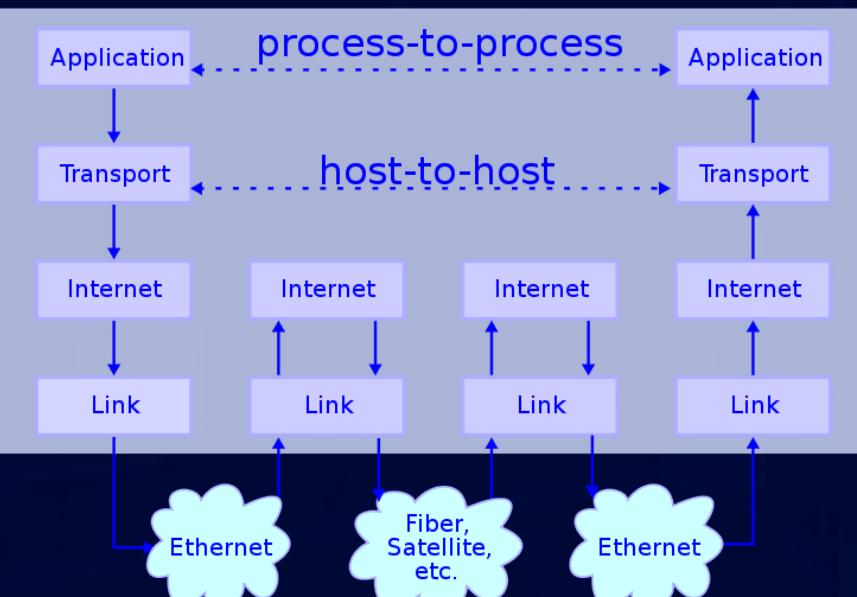
# Fluxo de Dados

Fluxo de dados conceituais em uma topologia de rede simples de dois hosts (A e B) conectados por um link entre seus respectivos roteadores.

## Network Topology



## Data Flow

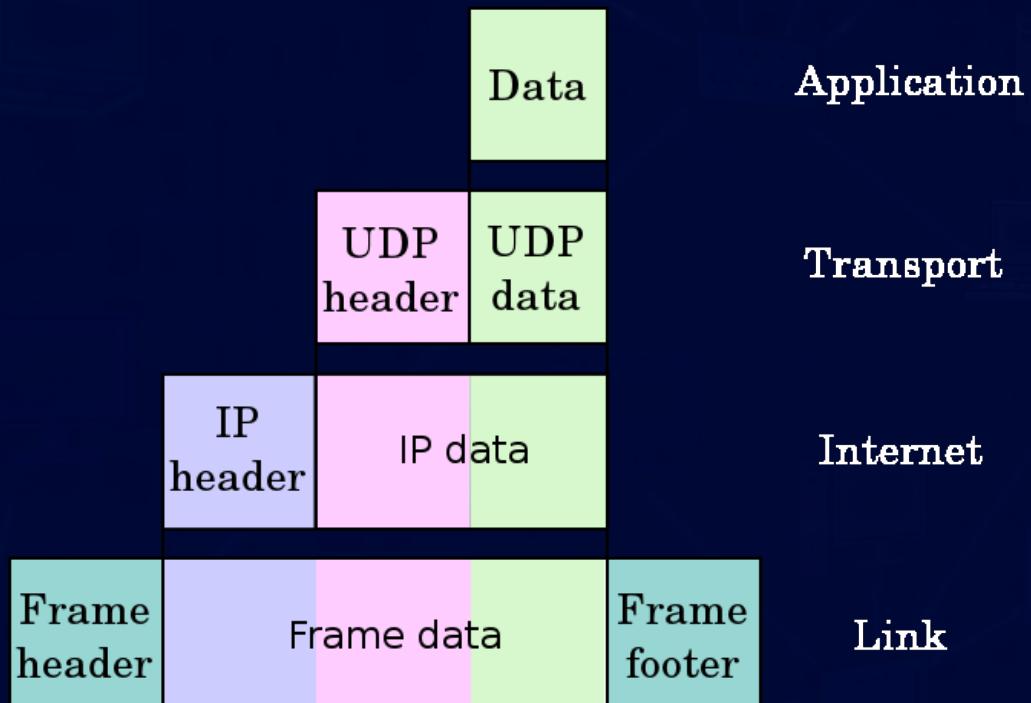


# Fluxo de Dados

- A aplicação em cada host executa operações de leitura e gravação como se os processos estivessem diretamente conectados entre si por algum tipo de canal de dados.
- Após o estabelecimento desse canal, a maioria dos detalhes da comunicação são ocultados de cada processo, pois os princípios básicos de comunicação são implementados nas camadas inferiores do protocolo.
- Por analogia, na **camada de transporte** a comunicação aparece como host-a-host, sem conhecimento das estruturas de dados da aplicação e dos roteadores de conexão, enquanto na **camada de internetworking**, os limites de rede individuais são atravessados em cada roteador.

# Encapsulamento UDP

Nesta figura temos o encapsulamento de dados de aplicativos descendentes através das camadas descritas no RFC 1122.

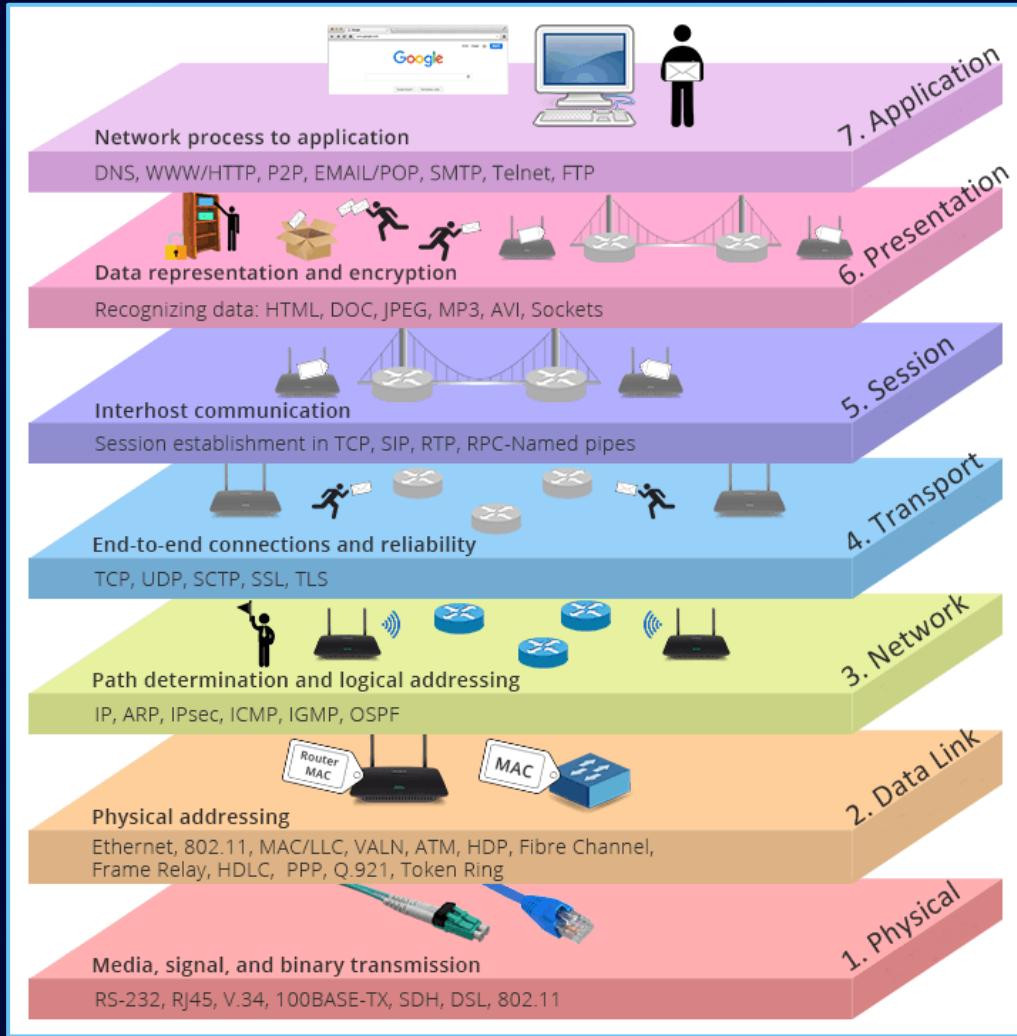


# Modelo OSI

- O Open Systems Interconnection model (modelo OSI) é um modelo conceitual que caracteriza e padroniza as funções de comunicação de um sistema de telecomunicações ou computação sem levar em conta sua estrutura interna e tecnologia subjacentes.
- Seu objetivo é a interoperabilidade de diversos sistemas de comunicação com protocolos de comunicação padrão.
- O modelo partitiona o fluxo de dados em um sistema de comunicação em sete camadas de abstração, desde a implementação física de transmissão de bits em um meio de comunicação até a representação de dados de mais alto nível de uma aplicação distribuído.

# Modelo OSI

A figura ao lado mostra as sete camadas do modelo OSI



# Modelo OSI

- Cada camada intermediária fornece uma classe de funcionalidade para a camada acima dela e é atendida pela camada abaixo dela.
- As classes de funcionalidade são realizadas no software por protocolos de comunicação padronizados.
- O modelo OSI pode ser visto como uma linguagem universal para redes de computadores.
- A seguir vamos definir as setes camadas de abstração do modelo OSI.

# 7. Camada de Aplicação



- Essa é a única camada que interage diretamente com os dados do usuário.
- Os softwares aplicativos, como navegadores web e clientes de e-mail, dependem da camada de aplicação para iniciar as comunicações.
- Mas é preciso deixar claro que os softwares aplicativos clientes não fazem parte da camada de aplicação, que, na verdade, é responsável pelos protocolos e manipulação de dados dos quais o software depende para apresentar dados significativos ao usuário.
- Os protocolos da camada de aplicação incluem o **HTTP** e o **SMTP** (Simple Mail Transfer Protocol, um dos protocolos que permite a comunicação por e-mail).

# 6. Camada de Apresentação



- Essa camada é a principal responsável pela **preparação** dos dados para que possam ser usados pela camada de aplicação; em outras palavras, a camada 6 torna os dados apresentáveis para que os aplicativos os consumam.
- A camada de apresentação é responsável pela **tradução**, **criptografia** e **compactação** dos dados.
- Dois dispositivos de comunicação que se comunicam podem usar métodos de codificação diferentes; por isso, a camada 6 é responsável pela tradução dos dados de entrada em uma sintaxe que a camada de aplicação do dispositivo receptor possa entender.

# 6. Camada de Apresentação



- Se os dispositivos se comunicarem por meio de uma conexão criptografada, a camada 6 será responsável por adicionar a criptografia na extremidade do remetente e decodificar a criptografia na extremidade do destinatário, podendo, assim, apresentar dados não criptografados e legíveis à camada de aplicação.
- Finalmente, a camada de apresentação também é responsável por compactar os dados recebidos da camada de aplicação antes de entregá-los à camada 5. Isso ajuda a aumentar a velocidade e a eficiência da comunicação ao minimizar a quantidade de dados que serão transferidos.

# 5. Camada de Sessão



- Essa é a camada responsável pela abertura e fechamento da comunicação entre os dois dispositivos.
- O tempo decorrido entre o momento em que a comunicação é aberta e fechada é conhecido como "**sessão**".
- A camada de sessão garante que a sessão permaneça aberta pelo tempo necessário para transferir todos os dados que estão sendo trocados e, em seguida, fecha imediatamente a sessão para evitar o desperdício de recursos.

# 5. Camada de Sessão



- A camada de sessão também sincroniza a transferência de dados com pontos de verificação. Por exemplo, se um arquivo de 100 megabytes estiver sendo transferido, a camada de sessão poderá definir um ponto de verificação a cada 5 megabytes.
- No caso de uma desconexão ou falha após a transferência de 52 megabytes, a sessão pode ser retomada a partir do último ponto de verificação, o que significa que apenas mais 50 megabytes de dados precisam ser transferidos.
- Sem os pontos de verificação, a transferência inteira teria que começar novamente do zero.

# 4. Camada de Transporte



- A camada 4 é responsável pela comunicação de ponta a ponta entre os dois dispositivos.
- Isso inclui pegar os dados da camada de sessão e dividi-los em porções chamadas segmentos antes de enviá-los para a camada 3.
- A camada de transporte no dispositivo receptor é responsável por remontar os segmentos em dados que a camada de sessão possa consumir.

# 4. Camada de Transporte



- A camada de transporte também é responsável pelo controle de **fluxo** e pelo controle de **erros**. O controle de fluxo determina uma velocidade de transmissão ideal para garantir que um remetente com uma conexão rápida não sobrecarregue um receptor com uma conexão lenta.
- A camada de transporte executa o controle de erros no lado do receptor, garantindo que os dados recebidos estejam completos e solicitando uma retransmissão caso não estejam.

# 3. Camada de Rede



- A camada de rede é responsável por facilitar a transferência de dados entre duas redes diferentes. Se os dois dispositivos que estão se comunicando estiverem na mesma rede, a camada de rede será desnecessária.
- A camada de rede divide os segmentos da camada de transporte em unidades menores denominadas pacotes no dispositivo remetente e remonta esses pacotes no dispositivo receptor.
- A camada de rede também encontra o melhor caminho físico para que os dados cheguem ao seu destino, o que é conhecido como "roteamento".

## 2. Camada de Enlace de Dados



- A camada de enlace de dados é muito semelhante à camada de rede, a não ser pelo fato de que a camada de enlace de dados facilita a transferência de dados entre dois dispositivos na mesma rede.
- A camada de enlace de dados pega os pacotes da camada de rede e os divide em pedaços menores denominados "quadros" (frames).
- Como a camada de rede, a camada de enlace de dados também é responsável pelo controle de fluxo e pelo controle de erros na comunicação intrarrede (a camada de transporte faz o controle de fluxo e o controle de erros para comunicações inter-rede).

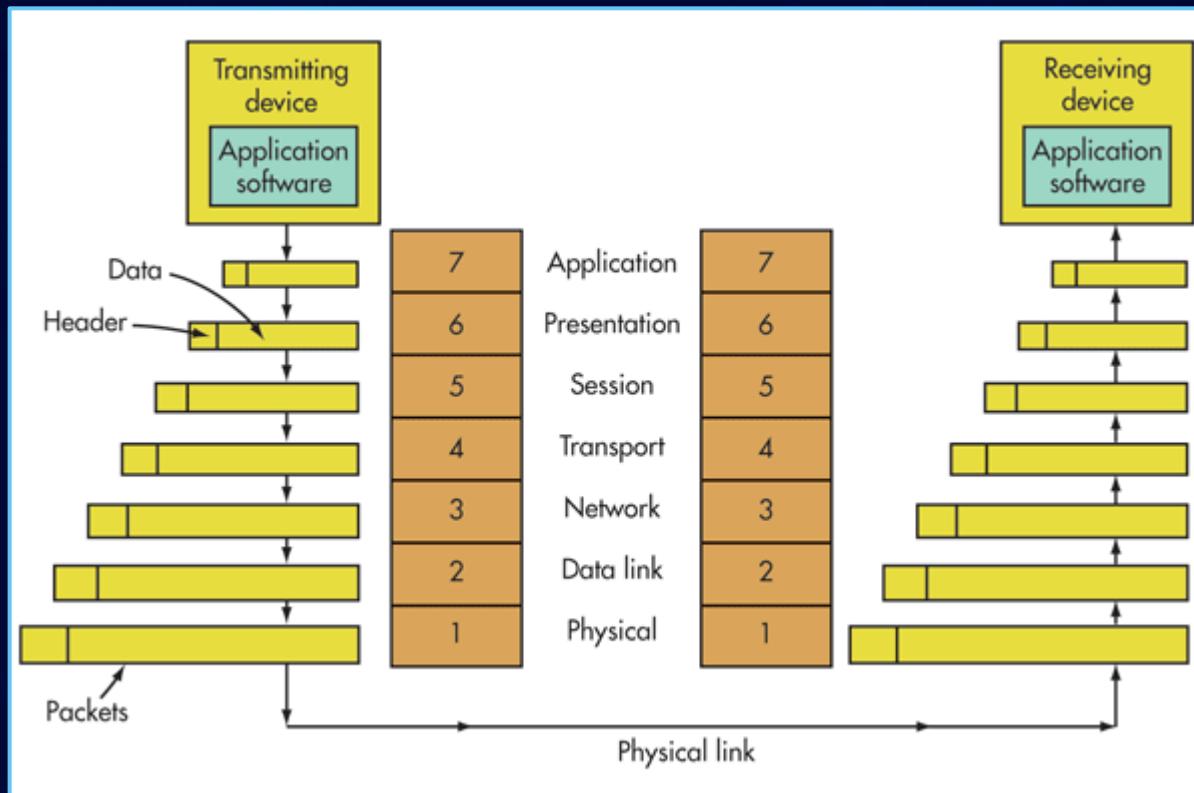
# 1. Camada Física



- Essa camada inclui o equipamento físico envolvido na transferência de dados, como cabos e comutadores.
- Essa também é a camada em que os dados são convertidos em um fluxo de bits, que é uma sequência de 1's e 0's.
- A camada física de ambos os dispositivos também precisa aceitar de comum acordo uma convenção de sinal para que se possa distinguir os 1s dos 0s em ambos os dispositivos.

# Fluxo de Dados (Modelo OSI)

Para que informações legíveis por humanos sejam transferidas por uma rede de um dispositivo para outro, os dados devem percorrer as sete camadas do modelo OSI na ordem decrescente no dispositivo que os envia e, em seguida, percorrer as sete camadas na ordem crescente na extremidade que os recebe.



# Fluxo de Dados (Modelo OSI)

- Por exemplo: Bob quer enviar um e-mail à Alice. O Bob escreve sua mensagem no aplicativo de e-mail do seu notebook e, em seguida, pressiona "enviar". Seu aplicativo de e-mail passa sua mensagem de e-mail para a camada de aplicação, que seleciona um protocolo (SMTP) e passa os dados para a camada de apresentação. A camada de apresentação compacta os dados que, em seguida, chegam à camada de sessão, que inicia a sessão de comunicação.
- Em seguida os dados chegam à camada de transporte do remetente, onde são segmentados; esses segmentos são divididos em pacotes na camada de rede e os pacotes, por sua vez, são divididos em quadros na camada de enlace de dados. A camada de enlace de dados a seguir entrega esses quadros à camada física, que converte os dados em um fluxo de bits de 1's e 0's e os envia por meio de uma mídia física, como um cabo.

# Fluxo de Dados (Modelo OSI)

- Assim que o computador da Alice recebe o fluxo de bits por meio de uma mídia física (como o seu wi-fi), os dados fluem através da mesma série de camadas em seu dispositivo, mas na ordem inversa. Primeiro, a camada física converte o fluxo de bits de 1's e 0's em quadros, que são passados para a camada de enlace de dados. A camada de enlace de dados remonta os quadros em pacotes para a camada de rede. A camada de rede cria segmentos remontando os pacotes para a camada de transporte, que remonta os segmentos em um simples dado.
- Os dados em seguida fluem para a camada de sessão do receptor, que os transmite para a camada de apresentação e em seguida encerra a sessão de comunicação. A camada de apresentação então remove a compactação e passa os dados brutos para a camada de aplicação. A camada de aplicação alimenta o software de e-mail da Alice com dados legíveis por humanos, permitindo que ela leia o e-mail do Bob na tela do seu notebook.

# Protocolos Populares

- Discutimos sobre protocolos essenciais como TCP, UDP, IP, SMTP.
- Outros protocolos populares incluem:
  - ◆ Ethernet
  - ◆ Internet Control Message Protocol ([ICMP](#))
  - ◆ Address Resolution Protocol ([ARP](#))
  - ◆ Hypertext Transfer Protocol ([HTTP](#))
  - ◆ Dynamic Host Configuration Protocol ([DHCP](#))
  - ◆ Spanning Tree Protocol ([STP](#))
  - ◆ File Transfer Protocol ([FTP](#))
  - ◆ Secure Shell ([SSH](#))
  - ◆ SSH File Transfer Protocol ([SFTP](#))

# Ethernet

- Ethernet é um protocolo feito para Local Area Networks (LAN).
- Ele foi padronizado pela primeira vez em 1983 como IEEE 802.3 e usado com o cabo coaxial único grosso 10BASE-5.
- Existem várias versões do protocolo IEEE 802.3, por exemplo, 802.3a, 802.3i, 802.3j. Cada versão é projetada para funcionar em diferentes tipos de cabos.
- Outro protocolo amplamente usado é o IEEE 802.11, que especifica a camada física e os protocolos de controle de acesso à mídia (MAC) para implementar a wireless local area network (WLAN). Este protocolo é um padrão de rede de computador sem fio e usado para permitir que laptops e smartphones se comuniquem sem estar conectados com um cabo.

# Internet Control Message Protocol

- O protocolo ICMP é feito para enviar mensagens de erro em uma rede.
- Funciona com o protocolo IP.
- Ajuda a diagnosticar problemas de comunicação de rede. O ICMP é usado principalmente para determinar se os dados estão ou não alcançando seu destino especificado da melhor maneira.
- Uma vez que este protocolo envia mensagens de erro, esses erros são determinados por um código e tipo. Uma soma de verificação especifica a precisão da mensagem, e mais informações sobre o erro serão salvas no campo de informações do header.
- Ao contrário do IP, o ICMP é um protocolo **connectionless**. Para enviar uma mensagem ICMP de um sistema para outro, não é necessário estabelecer uma conexão entre os sistemas.
- Geralmente, o ICMP é encontrado em dispositivos de rede como roteadores.

# Address Resolution Protocol

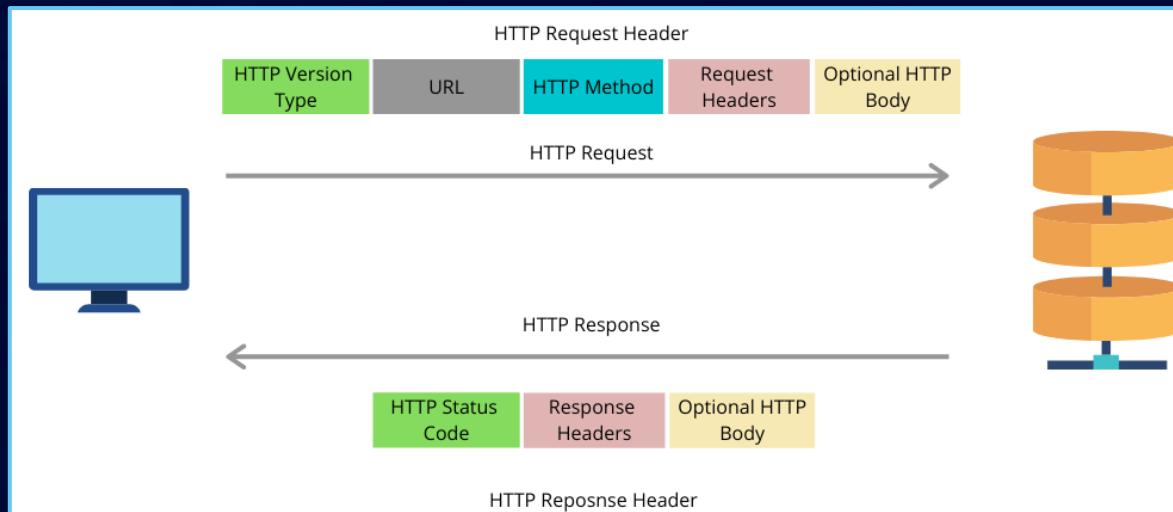
- Os aplicativos de computador usam o endereço lógico para se comunicar com outras aplicações. Mas para nos comunicarmos com outras aplicações, precisamos de um endereço físico (endereço MAC). É aqui que precisamos do **Address Resolution Protocol** (ARP).
- Ele mapeia os endereços de rede para os endereços físicos usados por um protocolo de enlace de dados. É o processo de localização do endereço de um computador em uma rede. O ARP traduz endereços da camada de rede em endereços da camada de enlace de dados do modelo de rede OSI.
- O ARP é um dos pilares mais importantes no processo de rede e é comumente usado com o **IP protocols suite**.

# Hypertext Transfer Protocol

- O Hypertext Transfer Protocol (HTTP) é a base da World Wide Web (WWW) e é usado para carregar páginas da web usando links de hipertexto.
- HTTP é um protocolo de camada de aplicação, que permite ao usuário ver uma interface amigável projetada para transferir informações entre dispositivos em rede. É o protocolo que ajuda os aplicativos a se comunicarem com os usuários.
- Um cliente da web é qualquer aplicativo de usuário, como um navegador da web. Um servidor é um sistema computacional geralmente armazenado na nuvem. Quando um cliente da web deseja se comunicar com um servidor da web por meio da WWW, ele envia uma solicitação HTTP ao servidor. Assim que o servidor recebe a solicitação, ele a processa e envia uma resposta HTTP ao cliente. O cliente recebe a resposta HTTP.

# Hypertext Transfer Protocol

- Deve-se observar que um header de solicitação HTTP não é o mesmo que um header de resposta:



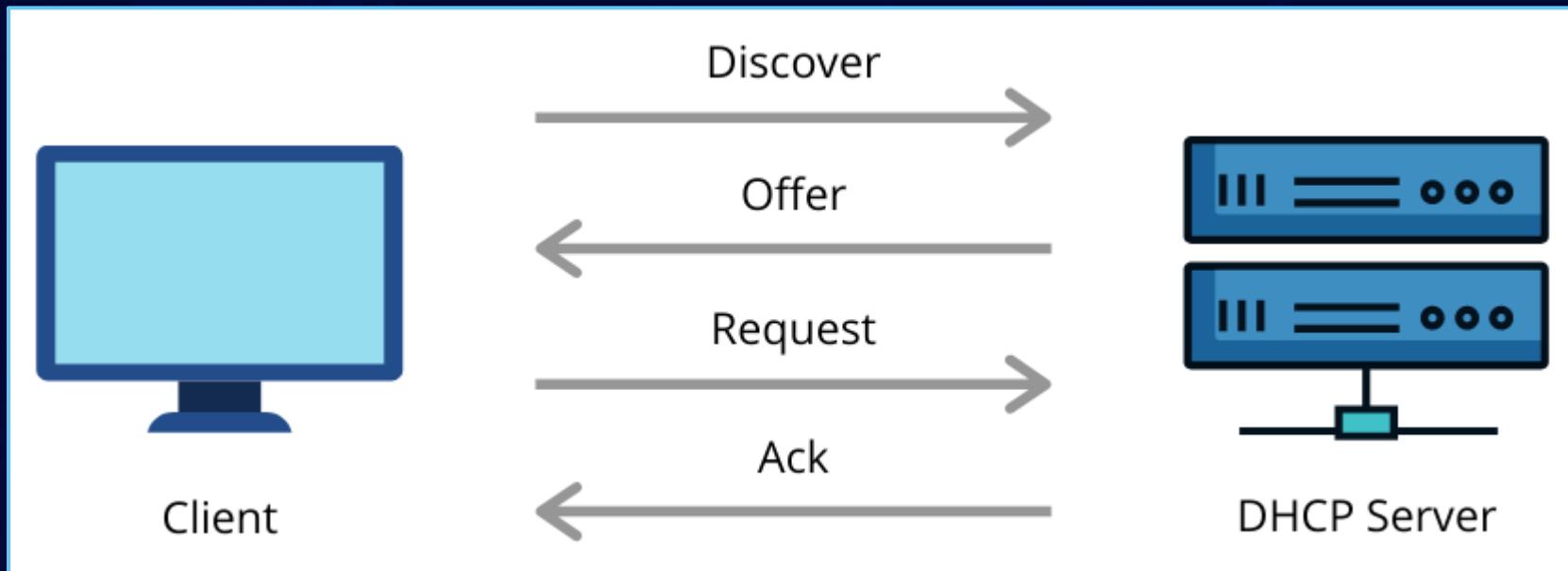
HTTP é um protocolo **connectionless** e **stateless**. Um cliente e um servidor se conhecem apenas durante a comunicação. Assim que completam a comunicação, os dois esquecem um do outro. Também é independente da mídia. Todos os dados podem ser enviados por HTTP.

# Dynamic Host Configuration Protocol

- Este protocolo funciona em redes IP, atribuindo endereços IP a dispositivos e hosts conectados à rede. Também permite que eles se comuniquem uns com os outros com eficiência.
- Além do endereço IP, o DHCP também atribui a máscara de sub-rede, o endereço do **default gateway**, o endereço do **domain name server** (DNS) e outros parâmetros de configuração pertinentes.
- Um dispositivo cliente envia mensagens de descoberta por meio de uma rede para um servidor DHCP, que envia uma oferta ao cliente.

# Dynamic Host Configuration Protocol

- O cliente então envia de volta sua solicitação, permitindo que o servidor DHCP reconheça a consulta:



# Spanning Tree Protocol

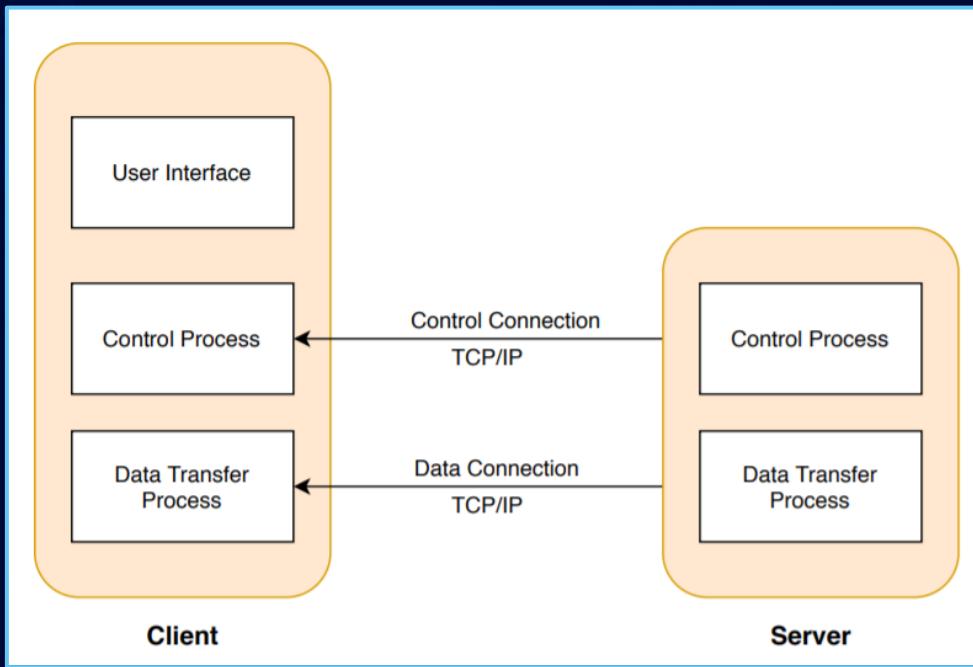
- Definido pelo IEEE 802.1d, este protocolo evita loops na LAN. O STP trata de questões relacionadas a redes com bridges. Elimina links redundantes e processa alterações e falhas na rede.
- O STP monitora todos os links da rede. Para encontrar qualquer problema presente nos links ou em um link redundante, ele aplica o spanning-tree algorithm (STA).
- O STA constrói uma topologia da rede atual e remove os links redundantes. Quando um novo link é adicionado à rede existente, o STP executa novamente o STA para garantir que o novo link não seja redundante.

# File Transfer Protocol

- O File Transfer Protocol (FTP) é um protocolo de rede padrão fornecido pelo TCP/IP e é usado para transferir arquivos de um servidor para outro.
- É responsável pela transferência **confiável** e **eficiente** de arquivos.
- Transferir um arquivo de um servidor para outro é simples, mas podem surgir vários problemas. O sistema emissor e o servidor receptor podem ter convenções de arquivo diferentes ou maneiras diferentes de representar os dados.
- Em alguns casos, as estruturas de diretório de dois sistemas podem ser diferentes uma da outra. O FTP resolve todos esses problemas.

# File Transfer Protocol

- Ao transferir um arquivo entre dois sistemas, ele estabelece duas conexões. Uma conexão é para a **transferência de dados** e a outra é para a conexão de **controle**:



# File Transfer Protocol

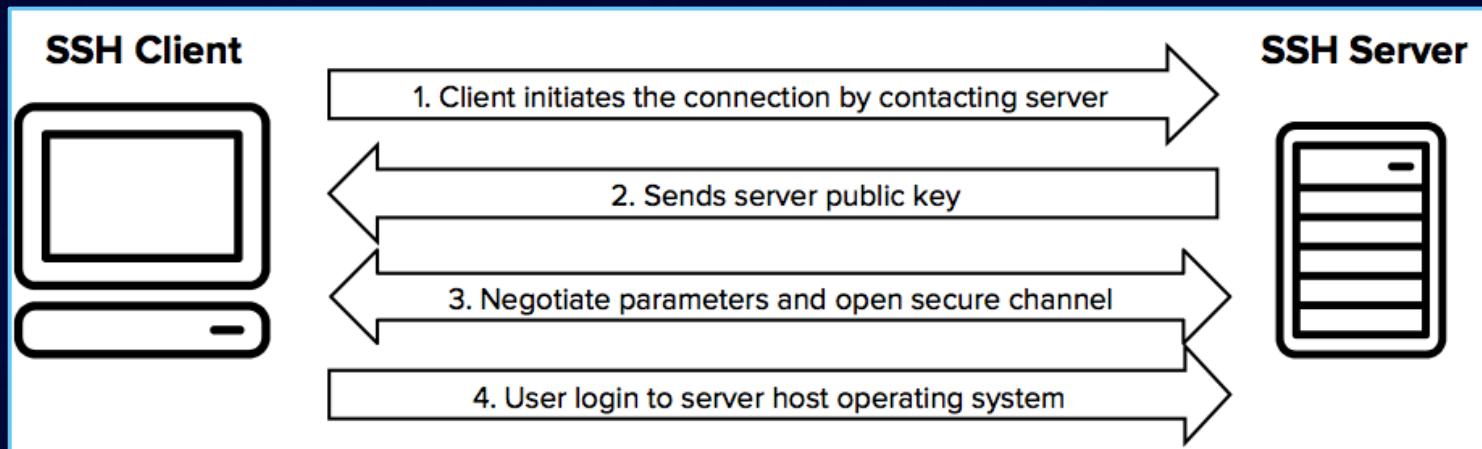
FileZilla é um software livre, famoso aplicativo de FTP cross-platform, que consiste em FileZilla Client e FileZilla Server.



- A vantagem do FTP é a **velocidade** e **eficiência**. Além disso, oferece segurança.
- O usuário precisa ter um **nome de usuário** e uma **senha** para acessar os dados do servidor FTP.
- O FTP suporta o movimento de ida e volta dos dados. Assim, o remetente e o destinatário podem enviar dados um ao outro.

# Secure Shell

- Secure Shell (SSH) é um protocolo de rede que usa criptografia para proteger serviços de rede em redes não seguras.
- Muitas aplicações necessitam da execução de um comando remotamente, o acesso a um computador remoto pode ser protegido com SSH.

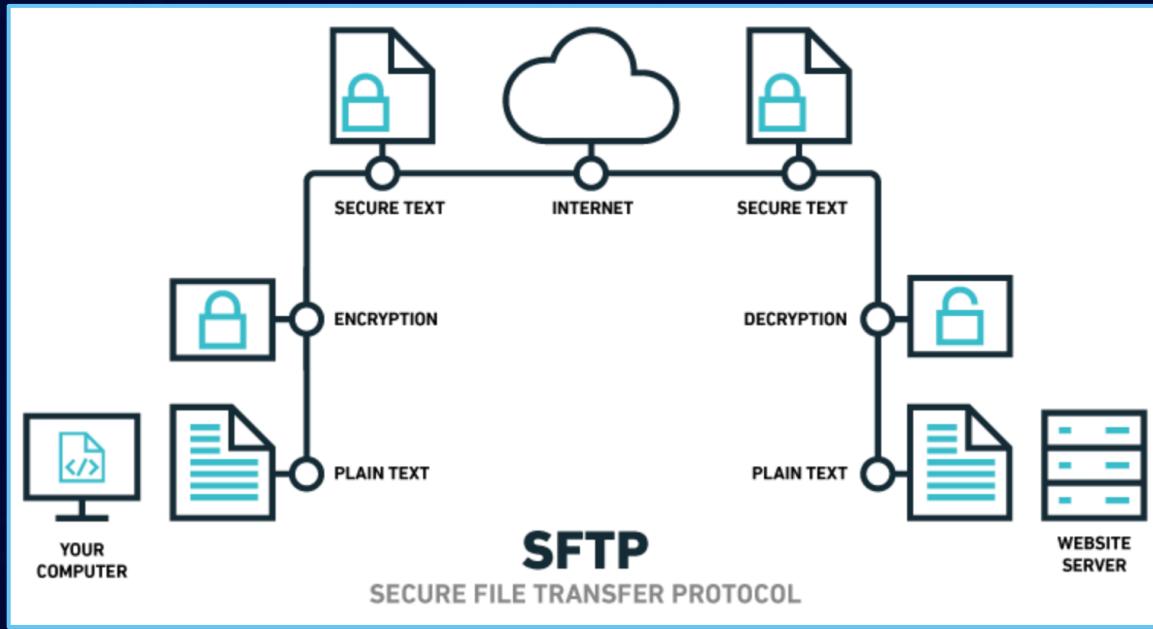


# SSH File Transfer Protocol

- O SSH File Transfer Protocol (SFTP), também conhecido como **FTP seguro**, é usado para proteger a conexão quando um arquivo é enviado remotamente de um sistema para outro.
- Ele usa **criptografia de chave pública** para proteger a comunicação pela Internet e também para facilitar a autenticação forte do usuário.
- A Internet Engineering Task Force (IETF) desenvolveu esse protocolo em 2006 para fornecer segurança aos protocolos do shell.
- Existem duas maneiras de um usuário estabelecer uma conexão com um servidor SFTP: por autenticação de senha ou por autenticação de chave privada/pública.

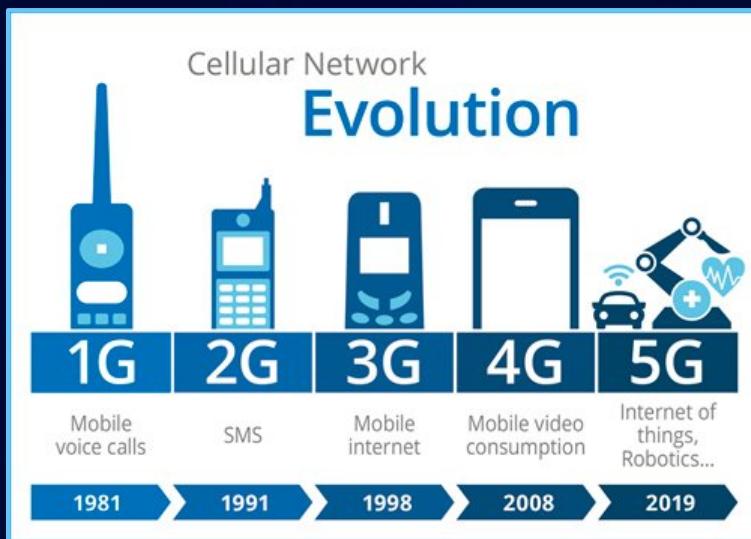
# SSH File Transfer Protocol

- O FTP usa duas conexões para enviar os dados. SFTP pode enviar um arquivo por meio de uma única conexão. Isso elimina a inconveniência para administradores de servidor.



# Cellular Standards

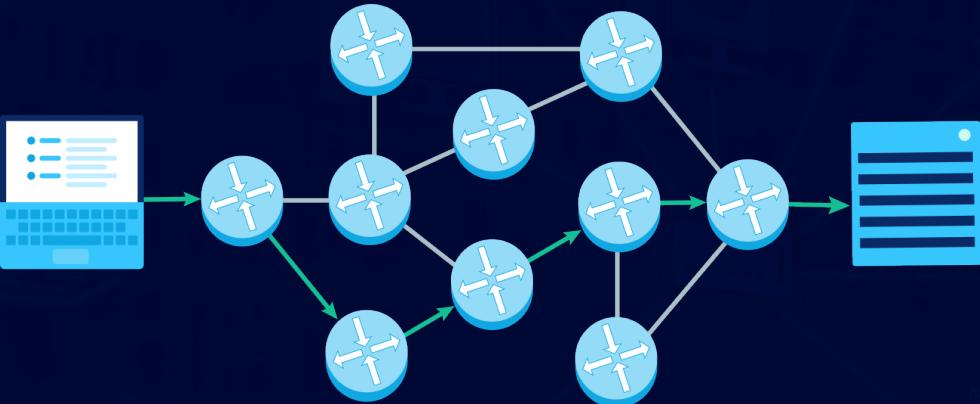
- Existem vários digital cellular standards diferentes, incluindo: Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), cdmaOne, CDMA2000, Evolution-Data Optimized (EV-DO), Enhanced Data Rates para GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), Digital Enhanced Cordless Telecommunications (DECT), Digital AMPS (IS-136 / TDMA) e Integrated Digital Enhanced Network (iDEN).



# Roteamento

- O roteamento é o processo de seleção de caminhos de rede para transportar o tráfego de rede.
- O roteamento é executado para muitos tipos de redes, incluindo **circuit switching networks** e **packet switched networks**.
- Em **packet-switched networks**, os protocolos de roteamento direcionam o encaminhamento de pacotes (o trânsito de pacotes de rede endereçados logicamente de sua origem até seu destino final) por meio de nós intermediários.
- Nós intermediários são normalmente dispositivos de hardware de rede, como **roteadores**, **bridges**, **gateways**, **firewalls** ou **switches**.
- Computadores de uso geral também podem encaminhar pacotes e realizar roteamento, embora não sejam hardware especializado e possam sofrer com o desempenho limitado.

# Roteamento



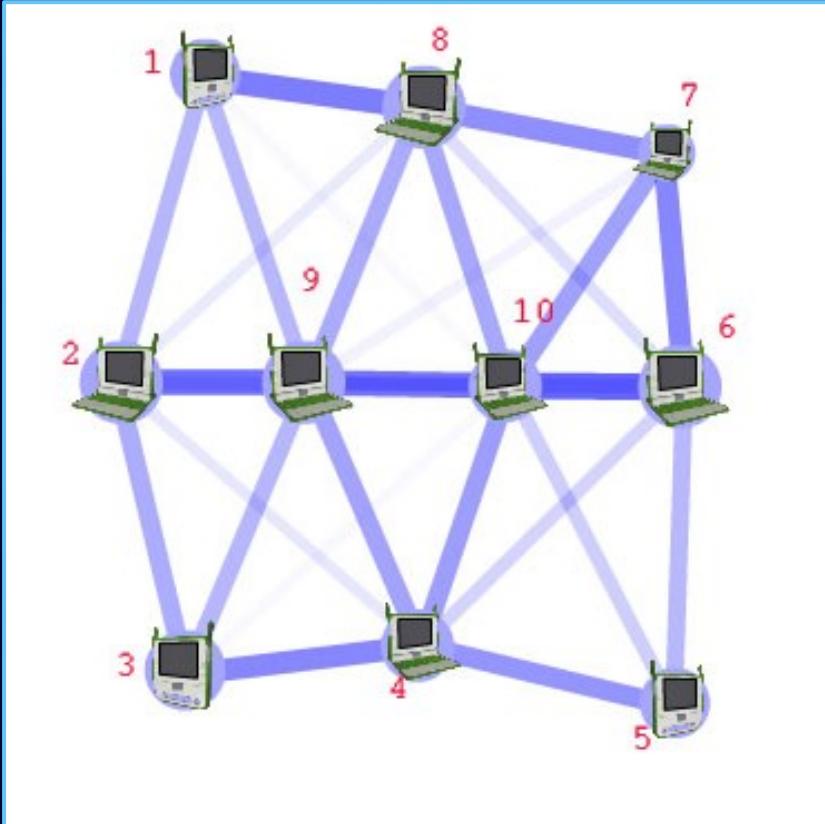
- O processo de roteamento geralmente direciona o encaminhamento com base em **tabelas de roteamento**, que mantêm um registro das rotas para vários destinos da rede.
- Portanto, construir tabelas de roteamento, que são mantidas na **memória do roteador**, é muito importante para um roteamento eficiente.

# Roteamento

- Normalmente existem várias rotas que podem ser tomadas e, para escolher entre elas, diferentes elementos podem ser considerados para decidir quais rotas serão instaladas na tabela de roteamento, como (classificadas por prioridade):
  1. Comprimento do prefixo: onde máscaras de sub-rede mais longas são preferidas (independente se estiver em um protocolo de roteamento ou em um protocolo de roteamento diferente).
  2. Métrica: onde uma métrica / custo mais baixo é preferida (válido apenas dentro de um e o mesmo protocolo de roteamento).
  3. Distância administrativa: onde uma distância menor é preferida (válido apenas entre diferentes protocolos de roteamento)

# Roteamento

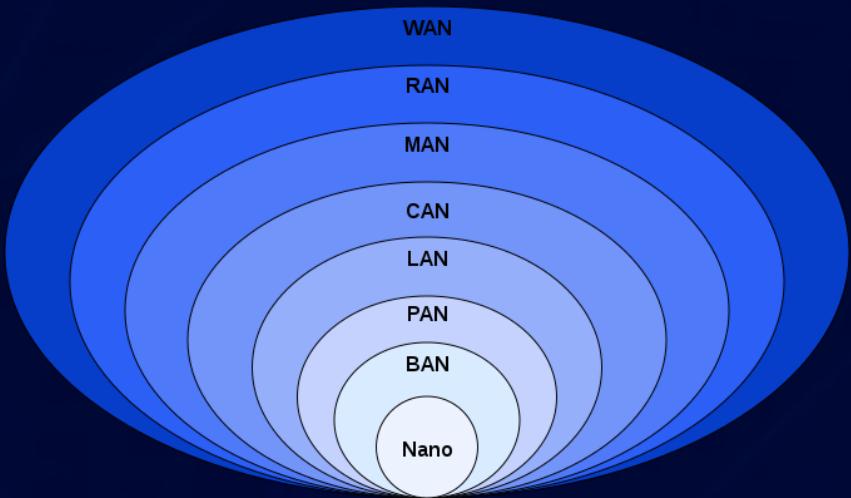
- O roteamento calcula bons caminhos através de uma rede para obter informações.
- Por exemplo, do nó 1 ao nó 6, as melhores rotas são provavelmente 1-8-7-6 ou 1-8-10-6, já que tem as rotas mais espessas.



# Roteamento

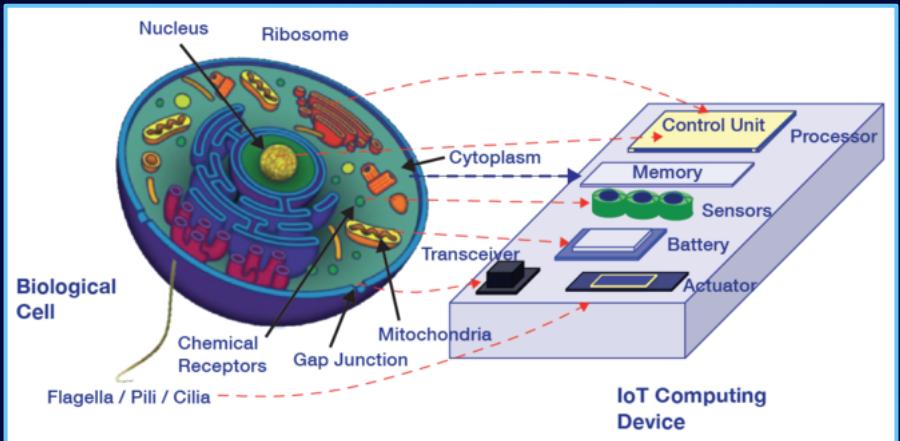
- A maioria dos algoritmos de roteamento usa apenas um caminho de rede por vez. As técnicas de roteamento de vários caminhos permitem o uso de vários caminhos alternativos.
- O roteamento, no sentido mais restrito do termo, é freqüentemente contrastado com “**bridging**” em sua suposição de que os endereços de rede são estruturados e que endereços semelhantes implicam proximidade dentro da rede.
- Os endereços estruturados permitem que uma única entrada na tabela de roteamento represente a rota para um grupo de dispositivos.
- Em grandes redes, o **endereçamento estruturado** (roteamento, no sentido estrito) supera o **endereçamento não estruturado** (bridging). O roteamento se tornou a forma dominante de endereçamento na Internet. Bridging ainda é amplamente usado em ambientes localizados.

# Escala Geográfica



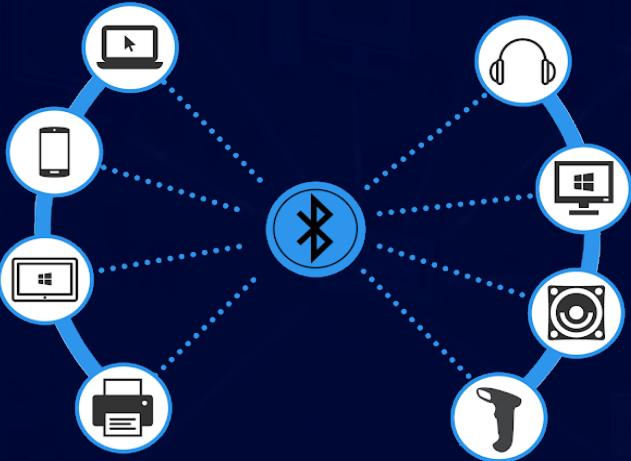
- As redes podem ser caracterizadas por muitas propriedades ou recursos, como capacidade física, finalidade organizacional, autorização do usuário, direitos de acesso e outros.
- Outro método de classificação distinto é o da extensão física ou escala geográfica.

# Nanoscale Network



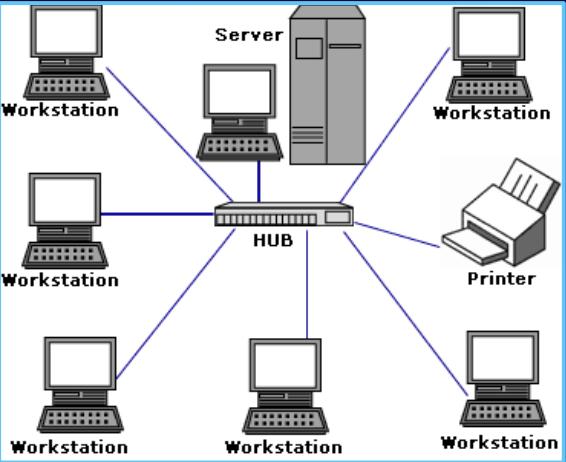
- Uma rede de comunicação em nanoescala tem componentes-chave implementados em nanoescala, incluindo portadores de mensagem e alavancas principios físicos que diferem dos mecanismos de comunicação em macroescala.
- A comunicação em nanoescala estende a comunicação a sensores e atuadores muito pequenos, como os encontrados em sistemas biológicos, e também tende a operar em ambientes que seriam muito adversos para a comunicação clássica.

# Personal Area Network



- Uma **personal area network** (PAN) é uma rede de computadores usada para comunicação entre computadores e diferentes dispositivos tecnológicos de informação próximos a uma pessoa.
- Alguns exemplos de dispositivos usados em um PAN são computadores pessoais, impressoras, aparelhos de fax, telefones, PDAs, scanners e até mesmo consoles de videogame.
- Um PAN pode incluir dispositivos com e sem fio. Um PAN com fio geralmente é construído com conexões USB e FireWire, enquanto tecnologias como Bluetooth e comunicação infravermelha normalmente formam um PAN sem fio.

# Local Area Network



- Uma **local area network** (LAN) é uma rede que conecta computadores e dispositivos em uma área geográfica limitada, como uma casa, escola, prédio comercial ou grupo de edifícios próximos.
- Cada computador ou dispositivo na rede é um nó. As LANs com fio são provavelmente baseadas na tecnologia Ethernet.
- Uma **LAN** pode ser conectada a uma **WAN** usando um roteador.

# Backbone Network

- Uma rede de backbone é parte de uma infraestrutura de rede de computadores que fornece um caminho para a troca de informações entre diferentes LANs ou sub-redes. Um backbone pode unir diversas redes dentro do mesmo edifício, em diferentes edifícios ou em uma área ampla.
- Por exemplo, uma grande empresa pode implementar uma rede de backbone para conectar departamentos localizados em todo o mundo. O equipamento que une as redes departamentais constitui o backbone da rede.
- Ao projetar um backbone de rede, o desempenho e o congestionamento da rede são fatores críticos a serem levados em consideração. Normalmente, a capacidade da rede de backbone é maior do que a das redes individuais conectadas a ela.
- Outro exemplo de rede de backbone é o backbone da Internet, que é um sistema massivo e global de cabos de fibra ótica e redes ópticas que transportam a maior parte dos dados entre redes de longa distância (WANs), redes metropolitanas, regionais, nacionais e transoceânicas.

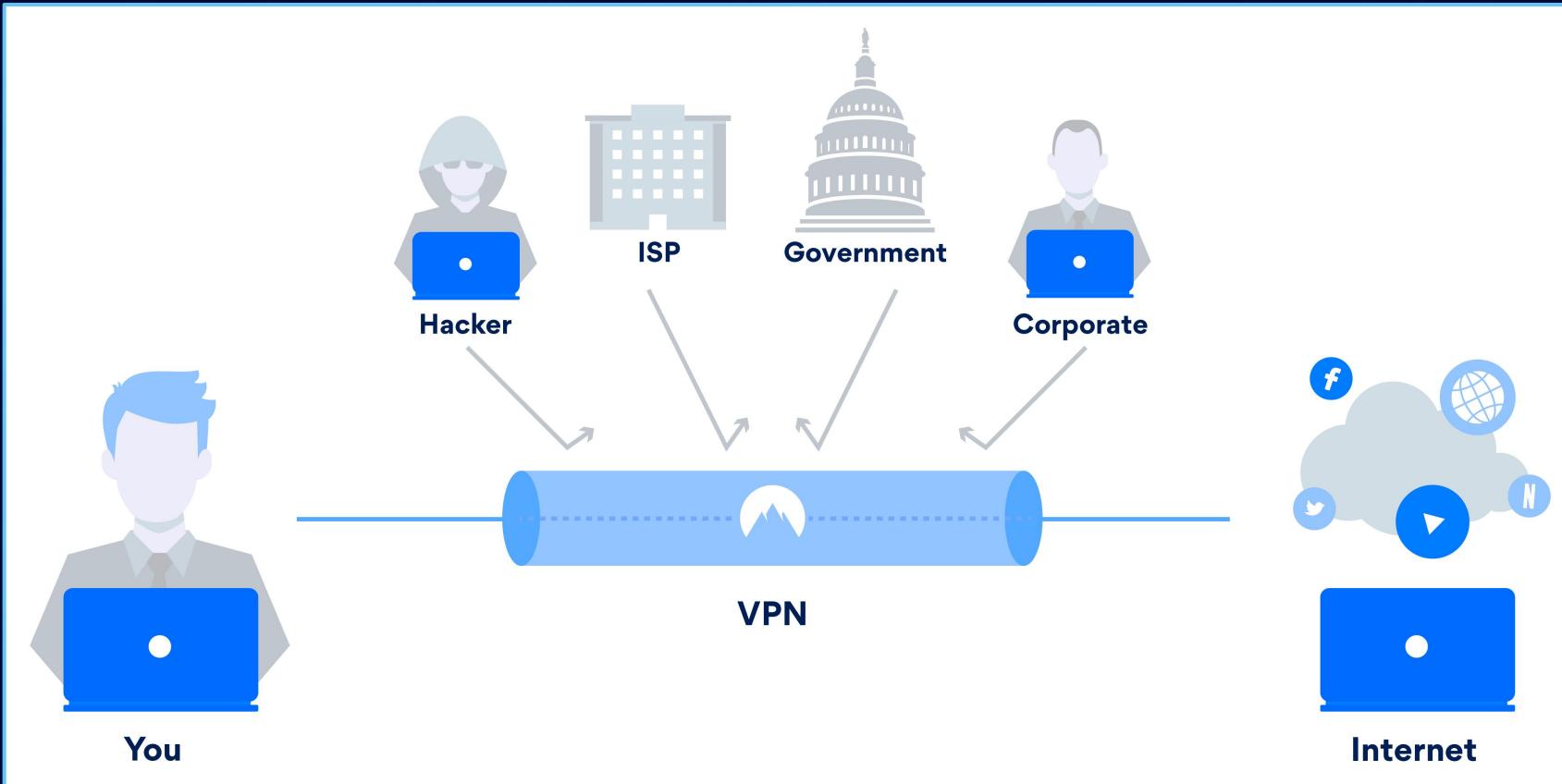
# Wide Area Network

- Uma **wide area network (WAN)** é uma rede de computadores que cobre uma grande área geográfica, como uma cidade, país, ou abrange distâncias intercontinentais.
- Uma WAN usa um canal de comunicação que combina muitos tipos de mídia, como linhas telefônicas, cabos e ondas aéreas.
- Uma WAN geralmente usa recursos de transmissão fornecidos por operadoras comuns, como companhias telefônicas.
- As tecnologias WAN geralmente funcionam nas três camadas inferiores do modelo de referência OSI: a **camada física**, a **camada de enlace de dados** e a **camada de rede**.

# Virtual Private Network

- Uma **rede privada virtual** (VPN) é uma **overlay network** em que alguns dos links entre os nós são transportados por conexões abertas ou circuitos virtuais em alguma rede maior (por exemplo, a Internet) em vez de por fios físicos.
- Diz-se que os protocolos da camada de enlace de dados da rede virtual são encapsulados pela rede maior quando esse for o caso. Uma aplicação comum é a **comunicação segura** pela Internet pública, mas uma VPN não precisa ter recursos de segurança explícitos, como autenticação ou criptografia de conteúdo.

# Virtual Private Network

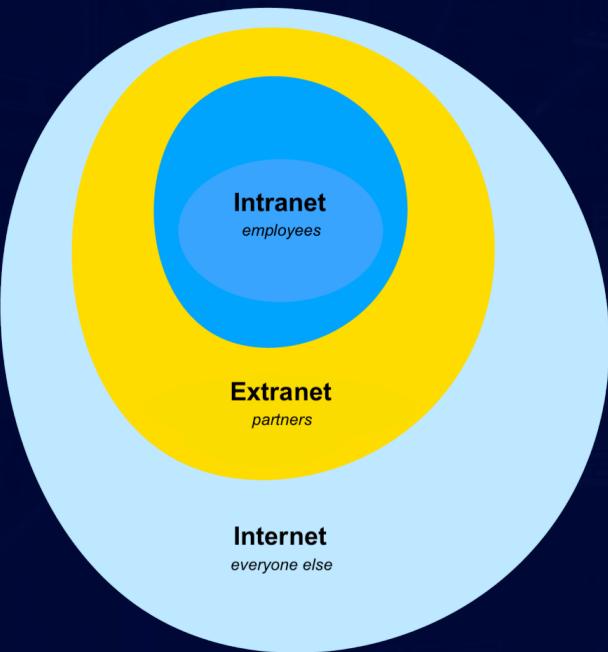


# Global Area Network



- Uma **global area network** (GAN) é uma rede usada para suportar dispositivos móveis em um número arbitrário de LANs sem fio, áreas de cobertura de satélite, etc.
- O principal desafio nas comunicações móveis é transferir as comunicações do usuário de uma área de cobertura local para a próxima.
- No **Projeto 802** do **IEEE**, isso envolve uma sucessão de LANs sem fio terrestres.

# Escopo Organizacional



- As redes são normalmente gerenciadas pelas organizações que as possuem.
- As redes de empresas privadas podem usar uma combinação de **intranets** e **extranets**.
- Eles também podem fornecer acesso de rede à **Internet**, que não tem um único proprietário e permite conectividade global virtualmente ilimitada.

# Intranet

- Uma **intranet** é um conjunto de redes que estão sob o controle de uma única entidade administrativa.
- A intranet usa o protocolo IP e ferramentas baseadas em IP, como navegadores da web e aplicativos de transferência de arquivos.
- A entidade administrativa limita o uso da intranet aos usuários autorizados.
- Mais comumente, uma intranet é a LAN interna de uma organização. Uma grande intranet normalmente tem pelo menos um servidor da web para fornecer aos usuários informações organizacionais.
- Uma intranet também está atrás do roteador em uma rede local.

# Extranet

- Uma **extranet** é uma rede que também está sob o controle administrativo de uma única organização, mas oferece suporte a uma conexão limitada a uma rede externa específica.
- Por exemplo, uma organização pode fornecer acesso a alguns aspectos de sua intranet para compartilhar dados com seus parceiros de negócios ou clientes.
- Essas outras entidades não são necessariamente confiáveis do ponto de vista de segurança. A conexão de rede a uma extranet é frequentemente, mas nem sempre, implementada por meio da tecnologia **WAN**.

# Internet

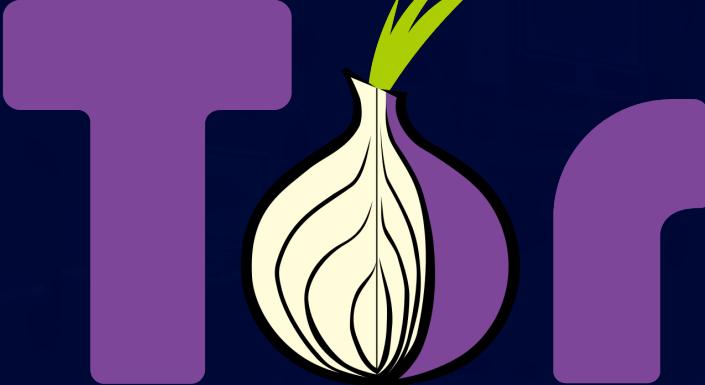


- Uma internetwork é a conexão de vários tipos diferentes de redes de computadores para formar uma única rede de computadores, sobrepondo-se aos diferentes softwares de rede e conectando-os usando roteadores.
- A Internet é o maior exemplo de internetwork. É um sistema global de redes de computadores governamentais, acadêmicas, corporativas, públicas e privadas interconectadas.
- É baseado nas tecnologias de rede do Internet Protocol Suite.
- É o sucessor da Advanced Research Projects Agency Network (ARPANET) desenvolvida pela DARPA do Departamento de Defesa dos Estados Unidos.
- A Internet utiliza comunicações de cobre e backbone óptico de rede para habilitar a World Wide Web (WWW), a Internet of Things, transferência de vídeo e uma ampla gama de serviços de informação.

# Internet

- Os participantes da Internet usam uma gama diversificada de métodos de várias centenas de protocolos documentados e frequentemente padronizados compatíveis com o Internet Protocol Suite e um sistema de endereçamento (endereços IP) administrado pela Internet Assigned Numbers Authority e registros de endereços.
- Provedores de serviços e grandes empresas trocam informações sobre a acessibilidade de seus espaços de endereço por meio do Border Gateway Protocol (BGP), formando uma malha mundial redundante de caminhos de transmissão.

# Darknet

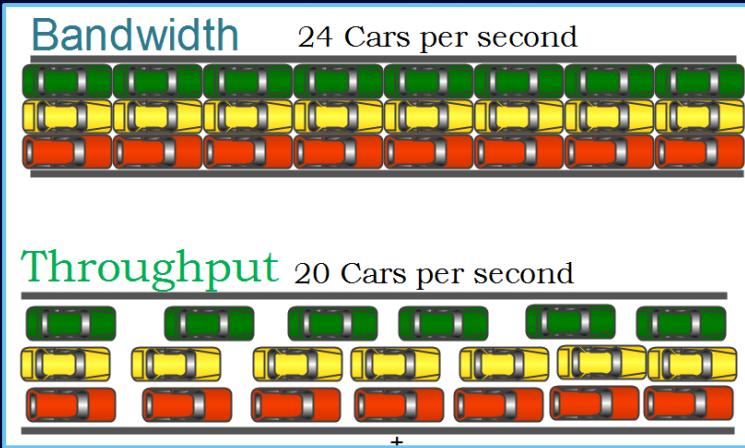


- Uma **darknet** é uma **overlay network**, normalmente executada na Internet, que só pode ser acessada por meio de um software especializado.
- Uma **darknet** é uma rede anônima em que as conexões são feitas apenas entre pares confiáveis usando protocolos e portas não padrão.
- Darknets são diferentes de outras redes ponto a ponto distribuídas, pois o compartilhamento é anônimo.
- Ou seja, os endereços IP não são compartilhados publicamente) e, portanto, os usuários podem se comunicar com pouco medo de interferência governamental ou corporativa.

# Serviços de Rede

- Os serviços de rede são aplicações hospedadas por servidores em uma rede de computadores, para fornecer alguma funcionalidade para membros ou usuários da rede, ou para ajudar a própria rede a operar.
- A **World Wide Web, e-mail, impressão e compartilhamento de arquivos** de rede são exemplos de serviços de rede bem conhecidos. Serviços de rede como **DNS** (Domain Name System) fornecem nomes para endereços IP e MAC (as pessoas se lembram de nomes como "google.com" melhor do que números como "210.121.67.18") e **DHCP** para garantir que o equipamento na rede tenha um endereço IP válido.
- Os serviços são geralmente baseados em um protocolo de serviço que define o formato e o sequenciamento das mensagens entre clientes e servidores desse serviço de rede.

# Desempenho da Rede



- Largura de banda (**bandwidth**) em **bit/s** pode referir-se à largura de banda consumida, correspondendo ao throughput alcançado ou goodput, isto é, a taxa média de transferência de dados bem-sucedida através de um caminho de comunicação.
- A taxa de transferência (**throughput**) é afetada por tecnologias como modelagem de largura de banda, gerenciamento de largura de banda, limitação de largura de banda, limite de largura de banda, alocação de largura de banda (por exemplo, bandwidth allocation protocol de banda e alocação dinâmica de largura de banda), etc.

# Desempenho da Rede

- O atraso da rede (**network delay**) é uma característica de design e desempenho de uma rede de telecomunicações.
- Ele especifica a latência de um bit de dados para viajar pela rede de um ponto de extremidade de comunicação para outro.
- Normalmente é medido em múltiplos ou frações de segundo. O atraso pode ser um pouco diferente, dependendo da localização do par específico de terminais de comunicação.
- Os engenheiros geralmente relatam o atraso máximo e médio, e eles dividem o atraso em várias partes:
  - **Processing delay** - tempo que um roteador leva para processar o header do pacote
  - **Queuing delay** - tempo que o pacote passa nas filas de roteamento
  - **Transmission delay** - tempo que leva para enviar os bits do pacote para o link
  - **Propagation delay** - tempo para um sinal se propagar através da mídia

# Desempenho da Rede

- Um certo nível mínimo de atraso é experimentado pelos sinais devido ao tempo que leva para transmitir um pacote em série por meio de um link.
- Este atraso é estendido por mais níveis variáveis de atraso devido ao congestionamento da rede.
- Os atrasos da rede IP podem variar de alguns milissegundos a várias centenas de milissegundos.
- O congestionamento da rede ocorre quando um link ou nó é submetido a uma carga de dados maior do que a nominal, resultando na deterioração de sua qualidade de serviço. Quando as redes estão congestionadas e as filas ficam muito cheias, os pacotes precisam ser descartados e, portanto, as redes dependem da retransmissão.
- Para a Internet, o RFC 2914 aborda o assunto do controle de congestionamento em detalhes.

# Segurança



- As redes de computadores também são usadas por **hackers** para implantar vírus ou worms de computador em dispositivos conectados à rede ou para impedir que esses dispositivos accessem a rede por meio de um **denial-of-service attack** (DOS).

# Segurança da Rede



- A **segurança da rede** consiste em disposições e políticas adotadas pelo administrador da rede para prevenir e monitorar o acesso não autorizado, uso indevido, modificação ou negação da rede de computadores e seus recursos acessíveis pela rede.
- A segurança da rede é a autorização de acesso aos dados em uma rede, que é controlada pelo administrador da rede.
- Os usuários recebem um **ID** e uma **senha** que lhes permite acessar informações e programas dentro de sua autoridade.
- A segurança de rede é usada em uma variedade de redes de computadores, tanto públicas quanto privadas, para proteger as transações e comunicações diárias entre empresas, agências governamentais e indivíduos.

# Vigilância de Rede

- Vigilância de rede é o monitoramento de dados sendo transferidos por redes de computadores, como a Internet.
- O monitoramento geralmente é feito secretamente e pode ser feito por ou a mando de governos, por empresas, organizações criminosas ou indivíduos.
- Pode ou não ser legal e pode ou não exigir autorização de um tribunal ou outra agência independente.
- Os programas de vigilância de computador e rede são amplamente difundidos hoje em dia, e quase todo o tráfego da Internet é ou pode ser monitorado em busca de pistas de atividades ilegais.

# Vigilância de Rede



- A vigilância é muito útil para governos e agentes da lei para manter o controle social, reconhecer e monitorar ameaças e prevenir/investigar atividades criminosas.
- Com o advento de programas como o programa **Total Information Awareness**, tecnologias como computadores de vigilância de alta velocidade e software biométrico, e leis como o **Communications Assistance For Law Enforcement Act**, os governos agora possuem uma capacidade sem precedentes de monitorar as atividades dos cidadãos.

# End to end Encryption

- End-to-end encryption (E2EE) é um paradigma de comunicação digital de proteção ininterrupta de dados que trafegam entre duas partes em comunicação.
- Envolve a parte de origem que criptografa os dados de forma que apenas o destinatário pretendido possa descriptografá-los, sem dependência de terceiros.
- End-to-end encryption evita que intermediários, como provedores de Internet ou provedores de serviços de aplicativos, descubram ou interfiram nas comunicações.
- End-to-end encryption geralmente protege tanto a confidencialidade quanto a integridade.

# End to end Encryption

- Exemplos de end-to-end encryption incluem HTTPS para tráfego da web, PGP para e-mail, OTR para mensagens instantâneas, ZRTP para telefonia e TETRA para rádio.



# SSL/TLS

- A introdução e o rápido crescimento do comércio eletrônico na World Wide Web em meados da década de 1990 tornaram óbvio que alguma forma de autenticação e criptografia era necessária.
- A **Netscape** deu o primeiro passo em um novo padrão. Na época, o navegador dominante era o Netscape Navigator. A Netscape criou um padrão chamado **secure socket layer (SSL)**.
- SSL requer um servidor com um certificado. Quando um cliente solicita acesso a um servidor protegido por SSL, o servidor envia uma cópia do certificado ao cliente. O cliente SSL verifica este certificado (todos os navegadores da web vêm com uma lista exaustiva de certificados raiz CA pré-carregados) e, se o certificado for verificado, o servidor é autenticado e o cliente negocia uma **cifra de chave simétrica** para uso na sessão. A sessão agora está em um túnel criptografado muito seguro entre o servidor SSL e o cliente SSL.

# Visão das Redes

- Usuários e administradores de rede geralmente têm visões diferentes de suas redes.
- Os usuários podem compartilhar impressoras e alguns servidores de um grupo de trabalho, o que geralmente significa que eles estão na mesma localização geográfica e na mesma LAN, enquanto um administrador de rede é responsável por manter essa rede em funcionamento.
- Os administradores de rede podem ver as redes de perspectivas físicas e lógicas.

# Visão das Redes

- A perspectiva física envolve localizações geográficas, cabeamento físico e os elementos de rede (por exemplo, roteadores, bridges e gateways de camada de aplicação) que se interconectam por meio da mídia de transmissão.
- As redes lógicas, chamadas, na arquitetura TCP/IP, de sub-redes, são mapeadas em um ou mais meios de transmissão. Por exemplo, uma prática comum em um campus de edifícios é fazer um conjunto de cabos LAN em cada edifício parecer uma sub-rede comum, usando a tecnologia LAN virtual (VLAN).
- Tanto os usuários quanto os administradores estão cientes, em graus variados, das características de confiança e escopo de uma rede.

# Visão das Redes

- Extraoficialmente, a Internet é o conjunto de usuários, empresas e provedores de conteúdo que estão interconectados por **Internet Service Providers (ISP)**.
- Do ponto de vista da engenharia, a Internet é o conjunto de sub-redes e agregados de sub-redes que compartilham o espaço de endereço IP registrado e trocam informações sobre a acessibilidade desses endereços IP usando o **Border Gateway Protocol**.
- Normalmente, os nomes legíveis por humanos dos servidores são convertidos em endereços IP, de forma transparente para os usuários, por meio da função de diretório do **Domain Name System (DNS)**.

# Implementações

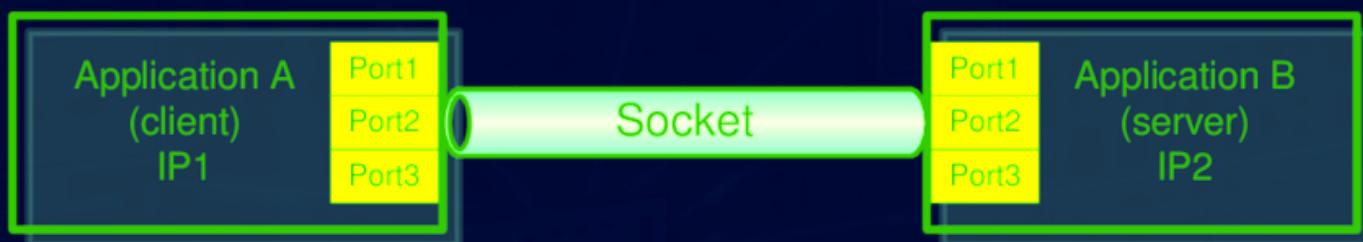
- O Internet protocol suite não pressupõe nenhum ambiente de hardware ou software específico.
- Requer apenas a existência de uma camada de hardware e software capaz de enviar e receber pacotes em uma rede de computadores.
- Como resultado, o suite foi implementado em praticamente todas as plataformas de computação.
- Uma implementação mínima de TCP/IP inclui o seguinte: Internet Protocol (IP), Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP) e Internet Group Management Protocol (IGMP).

# Implementações

- Os programadores de aplicativos normalmente se preocupam apenas com as interfaces na camada de aplicação e, muitas vezes, também na camada de transporte, enquanto as camadas abaixo são serviços fornecidos pela stack TCP/IP no sistema operacional.
- A maioria das implementações de IP são acessíveis aos programadores por meio de sockets e APIs.

# Socket de Rede

- Um **socket** de rede é uma estrutura de software dentro de um nó de rede de uma rede de computadores que serve como um ponto final para enviar e receber dados pela rede.
- A estrutura e as propriedades de um socket são definidas por uma **application programming interface** (API) para a arquitetura de rede.



# Echo Server

- Um Echo Server é um aplicativo que permite que um cliente e um servidor se conectem para que um cliente possa enviar uma mensagem ao servidor e o servidor possa receber a mensagem e enviá-la ou ecoá-la de volta para o cliente.



# Echo Server (Python)

- A seguir temos o exemplo de um Echo Server em Python:

```
import socket

HOST = 'localhost'
PORT = 12345
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.bind((HOST,PORT))
s.listen(1)
print('Aguardando conexão...')
conn, addr = s.accept()
print('Conectado por: {}'.format(addr))

while True:
    data = conn.recv(1024)
    if not data:
        break
    print('Dados Recebidos: {}'.format(data))
    conn.sendall(data)
print('Fechando conexão.')
conn.close()
```

# Echo Client (Python)

- A seguir temos o exemplo de um Echo Client em Python:

```
import socket

HOST = 'localhost'
PORT = 12345
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((HOST,PORT))
s.sendall(b'Hello, World!')
data = s.recv(1024)
s.close()
print('Recebido: {}'.format(repr(data)))
```

# Comandos de Rede no Linux



- A rede é uma parte essencial de um sistema operacional.
- Como vimos, a maioria dos computadores do mundo se conecta por meio de uma rede.
- Essa rede pode ser uma pequena e simples baseada em casa ou tão complexa quanto um data center de computação em nuvem.
- As tarefas de rede incluem configurações, monitoramento de tráfego e solução de problemas.
- A seguir veremos comandos de rede Linux úteis que podem nos ajudar a configurar ou solucionar problemas relacionados à rede.

# Comandos de Rede no Linux

- `ifconfig` (configurador de interface) é um dos comandos mais básicos e comumente usados para localizar detalhes de rede. Ele também é usado para configurar os parâmetros da interface de rede.
- Podemos usar este comando para obter o endereço IP, endereço MAC e MTU das redes disponíveis.

```
$ ifconfig
```

- O comando `ip` é a versão mais recente do `ifconfig`. É mais poderoso do que o comando `ifconfig`, pois pode realizar várias outras tarefas, como configuração de roteamento padrão ou estático, mostrando endereços IP e suas propriedades, configurando endereços IP e rotas para interfaces de rede.

```
$ ip address
```

# Comandos de Rede no Linux

- O comando `traceroute` é comumente usado para solucionar problemas da rede. Ele descobre o delay e o caminho para o seu destino. Ele determina e relata de onde vem a latência da rede.

```
$ traceroute google.com
```

- `ping` (Packet INternet Groper) é outro comando de rede mais comumente usado para verificar a conectividade entre dois nós de rede. É usado para medir a resposta média. Se pudermos enviar um ping para qualquer host e ele não tiver respondido, podemos presumir que o host não está acessível devido a algum problema de rede ou seu firewall está bloqueando a solicitação.

```
$ ping -c 6 google.com
```

# Comandos de Rede no Linux

- O comando **netstat** é usado para revisar cada conexão de rede e sockets abertos no dispositivo Linux. Ele fornece informações sobre conexões, sockets abertos e tabelas de roteamento.

```
$ netstat -nltp
```

- Comando **nslookup** (Name Server Lookup) usado para consultar o **DNS** para obter um nome de domínio, mapeamento de endereço IP ou registros DNS.

```
$ nslookup google.com
```

# Comandos de Rede no Linux

- dig (Domain Information Groper) é outro comando usado para investigar o DNS. É uma versão atualizada do nslookup.
- Ele executa uma consulta DNS Lookup e exibe a resposta retornada dos servidores de nomes. Ele também é usado para verificar mapeamentos DNS, registros MX e outros registros DNS.

```
$ dig google.com
```

- O comando route é usado para mostrar ou modificar a tabela de roteamento do sistema. Usando este comando, você pode solucionar o problema de rede causado por uma entrada incorreta na tabela de roteamento do sistema. Definir uma tabela de roteamento é muito importante para que o roteador funcione corretamente.

```
$ route
```

# Comandos de Rede no Linux

- O comando `host` é usado para exibir o nome de domínio de um endereço IP ou o endereço IP de um nome de domínio. Também pode ser usado para consultar o DNS.

```
$ host google.com
```

- `arp` (Address Resolution Protocol) é usado para manipular a tabela ARP do kernel.
- Usando este comando, você pode visualizar, adicionar, atualizar ou remover entradas na tabela ARP do kernel.

```
$ arp
```

# Comandos de Rede no Linux

- O comando `iwconfig` é usado para configurar a interface WLAN.
- Ele pode visualizar ou configurar propriedades básicas de interface de rede sem fio, como `SSID` e tipo de criptografia.

```
$ iwconfig
```

- `curl` é um utilitário usado para transferir dados de e para um servidor sem interação do usuário. Ele pode se comunicar usando os protocolos `HTTP`, `HTTPS`, `FTP`, `SFTP` e `SCP`. Ele pode ser usado para fazer upload ou download de dados usando qualquer um dos protocolos acima. Você pode transferir dados permitindo retomar, configurar limite de largura de banda e autenticação de usuário, e muitas outras coisas com o `curl`. Ele é instalado por padrão na maioria dos sistemas Linux. Você também pode baixar um arquivo usando `curl`.

```
$ curl example.com
```

# Comandos de Rede no Linux

- `wget` também é um pacote pré-instalado. Ele é usado para baixar arquivos usando protocolos `HTTP`, `HTTPS`, `FTP`. Ele oferece a capacidade de baixar vários arquivos, retomar downloads, baixar em segundo plano, etc.

```
$ wget https://arquivos.netlify.app/images/alchemy.jpg
```

- O comando `telnet` usa o protocolo Telnet para se comunicar com o host de destino. Você deve especificar o host com a porta (principalmente a porta 443).

```
$ telnet google.com 443
```

- O comando `whois` é usado para obter todas as informações sobre um site. Você pode obter todos os detalhes de registro e propriedade usando-o.

```
$ whois google.com
```

# Comandos de Rede no Linux

- `tcpdump` é um sniffer de pacotes de linha de comando mais poderoso e amplamente usado ou uma ferramenta analisadora de pacotes que é usada para capturar ou filtrar pacotes TCP/IP recebidos ou transferidos por uma rede em uma interface específica.
- Ele está disponível na maioria dos sistemas operacionais baseados em Linux/Unix. O `tcpdump` também nos dá a opção de salvar os pacotes capturados em um arquivo para análise futura.
- Ele salva o arquivo em um formato `pcap`, que pode ser visualizado pelo comando `tcpdump` ou uma ferramenta baseada em GUI de código aberto chamada `Wireshark` (Network Protocol Analyzer) que lê arquivos no formato `pcap` `tcpdump`.
- Muitas das distribuições do Linux já vêm com a ferramenta `tcpdump`, caso você não a tenha nos sistemas, você pode instalá-la usando o seguinte comando `apt`.

```
$ sudo apt install tcpdump
```

# Comandos de Rede no Linux

- Quando executarmos o comando `tcpdump`, ele irá capturar de todas as interfaces, porém com a chave `-i` ele captura apenas da interface desejada.

```
$ tcpdump -i eth0
```

- Quando você executa o comando `tcpdump`, ele captura todos os pacotes da interface especificada, até que você pressione o botão Cancelar. Mas usando a opção `-c`, você pode capturar um número especificado de pacotes. O exemplo abaixo irá capturar apenas 6 pacotes.

```
$ tcpdump -c 5 -i wlp3s0
```

# Comandos de Rede no Linux

- O comando `tcpdump` abaixo com a opção `-A` exibe o pacote no formato **ASCII**. É um formato de esquema de codificação de caracteres.

```
$ tcpdump -A -i eth0
```

- Para listar o número de interfaces disponíveis no sistema, execute o seguinte comando com a opção `-D`.

```
$ tcpdump -D
```

- O comando a seguir com a opção `-XX` captura os dados de cada pacote, incluindo seu header de nível de link em formato **HEX** e **ASCII**.

```
$ tcpdump -XX -i eth0
```

# Comandos de Rede no Linux

- Como citamos, o tcpdump possui a funcionalidade de capturar e salvar o arquivo no formato pcap, para isso basta executar o comando com a opção -w.

```
$ tcpdump -w 0001.pcap -i eth0
```

- Para ler e analisar o arquivo do pacote 0001.pcap capturado, use o comando com a opção -r, conforme mostrado abaixo.

```
$ tcpdump -r 0001.pcap
```

- Para capturar pacotes com base na porta TCP, execute o seguinte comando com a opção tcp.

```
$ tcpdump -i eth0 tcp
```

# Comandos de Rede no Linux

- Digamos que você queira capturar pacotes para a porta 22 específica, execute o comando abaixo especificando o número da porta 22.

```
$ tcpdump -i eth0 port 22
```

- Para capturar pacotes do IP de origem, digamos que você queira capturar pacotes para 192.168.0.2, use o comando a seguir.

```
$ tcpdump -i eth0 src 192.168.0.2
```

- Para capturar pacotes do IP de destino, digamos que você queira capturar pacotes para 50.116.66.139, use o comando a seguir.

```
$ tcpdump -i eth0 dst 50.116.66.139
```

# Wireshark

# WIRESHARK

- O Wireshark é um analisador de pacotes gratuito e de código aberto.
- É usado para solução de problemas de rede, análise, desenvolvimento de software e protocolo de comunicação e educação.
- O Wireshark é muito semelhante ao tcpdump, mas tem um front-end gráfico, além de algumas opções integradas de classificação e filtragem.
- O Wireshark usa pcap para capturar pacotes, portanto, ele só pode capturar pacotes nos tipos de redes que o pcap suporta.
- Para conhecer mais detalhes, você pode visitar: <https://www.wireshark.org/>

# Nmap



- Nmap, ou [Network Mapper](#), é uma ferramenta de linha de comando Linux de código aberto para exploração de rede e auditoria de segurança.
- Com o Nmap, os administradores de servidor podem revelar rapidamente [hosts](#) e [serviços](#), pesquisar problemas de segurança e escanear [portas abertas](#).
- A ferramenta Nmap pode auditar e descobrir portas abertas locais e remotas, bem como informações de rede e hosts.
- A seguir veremos alguns dos comandos Nmap mais úteis no Linux com exemplos.

# Nmap

- Ao escanear hosts, os comandos Nmap podem usar nomes de servidor, endereços IPV4 ou endereços IPV6. Um comando básico do Nmap produzirá informações sobre o host fornecido.

```
$ nmap scanme.nmap.org
```

- Sem sinalizadores, como escrito acima, o Nmap revela serviços e portas abertos no host ou hosts fornecidos.

```
$ nmap 192.168.0.1
```

- Se você precisar realizar uma varredura rapidamente, pode usar o sinalizador -F. Como o sinalizador -F “Fast Scan” não verifica tantas portas, não é tão completo.

```
$ nmap -F 192.168.0.1
```

# Nmap

- O Nmap pode escanear vários locais de uma vez em vez de escanear um único host por vez. Isso é útil para infraestruturas de rede mais extensas. Existem várias maneiras de verificar vários locais ao mesmo tempo, dependendo de quantos locais você precisa examinar.
- Adicione vários domínios ou vários endereços IP em uma linha para fazer a varredura de vários hosts ao mesmo tempo.

```
$ nmap 192.168.0.1 192.168.0.2 192.168.0.3
```

- Use o *wildcard*\* para verificar uma sub-rede inteira de uma vez.

```
$ nmap 192.168.0.*
```

- Separe as terminações de endereços diferentes com vírgulas, em vez de digitar todo o endereço IP.

```
$ nmap 192.168.0.1,2,3
```

# Nmap

- Além de informações gerais, o Nmap também pode fornecer detecção de sistema operacional, varredura de script, traceroute e detecção de versão.
- É importante notar que o Nmap fará o seu melhor para identificar elementos como sistemas operacionais e versões, mas pode nem sempre ser totalmente preciso.
- Adicione o sinalizador `-A` em seu comando Nmap, você pode descobrir as informações do sistema operacional dos hosts que são mapeados.

```
$ nmap -A 192.168.0.1
```

- Usar o sinalizador `-O` em seu comando Nmap revelará mais informações do sistema operacional dos hosts mapeados. O sinalizador `-O` ativa a detecção do sistema operacional. Tags adicionais incluem `-osscan-limit` e `-osscan-guess`.

```
$ nmap -O 192.168.0.1
```

# Nmap

- A detecção de configurações de firewall pode ser útil durante o teste de penetração e varreduras de vulnerabilidade.
- Várias funções podem ser usadas para detectar configurações de firewall nos hosts fornecidos, mas o sinalizador -sA é o mais comum.

```
$ nmap -sA 192.168.0.1
```

- Às vezes, você pode precisar detectar informações de serviço e versão de portas abertas.
- Isso é útil para solucionar problemas, verificar vulnerabilidades ou localizar serviços que precisam ser atualizados.

```
$ nmap -sV 192.168.0.1
```

# Nmap

- A varredura de portas é um dos utilitários básicos que o Nmap oferece e, consequentemente, existem algumas maneiras de personalizar esse comando.
- Com o sinalizador `-p` seguido por uma porta, você pode procurar informações sobre uma porta específica em um host.

```
$ nmap -p 443 192.168.0.1
```

- Você pode fazer a varredura de várias portas com o sinalizador `-p`, separando-as com uma vírgula.

```
$ nmap -p 80,443 192.168.0.1
```

- Você também pode procurar várias portas com o sinalizador `-p` marcando um intervalo com o hífen.

```
$ nmap -p 80-443 192.168.0.1
```

# Nmap

- Se for necessário completar uma varredura furtiva, use o sinalizador `-sS`.

```
$ nmap -sS 192.168.0.1
```

- Existem algumas maneiras de implementar a descoberta de host por meio do Nmap. O mais comum deles é por meio de `-sL`.

```
$ nmap -sL 192.168.0.1
```

- Se você tiver uma longa lista de endereços que precisa verificar, poderá importar um arquivo diretamente por meio da linha de comando.

```
$ nmap -iL /arquivo.txt
```

- O sinalizador `-v` fornecerá informações adicionais sobre uma varredura concluída. Ele pode ser adicionado à maioria dos comandos para fornecer mais informações.

```
$ nmap -v 192.168.0.1
```

# Nmap

- O IPv6 está se tornando mais comum e o Nmap o suporta da mesma forma que suporta domínios e endereços de IP mais antigos.
- O IPv6 funciona com qualquer um dos comandos Nmap disponíveis. Mas, um sinalizador é necessário para informar ao Nmap que um endereço IPv6 está sendo referenciado.
- Use o sinalizador `-6` com outros sinalizadores e comandos para executar funções Nmap mais complicadas com IPv6.

```
$ nmap -6 ::ffff:c0a8:1
```

- Uma das habilidades mais simples do Nmap é a habilidade de executar ping em máquinas ativas. O sinalizador `-sP` localiza máquinas.

```
$ nmap -sP 192.168.0.0/24
```

- Pode ser necessário encontrar interfaces de host, interfaces de impressão e rotas para depurar. Para fazer isso, use o comando `iflist`.

```
$ nmap --iflist
```

# Nmap

- Às vezes, você pode precisar fazer uma varredura mais agressivamente ou deseja executar uma varredura rápida. Você pode controlar isso usando os mecanismos de temporização (T1, T2, T3, etc).
- No Nmap, o tempo controla a velocidade e a profundidade da varredura.

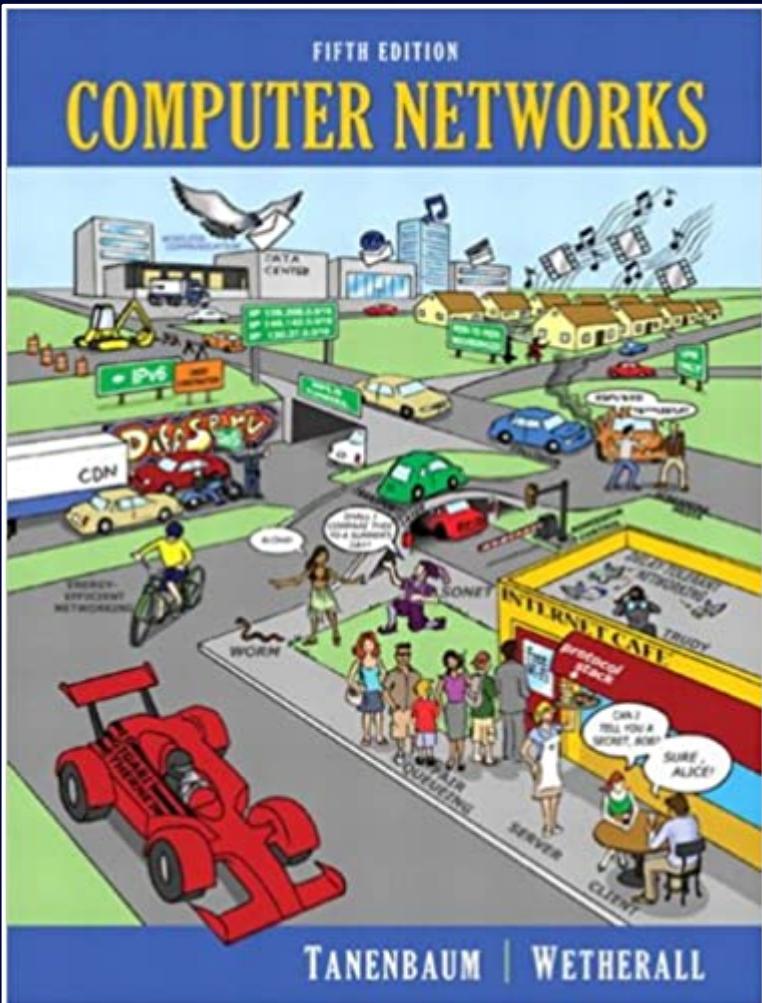
```
$ nmap -T5 192.168.0.1
```

- Para consultar o manual do Nmap digite o comando a seguir.
- Para obter ajuda e informações sobre os sinalizadores, assim como exemplos, digite o comando a seguir.

```
$ nmap -h
```

# Mais Detalhes

Para aprofundar o seu conhecimento em redes de computadores você pode usar o famoso livro **Computer Networks** (5th Edition), de **Andrew Tanenbaum**, que possui uma abordagem estruturada para explicar como as redes funcionam de dentro para fora. Ele começa com uma explicação da camada física da rede, hardware de computador e sistemas de transmissão; em seguida, segue seu caminho até os aplicativos de rede.



# Considerações Finais

“The Internet is not just one thing, it's a collection of things - of numerous communications networks that all speak the same digital language.” James H. Clark



# Referências

- [https://en.wikipedia.org/wiki/Computer\\_network](https://en.wikipedia.org/wiki/Computer_network)
- <https://www.cloudflare.com/pt-br/learning/ddos/glossary/open-systems-interconnection-model-osi/>
- [https://en.wikipedia.org/wiki/OSI\\_model](https://en.wikipedia.org/wiki/OSI_model)
- <https://docs.microsoft.com/en-us/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting>
- [https://en.wikipedia.org/wiki/Internet\\_protocol\\_suite](https://en.wikipedia.org/wiki/Internet_protocol_suite)
- <https://www.baeldung.com/cs/popular-network-protocols>