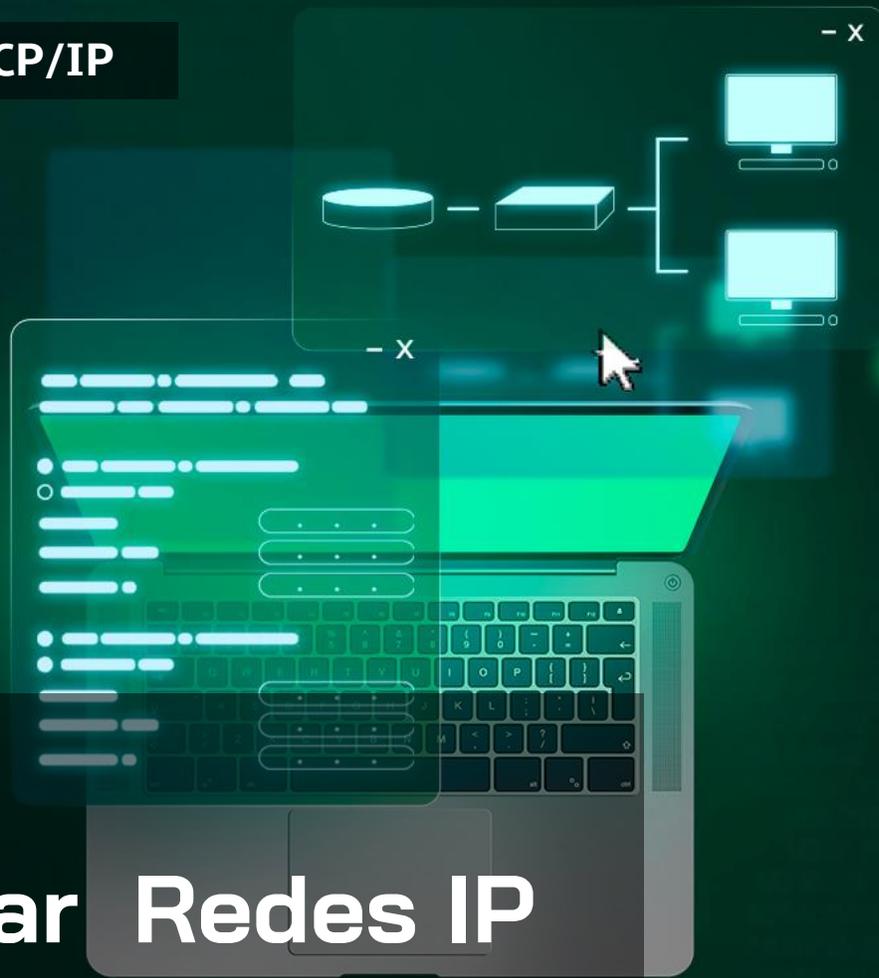


Módulo 01: Introdução ao TCP/IP



REDES

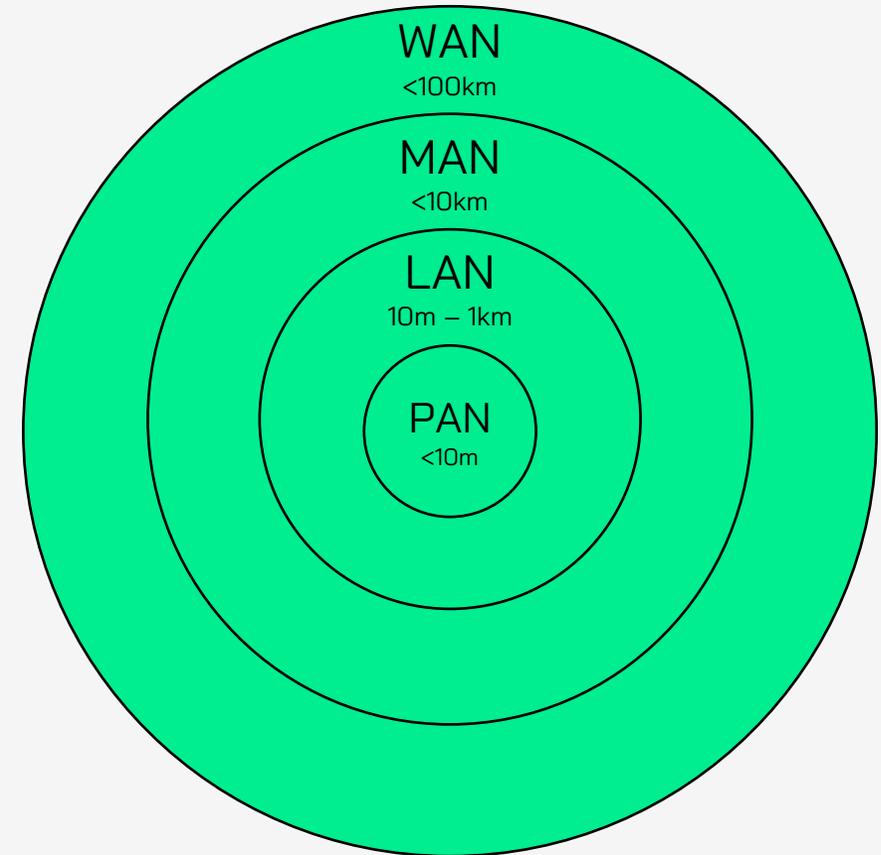
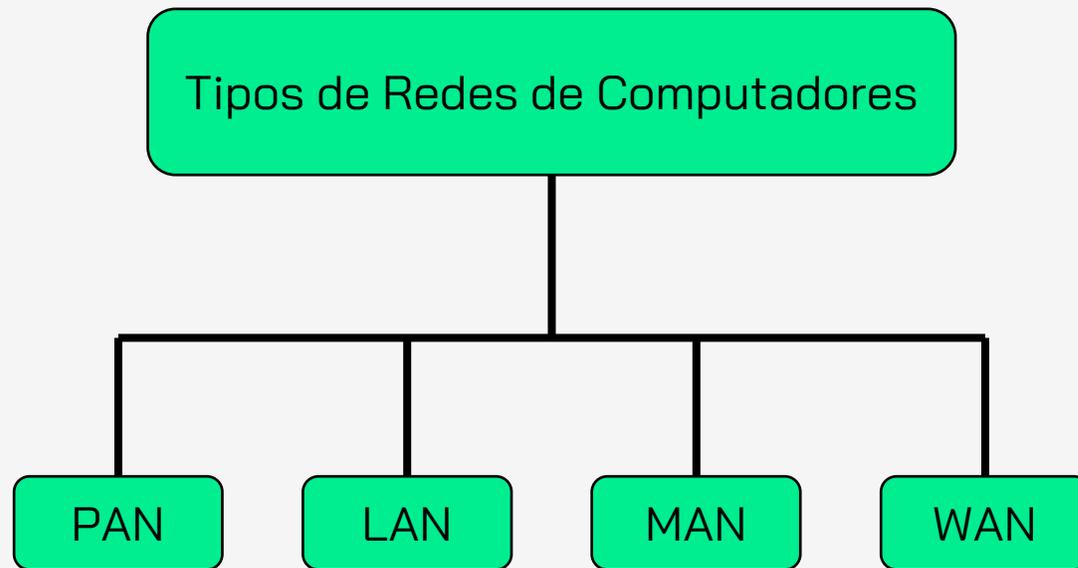
TCP /IP

AULA #1

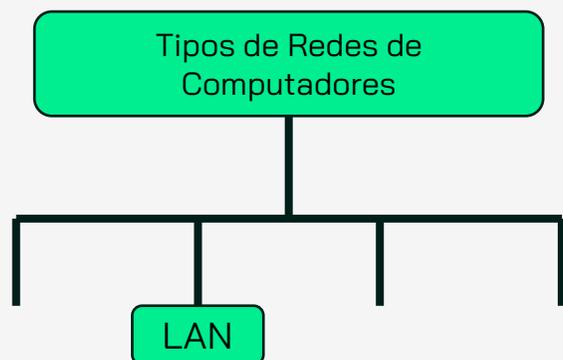
Porque estudar Redes IP

BÁSICO

Porque estudar IP?



Porque estudar IP?



Local Area Network

São chamadas de LAN, ou Redes Locais, as redes que interligam computadores e dispositivos que estejam dentro do mesmo espaço físico.

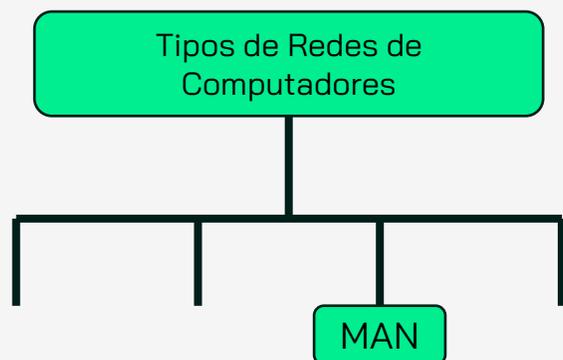
Exemplos:

Computadores dentro de uma empresa;

Computadores de uma escola;

Dispositivos em rede de uma casa

Porque estudar IP?



Metropolitan Area Network

São chamadas de redes MAN aquelas que pertencem dentro de uma área metropolitana. As redes MAN podem ser usadas para conectar várias redes LAN e permitir que pessoas de diferentes prédios se comuniquem e compartilhem recursos.

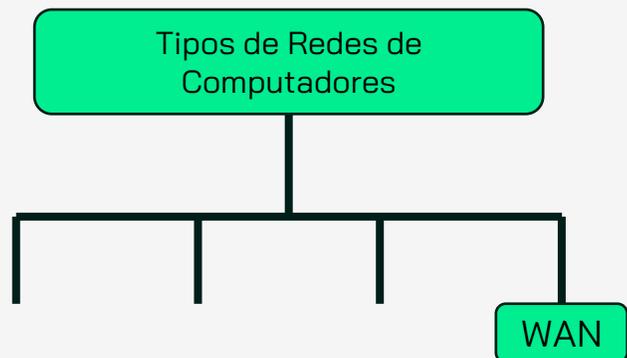
Exemplos:

Interligação de vários prédios em uma universidade;

Comunicação entre matriz e filial de uma empresa;

Redes de transporte público (coordenar e monitorar veículos em tempo real);

Porque estudar IP?



Wide Area Network

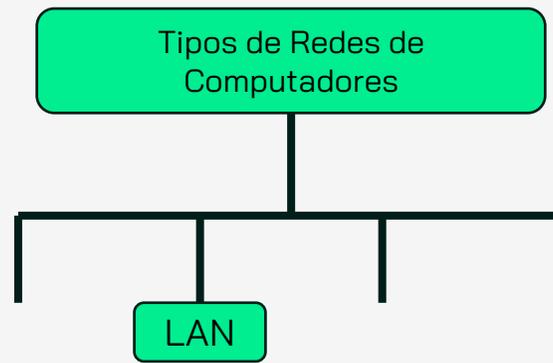
São chamadas de redes WAN, ou redes de longa distância aquelas que vão mais além da MAN e consegue abranger uma área maior (país, continente...).

Exemplos:

Interligação entre matriz e filiais espalhadas por estados ou países diferentes;

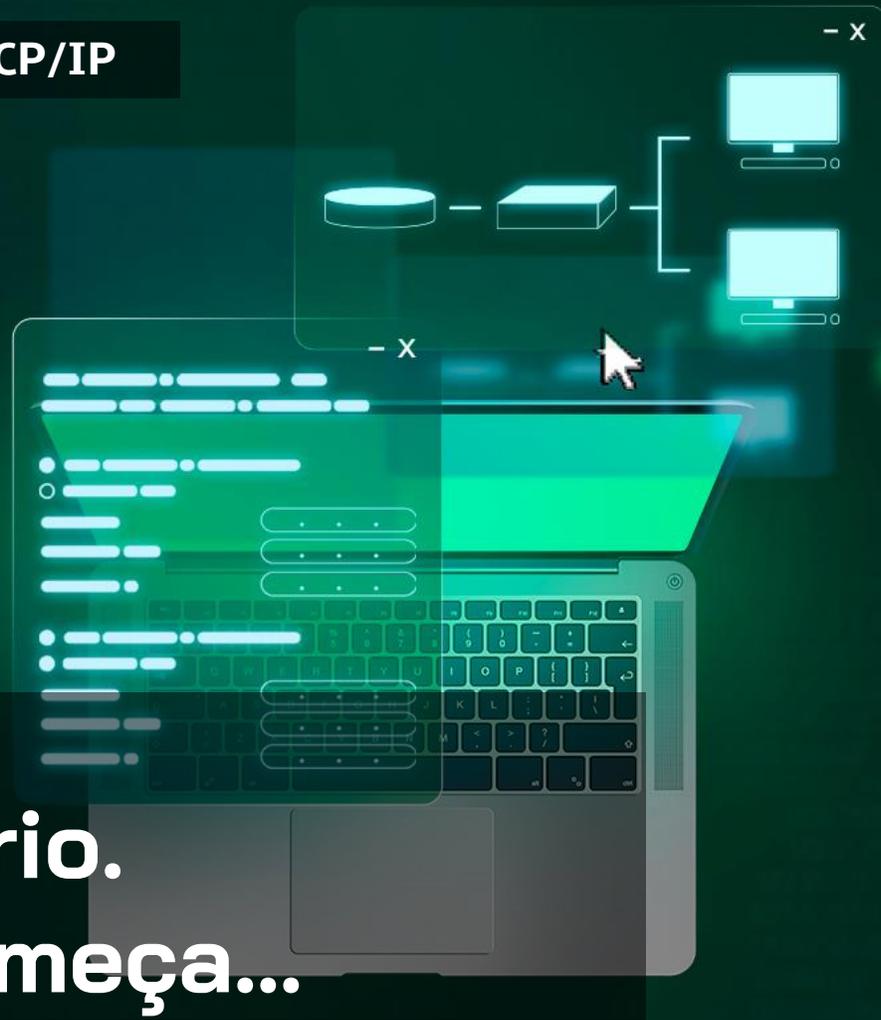
Internet é a maior WAN do mundo

Porque estudar IP?



Nesse curso de TCP/IP Básico vamos focar em redes LAN!

Módulo 01: Introdução ao TCP/IP



REDES

TCP /IP

AULA #2

Sistema Binário.

Onde tudo começa...

BÁSICO

Sistema Binário

Sistema decimal..
Tenho certeza que você conhece!

0 1 2 3 4 5 6 7 8 9



10 dígitos

Sistema Binário

E o sistema Binário?

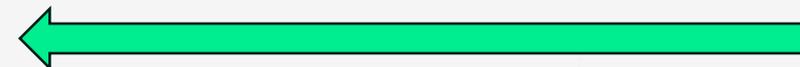
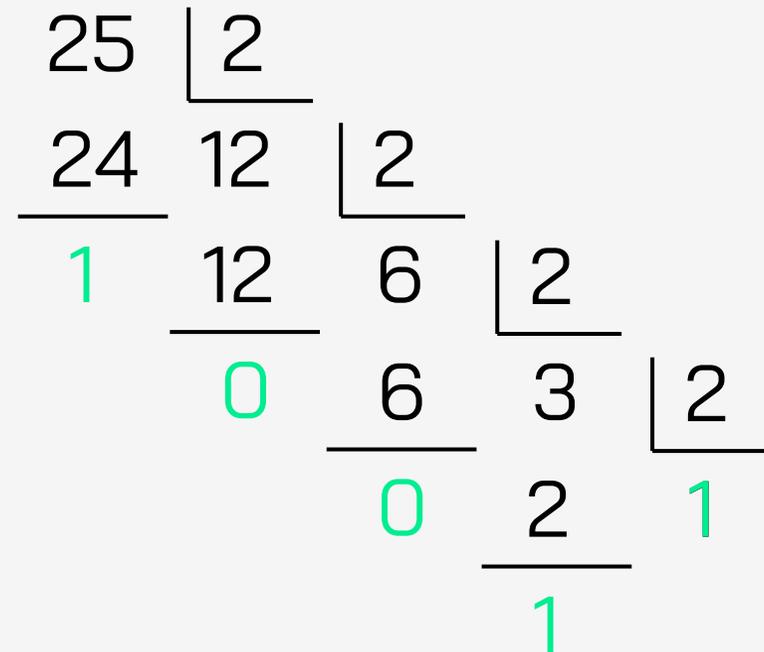


Sistema Binário

Entendendo a lógica...

Como converter o número 25 em binário?

11001



Sentido de leitura da representação binária

Sistema Binário

2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
512	256	128	64	32	16	8	4	2	1
					1	1	0	0	1

25 → 11001

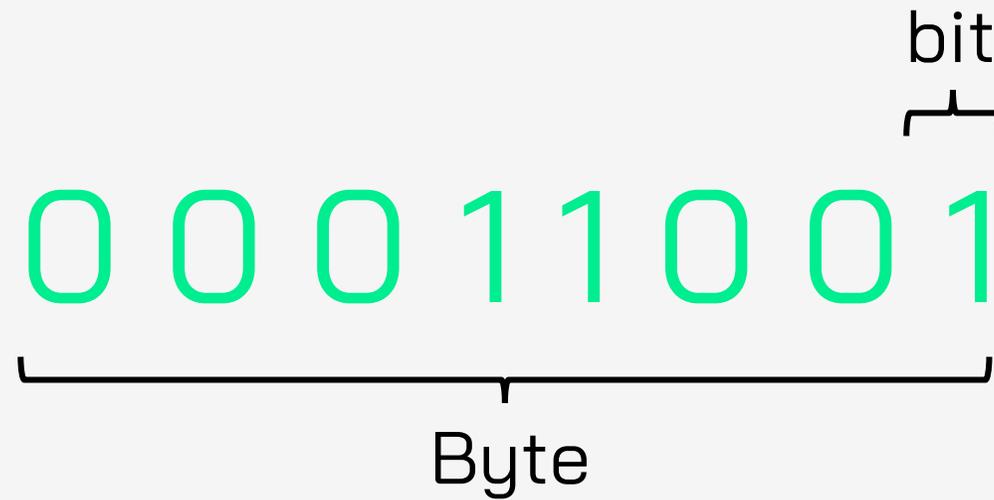
Sistema Binário

E porque eu preciso saber disso ???

- 1 – Os dispositivos processam bits
- 2 – Os pacotes de dados que são transmitidos são bits
- 3 – As unidades de medida são bits

Sistema Binário

bit e Byte



Sistema Binário

Unidades de medida

Para expressar o tamanho de arquivos, são utilizadas outras formas de representação, conforme abaixo:

- 1 Byte = 8 bits
- 1 Kilobyte (KB ou Kbytes) = 1024 bytes
- 1 Megabyte (MB ou Mbytes) = 1024 kilobytes
- 1 Gigabyte (GB ou Gbytes) = 1024 megabytes
- Existem também Terabyte (TB), Petabyte (PB), Exabyte (EB), Zettabyte (ZB) e o Yottabyte (YB).

Curiosidade: um arquivo de 1 gigabyte (GB) é igual a 8.589.934.592 bits

Sistema Binário

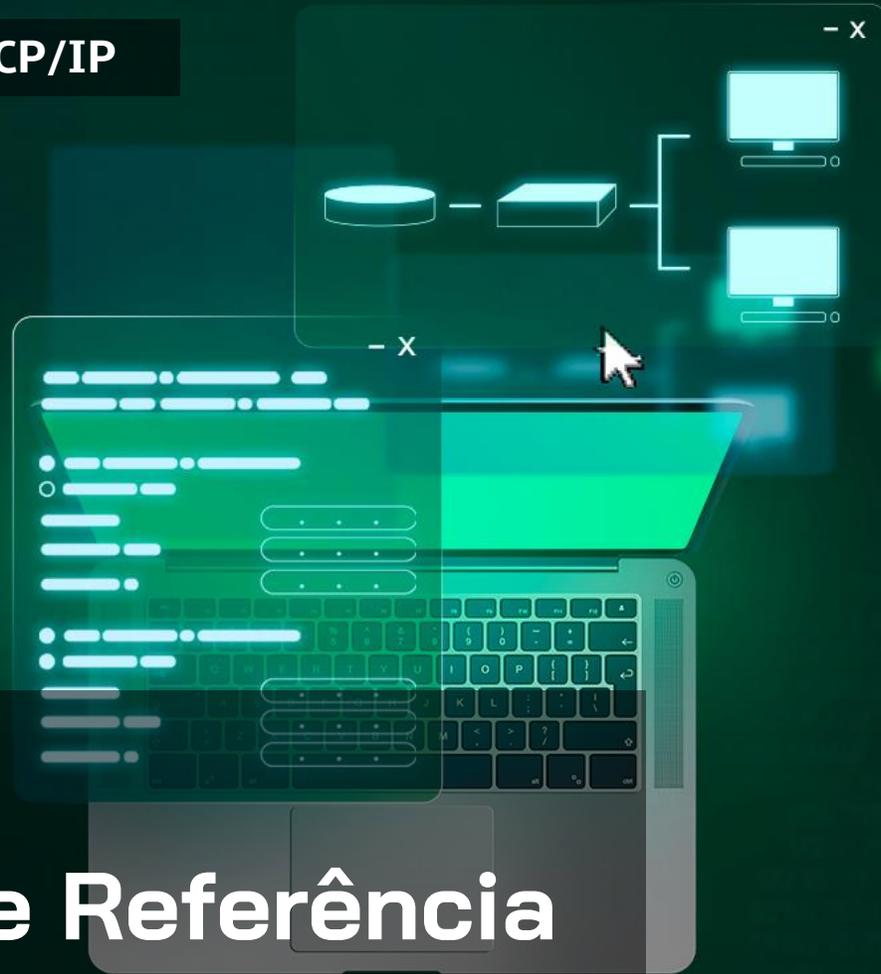
Velocidades

Em redes de Telecomunicações, as velocidades são descritas com taxas em bits, como por exemplo:

Internet de 100 mbps
100 mega bits por segundo
100.000.000 bits por segundo (100 milhões)

* Uma interface de rede ou um plano de 1Gbps por segundo transmite 1 bilhão de bits por segundo

Módulo 01: Introdução ao TCP/IP



REDES

TCP /IP

AULA #3
Modelo OSI de Referência

BÁSICO

Modelo OSI de Referência

Modelo OSI - Open Systems Interconnection

Criado pela International Organization for Standardization (ISO) em 1984.

O modelo OSI foi criado com o objetivo de padronizar a comunicação entre diferentes sistemas de computadores.

Antes de um modelo padrão para padronização, cada fabricante de equipamento de rede tinha sua própria forma de desenvolver e projetar seus sistemas. O que causava problemas de interoperabilidade entre equipamentos.

O modelo estabeleceu uma arquitetura para que equipamentos de fabricantes distintos pudessem se comunicar de forma padronizada.

Modelo OSI de Referência

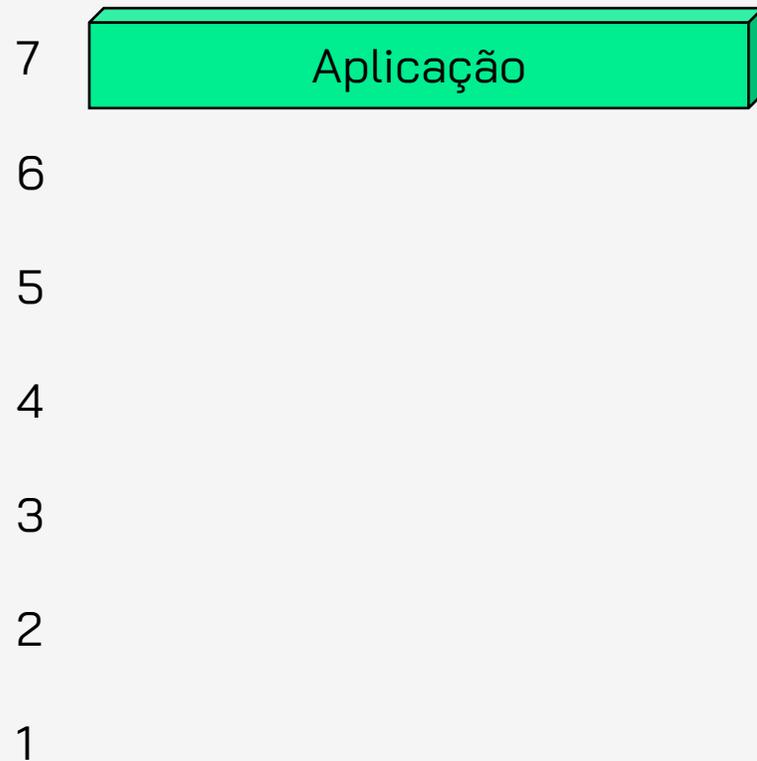
- "OSI: The Internet That Wasn't" de Glenn Kowack e Allan Leinwand
- "Computer Networks" de Andrew S. Tanenbaum
- "TCP/IP Illustrated, Volume 1: The Protocols" de W. Richard Stevens
- "Data and Computer Communications" de William Stallings
- "Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture" de Douglas E. Comer

Essas obras são consideradas referências importantes na área de redes de computadores e abrangem desde os fundamentos básicos até tópicos mais avançados sobre o modelo OSI e o protocolo TCP/IP.

Modelo OSI de Referência



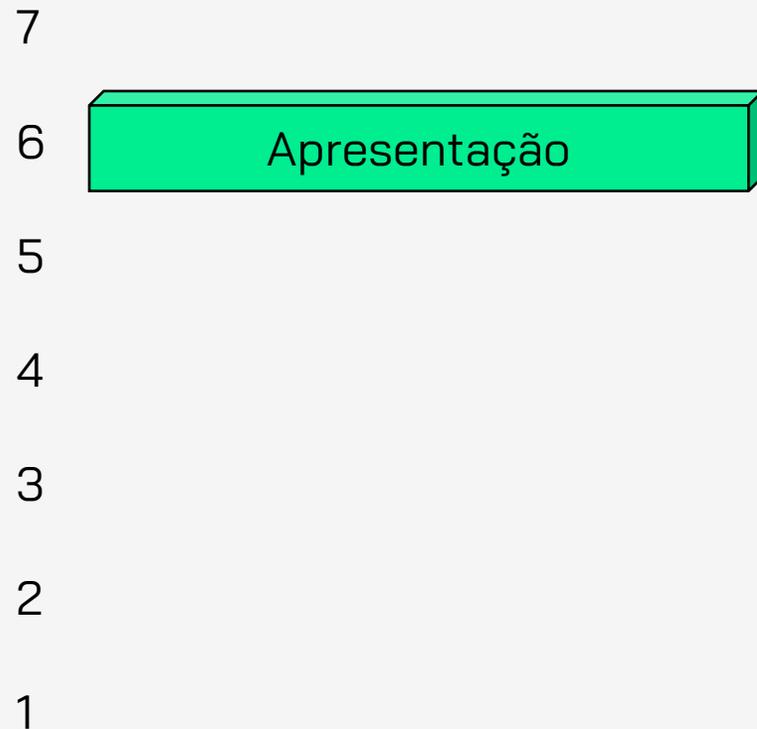
Modelo OSI de Referência



A camada de aplicação fornece serviços para aplicativos que utilizam a rede, como e-mail, transferência de arquivos, navegação na web, entre outros.

Ela permite que os aplicativos se comuniquem com outros dispositivos na rede e define os protocolos e formatos de dados utilizados para essa comunicação.

Modelo OSI de Referência



A camada de apresentação é responsável pela formatação dos dados para que possam ser interpretados corretamente pelo receptor.

Ela é responsável pela codificação e decodificação dos dados, compressão e criptografia.

Modelo OSI de Referência



A camada de sessão estabelece, gerencia e encerra conexões entre aplicativos em dispositivos diferentes. Ela fornece funções para controle de diálogo, para que as sessões de comunicação entre aplicativos possam ser estabelecidas e encerradas corretamente.

Modelo OSI de Referência



A camada de transporte fornece serviços de transferência de dados confiáveis entre aplicativos em diferentes dispositivos.

Ela garante que os dados sejam entregues na ordem correta, sem perda ou duplicação, e oferece funções de controle de fluxo e congestionamento para garantir uma transmissão suave dos dados.

Modelo OSI de Referência

7

6

5

4

3



2

1

A camada de rede é responsável pelo roteamento dos dados de um dispositivo para outro em uma rede.

Ela define os padrões para a criação de pacotes de dados, que contêm informações como o endereço de origem e destino, e gerencia o fluxo de tráfego de rede. Ela também fornece funções de controle de congestionamento para evitar que as redes fiquem sobrecarregadas.

Modelo OSI de Referência

7

6

5

4

3

2

1



A camada de enlace de dados fornece um serviço confiável de transmissão de dados de um dispositivo para outro em uma rede local.

Ela é responsável por dividir os dados recebidos em quadros (frames) e adicionar informações de controle para ajudar a detectar erros na transmissão. Ela também gerencia o acesso ao meio físico, para evitar colisões de dados entre dispositivos que compartilham o mesmo meio.

Modelo OSI de Referência

7

6

5

4

3

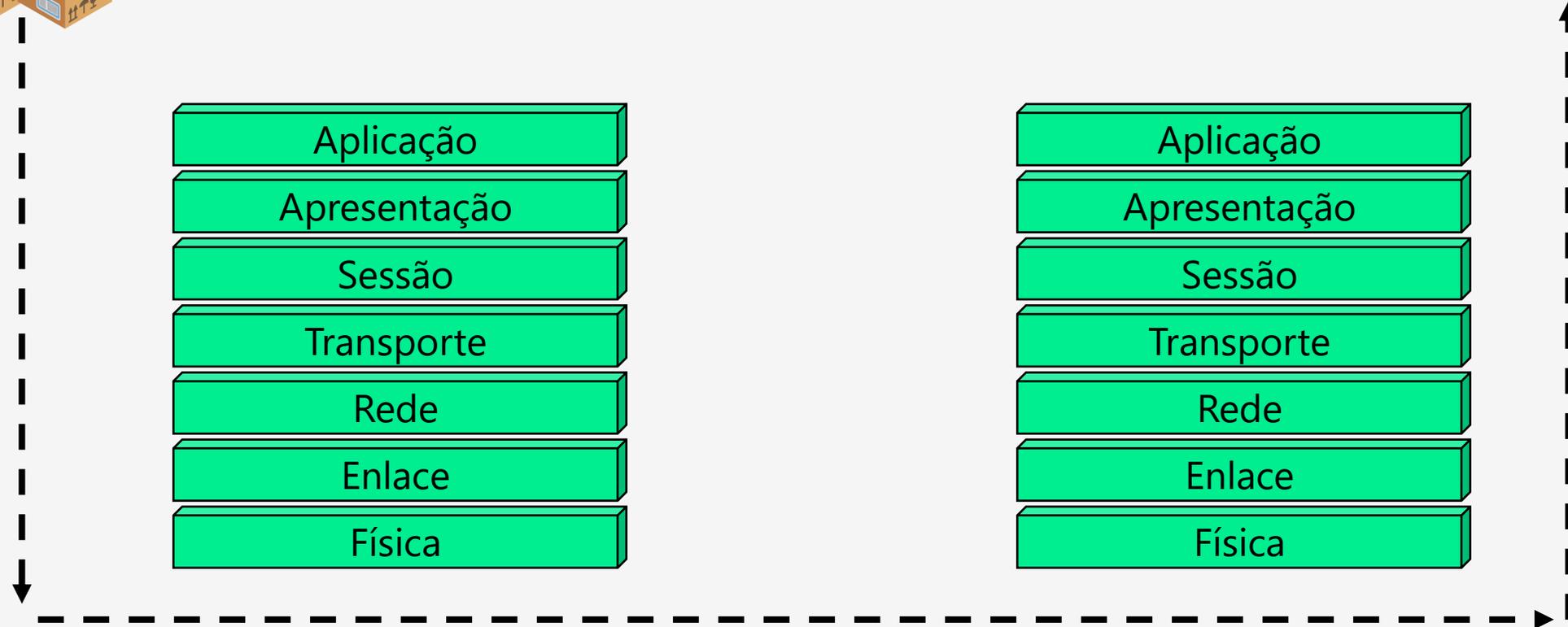
2

1



Esta camada é responsável pela transmissão de bits brutos de um dispositivo para outro através de um meio físico de comunicação, como cabos, fibra óptica ou ondas de rádio. Ela define os padrões para a transmissão de dados, como tensão elétrica, frequência, velocidade de transmissão e comprimento máximo do cabo.

Modelo OSI de Referência



Modelo OSI de Referência

Aplicação

As representações de dados são entregues às aplicações de destino, que interpretam e processam os dados de acordo com as suas necessidades

Apresentação

As sessões são encapsuladas em representações de dados, que podem ser formatadas e transformadas de acordo com as necessidades da aplicação.

Sessão

Os segmentos são encapsulados em sessões, que contêm informações sobre como estabelecer, manter e encerrar conexões entre as aplicações.

Transporte

Os pacotes são encapsulados em segmentos, contendo informações de portas de origem e destino, e outras informações necessárias para garantir que os dados sejam entregues corretamente.

Rede

Os frames são encapsulados em pacotes (datagramas) que contêm informações de endereçamento IP (IP de origem e destino) e outras informações necessárias para encaminhar os pacotes pela rede.

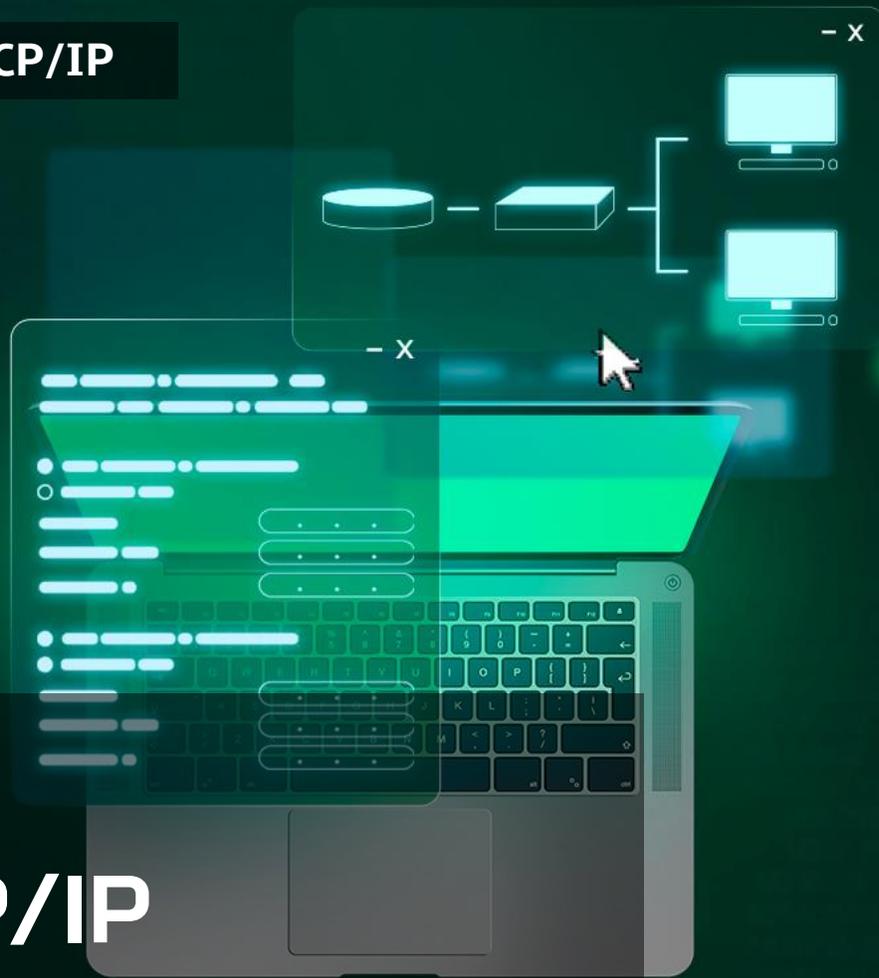
Enlace

Os bits são agrupados em frames (quadros) que possuem um cabeçalho e um rodapé. O cabeçalho contém informações sobre o endereço MAC do remetente e do destinatário.

Física

O dado é transmitido como uma sequência de bits (0's e 1's) através do meio físico, como cabos de cobre ou fibra ótica.

Módulo 01: Introdução ao TCP/IP



REDES

TCP /IP

AULA #4
Camadas TCP/IP

BÁSICO

Camadas TCP/IP

O TCP/IP foi desenvolvido pelo Departamento de Defesa dos EUA para especificar como os computadores transferem dados de um dispositivo para outro. O TCP/IP enfatiza muito a precisão e tem várias etapas para garantir que os dados sejam transmitidos corretamente entre os dois computadores.

Sua arquitetura foi desenvolvida na década de 1970

O objetivo de desenvolver um protocolo de comunicação confiável e robusto para conectar sistemas computacionais militares em uma rede descentralizada.

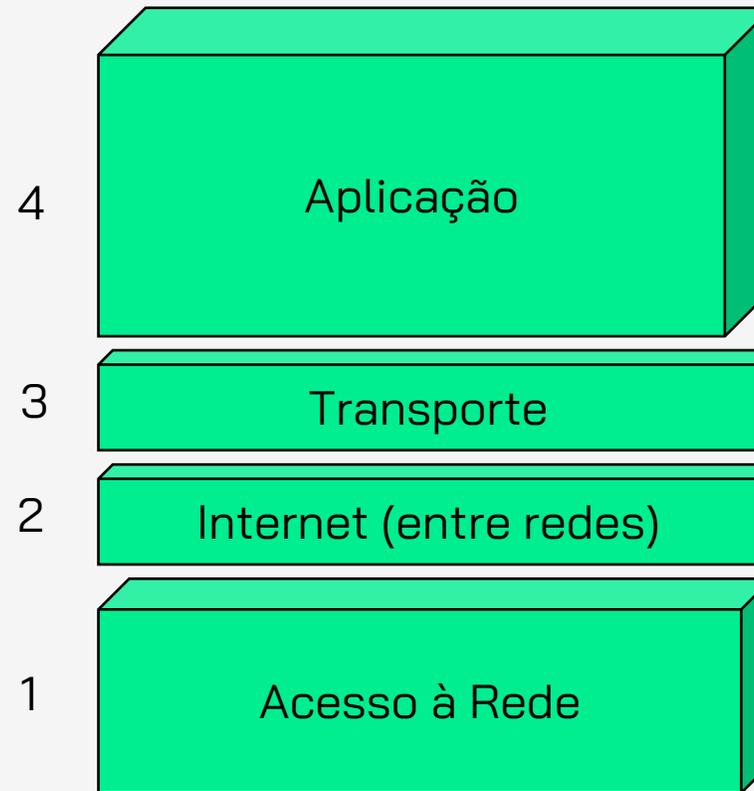
Com o tempo, o TCP/IP se tornou a base da Internet, permitindo que computadores em todo o mundo se comuniquem de forma padronizada e interconectada.

Camadas TCP/IP

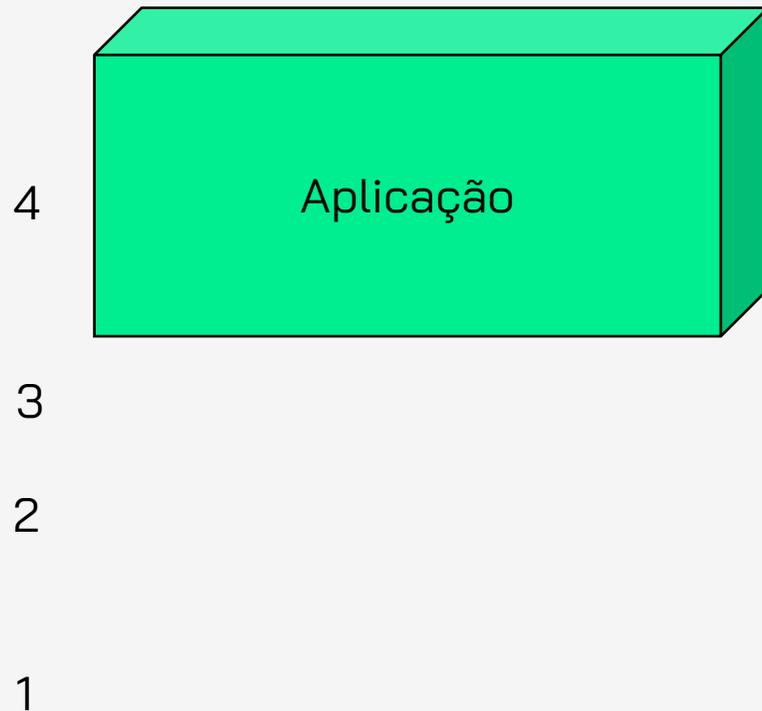
Modelo OSI



TCP/IP



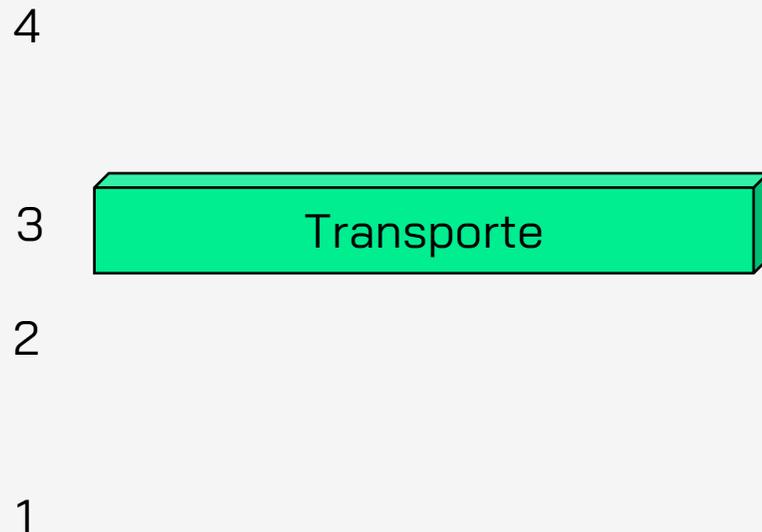
Camadas TCP/IP



Esta camada é responsável por fornecer serviços de rede às aplicações em execução nos dispositivos finais. Ela inclui uma grande variedade de protocolos que permitem que diferentes tipos de aplicações, como e-mail, navegação na web, compartilhamento de arquivos, entre outros, funcionem na rede.

Alguns protocolos comuns nesta camada são HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), DNS (Domain Name System), SMTP (Simple Mail Transfer Protocol), entre outros.

Camadas TCP/IP



Esta camada é responsável pela entrega confiável dos dados entre as aplicações em execução nos dispositivos finais.

Ela garante que os dados sejam entregues corretamente, sem perda ou corrupção, e no tempo necessário.

Os protocolos mais comuns nesta camada são TCP (Transmission Control Protocol), UDP (User Datagram Protocol), entre outros.

Camadas TCP/IP

4

3

2



1

Esta camada é responsável pelo roteamento de pacotes de dados na rede, ou seja, ela permite que um pacote de dados seja enviado de um ponto a outro da rede, independentemente das redes físicas subjacentes que conectam os dois pontos.

Os protocolos mais comuns nesta camada são IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), entre outros.

Camadas TCP/IP



Esta camada é responsável por lidar com os detalhes físicos da transmissão de dados, como o acesso à rede, a transmissão de sinais elétricos e a codificação de dados. Os protocolos mais comuns nesta camada são Ethernet, Wi-Fi, Bluetooth, Token Ring, entre outros.

Módulo 02: Endereçamento IPv4 e IPv6



REDES

TCP /IP

AULA #1
Endereçamento de IP

BÁSICO

Endereçamento de IP

Exemplo endereço IPv4

0.0.0.0
0.0.0.1
0.0.0.2
0.0.0.3
...
...
...
...
...
255.255.255.255

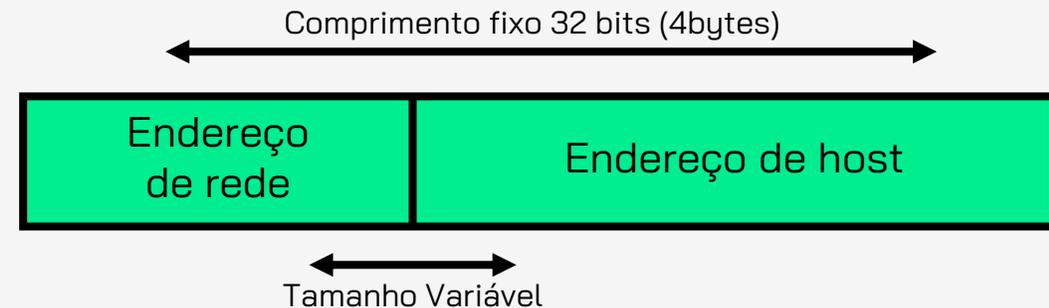
Endereçamento de IP

Exemplo endereço IPv4:
192.168.0.1

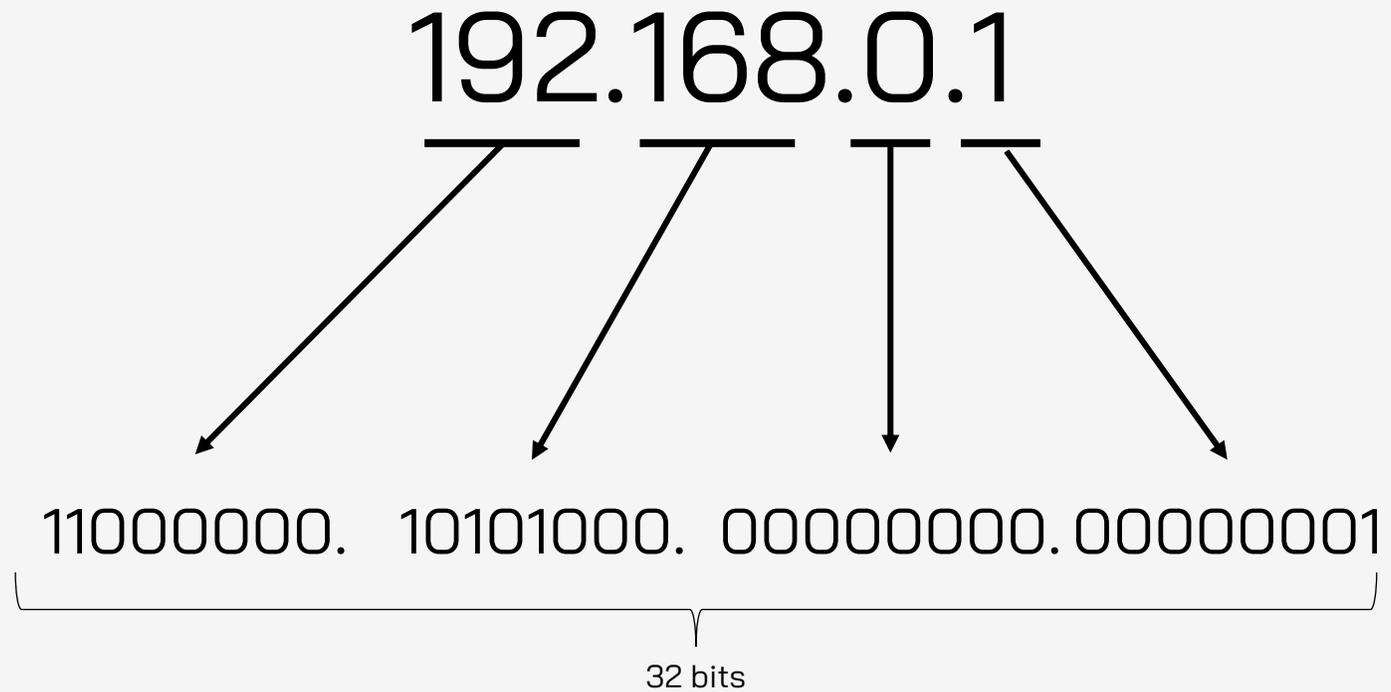
Forma Decimal
(mas computadores processam binário)



Estrutura endereço IPv4:



Endereçamento de IP



Menor endereço: 0.0.0.0
00000000.00000000.00000000.00000000

Maior endereço: 255.255.255.255
11111111.11111111.11111111.11111111

Endereçamento de IP

Divisão de endereços IP por classes:

CLASSE A: 0.0.0.0 até 127.255.255.255

CLASSE B: 128.0.0.0 até 191.255.255.255

CLASSE C: 192.0.0.0 até 223.255.255.255

CLASSE D: 224.0.0.0 até 239.255.255.255

CLASSE E: 240.0.0.0 até 247.255.255.255

Endereçamento de IP

IP Privado

São aqueles que são diretamente acessíveis apenas dentro da própria rede.

10.0.0.0 até 10.255.255.255

Eles não estão diretamente conectados a internet (ficam protegidos abaixo de roteadores e firewall).

172.16.0.0 até 172.31.255.255

Exemplo: 192.168.0.1

192.168.0.0 até 192.168.255.255

Endereçamento de IP

IP Público

Os endereços IP públicos são aqueles que podem ser acessados pela Internet pública e são exclusivos para cada dispositivo conectado à Internet. Esses endereços IP são fornecidos pelos provedores de serviços de Internet (ISPs) e estão disponíveis em quantidades limitadas.

Exemplo: 157.240.22.35 (facebook.com)

Endereçamento de IP

IPv4 -> IPv6

O IPv4 suporta cerca de **4,3 bilhões** de endereços IP únicos. Quantidade que é considerada baixa devido ao grande aumento de dispositivos conectados globalmente.

Em 2011 a IANA comunicou que haviam alocado o último bloco de endereços IPv4.

A IANA (Internet Assigned Numbers Authority) é uma organização responsável pela atribuição global de endereços IP, identificadores de protocolos, números de portas e outros parâmetros relacionados ao funcionamento da internet. A IANA é uma função desempenhada pela Internet Corporation for Assigned Names and Numbers (ICANN).

Endereçamento de IP

Entenda os números...

O IPv6 é como a quantidade de estrelas em nossa galáxia, a Via Láctea, que tem cerca de 400 bilhões de estrelas. Agora imagine 850 vezes mais estrelas do que isso - esse é o tamanho do IPv6.

O IPv6 é como a quantidade de grãos de areia em 36 praias, cada uma com 10 km de extensão. É difícil imaginar, mas é uma quantidade incrivelmente grande.

Endereçamento de IP

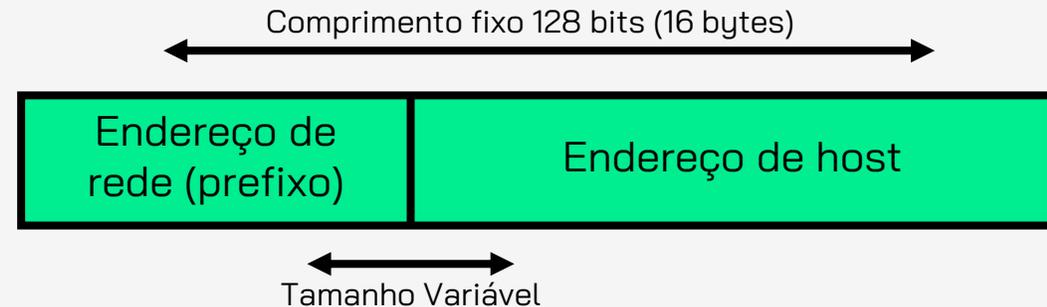
Exemplo endereço IPv6:

2a03:2880:f048:0011:face:b00c:0000:0002

Formato Hexadecimal
(mas computadores processam binário)



Estrutura endereço IPv6:



Endereçamento de IP

Exemplo endereço IPv6

2a03:2880:f048:0011:face:b00c:0000:0002

O IPv6 é representado em hexadecimal, que é um sistema de numeração com base 16. Ele utiliza 16 símbolos diferentes para representar valores de 0 a 15.

Decimal Hexadecimal

0	→	0
1	→	1
2	→	2
3	→	3
4	→	4
5	→	5
6	→	6
7	→	7
8	→	8
9	→	9
10	→	A
11	→	B
12	→	C
13	→	D
14	→	E
15	→	F

Endereçamento de IP

Exemplo Conversões

Decimal -> Hexadecimal

10 -> A

16 -> 10

22 -> 16

100 -> 64

25500 -> 639C

Decimal Hexadecimal

0	→	0
1	→	1
2	→	2
3	→	3
4	→	4
5	→	5
6	→	6
7	→	7
8	→	8
9	→	9
10	→	A
11	→	B
12	→	C
13	→	D
14	→	E
15	→	F

Endereçamento de IP

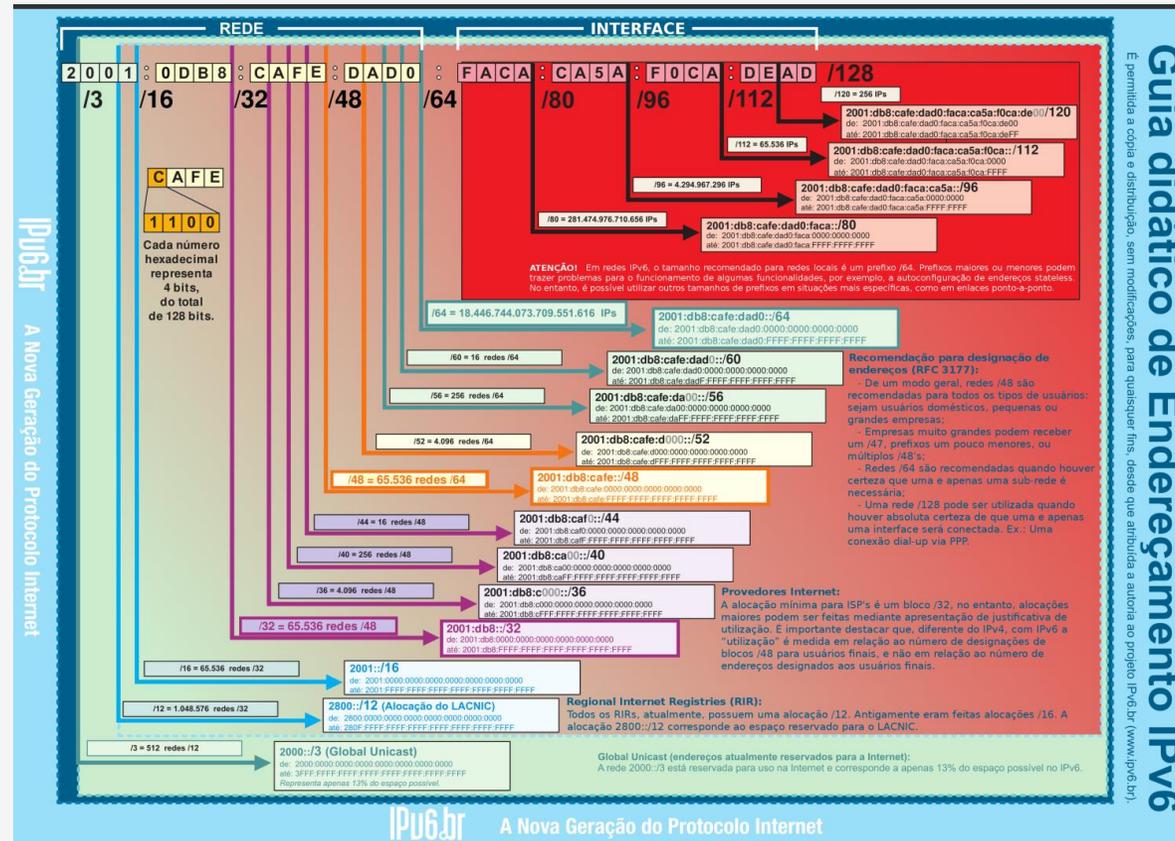
Exemplo endereço IPv6

2a03:2880:f048:0011:face:b00c:0000:0002



Endereçamento de IP

Guia IPv6 Elaborado pelo NIC.br



Guia didático de Endereçamento IPv6
É permitida a cópia e distribuição, sem modificações, para quaisquer fins, desde que atribuída a autoria ao projeto IPv6.br (www.ipv6.br).

<https://ipv6.br/media/arquivo/ipv6/file/46/enderec-v6.pdf>

Endereçamento de IP

O endereço MAC (Media Access Control)

É um identificador exclusivo de hardware atribuído a uma placa de rede ou adaptador de rede sem fio.

Composto por um conjunto de seis pares de caracteres hexadecimais, separados por dois pontos, e é usado para identificar dispositivos em uma rede local. Cada fabricante de hardware tem uma série de códigos de identificação exclusivos que são incorporados aos endereços MAC de seus produtos.

O endereço MAC é usado em conjunto com o protocolo ARP (Address Resolution Protocol) para permitir que um dispositivo na rede encontre e se comunique com outros dispositivos na mesma rede. Ao contrário do endereço IP, o endereço MAC é exclusivo para cada dispositivo e não pode ser alterado.

Endereçamento de IP

MAC Address

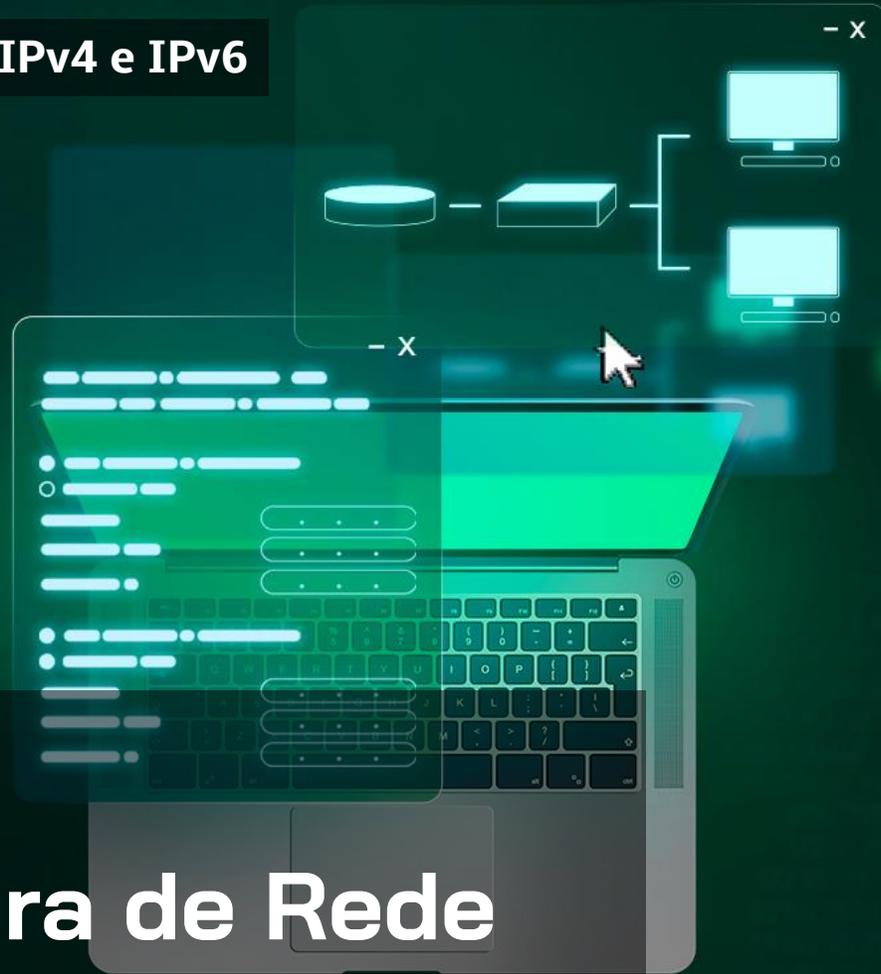
48 bits

98:83:89:CE:01:79

Identifica o fabricante
Organizationally Unique Identifier

Identifica a placa

Módulo 02: Endereçamento IPv4 e IPv6



REDES

TCP
/IP

AULA #2
CIDR e Máscara de Rede

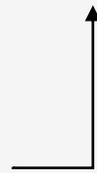
BÁSICO

CIDR e Máscara de Rede

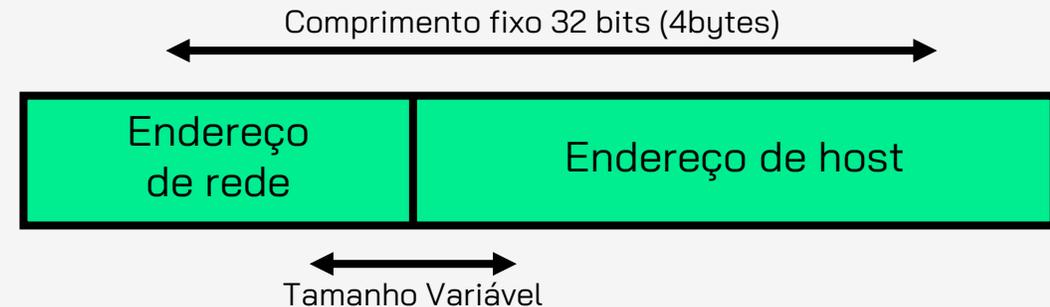
Lembra dessa aula???

Exemplo endereço IPv4:
192.168.0.1

Forma Decimal
(mas computadores processam
binário)

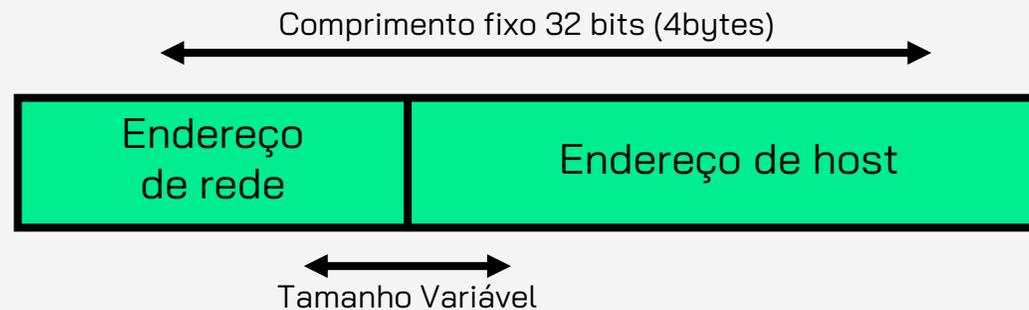


Estrutura endereço IPv4:



CIDR e Máscara de Rede

A máscara de rede é usada para determinar quais bits de um endereço IP pertencem à rede e quais bits pertencem ao host.



Pode ser chamada de duas formas:

Máscara de rede (Máscara de sub-rede)
CIDR (Classless Inter-Domain Routing)

OBS: Máscara também tem tamanho de 32 bits

CIDR e Máscara de Rede

Endereço IPv4



Máscara de rede



CIDR e Máscara de Rede

Endereço IPv4

11000000.10101000.00000000.00000001

192

168

0

1

Máscara de rede

11111111.11111111.11111111.00000000

255

255

255

0

CIDR e Máscara de Rede

Endereço IPv4: 11000000.10101000.00000000.00000001

Máscara de Rede: 11111111.11111111.11111111.00000000

Primeiro endereço IPv4 da Rede: 11000000.10101000.00000000.00000000

Último endereço IPv4 da Rede: 11000000.10101000.00000000.11111111

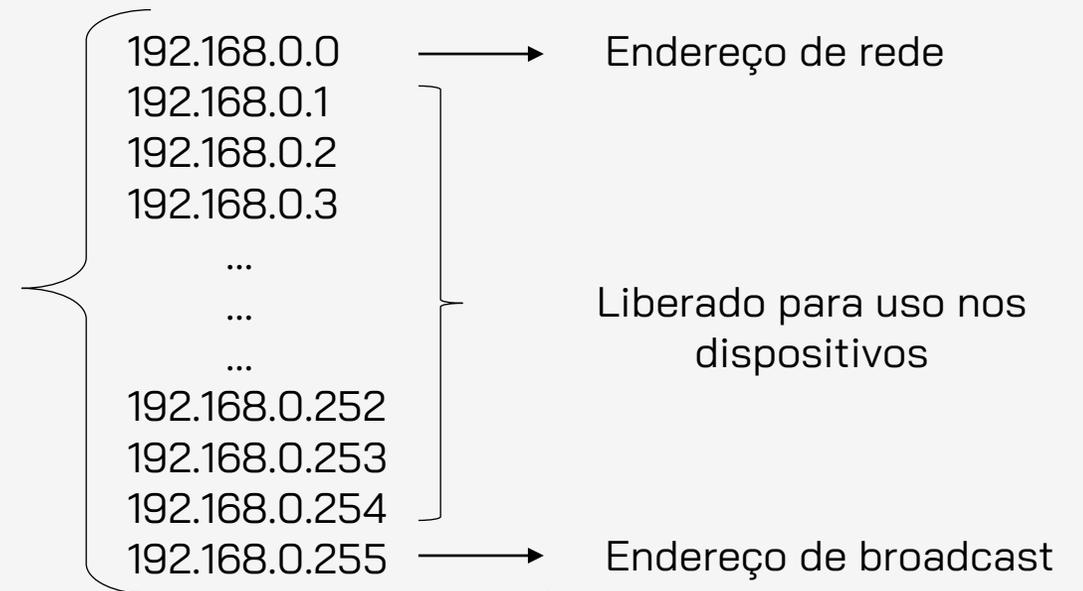
CIDR e Máscara de Rede

Endereço IPv4: 192.168.0.1

Máscara de Rede: 255.255.255.0

Primeiro endereço IPv4 da Rede: 192.168.0.0

Último endereço IPv4 da Rede: 192.168.0.255



CIDR e Máscara de Rede

Endereço IPv4

11000000.10101000.00000000.00000001

192

168

0

1

Máscara de rede

11111111.11111111.00000000.00000000

255

255

0

0

CIDR e Máscara de Rede

Endereço IPv4: 11000000.10101000.00000000.00000001

Máscara de Rede: 11111111.11111111.00000000.00000000

Primeiro endereço IPv4 da Rede: 11000000.10101000.00000000.00000000

Último endereço IPv4 da Rede: 11000000.10101000.11111111.11111111

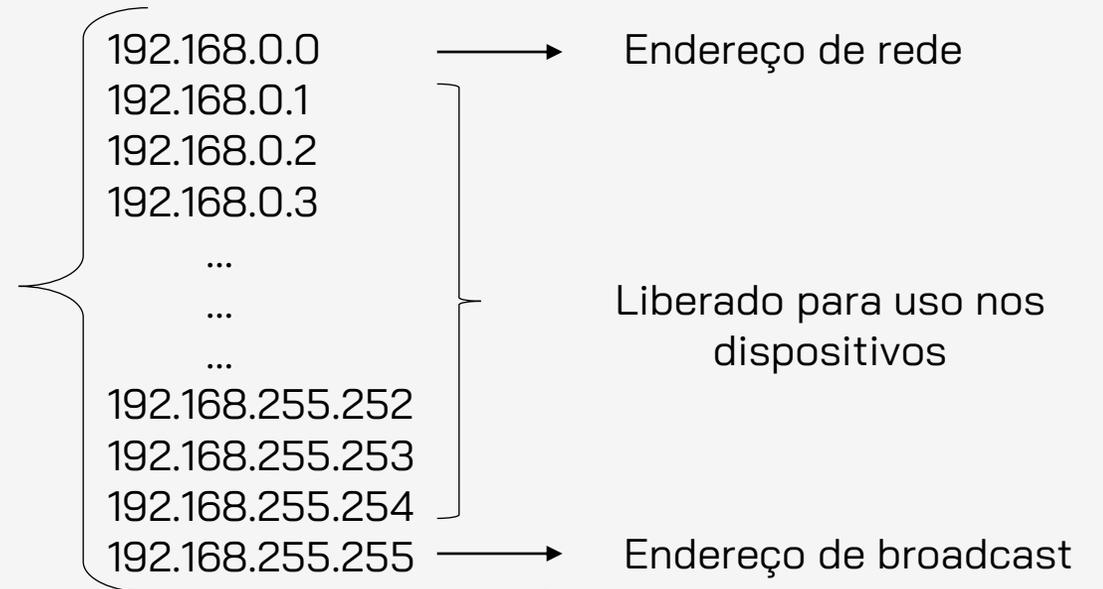
CIDR e Máscara de Rede

Endereço IPv4: 192.168.0.1

Máscara de Rede: 255.255.0.0

Primeiro endereço IPv4 da Rede: 192.168.0.0

Último endereço IPv4 da Rede: 192.168.255.255



CIDR e Máscara de Rede

CIDR - Classless Inter-Domain Routing

É um método de designação de endereços IP que utiliza uma notação que combina o endereço IP e a máscara de rede em um único valor, separados por uma barra.

Exemplo: 192.168.0.1/24

Isso significa que os 24 primeiros bits são usados para identificar a rede. Ou seja, dizer que o Endereço de IP 192.168.0.1 possui a máscara 255.255.255.0 é a mesma coisa que dizer que o Endereço de IP é 192.168.0.1/24.

Além de ser uma forma mais simplificada de representação, é uma forma mais eficiente dos equipamentos encaminharem as informações em uma rede.

CIDR e Máscara de Rede

Cálculo de Máscara de Rede

Isso não é algo que você vai aprender no curso básico. Pois criação de sub-redes geralmente são realizadas por Analistas de Redes, profissionais que operam no suporte N2 ou N3.

Você vai aprender sobre o cálculo nos cursos de TCP/IP Intermediário e TCP/IP Avançado.

Mas pra que você possa entender um pouco melhor, vou te apresentar duas calculadoras online pra cálculo de mascara de rede.

<https://www.site24x7.com/pt/tools/ipv4-sub-rede-calculadora.html>

<https://ip4calculator.com/>

CIDR e Máscara de Rede

IPv6

No IPv6 existe um prefixo. É uma notação similar à máscara de sub-rede do IPv4, na medida em que define a porção do endereço que identifica a rede e a porção que identifica o host.

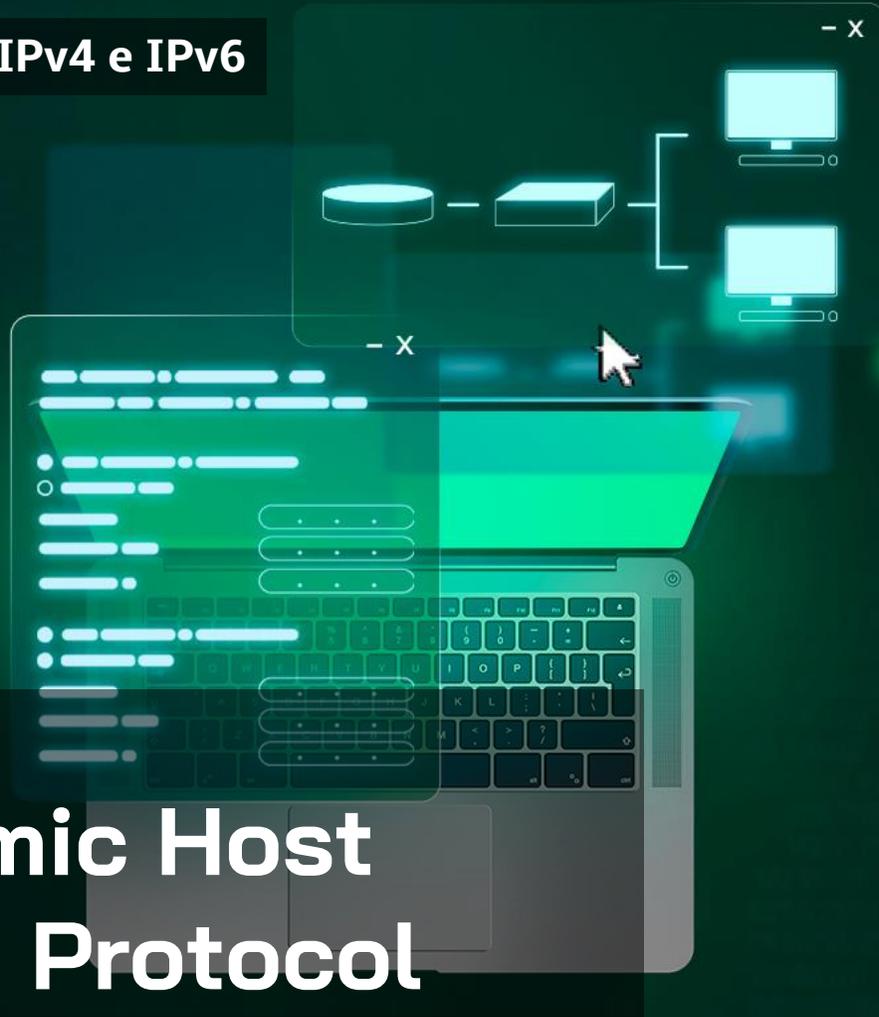
CIDR e Máscara de Rede

Cada provedor de internet (ISP) possui um bloco de endereços IPv6 designado a eles pela Autoridade de Atribuição de Números da Internet (IANA) ou por uma organização regional que coordena a distribuição de endereços IPv6.

Esse bloco de endereços é conhecido como Prefixo de Agregação Global (Globally Aggregated Prefix, GUA) e é usado para fornecer endereços IPv6 para seus clientes.

O ISP geralmente divide o GUA em vários prefixos menores para fornecer a seus clientes. Esses prefixos menores são conhecidos como Prefixos de Rede de Localização de Site (Site Local Network Prefixes, SLNP).

Módulo 02: Endereçamento IPv4 e IPv6



REDES

TCP
/IP

AULA #3

**DHCP - Dynamic Host
Configuration Protocol**

BÁSICO

DHCP - Dynamic Host Configuration Protocol

DHCP (Dynamic Host Configuration Protocol) é um protocolo de rede que permite que dispositivos obtenham automaticamente um endereço IP e outras informações de configuração de rede, como máscara de sub-rede, gateway padrão e servidores DNS, a partir de um servidor DHCP.

Quando um dispositivo se conecta a uma rede, ele envia uma solicitação de DHCP para o servidor DHCP, que responde com um endereço IP disponível na rede e outras informações de configuração. O servidor DHCP também pode fornecer um tempo de concessão, que é a quantidade de tempo que o dispositivo pode usar o endereço IP atribuído antes de precisar renovar a solicitação de DHCP.

O DHCP torna a configuração de rede mais fácil e eficiente, pois os dispositivos não precisam ser configurados manualmente com informações de rede, o que pode ser um processo demorado e propenso a erros. Além disso, o DHCP permite a alocação dinâmica de endereços IP, o que significa que os endereços IP são atribuídos apenas quando necessário, permitindo que a rede aproveite ao máximo o espaço de endereço disponível.

Módulo 03: Principais Protocolos e suas Camadas



REDES

TCP
/IP

AULA #1
Camada 7 - Aplicação

BÁSICO

Camada 7 - Aplicação



Esta camada é responsável pelas aplicações de rede que interagem diretamente com o usuário final.

- **HTTP:** Hypertext Transfer Protocol, usado para transferir dados na web, exemplo: navegação em sites usando um navegador web como o Google Chrome.
- **FTP:** File Transfer Protocol, usado para transferir arquivos pela internet, exemplo: transferência de arquivos de um servidor para um computador local usando programas de FTP como o FileZilla.
- **DNS:** Domain Name System, usado para resolver nomes de domínio em endereços IP, exemplo: quando você digita um endereço de site no navegador, o DNS converte o nome do site em um endereço IP para que a comunicação possa ocorrer.

Camada 7 - Aplicação



- **SMTP:** Simple Mail Transfer Protocol, usado para enviar e-mail, exemplo: envio de e-mails por meio de clientes de e-mail como o Microsoft Outlook ou o Gmail.
- **POP:** Post Office Protocol, usado para recuperar e-mail de um servidor de e-mail, exemplo: recuperação de e-mails em um cliente de e-mail como o Microsoft Outlook ou o Thunderbird.
- **IMAP:** Internet Message Access Protocol, usado para sincronizar e-mails entre servidores e dispositivos, exemplo: sincronização de e-mails em vários dispositivos, como telefone celular, tablet e computador usando um cliente de e-mail.

Camada 7 - Aplicação



- **Telnet:** Telecommunication Network, usado para acesso remoto a um servidor ou dispositivo, exemplo: acesso a um roteador ou servidor usando um cliente Telnet.
- **SSH:** Secure Shell, usado para acesso remoto seguro a um servidor ou dispositivo, exemplo: acesso a um servidor usando um cliente SSH como o PuTTY.
- **SNMP:** Simple Network Management Protocol, usado para gerenciamento de rede, exemplo: monitoramento de dispositivos de rede, como roteadores e switches, usando ferramentas de gerenciamento de rede.

Módulo 03: Principais Protocolos e suas Camadas



REDES

TCP
/IP

AULA #2

Camada 6 - Apresentação

BÁSICO

Camada 6 - Apresentação



Esta camada é responsável pela conversão de dados entre o formato utilizado pela rede e o formato utilizado pelo aplicativo. Ela realiza funções como criptografia, compressão e codificação de caracteres.

SSL (Secure Sockets Layer) e TLS (Transport Layer Security) são protocolos de segurança da camada de transporte que fornecem autenticação, integridade e confidencialidade para as comunicações na internet. Alguns exemplos de aplicação desses protocolos são:

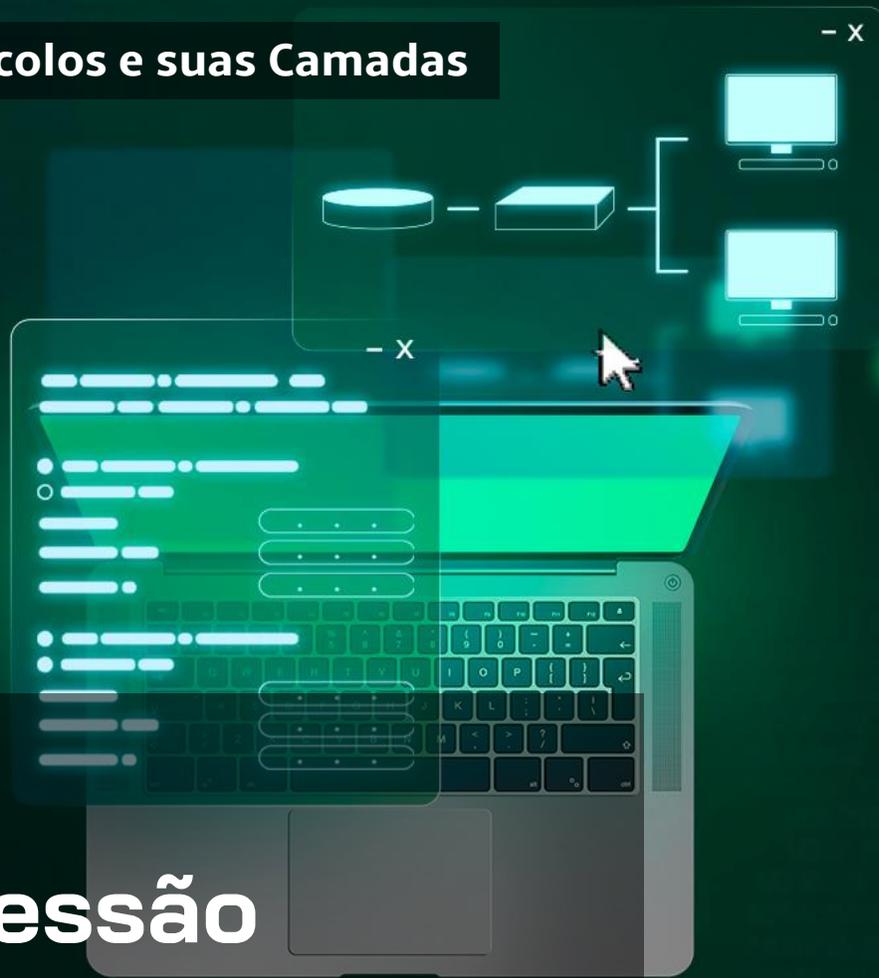
Camada 6 - Apresentação



SSL: Utilizado para proteger as comunicações entre clientes e servidores web em transações financeiras, comércio eletrônico, e-mail, redes privadas virtuais (VPN), entre outros.

TLS: Sucessor do SSL, é amplamente utilizado em serviços de e-mail, mensagens instantâneas, VPNs, e-commerce e outras aplicações para garantir a segurança das transações e comunicações online.

Módulo 03: Principais Protocolos e suas Camadas



REDES

TCP
/IP

AULA #3

Camada 5 - Sessão

BÁSICO

Camada 5 - Sessão



A camada de sessão é responsável pelo estabelecimento, manutenção e término de sessões de comunicação entre dois dispositivos.

A sessão é uma conexão lógica entre duas aplicações que estão em execução em dois dispositivos diferentes. A camada de sessão é responsável por controlar o acesso a essa conexão, garantindo que as informações enviadas por uma aplicação sejam entregues corretamente à outra aplicação, além de controlar a sincronização e a troca de dados entre as aplicações.

Camada 5 - Sessão



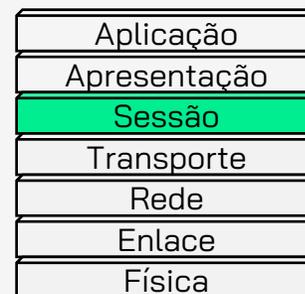
A camada de sessão do modelo OSI não possui protocolos específicos.

Ao invés disso, ela fornece serviços e mecanismos para que as aplicações possam estabelecer, manter e encerrar sessões de comunicação.

Alguns exemplos desses serviços incluem:

- Estabelecimento de conexão
- Autenticação e autorização
- Gerenciamento de sessão
- Sincronização de dados

Camada 5 - Sessão



Mas em algumas literaturas definem que alguns protocolos de aplicação podem incluir funcionalidades da camada de sessão, como o SSH (Secure Shell), que fornece recursos de autenticação e criptografia de dados, além de estabelecer uma sessão segura entre duas máquinas.

Um outro exemplo é o protocolo NetBIOS (NetBIOS Enhanced User Interface). Trata-se de uma tecnologia de rede de computadores desenvolvida pela IBM na década de 1980. Ele é usado para permitir que computadores em uma rede local se comuniquem uns com os outros.

Módulo 03: Principais Protocolos e suas Camadas



REDES

TCP
/IP

AULA #4
Camada 4 - Transporte

BÁSICO

Camada 4 – Transporte

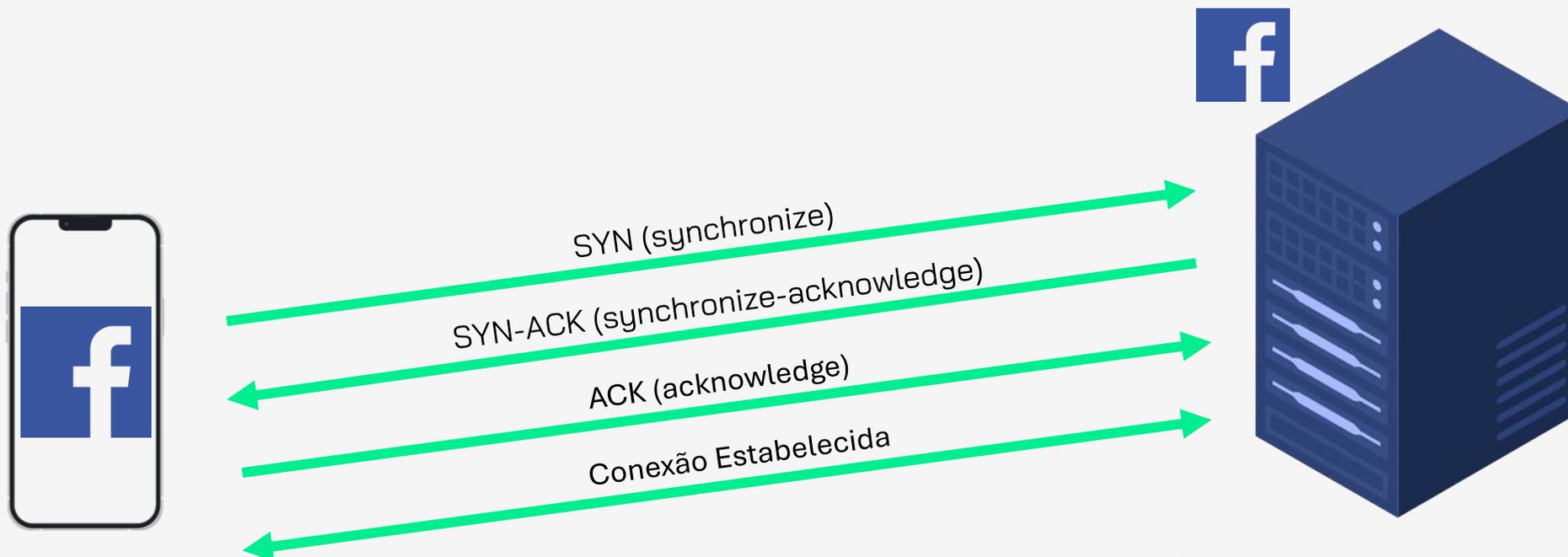


Esta camada é responsável pela entrega confiável de dados entre dispositivos de rede. Ela define protocolos como TCP (Transmission Control Protocol) e UDP (User Datagram Protocol), que fornecem serviços de transporte fim a fim.

Camada 4 – Transporte

- TCP – Transmission Control Protocol

Orientado a conexão (é criando uma conexão através do handshake)
Confiável (existe uma confirmação do recebimento dos dados)
Desvantagem: nível de complexibilidade maior, maior processamento



Camada 4 – Transporte

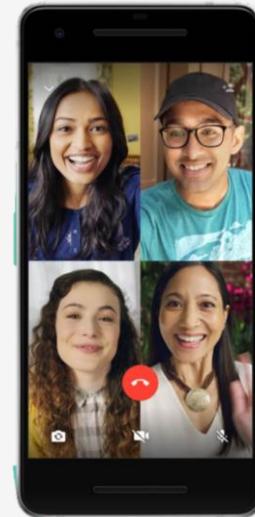


- UDP – User Datagram Protocol

Sem conexão

Não confiável

Vantagem: menor complexibilidade, menor processamento



Módulo 03: Principais Protocolos e suas Camadas



REDES

TCP
/IP

AULA #5
Camada 3 - Rede

BÁSICO

Camada 3 - Rede



A camada de rede é a terceira camada do modelo OSI, responsável pela entrega de pacotes de dados de origem para destino final em uma rede de computadores. É responsável pela criação de rotas de comunicação, possibilitando a interconexão de redes diferentes e a transmissão de dados em redes locais e remotas.

Algumas das principais funções da camada de rede incluem:

- Endereçamento lógico: cada dispositivo em uma rede recebe um endereço lógico único, que é usado para identificar o dispositivo na rede. O protocolo mais comum utilizado para endereçamento na camada de rede é o protocolo IP (Internet Protocol).

Camada 3 - Rede



- Roteamento: a camada de rede é responsável por escolher o melhor caminho para que os dados possam chegar ao destino final. Essa escolha é feita através de algoritmos de roteamento, que podem levar em consideração fatores como o número de saltos, a largura de banda disponível e o congestionamento da rede.
- Fragmentação e remontagem: quando um pacote de dados é muito grande para ser transmitido em uma única transmissão, a camada de rede é responsável por fragmentá-lo em pacotes menores para que possam ser transmitidos com sucesso. Na chegada, a camada de rede é responsável por remontar esses pacotes em sua forma original.
- Controle de congestionamento: a camada de rede é responsável por controlar a quantidade de tráfego de dados que está sendo transmitido em uma rede, a fim de evitar congestionamento e garantir um bom desempenho.

Camada 3 - Rede



- **IPv4 (Internet Protocol version 4):** Protocolo mais usado na Internet para roteamento de pacotes de dados entre dispositivos em redes diferentes.
- **IPv6 (Internet Protocol version 6):** Versão mais recente do protocolo IP, desenvolvido para substituir o IPv4 e ampliar a capacidade de endereçamento da Internet.
- **ICMP (Internet Control Message Protocol):** Protocolo usado para relatar erros e outras informações de controle em redes IP.

Camada 3 - Rede



- **IGMP (Internet Group Management Protocol):** Protocolo usado para gerenciar grupos de multicast em redes IP.
- **OSPF (Open Shortest Path First):** Protocolo de roteamento interno usado em redes IP que determina a melhor rota para um pacote de dados dentro de uma rede.
- **BGP (Border Gateway Protocol):** Protocolo de roteamento externo usado para roteamento entre redes autônomas (AS) na Internet.

Camada 3 - Rede



- **RIP (Routing Information Protocol):** Protocolo de roteamento interno usado em redes IP que determina a melhor rota para um pacote de dados dentro de uma rede baseado na distância.
- **IS-IS (Intermediate System to Intermediate System):** Protocolo de roteamento usado em grandes redes IP, como redes corporativas e provedores de serviços de Internet.

Módulo 03: Principais Protocolos e suas Camadas



REDES

TCP
/IP

AULA #6
Camada 2 - Enlace

BÁSICO

Camada 2 - Enlace



É responsável pela comunicação entre dispositivos em uma mesma rede física. Seu objetivo principal é garantir que os dados sejam transmitidos de forma confiável e eficiente do nó de origem para o nó de destino.

Algumas das principais funções da camada de enlace são:

Enquadramento: é o processo de dividir os dados recebidos da camada superior em quadros (frames) que possam ser transmitidos pela rede. Cada quadro contém informações de controle, como endereços de origem e destino, sequência de quadros e detecção de erros.

Camada 2 - Enlace



Controle de acesso ao meio (MAC): é o conjunto de regras que determinam como os dispositivos compartilham o meio físico de comunicação, garantindo que somente um dispositivo transmita por vez para evitar colisões de dados.

Detecção e correção de erros: a camada de enlace verifica se os quadros recebidos contêm erros e, se necessário, faz correções antes de repassá-los para a camada superior.

Endereçamento físico: cada dispositivo de rede possui um endereço físico exclusivo, conhecido como endereço MAC, que é utilizado pela camada de enlace para identificar os dispositivos na rede.

Camada 2 - Enlace



- **Ethernet:** protocolo de rede mais usado atualmente em redes locais (LANs). Ele permite a transmissão de dados em velocidades que variam de 10 Mbps a 100 Gbps.
- **Wi-Fi (IEEE 802.11):** protocolo usado em redes sem fio, que permite a conexão de dispositivos móveis, como smartphones, tablets e laptops.
- **PPP (Point-to-Point Protocol):** protocolo utilizado para estabelecer uma conexão ponto a ponto entre dois dispositivos, geralmente utilizado para conexões discadas de internet.
- **ARP (Address Resolution Protocol):** protocolo de camada de enlace que tem como objetivo mapear endereços IP em endereços MAC (Media Access Control) de dispositivos em uma rede local

Módulo 03: Principais Protocolos e suas Camadas



REDES

TCP /IP

AULA #7

Camada 1 - Física

BÁSICO

Camada 1 - Física



A camada física é a primeira camada do modelo OSI, responsável pela transmissão dos bits brutos em um meio de transmissão. Ela define as características físicas do meio de transmissão, como a voltagem dos sinais elétricos, o tipo de cabo ou fibra óptica utilizado, a taxa de transmissão de dados, entre outros.

A camada física atua diretamente com os dispositivos de rede, como cabos, conectores, interfaces de rede e modems, e é responsável pela transformação dos dados em sinais elétricos, ópticos ou eletromagnéticos que são transmitidos através do meio físico.

Camada 1 - Física



- **Ethernet:** tecnologia de rede com fio que utiliza cabos de cobre para transmitir dados em altas velocidades.
- **Wi-Fi:** tecnologia de rede sem fio que utiliza ondas de rádio para transmitir dados entre dispositivos.
- **Bluetooth:** tecnologia de rede sem fio de curto alcance que permite a conexão de dispositivos como fones de ouvido, teclados e mouses.
- **3G/4G/5G:** tecnologias de comunicação móvel que utilizam ondas de rádio para transmitir dados entre dispositivos e torres de celular.
- **Fibra óptica:** tecnologia de transmissão de dados que utiliza feixes de luz para transmitir informações através de cabos de fibra óptica.

Módulo 03: Principais Protocolos e suas Camadas



REDES

TCP
/IP

AULA #8

**Conceitos Intermediários que
você precisa aprender no básico**

BÁSICO

Conceitos intermediários que você precisa aprender no Básico

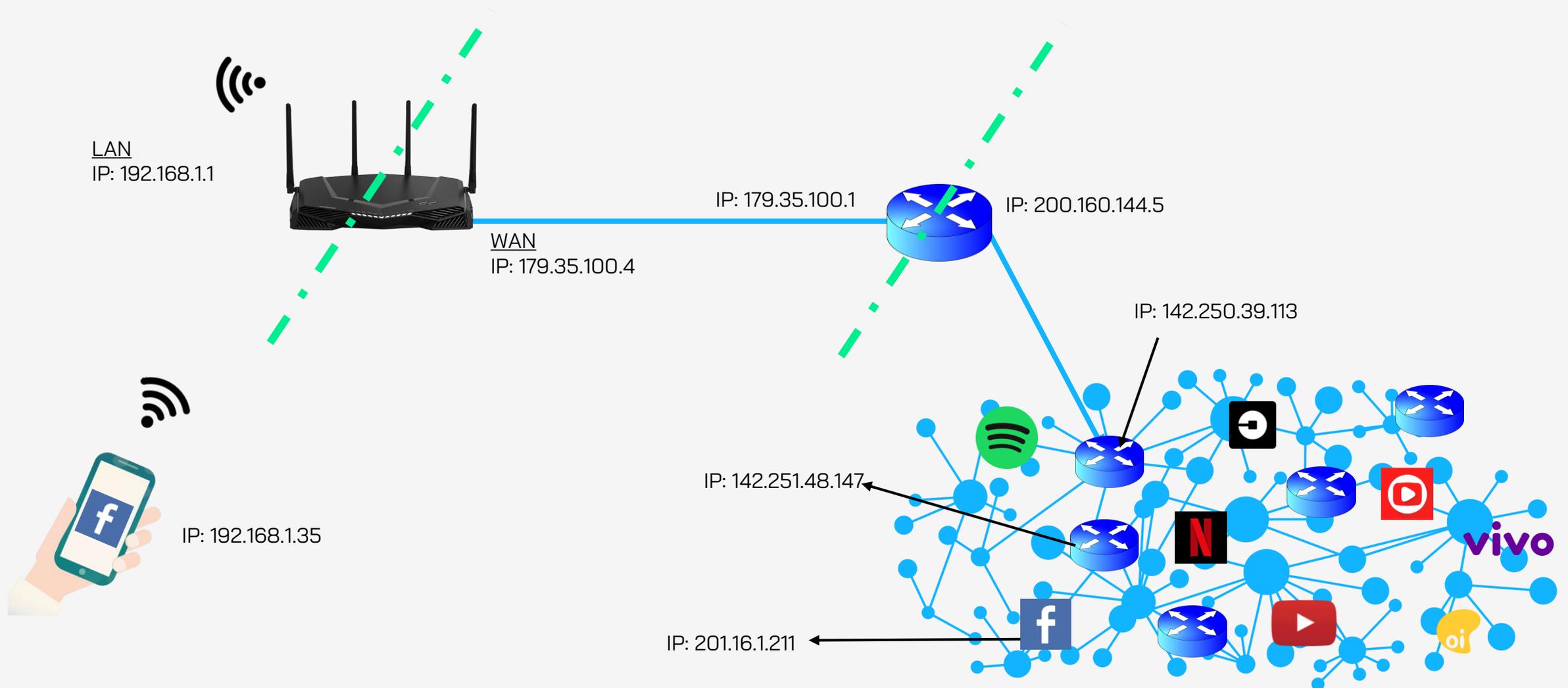
Gateway

Um gateway de rede é um dispositivo que atua como um ponto de entrada ou saída entre duas redes diferentes. Ele pode ser físico, como um roteador, ou lógico, como um software que executa funções de roteamento.

Em uma rede local (LAN), um gateway geralmente é um roteador que conecta a LAN à Internet ou a outra rede externa. O gateway é responsável por encaminhar o tráfego de rede entre as duas redes e também por realizar funções como a tradução de endereços de rede e a filtragem de pacotes.

É aqui no gateway que acontece a interligação entre a LAN e a WAN.

Conceitos intermediários que você precisa aprender no Básico



Conceitos intermediários que você precisa aprender no Básico

Firewall

Firewall é um dispositivo de segurança usado para monitorar e controlar o tráfego de rede. Ele é projetado para proteger uma rede contra acesso não autorizado ou indesejado, evitando que malware, hackers ou outros tipos de ameaças prejudiquem a rede.

Um firewall pode ser implementado como um dispositivo físico, como um roteador, ou como um software em um servidor. Ele trabalha filtrando o tráfego de rede, analisando o conteúdo de cada pacote que passa por ele e bloqueando o tráfego que não atende aos critérios de segurança pré-definidos.

O objetivo principal do firewall é garantir a segurança da rede, protegendo-a contra ataques externos e internos. Ele é uma peça fundamental na arquitetura de segurança de uma rede e pode ajudar a manter a confidencialidade, integridade e disponibilidade dos dados que circulam na rede.

Conceitos intermediários que você precisa aprender no Básico

O NAT (Network Address Translation)

Opera na camada de rede (camada 3) do modelo OSI. O NAT é um mecanismo utilizado para permitir que vários dispositivos em uma rede privada compartilhem um único endereço IP público para se comunicar na Internet.

Começou a ser amplamente utilizado na década de 2000. A ideia básica por trás do NAT já existia antes, mas o conceito moderno de NAT foi desenvolvido para ajudar a lidar com a escassez de endereços IPv4.

Conceitos intermediários que você precisa aprender no Básico

Ele funciona modificando o endereço de origem dos pacotes de rede que saem da rede privada e substituindo-o pelo endereço IP público do roteador de rede. Isso permite que os dispositivos privados se comuniquem com dispositivos em outras redes públicas, como a Internet, enquanto mantém sua identidade privada.

No processo inverso, quando a informação retornar, o NAT é responsável em de encaminhar a informação para a origem inicial, alterando o endereço de destino final para a origem inicial. Para o usuário esse processo é transparente.

Conceitos intermediários que você precisa aprender no Básico

Portas de Rede

As portas de acesso, ou portas de rede, são uma forma de identificar processos ou aplicativos que estão em execução em um dispositivo conectado à rede. Cada processo ou aplicativo é atribuído a uma porta específica, que permite que os pacotes de dados enviados pela rede cheguem ao destino correto.

As portas de acesso são identificadas por números de 16 bits que variam de 0 a 65535. As portas abaixo de 1024 são consideradas portas conhecidas e são geralmente reservadas para serviços padrão, como HTTP (porta 80) e FTP (porta 21). As portas acima de 1024 são consideradas portas dinâmicas ou privadas e podem ser atribuídas a processos ou aplicativos conforme necessário.

Conceitos intermediários que você precisa aprender no Básico

Quando um dispositivo de rede envia um pacote de dados, ele inclui o endereço IP do destino e o número da porta para garantir que o pacote chegue ao processo ou aplicativo correto. O firewall ou o roteador podem ser configurados para bloquear ou permitir o tráfego com base no número da porta.

Em resumo, as portas de acesso permitem que os processos e aplicativos identifiquem e recebam dados na rede, e o número da porta é usado para garantir que o tráfego de dados seja enviado e recebido pelo processo ou aplicativo correto.

Conceitos intermediários que você precisa aprender no Básico

VLAN (Virtual Local Area Network)

O conceito de virtualização é criar uma estrutura virtual que opere dentro de uma estrutura física, compartilhando recursos, otimizando processos e tornando escalável. Falando em redes LAN, tratase de uma rede LAN virtual que opera dentro de uma LAN.

Dependendo da configuração realizada, uma rede física pode possuir várias rede virtuais. Nesse caso, o meio físico da rede é compartilhado, mas toda a parte lógica não.

VLAN opera na camada 2 do modelo OSI (Rede).

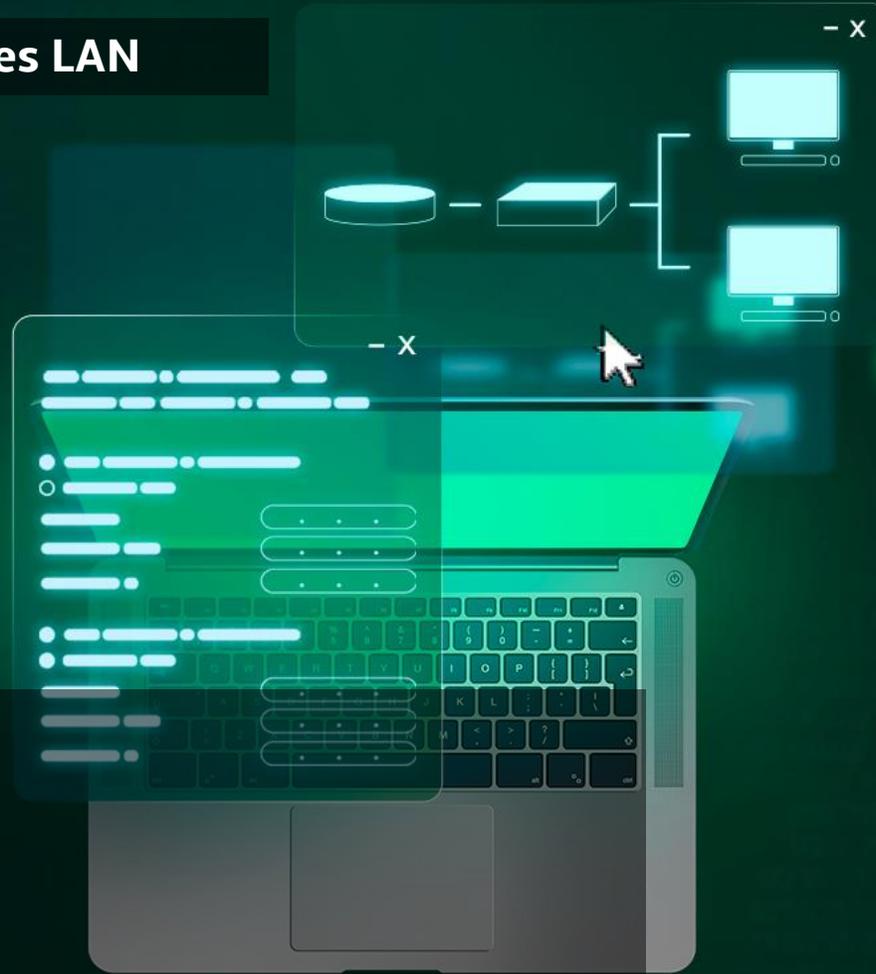
Conceitos intermediários que você precisa aprender no Básico

VLAN (Virtual Local Area Network)

VLAN Modo Access: Quando a interface está configurada em VLAN modo ACCESS, a interface fica responsável por adicionar e remover a TAG da VLAN nos pacotes que por ali passam. Esse modo também é chamado de UNTAGGED.

VLAN Modo Trunk: Quando a interface está configurada em VLAN modo TRUNK, a interface aceita que transitem apenas os pacotes que possuem aquelas TAGs configuradas.

Módulo 04: Cenários de Redes LAN



REDES

TCP
/IP

AULA #1
Topologias

BÁSICO

Topologias

Topologia de Rede

A topologia de rede refere-se à estrutura ou layout físico e lógico da rede de computadores. Ela descreve como os dispositivos de rede estão interconectados e como o fluxo de dados é gerenciado dentro da rede.

A topologia de rede pode ser vista como uma "mapa" que descreve a localização e a relação entre os dispositivos e os cabos que formam a rede. Existem vários tipos de topologias de rede, cada uma com suas próprias vantagens e desvantagens.

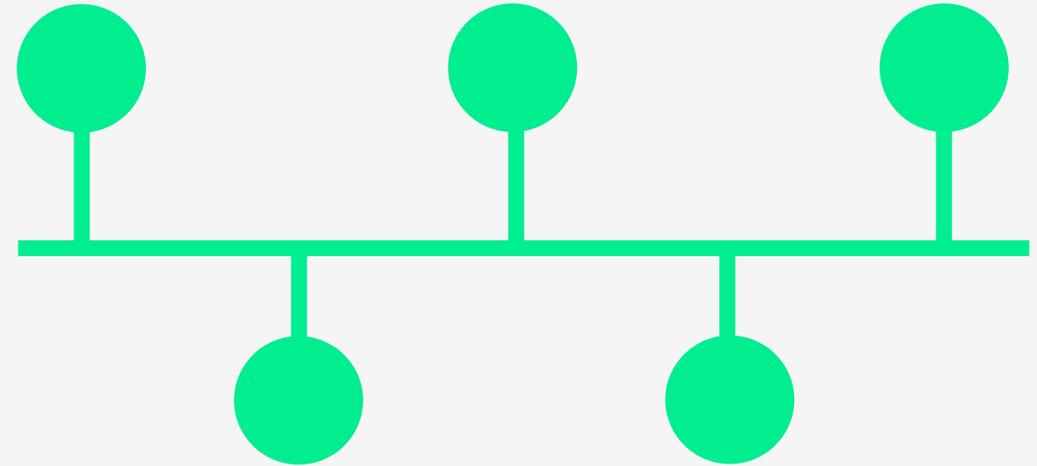
Topologias

Topologia em barramento:

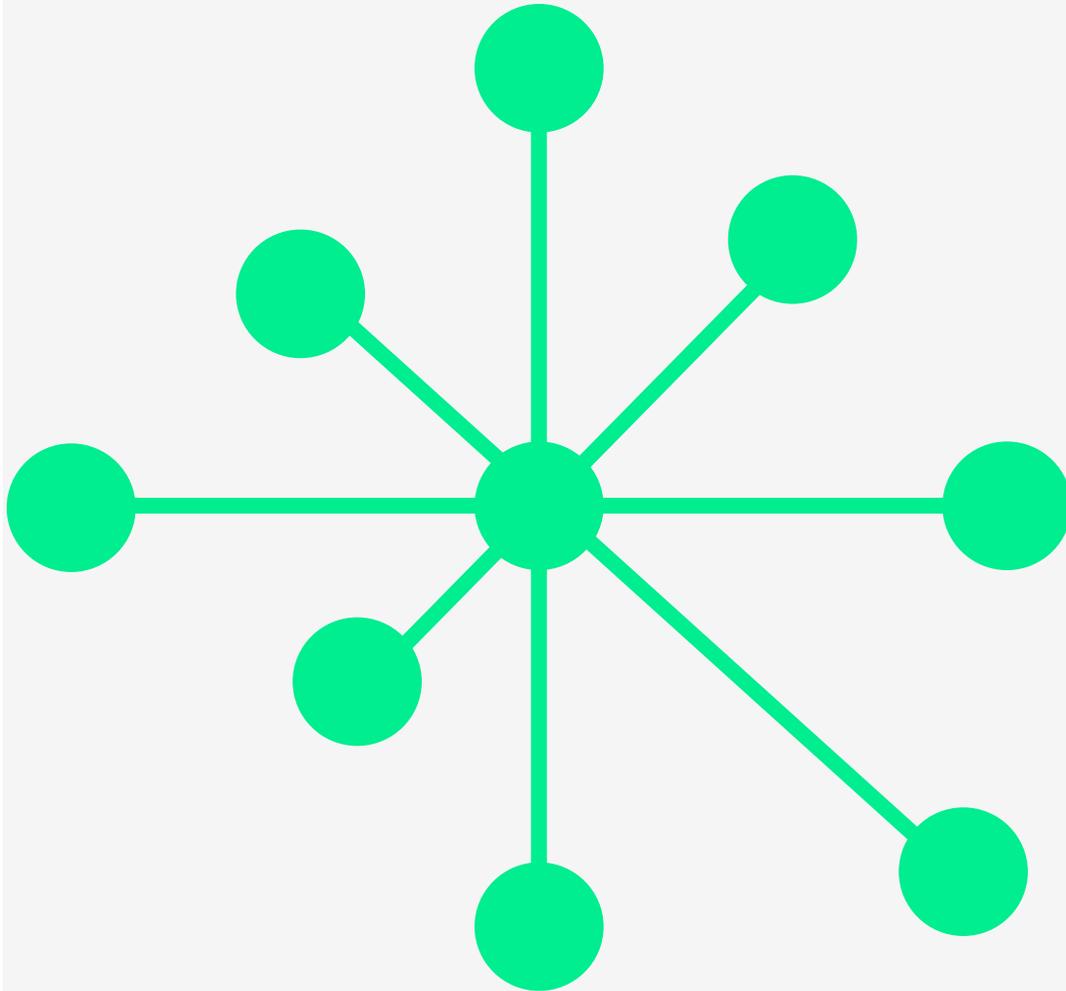
Todos os dispositivos são conectados a um único cabo, que é compartilhado por todos eles.

Quando um dispositivo envia dados, eles são enviados para todos os outros dispositivos na rede, mas apenas o destinatário correto os recebe.

Esta topologia é simples e fácil de configurar, mas pode ser afetada por problemas como colisões e falhas no cabo.



Topologias



Topologia em Estrela

Cada dispositivo é conectado a um ponto central, geralmente um hub ou switch.

Quando um dispositivo envia dados, eles são enviados diretamente para o ponto central, que os envia para o destinatário correto.

Esta topologia é mais confiável do que a em barramento, pois os problemas em um cabo não afetam o restante da rede.

No entanto, se o ponto central falhar, toda a rede será afetada.

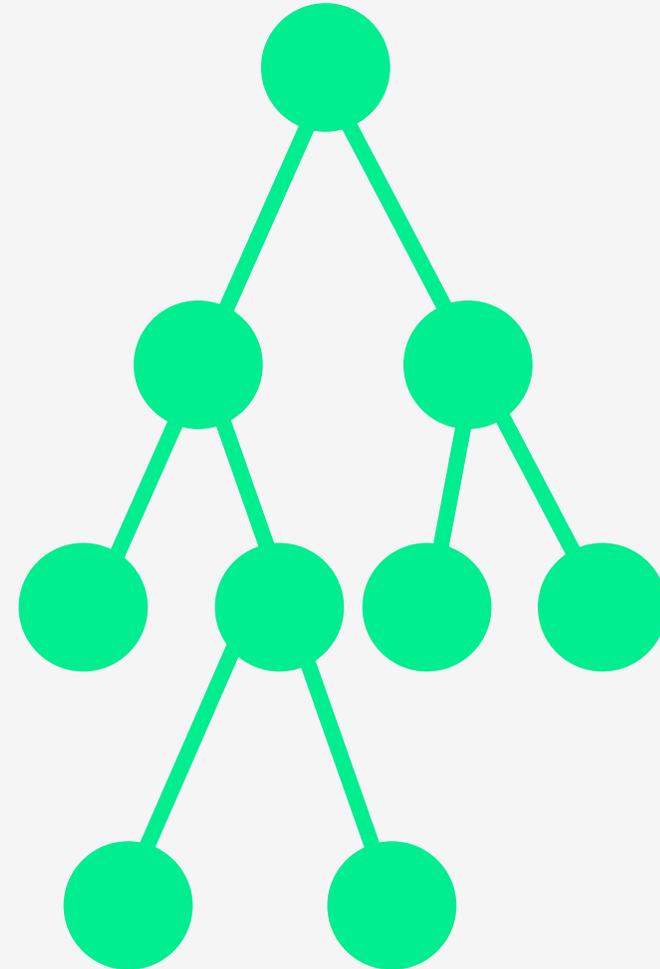
Topologias

Topologia em Árvore:

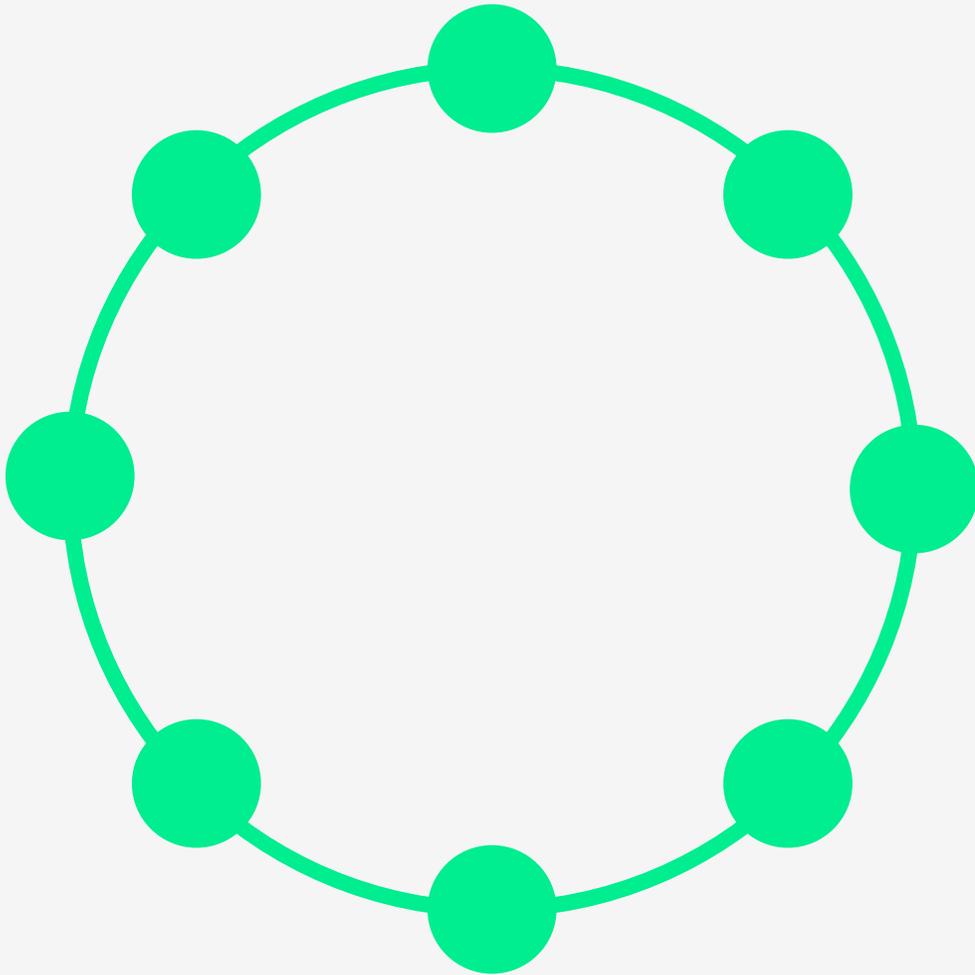
A topologia de rede árvore é caracterizada pela disposição dos nós em formato de árvore, semelhante a uma série de redes em estrela interconectadas, porém sem um nó central.

Nessa topologia, há um nó tronco, normalmente um hub ou switch, de onde partem as ramificações para os demais nós. Cada ramificação é conectada por um barramento a uma rede individual.

A árvore combina as vantagens da topologia em estrela com a topologia em barramento. Uma das desvantagens é que se ocorrer uma falha no segmento principal, toda a rede pode ficar inoperante.



Topologias



Topologia em Anel

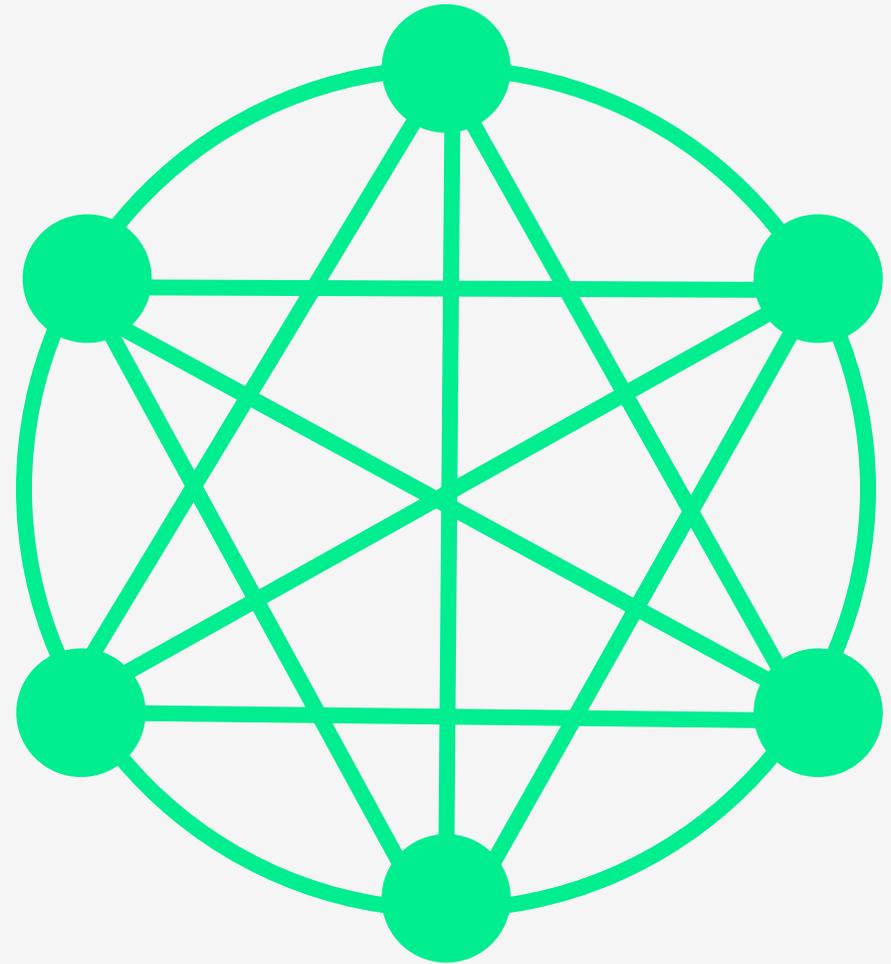
Na topologia em anel, cada dispositivo é conectado ao dispositivo adjacente, formando um anel fechado. Cada dispositivo recebe e transmite dados para o próximo dispositivo no anel até que os dados atinjam o destino desejado.

Portanto, a falha de um único dispositivo em um anel pode afetar apenas a comunicação entre o dispositivo falho e seus dispositivos adjacentes no anel.

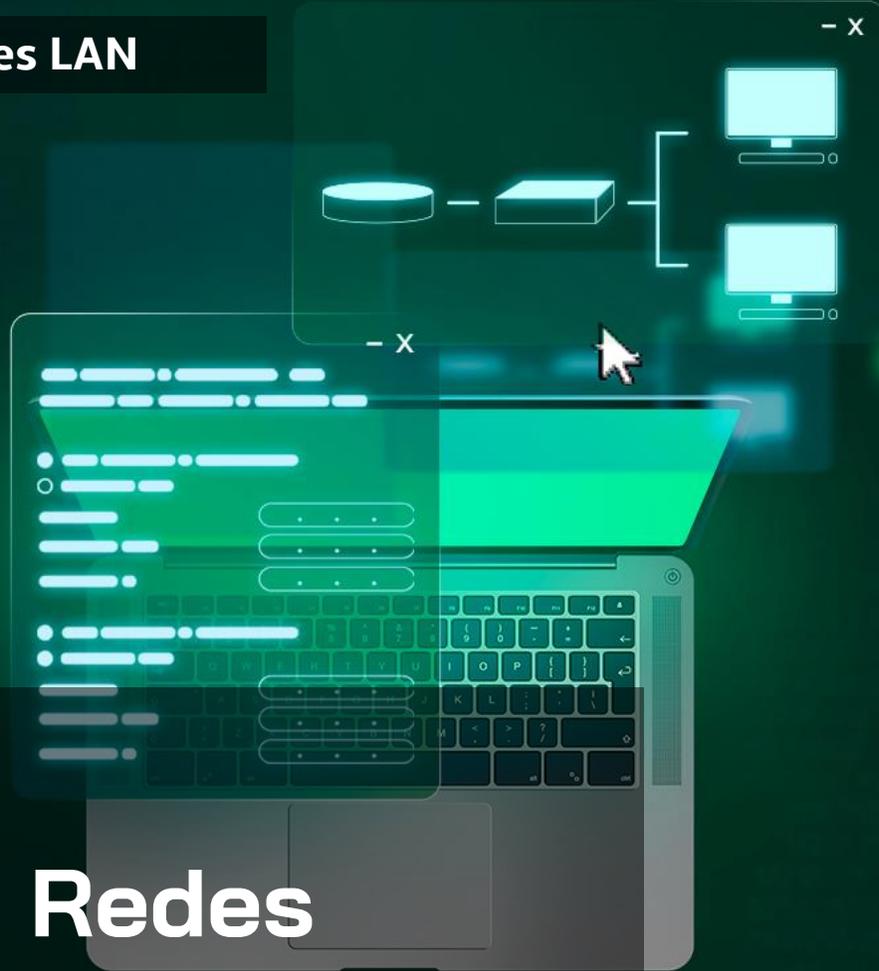
Topologias

Topologia em Malha

Cada dispositivo é conectado a todos os outros dispositivos da rede, criando uma rede totalmente conectada. Os dados são enviados diretamente de um dispositivo para outro, sem passar por um ponto central. Esta topologia é muito confiável, pois um dispositivo falhando não afeta o restante da rede, mas é também a mais cara e difícil de configurar.



Módulo 04: Cenários de Redes LAN



REDES

TCP
/IP

AULA #2
Hardware de Redes

BÁSICO

Hardwares de Rede

Switch

Um switch de rede é um dispositivo de hardware usado para conectar dispositivos em uma rede local.

Ele é responsável por encaminhar pacotes de dados entre dispositivos conectados à rede. O switch examina o endereço MAC (Media Access Control) de cada pacote que recebe e encaminha o pacote para o dispositivo de destino correto com base em sua tabela de endereços MAC.



Hardwares de Rede

Switch

O switch também pode ser configurado para separar a rede em várias VLANs (Virtual LANs), permitindo que diferentes dispositivos compartilhem a mesma rede física, mas estejam isolados em diferentes segmentos lógicos da rede. Isso ajuda a aumentar a segurança e a eficiência da rede.

Alguns switches também oferecem recursos avançados, como QoS (Quality of Service), que prioriza o tráfego de dados com base em sua importância ou tipo, e recursos de gerenciamento remoto para configurar e monitorar o switch em uma rede.

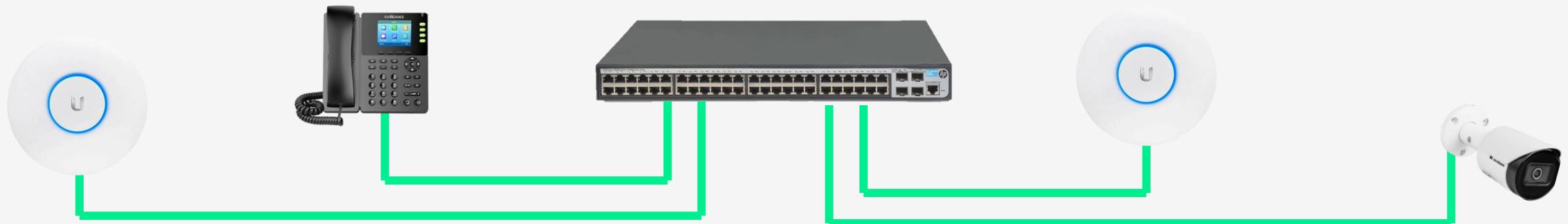
Hardwares de Rede

Switch

Alguns modelos podem possuir a funcionalidade de enviar energia para equipamentos conectados a ele, como por exemplo câmeras, telefones IP, Roteadores Wi-Fi, etc...

Essa funcionalidade é chamada de PoE –Power Over Ethernet.

802.11AF e 802.11AT São os padrões de portas e dispositivos que suportam PoE.



Hardwares de Rede

Roteador

Um roteador é um dispositivo de rede responsável por encaminhar dados entre diferentes redes, permitindo que os dispositivos conectados a essas redes possam se comunicar.

Ele funciona como um ponto de acesso para diferentes redes e conecta dispositivos em redes locais a outras redes, como a Internet.

Além disso, os roteadores também podem ser configurados para executar funções de segurança, como filtrar e bloquear o tráfego indesejado. Em resumo, o roteador é um elemento chave para a conexão de redes e para o acesso à Internet.

Hardwares de Rede

Roteador

Atualmente a maior rede de acesso a internet são as redes FTTx utilizando tecnologia PON. Nesse tipo de rede, os clientes recebem acesso por fibra óptica e é instalado uma ONT (Optical Network Terminal).

O papel da ONT é mudar o meio físico das informações, que chegam pela fibra óptica e são atrelados para Wi-Fi ou Ethernet.

A ONT pode possuir mais funcionalidades, exercendo o papel de Roteador, Gateway e Access Point.



Hardwares de Rede

Roteador



Hardwares de Rede

AP – Access Point

Um access point (AP) é um dispositivo de rede sem fio que permite a conexão de dispositivos móveis, como smartphones, tablets e laptops, à rede local por meio de uma conexão sem fio. O AP é conectado a LAN em um switch ou roteador e atua como uma ponte entre a rede cabeada e a rede sem fio.

O funcionamento do AP é relativamente simples. Ele transmite um sinal de rádio para os dispositivos sem fio próximos, permitindo que eles se conectem à rede sem fio.

Existem modelos que trabalham apenas em modo bridge e outros que podem operar também em modo Router.

Hardwares de Rede

AP – Access Point



Módulo 04: Cenários de Redes LAN



REDES

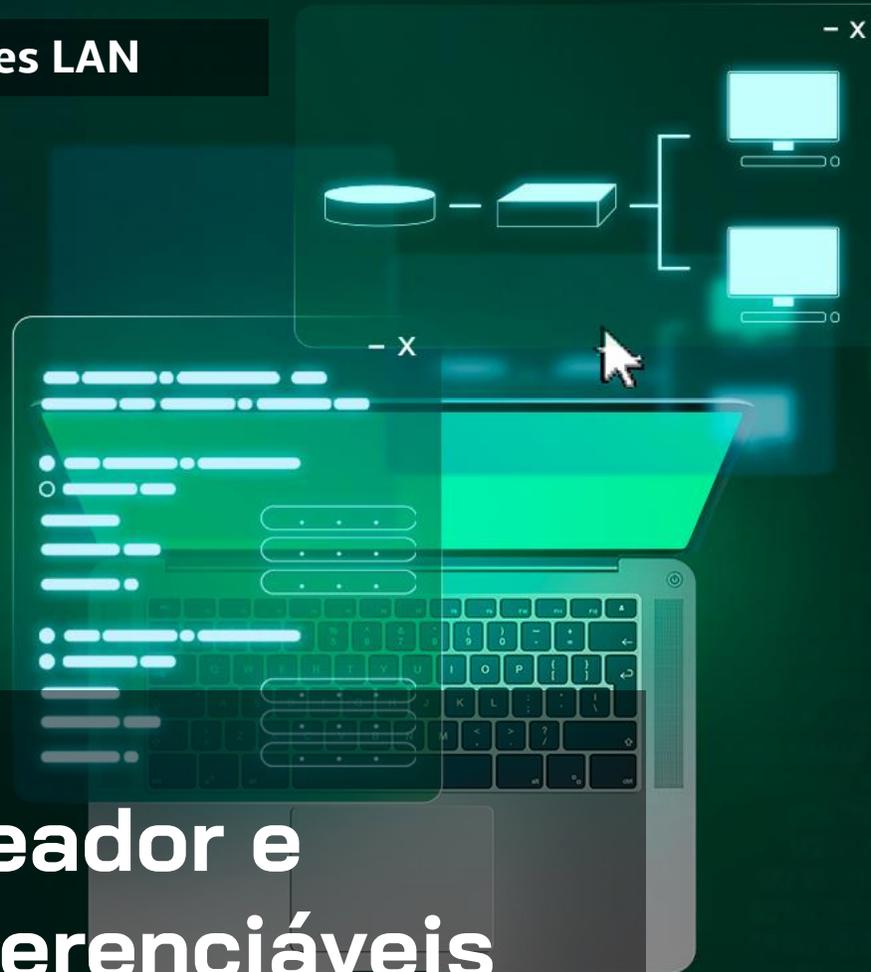
TCP
/IP

AULA #3

Rede simples com Roteador

BÁSICO

Módulo 04: Cenários de Redes LAN



REDES

TCP
/IP

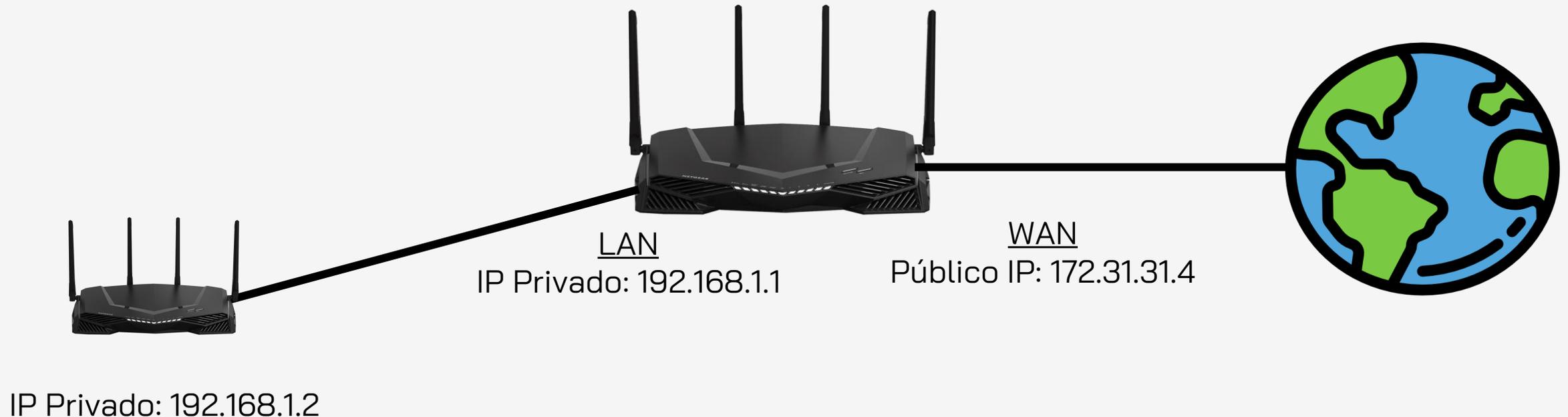
AULA #4

Rede com Roteador e
Dispositivos Gerenciáveis

BÁSICO

Rede com Roteador e Dispositivos Gerenciáveis

Redirecionamento de Portas

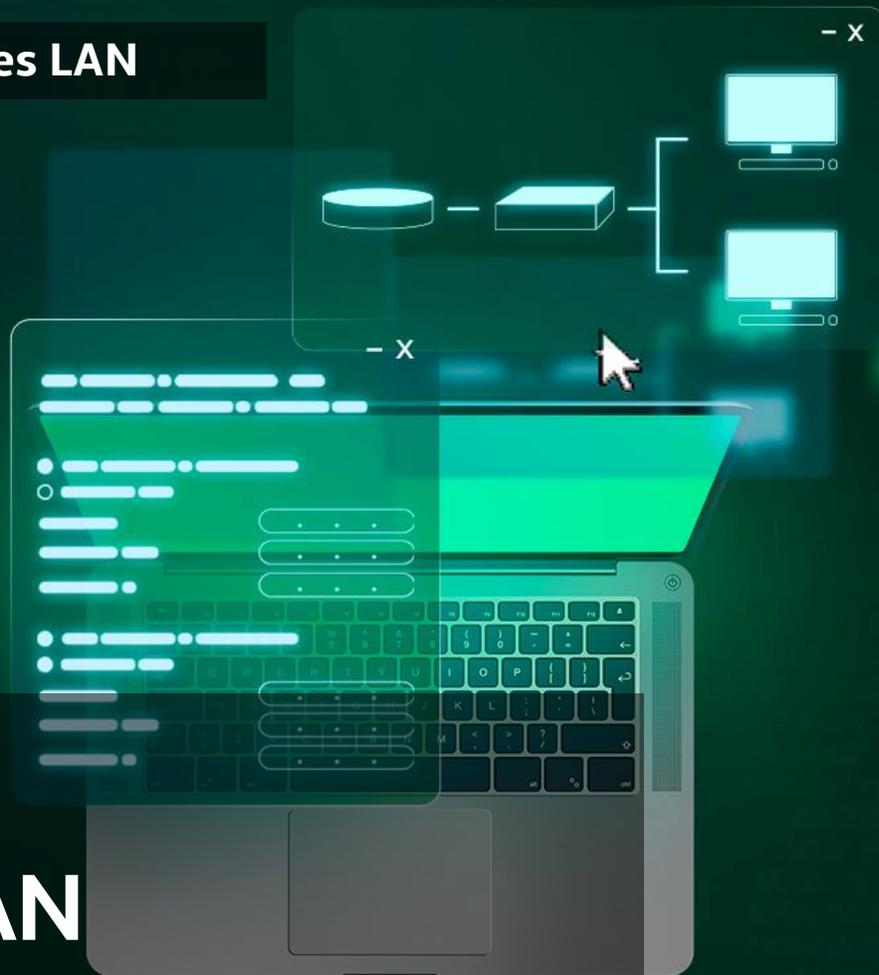


Rede com Roteador e Dispositivos Gerenciáveis

Redirecionamento de Portas

Enable	Name	WAN Host Start IP Address	WAN Start Port	LAN Host Start Port	WAN Connection	Modify	Delete
	Protocol	WAN Host End IP Address	WAN End Port	LAN Host End Port	LAN Host Address		
	AGENT_1	45.235.55.215	7881	80	RVT		
	TCP AND U	45.235.55.215	7881	80	192.168.1.15		

Módulo 04: Cenários de Redes LAN



REDES

TCP
/IP

AULA #5

Rede com VLAN

BÁSICO