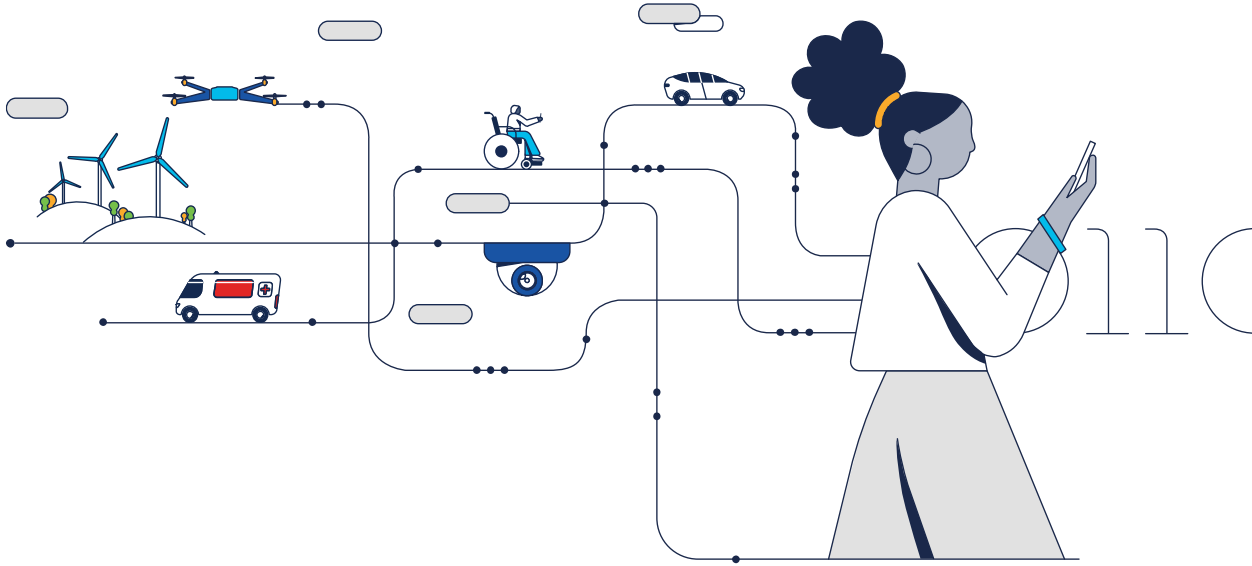
Nossos parceiros

TD SYNNEX

WISE
Women in Science
and Engineering
Inclusive Community

cisco
Networking
Academy



INTERNATIONAL
Girls in ICT Day
Brought to you by **WOMEN ROCK-IT**

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

CCNAv7 – ITN – Introduction to Networks

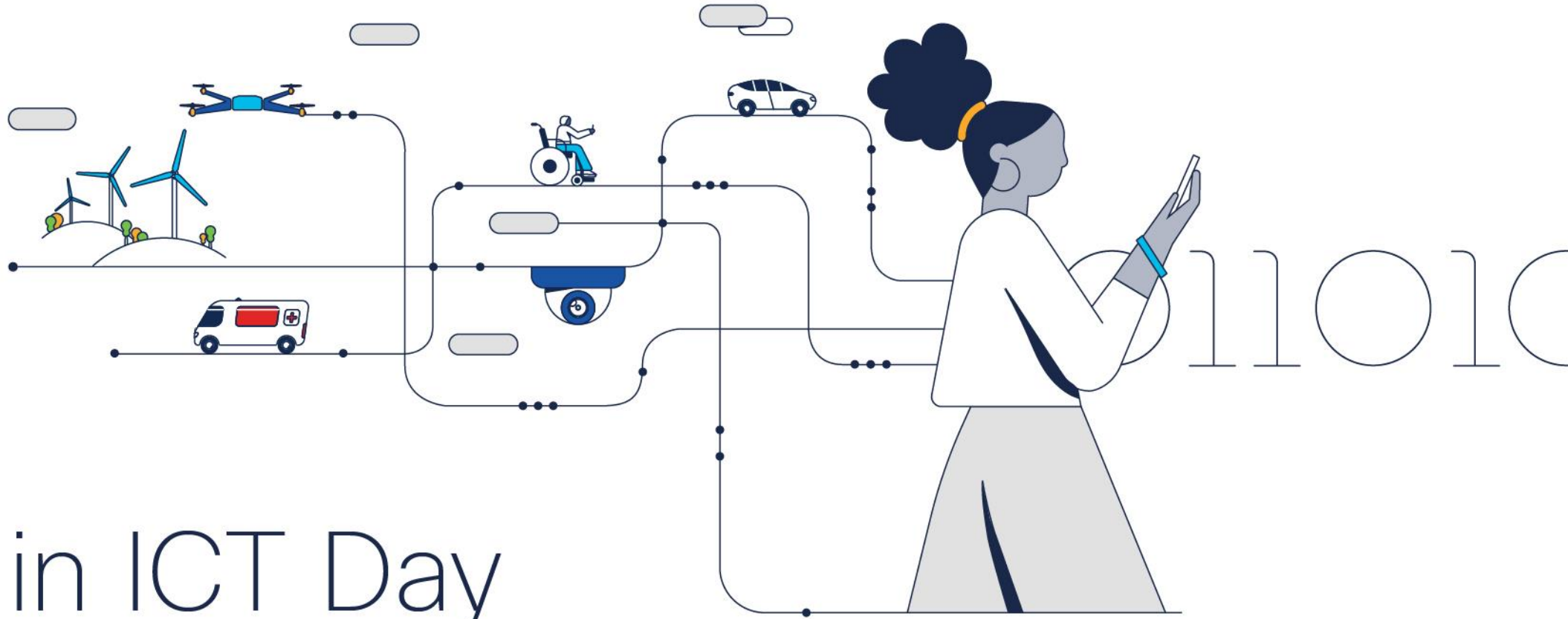
Módulo 1

Embaixadores do Programa 2020, 2021, 2022 & 2023:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

Networking
Academy



INTERNATIONAL

Girls in ICT Day

Brought to you by **WOMEN ROCK-IT**

Rede

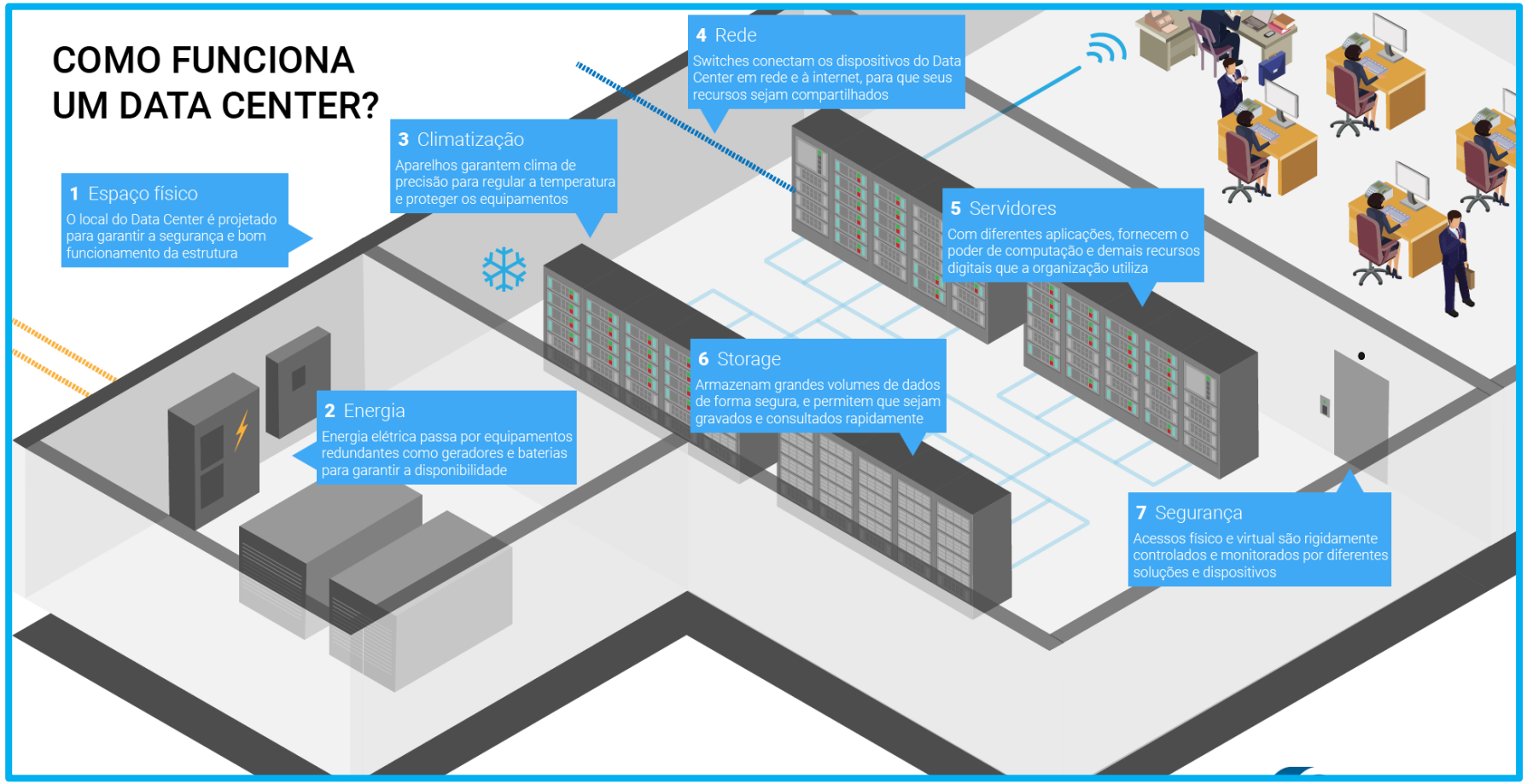
Rede:

- Conjunto de dispositivos interligados por uma única tecnologia.
- Conjunto de 2 ou mais dispositivos (nós) que usam um conjunto de regras (protocolos) em comum para compartilhar recursos entre si.

Protocolo:

- Conjunto de regras sobre o modo como se dará a comunicação entre as partes envolvidas. É a “língua” dos computadores.

Data Center

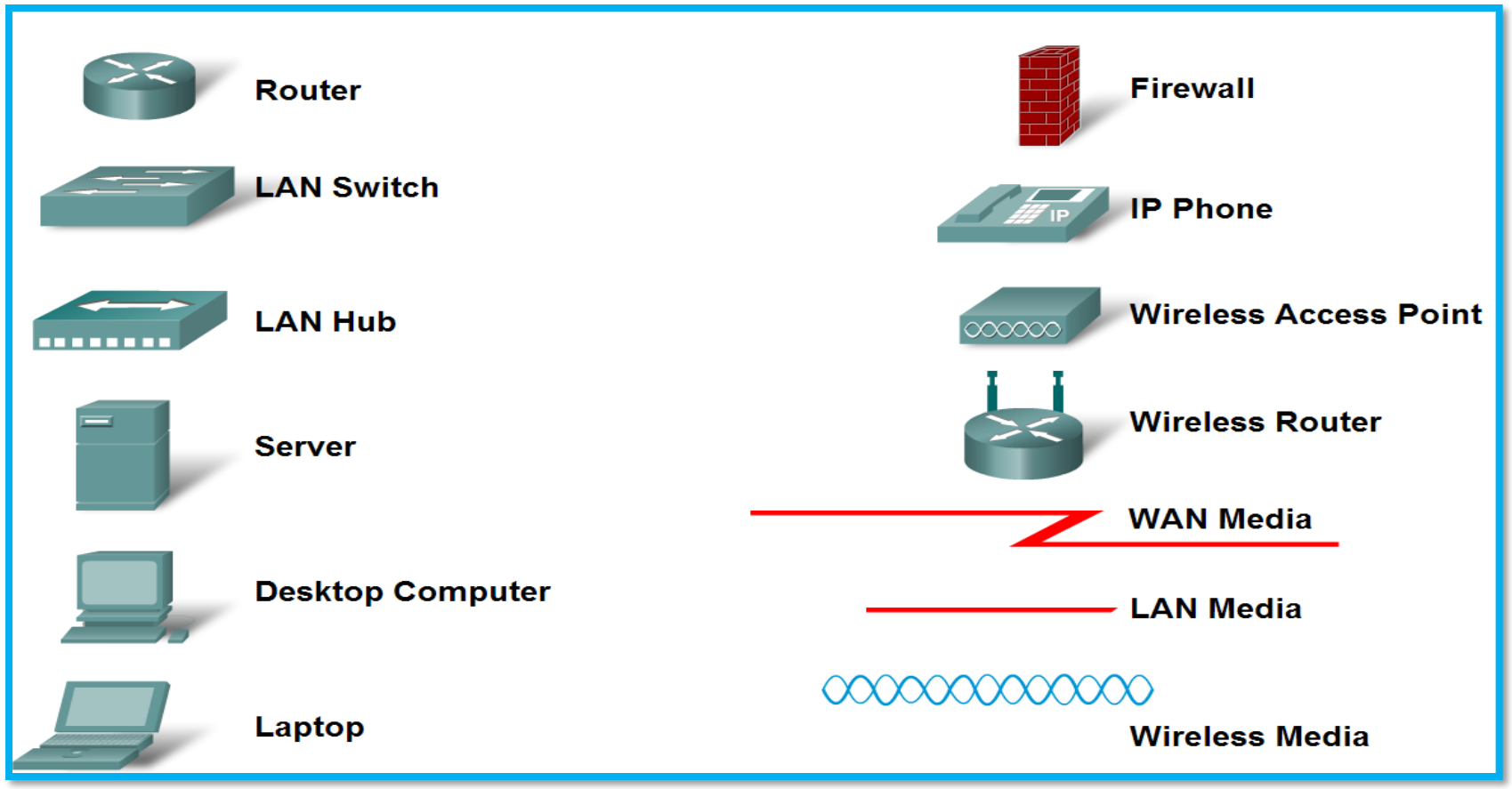


Networking Academy

INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Símbolos Comuns em Rede



Networking Academy

INTERNATIONAL Girls in ICT Day

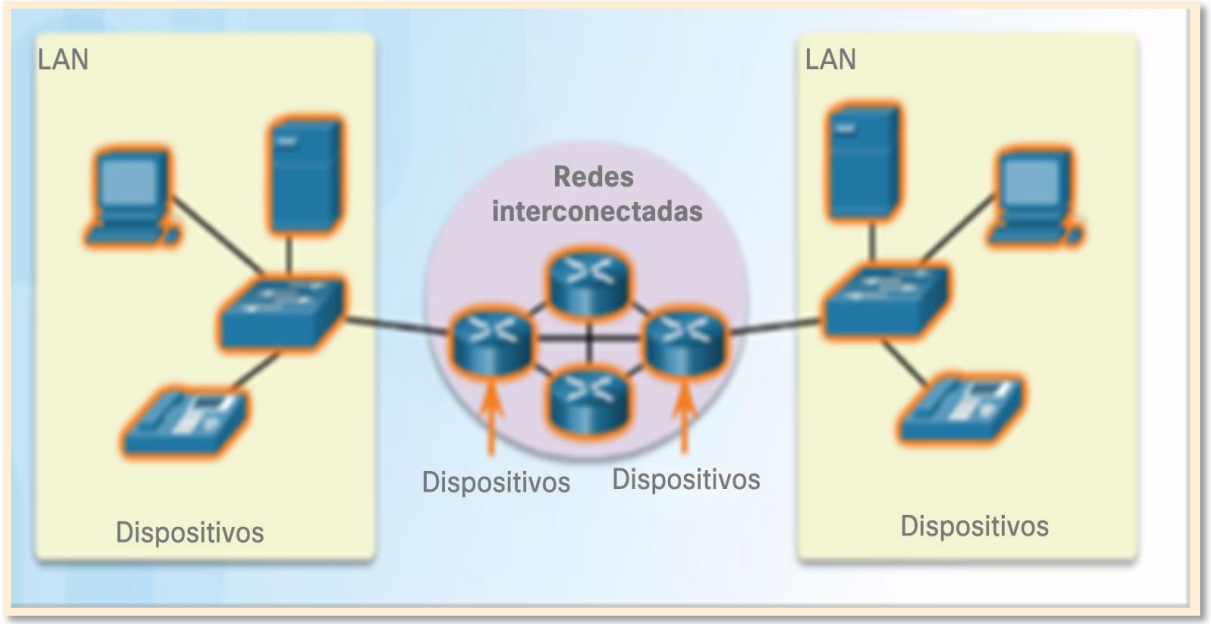
Brought to you by WOMEN ROCK-IT

Componentes da Rede

Uma rede pode ser tão simples quanto um único cabo conectando dois computadores ou tão complexa quanto uma coleção de redes que abrangem todo o mundo.

A infraestrutura de rede contém três categorias amplas de componentes de rede:

- *Dispositivos*
- *Meio físico*
- *Serviços*



Networking Academy

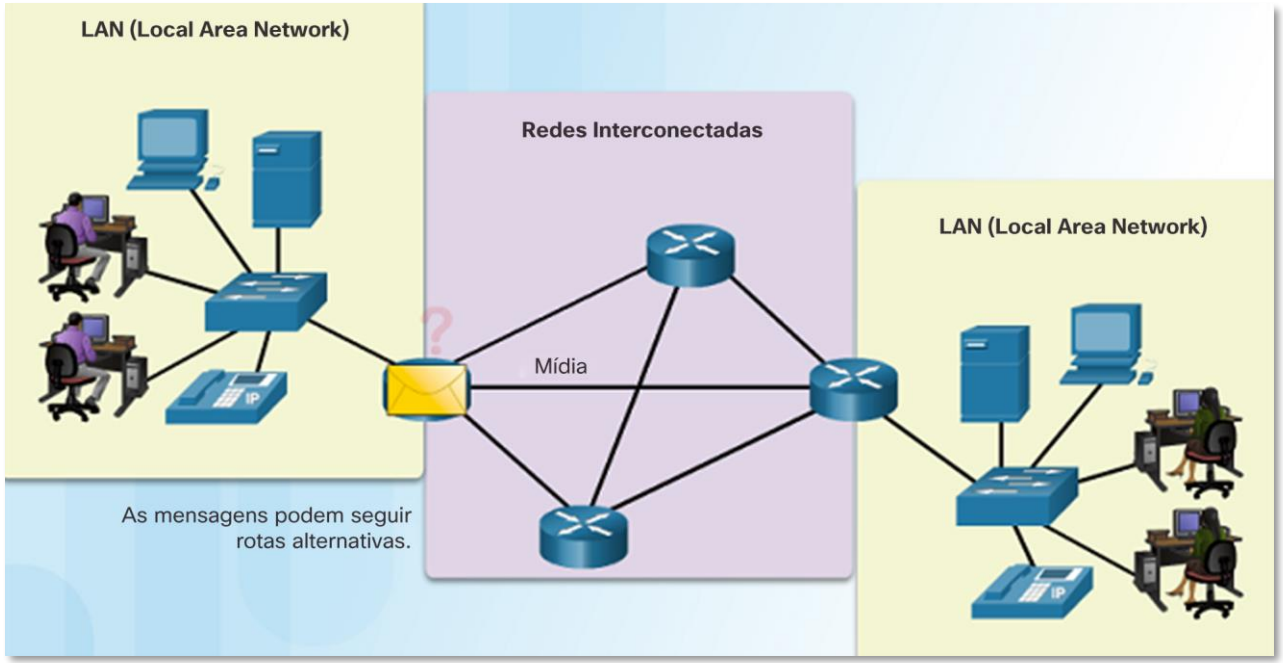
INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Componentes da Rede

Dispositivos Finais:

Um dispositivo final é onde uma mensagem se origina ou onde ela é recebida.

Os dados se originam em um dispositivo final, fluem pela rede e chegam a outro dispositivo final



Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Componentes da Rede

Um dispositivo intermediário interconecta os dispositivos finais em uma rede.

Os exemplos incluem: switches, access points sem fio, roteadores e firewalls.

O gerenciamento de dados na medida em que eles fluem por uma rede também é uma das funções de um dispositivo intermediário:

- Regenerar e retransmitir sinais de dados.
- Manter informação sobre quais caminhos existem pela rede e pela rede interconectada.
- Notificar outros dispositivos sobre erros e falhas de comunicação.

Componentes da Rede

A comunicação através de uma rede é transmitida por um meio que permite a uma mensagem se deslocar da origem até o destino. As redes normalmente usam três tipos de mídia:

- Fios metálicos dentro de cabos, como o cobre;
- Vidro, como os cabos de fibra óptica;
- Transmissão sem fio;

Networking Academy

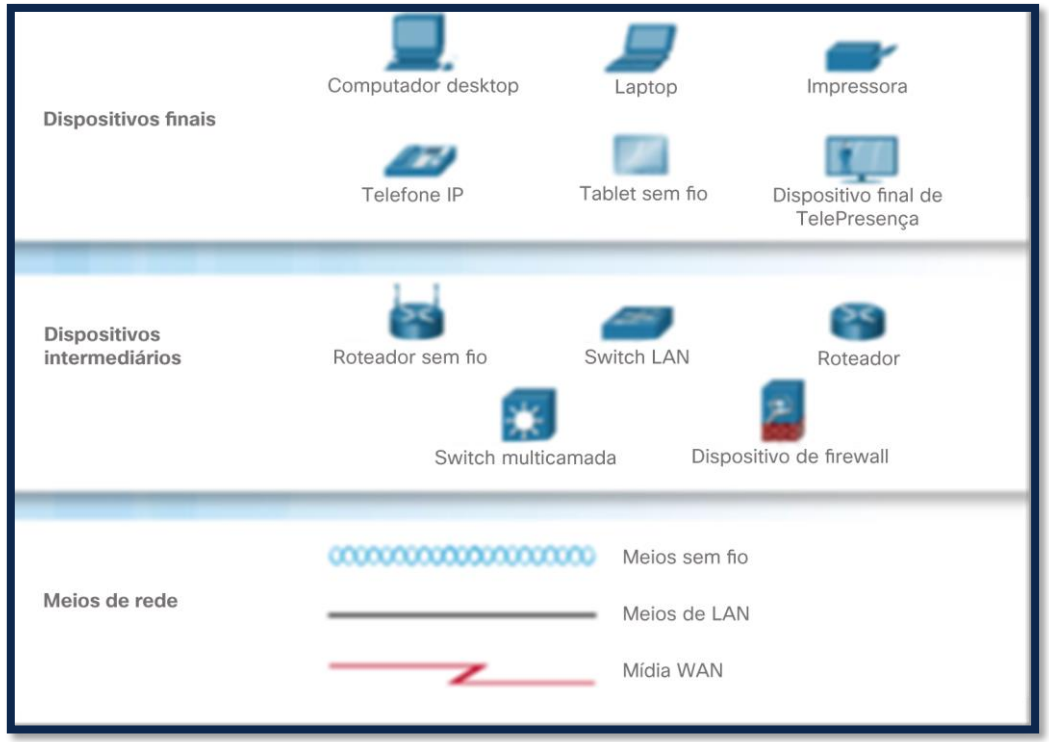
INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Componentes da Rede

Os diagramas de rede, muitas vezes chamados de diagramas de topologia, usam símbolos para representar os dispositivos na rede.

Além das representações do dispositivo à direita, é importante lembrar e entender os termos a seguir:

- Placa de rede
- Porta Física
- Interface



Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

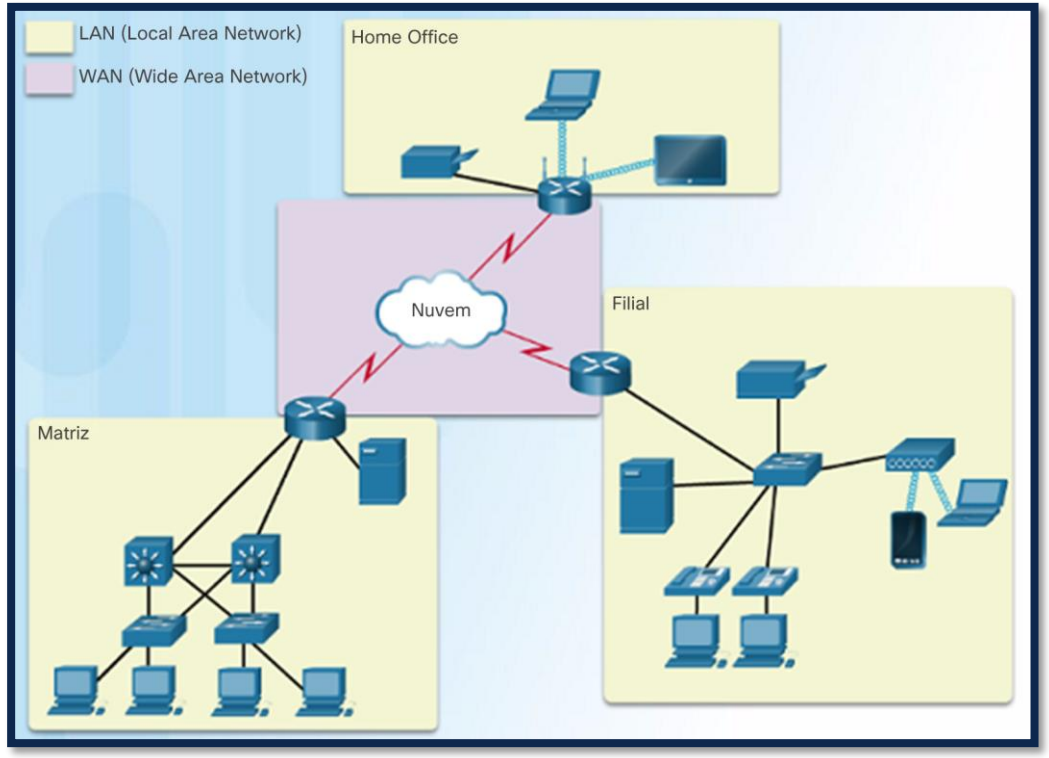
Tipos de Rede

Rede de área local (LAN) – abrange uma área geográfica pequena pertencente ou operada por um indivíduo ou pelo departamento de TI.

Rede de longa distância (WAN) – abrange uma grande área geográfica, normalmente envolvendo um provedor de serviços de telecomunicações.

Outros tipos de redes incluem:

- Rede de área metropolitana (MAN)
- LAN sem fio (WLAN)
- Rede de área de armazenamento (SAN)



cisco Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

A Internet

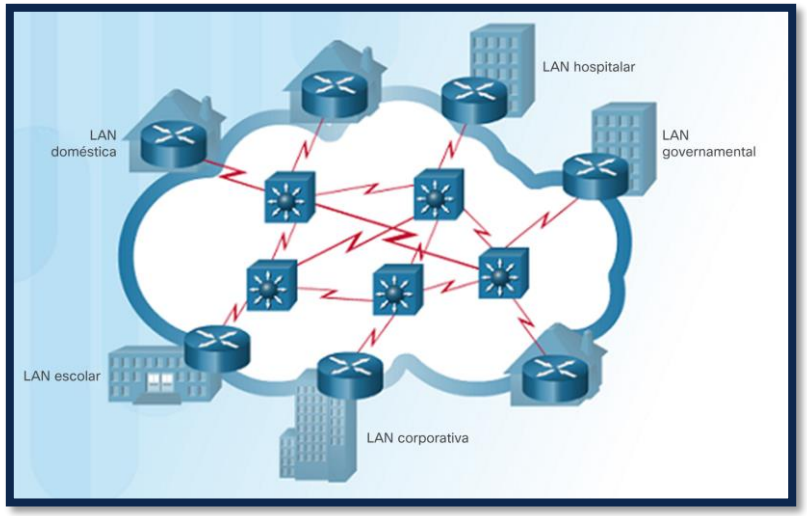
A Internet é um conjunto mundial de LANs e WANs interconectadas.

As LANs estão conectadas entre si usando as WANs.

As WANs estão conectadas entre si usando fios de cobre, cabos de fibra óptica e transmissões sem fio.

A Internet não pertence a qualquer indivíduo ou grupo, no entanto, os seguintes grupos foram desenvolvidos para ajudar a manter a estrutura:

- IETF
- ICANN
- IAB



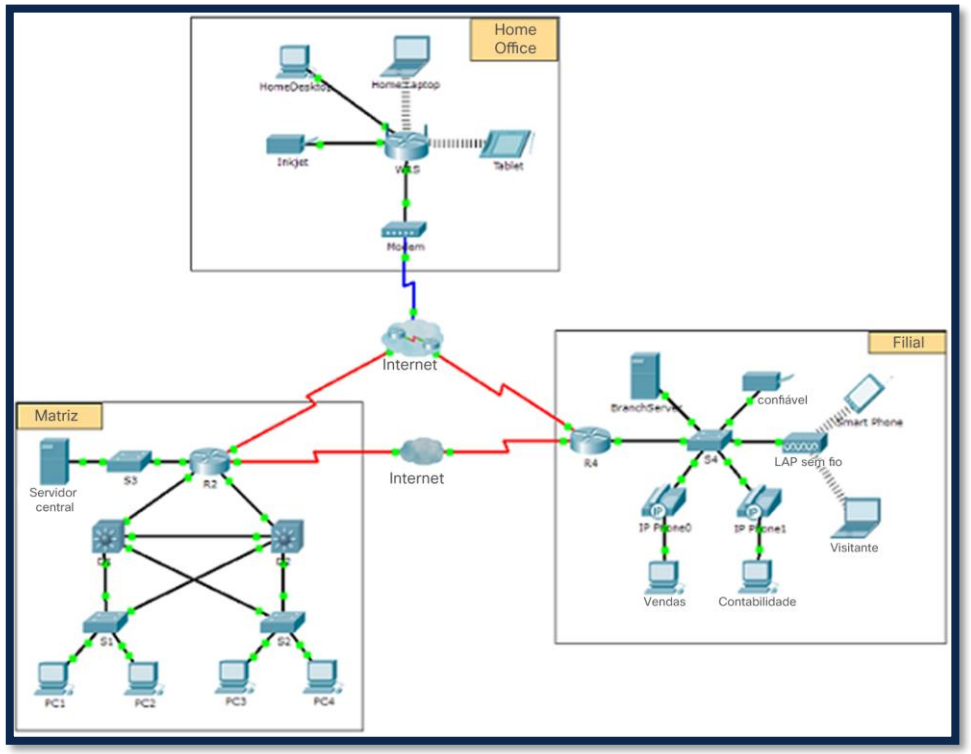
Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Packet Tracer

Visão geral do programa Packet Tracer:

- O Packet Tracer é um software divertido que vai ajudá-la com o CCNA, permitindo que você teste o comportamento da rede, construa redes e encontre as respostas às suas perguntas "e se?".



Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Certificação de Redes

A certificação Cisco Certified Network Associate (CCNA):

- Demonstra que você tem um conhecimento de tecnologias fundamentais
- Garante que você permaneça relevante com as habilidades necessárias para a adoção de tecnologias de próxima geração.

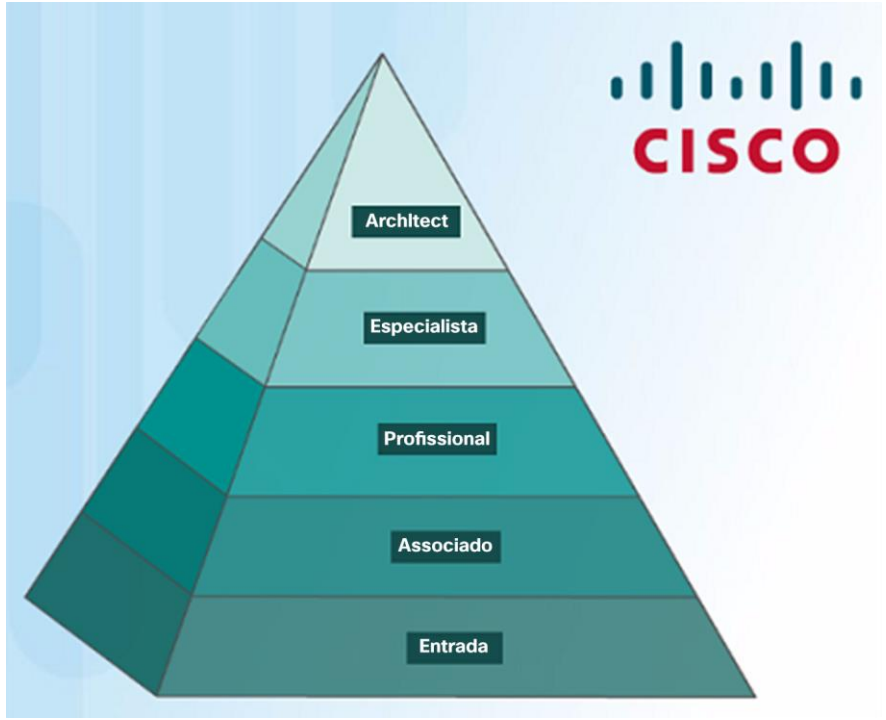
O novo foco da CCNA:

- Tópicos de base e segurança de IP
- Wireless, virtualização, automação e programação de rede.
- Novas certificações DevNet nos níveis de associado, especialista e profissional para validar as habilidades de desenvolvimento de software.
- A certificação especializada valida suas habilidades de acordo com seu papel e interesses profissionais.

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Certificação de Redes



Cisco Certified Network Associate (CCNA)

- Certificação de roteamento e switching;
- Você precisa ser aprovado nos dois exames:

✓ Primeiro exame: técnico de rede de entrada certificado da Cisco (CCENT).

✓ O segundo exame está voltado para as tecnologias WAN e roteamento de IPv4 e IPv6, bem como switching de LAN e infraestrutura de serviços/manutenção.

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

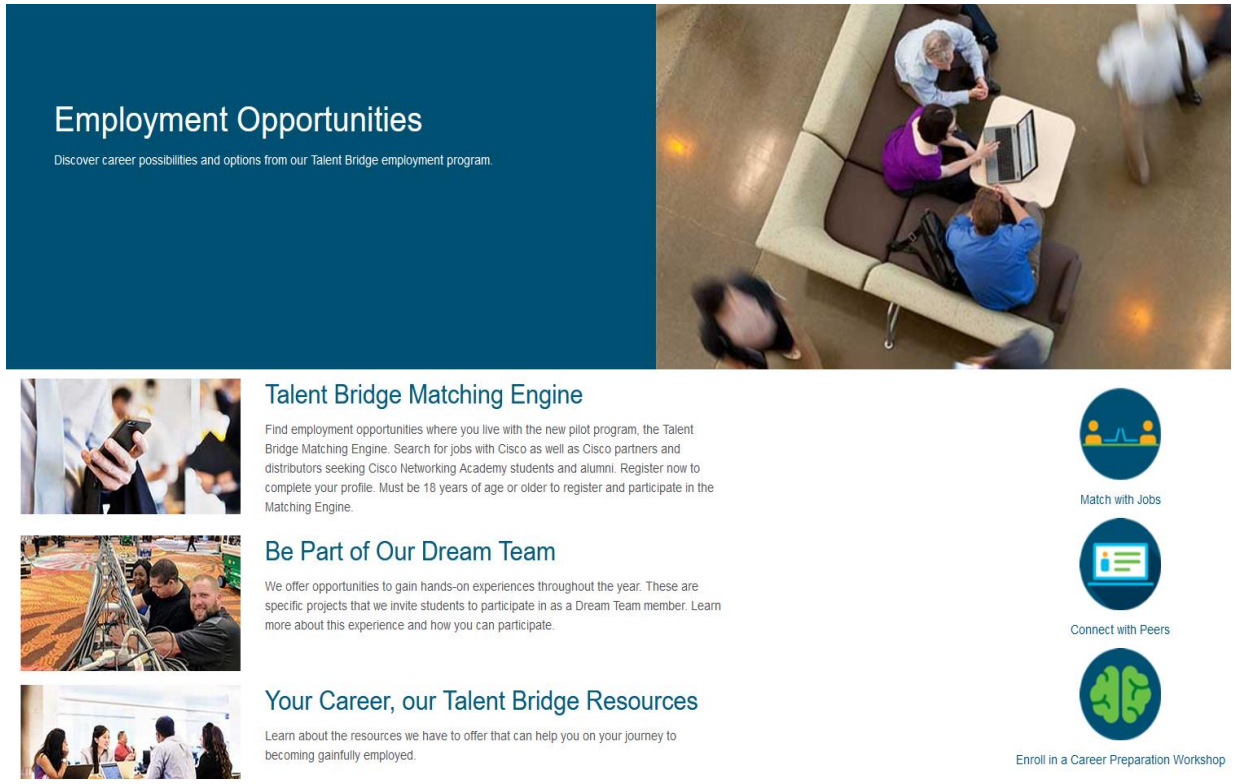
Apresentação CCNA

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Certificado CCNA Professor Gabriel Florêncio Alves

Profissional de TI



Em www.netacad.com você pode clicar no menu:

- Carreiras

Em seguida, selecione:

- Oportunidades de emprego.

Encontre oportunidades de emprego usando o Talent Bridge Matching Engine.

Procure empregos na Cisco, parceiros e distribuidores da Cisco que procuram alunos e ex-alunos da Cisco Networking Academy.

Cisco Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

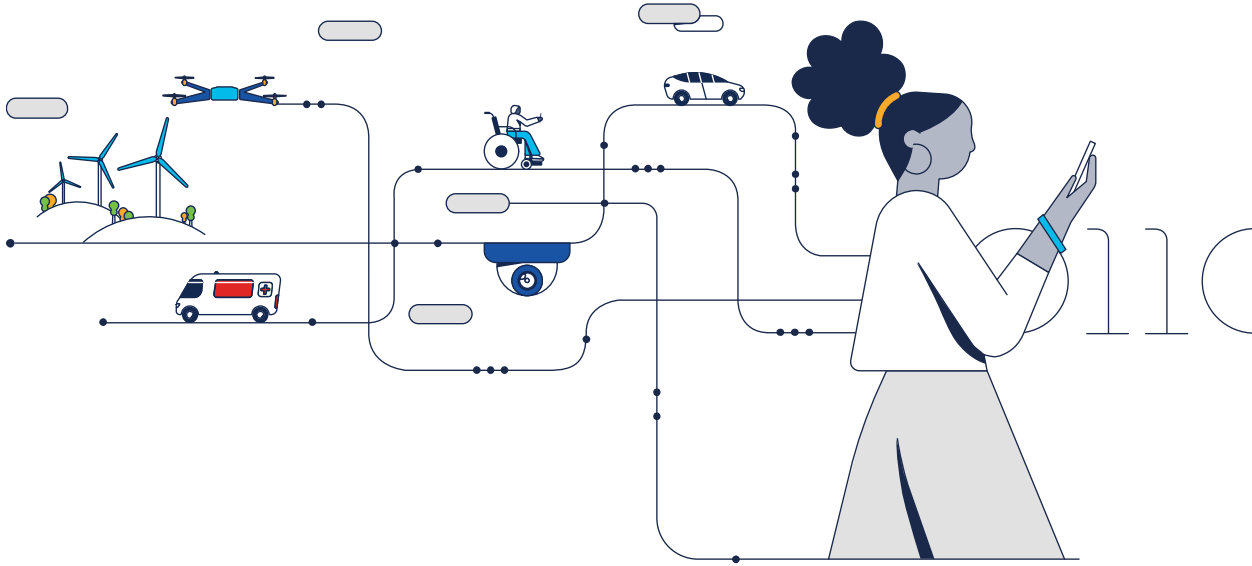
The bridge to possible

Nossos parceiros

TD SYNNEX

WISE
Women in Science
and Engineering
Inclusive Community

cisco
Networking
Academy



INTERNATIONAL
Girls in ICT Day
Brought to you by **WOMEN ROCK-IT**

Cisco Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

CCNAv7 – ITN – Configuração Básica do Switch e do Dispositivo Final

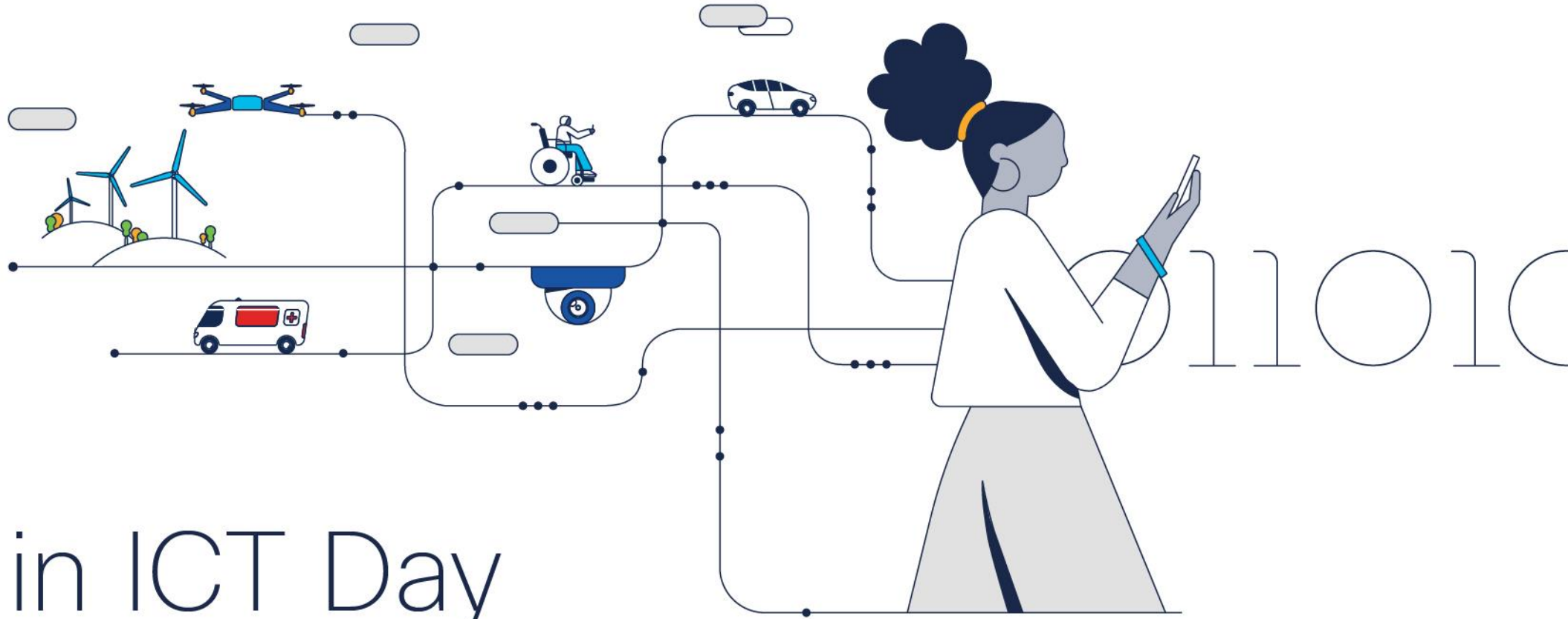
Módulo 2

Embaixadores do Programa 2020, 2021, 2022 & 2023:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

Networking
Academy



INTERNATIONAL

Girls in ICT Day

Brought to you by **WOMEN ROCK-IT**

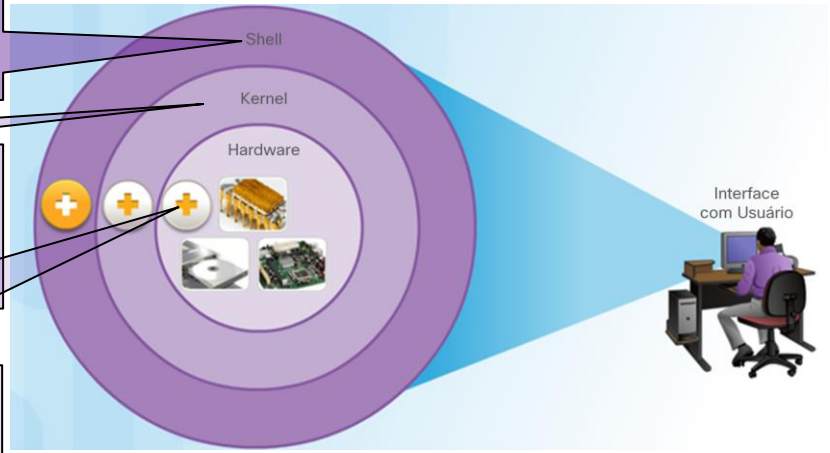
Sistema Operacional

- Todos os dispositivos eletrônicos exigem um sistema operacional.
  - Windows, Mac e Linux para PCs e notebooks
  - Apple IOS e Android para smartphones e tablets
  - Cisco IOS para dispositivos de rede (switches, roteadores, AP, firewall,..)

OS Shell
- O OS Shell pode ser uma interface da linha de comando (CLI) ou uma interface gráfica do usuário (GUI) e permite a interface de um usuário com aplicações.

Kernel do sistema operacional
- O kernel do sistema operacional se comunica diretamente com o hardware e gerencia como os recursos de hardware são usados para atender aos requisitos de software.

Hardware
- a parte física de um computador. Inclui peças eletrônicas subjacentes.



Os dispositivos da Cisco usam o Cisco **Internetwork Operating System, IOS (IOS)**.
- Embora seja usado pela Apple, o iOS é uma marca registrada da Cisco nos EUA e em outros países e é usada pela Apple sob licença.

Sistema Operacional

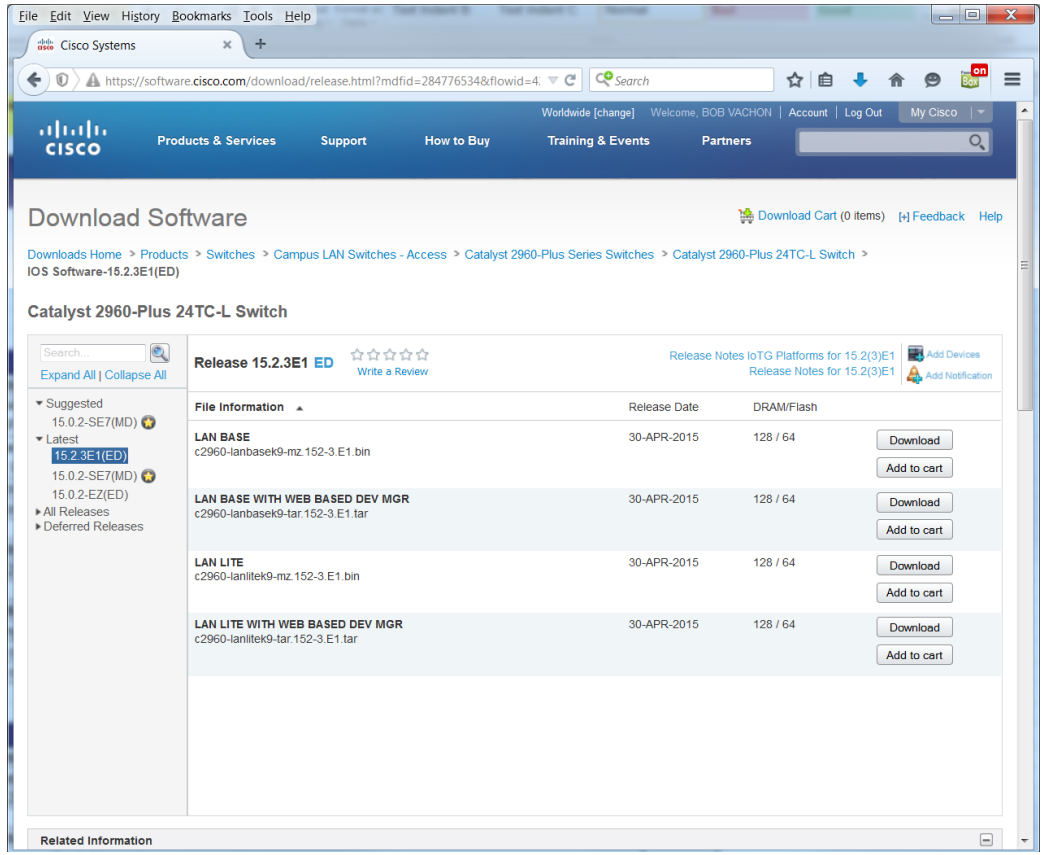
- A utilização da GUI permite ao usuário:
  - Utilizar um mouse para fazer seleções e executar programas
  - Inserir texto e comandos baseados em texto

- Utilizar uma CLI em um switch do Cisco IOS ou o roteador permite que um técnico de redes:
  - Use um teclado para executar programas de rede baseados na CLI
  - Use um teclado para inserir texto e comandos baseados em texto

- Existem muitas variações distintas do Cisco IOS:
  - O IOS para switches, roteadores e outros dispositivos de rede da Cisco
  - Versões numeradas de IOS para determinados dispositivos da rede da Cisco

SUBCAMADAS DE ENLACE IEEE 802 LAN/MAN

- Todos os dispositivos são fornecidos com um conjunto de IOS e recursos padrão.
- É possível atualizar a versão ou o conjunto de recursos do IOS.
- Um IOS pode ser baixado em cisco.com. No entanto, é necessária uma conta Cisco Connection Online (CCO).
- **Observação**: o foco deste curso será no Cisco IOS Versão 15.x.



Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Métodos de Acesso

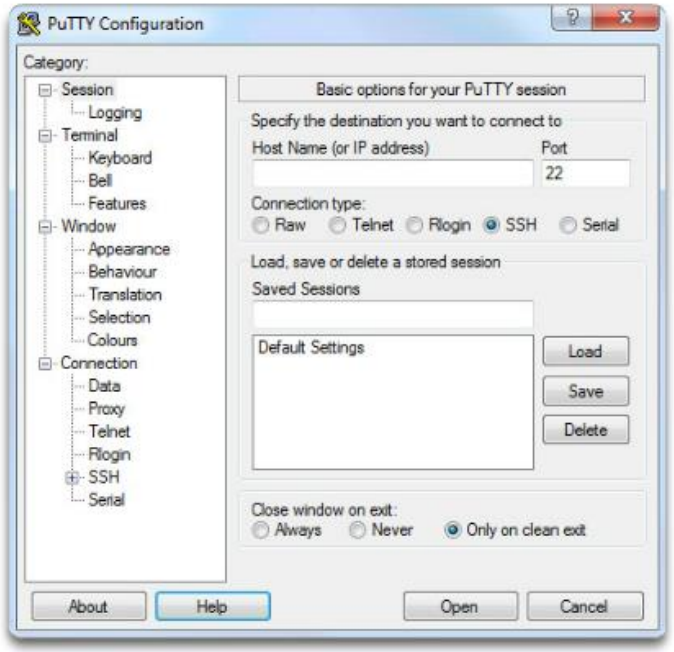
- As três maneiras mais comuns de acessar o IOS são:
  - **Porta do console** – porta serial fora da banda usada principalmente para gerenciamento, como a configuração inicial do roteador.
  - **Secure Shell (SSH)** – método na faixa para estabelecer de modo remoto e seguro uma sessão CLI em uma rede. A autenticação de usuário, as senhas e os comandos enviados pela rede são criptografados. Como prática recomendada, use o SSH em vez do Telnet sempre que possível.
  - **Telnet** – As interfaces na banda estabelecem remotamente uma sessão CLI por meio de uma interface virtual em uma rede. A autenticação de usuário, as senhas e os comandos são enviados pela rede como texto simples.
- **Observação**: A porta AUX é um método mais antigo para estabelecer uma sessão CLI de modo remoto, por meio de uma conexão discada por telefone usando um modem.

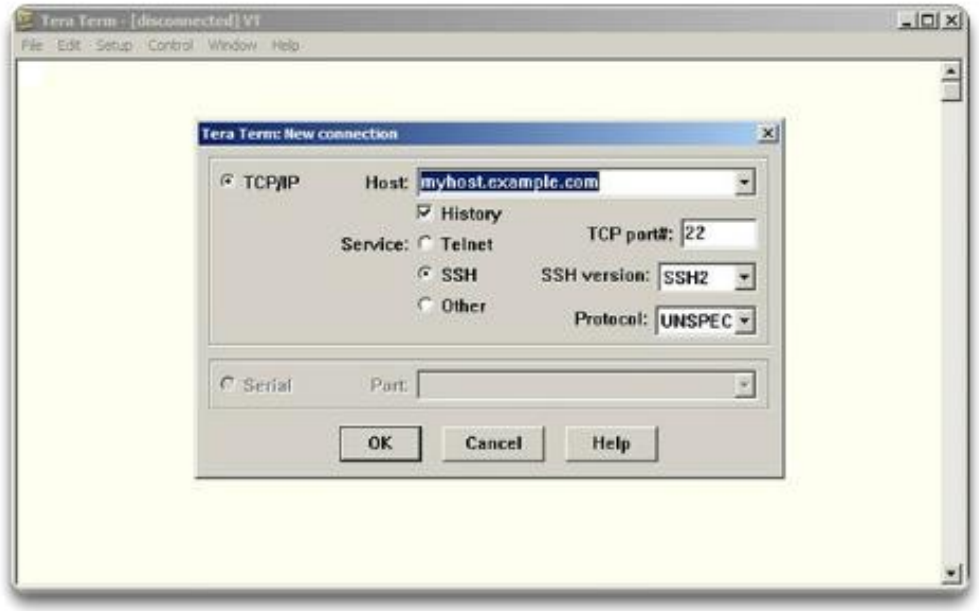
Métodos de Acesso

- Independentemente do método de acesso, será necessário um programa de emulação de terminal.

Os programas populares de emulação de terminal incluem PuTTY, Tera Term, SecureCRT e OS X Terminal.

PuTTY





Networking Academy

INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Navegação no IOS

- Os modos do Cisco IOS usam uma estrutura hierárquica de comando.
- Cada modo possui um prompt distinto e é usado para realizar determinadas tarefas com um conjunto específico de comandos disponíveis somente para aquele modo.
- O modo EXEC do usuário permite somente um número limitado de comandos básicos de monitoramento.
  - Ele é frequentemente chamado de modo de "visualização somente".
  - Por padrão, não há autenticação exigida para acessar o modo EXEC usuário do console, mas deve ser protegido.
- O modo EXEC privilegiado permite a execução de comandos de configuração e gerenciamento.
  - Muitas vezes chamado de "modo de ativação", pois ele precisa do comando EXEC **enable** do usuário.
  - Por padrão, não há autenticação exigida para acessar o modo EXEC usuário do console,

  mas deve ser protegido.

Modo de Comando	Descrição	Aviso padrão do dispositivo
Modo Exec do usuário	• O modo permite somente uma quantidade limitada de comandos básicos de monitoramento • Ele é frequentemente referido como modo somente de visualização.	`Switch>` `Router>`
Modo EXEC privilegiado	• O modo permite acesso a todos os comandos e recursos. • O usuário pode utilizar qualquer comando de monitoramento e executar comandos de configuração e gerenciamento.	`Switch#` `Router#`

Networking Academy

INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Navegação no IOS

- O modo de configuração primário é chamado de **global configuration** ou **global config**.
  - Use o comando **configure terminal** para acesso.
  - As alterações feitas afetam a operação do dispositivo.

- Modos de subconfiguração específicos podem ser acessadosno modo de configuração global. Cada um desses modos permite a configuração de uma parte particular ou função do dispositivo IOS.
  - **Modo de interface** – para configurar uma das interfaces de rede.
  - **Modo de linha** – para configurar o acesso ao console, AUX, Telnet ou SSH.

- A seguir há um exemplo da navegação entre os modos do IOS:
  - Entre no modo EXEC privilegiado usando o comando **enable**.
  - Entre no modo de configuração global usando o comando **configure terminal**.
  - Insira o modo de interface sub-config usando o comando **interface fa0/1**.
  - Saia de cada modo usando o comando **exit**.
  - O restante da configuração ilustra como você pode sair do modo de subconfiguração e retornar ao modo EXEC privilegiado usando uma combinação das teclas **end** ou **^Z**.

Estrutura de comandos

- Um dispositivo Cisco IOS é compatível com muitos comandos. Cada comando IOS possui um formato ou sintaxe específicos e só podem ser implementados no modo apropriado.

- A sintaxe para um comando é o comando seguido por quaisquer palavras-chave e argumentos adequados.
  - **Palavra-chave** – um parâmetro específico definido no sistema operacional (na figura, ip protocols)
  - **Argumento** – não predefinido; um valor ou variável definido pelo usuário (na figura, 192.168.10.5)
- Após a inserção de cada comando completo, inclusive palavras-chave e argumentos, pressione a tecla **Enter** para enviar o comando ao interpretador de comandos.

Estrutura de comandos

- Para determinar as palavras-chave e os argumentos necessários para um comando, consulte a sintaxe de comando
  - Consulte a tabela a seguir ao analisar a sintaxe do comando.

Convenção	Descrição
negrito	O texto em negrito indica comandos e palavras-chave que você insere literalmente, como mostradas.
itálico	O texto em itálico indica argumentos para os quais você fornece valores.
[x]	Colchetes indicam um elemento opcional (palavra-chave ou argumento).
{x}	Chaves indicam um elemento necessário (palavra-chave ou argumento).
[x {y | z}]	Chaves e linhas verticais entre colchetes indicam uma escolha obrigatória dentro de um elemento opcional.

- Exemplos:
  - **description** string – o comando é usado para adicionar uma descrição a uma interface. O argumento string é o texto inserido pelo administrador como **description** *Conectado à sede principal do switch do escritório*.
  - **Ping** ip-address – O comando é **ping** e o argumento definido pelo usuário é o ip-address do dispositivo de destino como no **ping** 10.10.10.5

Estrutura de comandos

- Verificação da sintaxe de comandos do IOS:
  - O interpretador de linha de comando verifica um comando inserido da esquerda para a direita, com o objetivo de determinar a ação que está sendo solicitada.
  - Se o intérprete entender o comando, a ação solicitada é executada e o CLI retorna ao prompt adequado.
  - Se o interpretador detecta um erro, o IOS geralmente fornece feedback como "Ambiguous command" (comando ambíguo), "Incomplete command" (comando incompleto) ou "Incorrect command" (comando incorreto).
- Os comandos e as palavras-chave podem ser abreviados para o número mínimo de caracteres que identifica uma seleção exclusiva.

- Por exemplo, o comando **configure** pode ser abreviado para **conf** porque configure é o único comando que se inicia com **conf**.
  - Uma versão ainda mais curta de **con** não dará certo porque mais de um comando se inicia com **con**.
  - Palavras-chave também podem ser abreviadas.

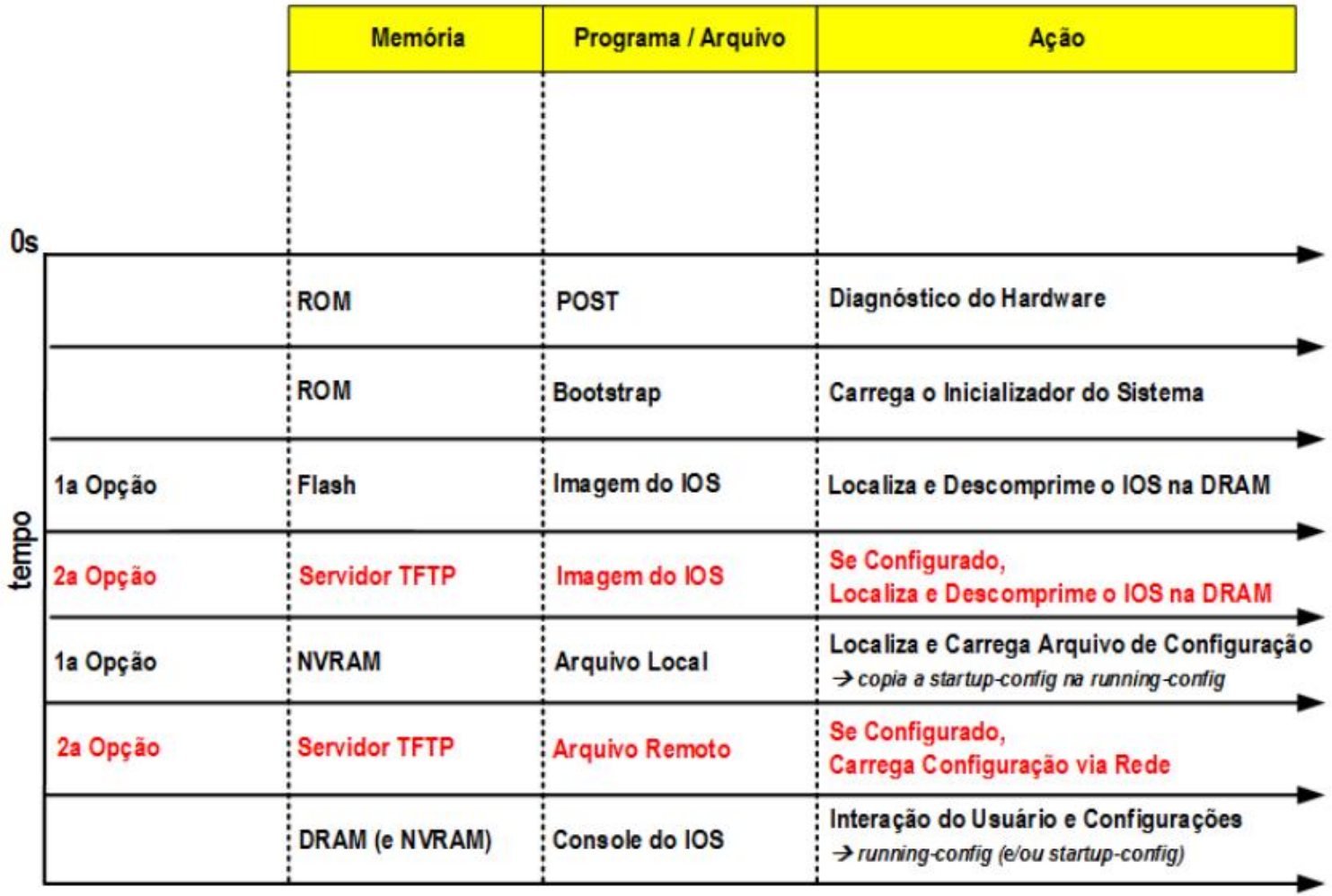
Estrutura de comandos

- A CLI do IOS é compatível com as seguintes teclas de acesso:
  - **Seta para baixo** – Permite que o usuário role pelo histórico de comandos.
  - **Seta para cima** – Permite que o usuário role para trás através de comandos anteriores.
  - **Tab** – Conclui o restante do comando parcialmente inserido.
  - **Ctrl-A** – Leva ao início da linha.
  - **Ctrl-E** – Leva ao final da linha.
  - **Ctrl-R** – Exibe a linha novamente.
  - **Ctrl-Z** – Sai do modo de configuração e retorna ao EXEC usuário.
  - **Ctrl-C** – Sai do modo de configuração ou aborta o comando atual.
  - **Ctrl-Shift-6** – Permite que o usuário interrompa processos do IOS (por exemplo, ping).

Memórias

Memória	Volatilidade	Funções
RAM ou DRAM	Volátil	Executa o IOS ativo Executa o arquivo de configuração ativo Running-config Buffer de pacotes e tabelas
ROM	Não-Volátil	Mini-IOS Limitado (ROMmon) Software de diagnóstico básico (POST) Instruções de Bootup/Bootloader
NVRAM	Não-Volátil	Arquivo de configuração inicial ou de backup Startup-config
Flash	Não-Volátil	Possui o arquivo de imagem comprimido do IOS Outros sistemas de arquivo

Inicialização



Networking Academy

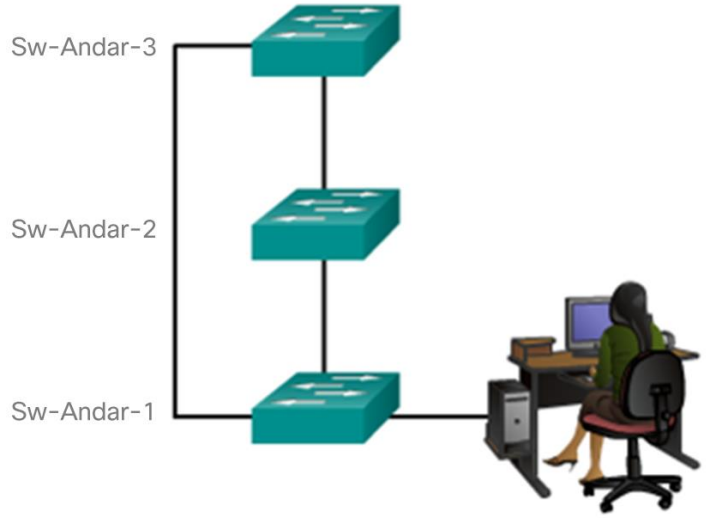
INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Nomes de dispositivos

- A primeira etapa ao configurar um switch é atribuir a ele um nome de dispositivo exclusivo, ou o nome do host.
  - Os nomes de host aparecem em prompts do CLI, podem ser usados em vários processos de autenticação entre os dispositivos e devem ser usados em diagramas de topologia.
  - Sem um nome de host, é difícil identificar os dispositivos de rede para fins de configuração.

Os nomes de host permitem que um administrador nomeie um dispositivo tornando mais fácil identificá-lo em uma rede.



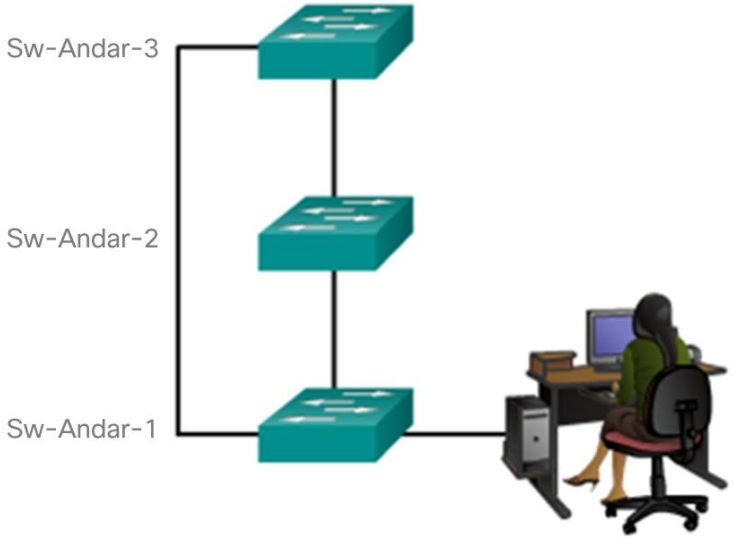
Networking Academy

Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Nomes de dispositivos

- Depois que a convenção de nomenclatura for identificada, a próxima etapa será aplicar os nomes aos dispositivos com o uso da CLI.

- O comando de configuração global **hostname** name é usado para atribuir um nome.




```
Switch>
Switch> enable
Switch#
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Configurações Gerais

Comando	Descrição
SW>	Modo EXEC Usuário
SW>enable	Habilita o modo privilegiado
SW#	Modo EXEC privilegiado
SW#configure terminal	Habilitar o modo de configuração
SW(config)#	Modo de configuração global
SW(config)#hostname SW-WRIT	Altera o nome do equipamento
SW(config)#enable password cisco	Habilita senha de enable (plain text)
SW(config)#enable secret 123	Habilita senha de enable (criptografada)
SW(config)#banner motd %Welcome%	Habilita banner de mensagem do dia
SW(config)#end	Retorna ao modo privilegiado
SW#copy running-config startup-config	Salva configuração atual da RAM na NVRAM

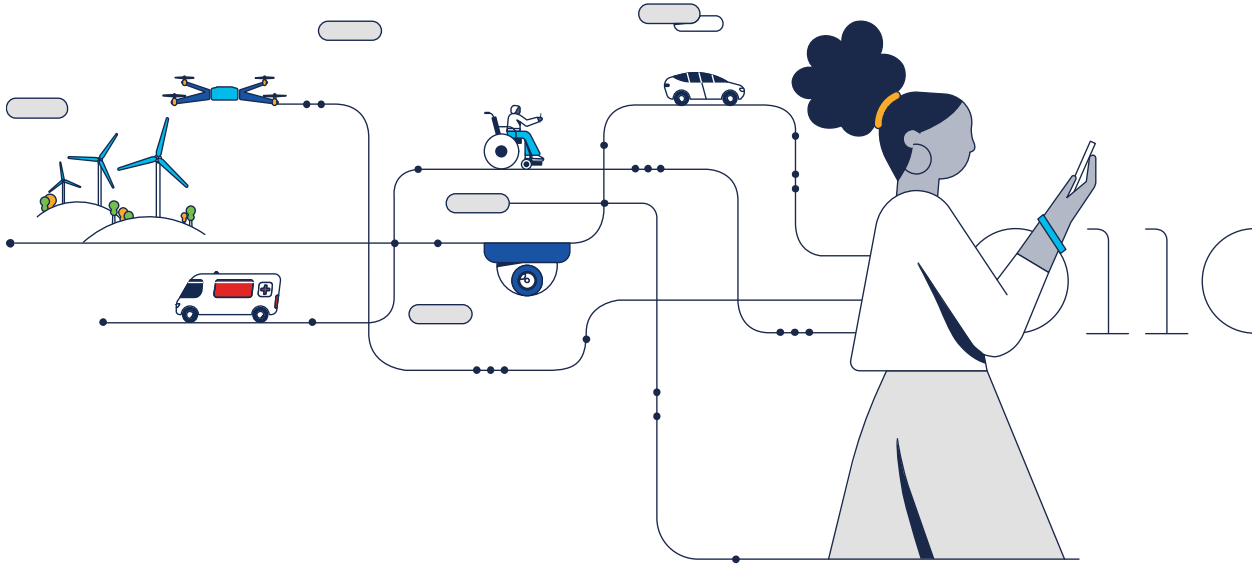
The bridge to possible

Nossos parceiros

TD SYNNEX

WISE
Women in Science
and Engineering
Inclusive Community

cisco
Networking
Academy



INTERNATIONAL
Girls in ICT Day
Brought to you by **WOMEN ROCK-IT**

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

CCNAv7 – ITN – Protocolos e Modelos

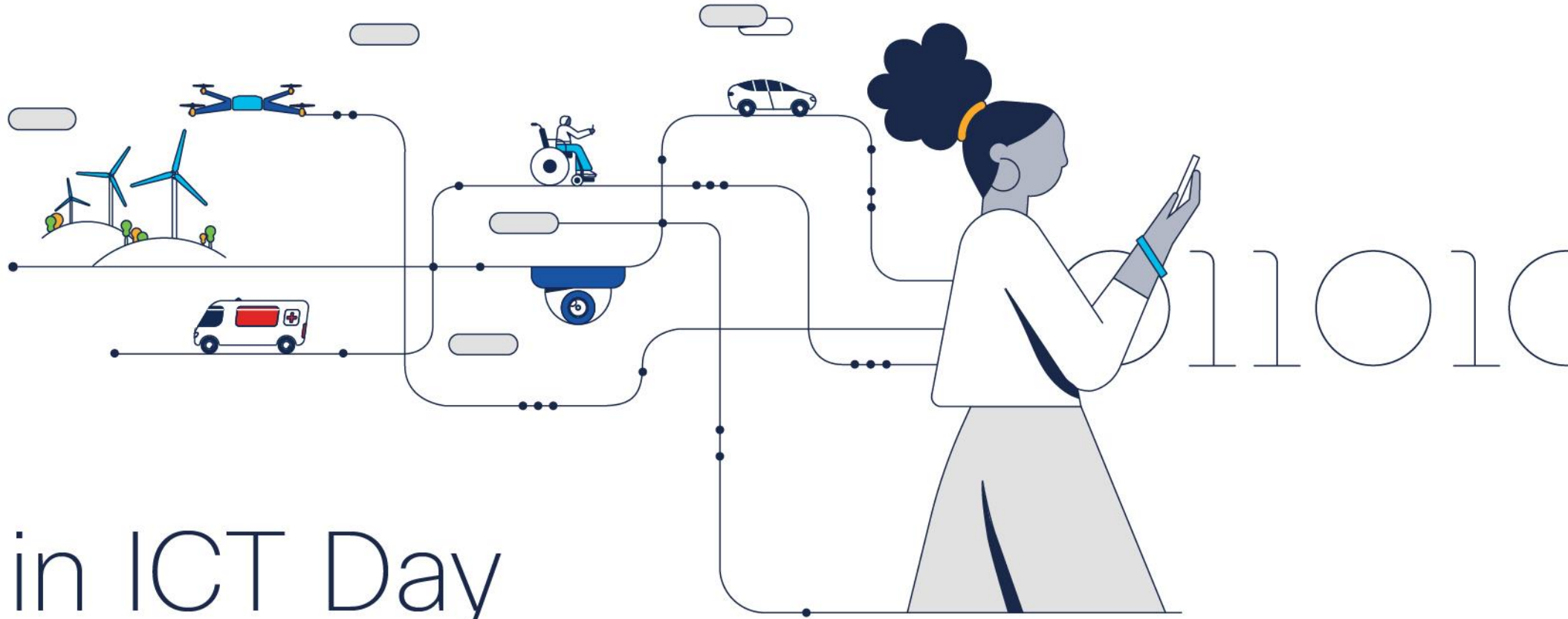
Módulo 3

Embaixadores do Programa 2020, 2021, 2022 & 2023:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

Networking
Academy



INTERNATIONAL

Girls in ICT Day

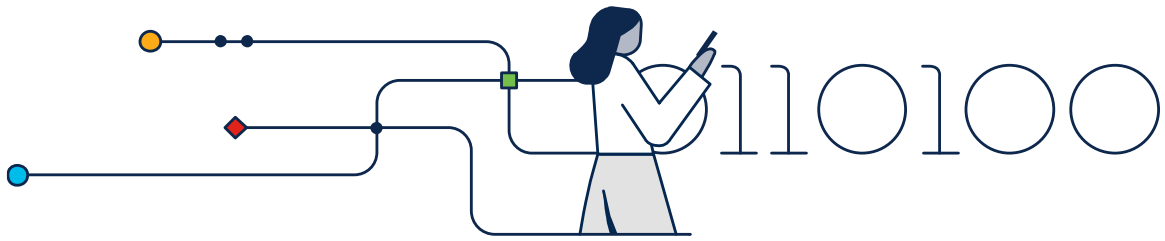
Brought to you by **WOMEN ROCK-IT**

Objetivos do Módulo

Título do Módulo: Protocolos e Modelos

Objetivo do Módulo:Explicar como os protocolos de rede permitem que dispositivos acessem recursos de rede locais e remotos.

Título do Tópico	Objetivo do Tópico
As regras	Descrever os tipos de regras que são necessárias para o êxito da comunicação.
Protocolos	Explicar a necessidade dos protocolos na comunicação de rede.
Conjuntos de protocolos	Explicar a finalidade da adesão a um conjunto de protocolos.
Empresas de padrões	Explicar a função de empresas de padrões no estabelecimento de protocolos para interoperabilidade de rede.
Modelos de referência	Explicar como o modelo TCP/IP e o modelo OSI são usados para facilitar a padronização no processo de comunicação.
Encapsulamento de dados	Explicar como o encapsulamento permite que os dados sejam transportados pela rede.
Acesso a dados	Explicar como os hosts locais acessam recursos locais em uma rede.



Regras

Princípios da Comunicação

As redes podem variar em tamanho e complexidade.

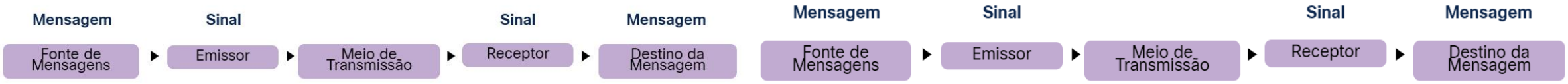
Não é suficiente ter uma conexão, os dispositivos devem concordar em “como” se comunicar.

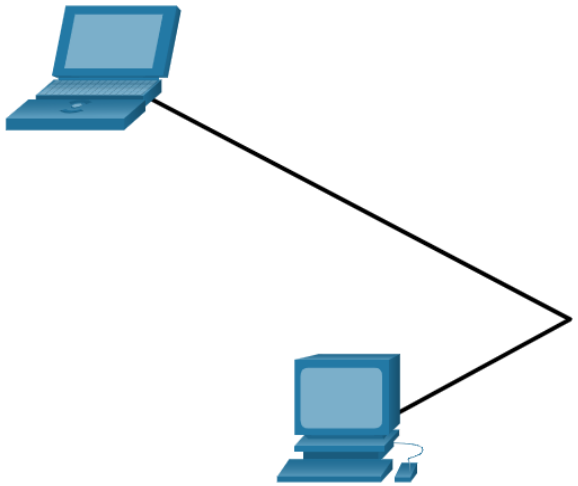
Há três elementos para qualquer comunicação:

- Haverá uma fonte (remetente).
- Haverá um destino (receptor).
- Haverá um canal (mídia) que prevê o caminho das comunicações para ocorrer.

Protocolos de Comunicação

- Todas as comunicações são regidas por protocolos.
- Protocolos são as regras que as comunicações seguirão.
- Essas regras variam de acordo com o protocolo.





Estabelecimento de metas

•Os indivíduos devem usar regras ou acordos estabelecidos para governar a conversa.

•A primeira mensagem é difícil de ler porque não está formatada corretamente. A segunda mostra a mensagem formatada corretamente

```
a comunicação humanos entre regras governam. É muito difícil entender mensagens que não são formatadas corretamente e não seguem as regras e os protocolos definidos. A estrutura da gramática, da língua, da pontuação e da sentença faz uma configuração humana compreensível por muitos indivíduos diferentes.
```

```
Regras governam a comunicação entre humanos. É muito difícil entender as mensagens que não são formatadas corretamente e não seguem as regras e os protocolos definidos. A estrutura da gramática, o idioma, a pontuação e a frase tornam a configuração humanamente compreensível para muitas pessoas diferentes.
```

Estabelecimento de Regras

Os protocolos devem ter os seguinte requisitos para entregar com êxito uma mensagem:

- Um emissor e um receptor identificados
- Língua e gramática comum
- Velocidade e ritmo de transmissão
- Requisitos de confirmação ou recepção

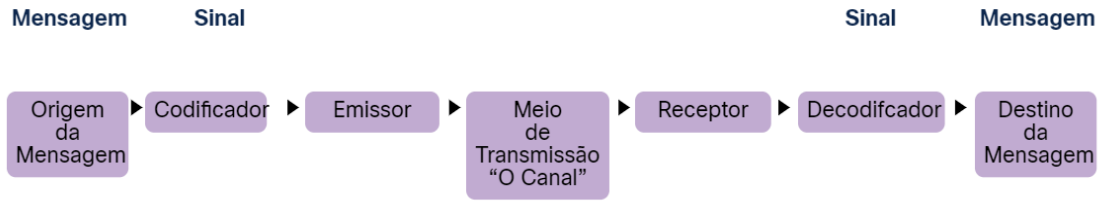
Requisitos do protocolo de rede

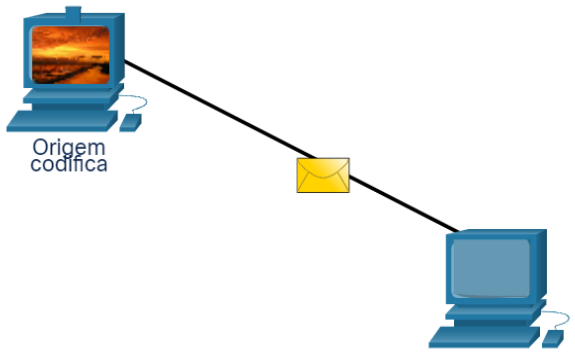
Protocolos de computador comuns devem estar de acordo e incluir os seguintes requisitos:

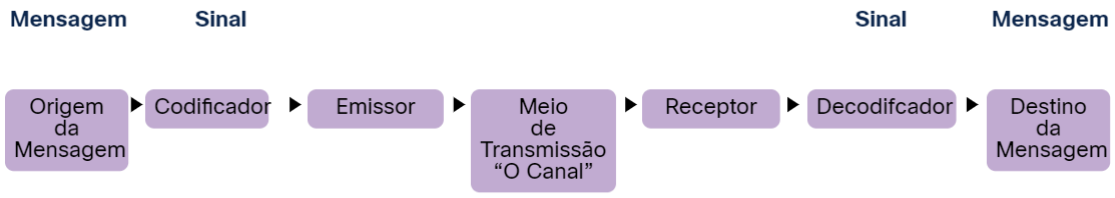
- Codificação de mensagens
- Formatação e encapsulamento de mensagens
- Tamanho da Mensagem
- Tempo da mensagem
- Opções de envio de mensagem

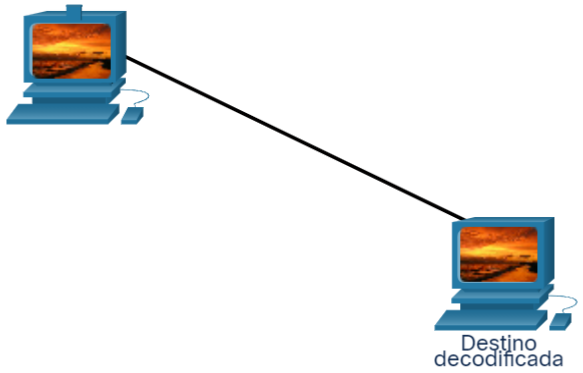
Codificação da mensagem

- A codificação é o processo de conversão de informações em outra forma aceitável para a transmissão.
- A decodificação reverte esse processo para interpretar como informações.







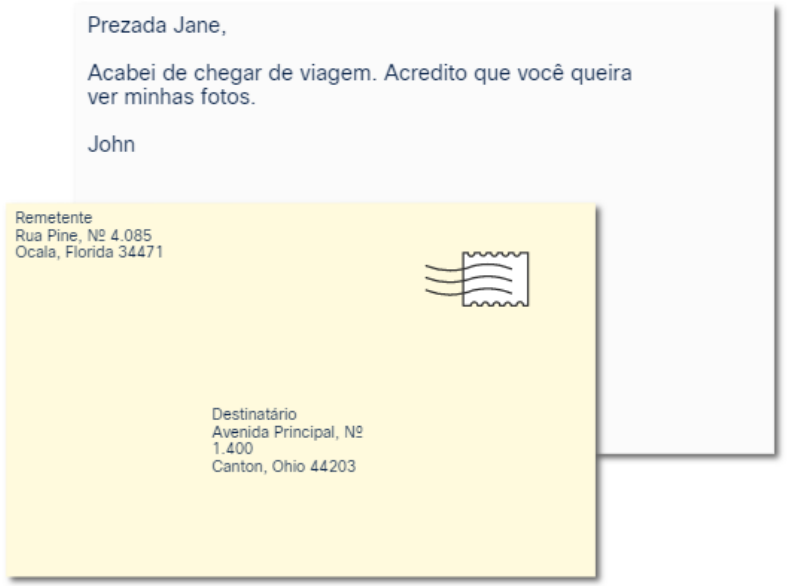


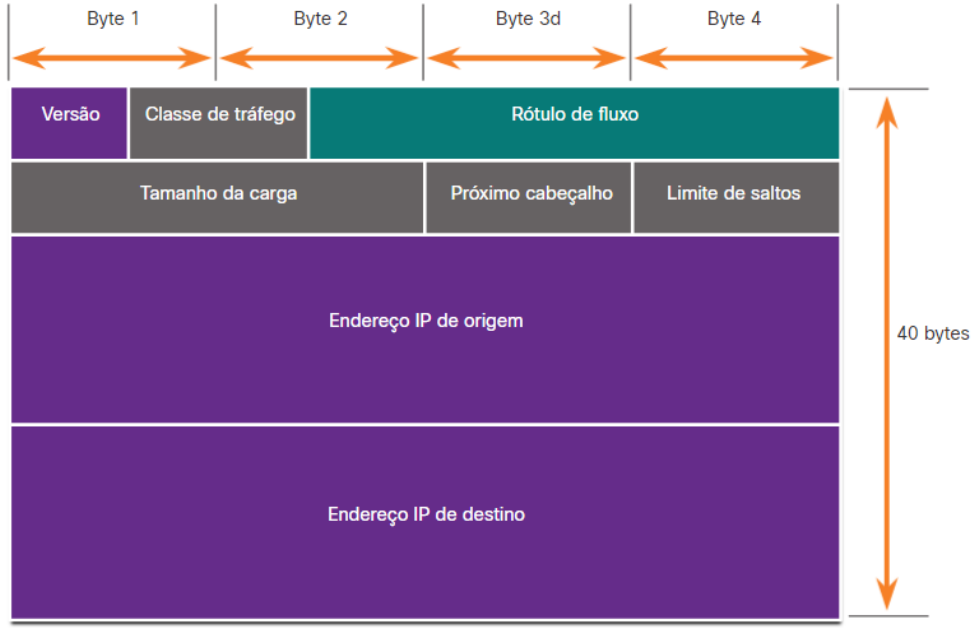
Cisco Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Formatação e encapsulamento da mensagem

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





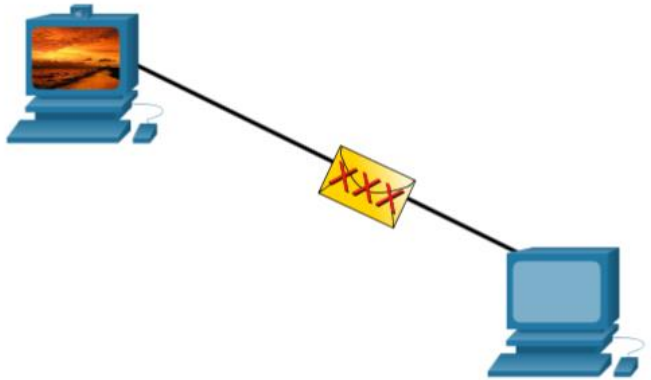
Networking Academy

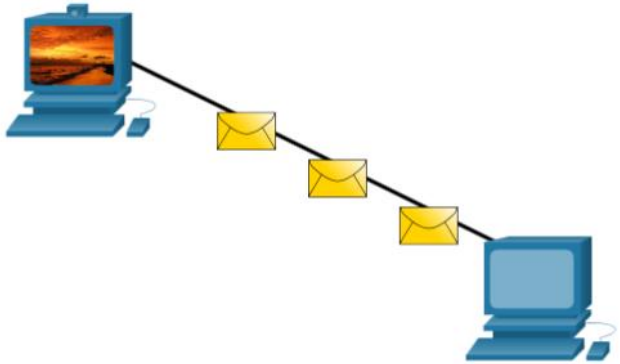
INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Tamanho da mensagem

A codificação entre hosts deve estar em um formato adequado para o meio físico.

- As mensagens enviadas pela rede são convertidas em bits
- Os bits são codificados em um padrão de luz, som ou impulsos elétricos.
- O host de destino deve decodificar os sinais para interpretar a mensagem.





Temporização de mensagem

A temporização da mensagem inclui o seguinte:

Controle de fluxo – gerencia a taxa de transmissão de dados e define quanta informação pode ser enviada e a velocidade na qual ela pode ser entregue.

Tempo limite de resposta — gerencia o tempo que um dispositivo espera quando não ouve uma resposta do destino.

Método de acesso – determinar quando alguém pode enviar uma mensagem.

- Pode haver várias regras que regem questões como “colisões”. Isso ocorre quando mais de um dispositivo envia tráfego ao mesmo tempo e as mensagens ficam corrompidas.
- Alguns protocolos são proativos e tentam evitar colisões; outros protocolos são reativos e estabelecem um método de recuperação após a colisão ocorrer.

Opções de entrega da mensagem

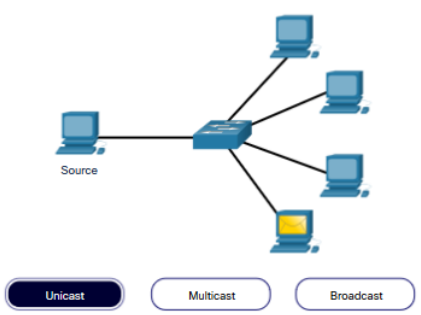
A entrega de mensagens pode ser um dos seguintes métodos:

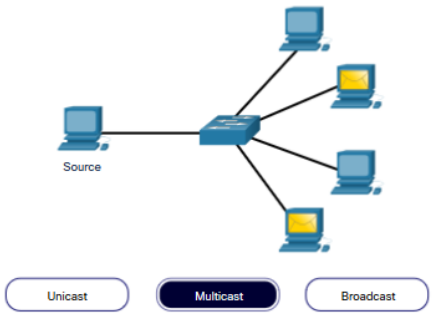
Unicast – comunicação um para um.

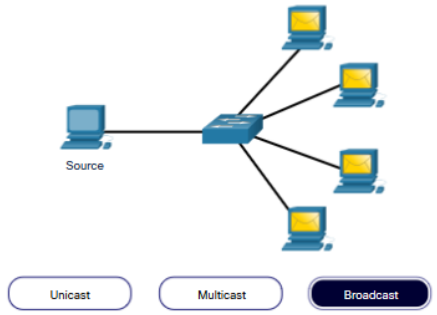
Multicast – um para muitos, geralmente não todos

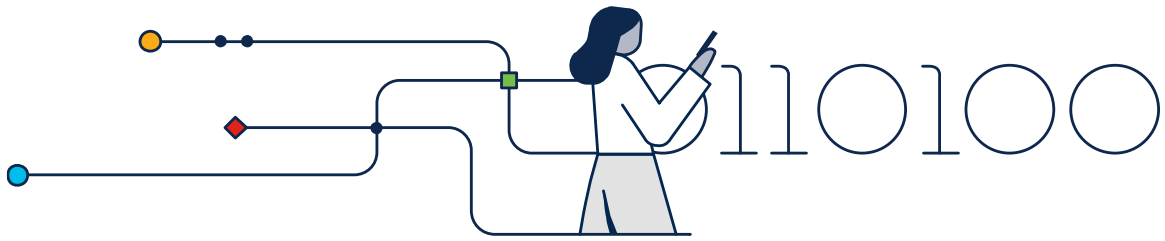
Broadcast – um para todos

Nota: Astransmissões são usadas em redes IPv4, mas não são uma opção para IPv6. Mais tarde, também veremos “Anycast” como uma opção de entrega adicional para IPv6.









Protocolos

Visão geral do protocolo de rede

Protocolos de rede definem um conjunto comum de regras.

Pode ser implementado em dispositivos em:

- Software
- Hardware
- Ambos

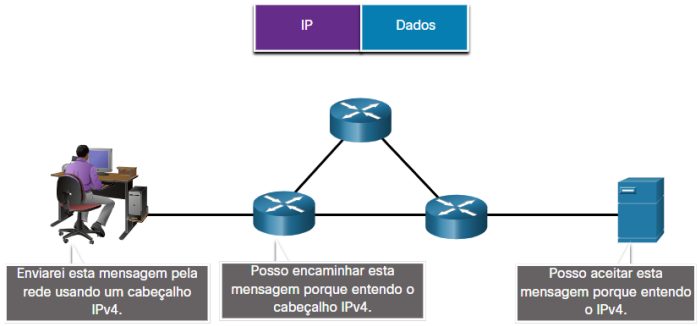
Cada protocolo tem sua própria:

- Função
- Formato
- Regras

Tipo de Protocolo	Descrição
Comunicações em Rede	permitir que dois ou mais dispositivos se comuniquem através de uma ou mais redes
Segurança da rede	dados seguros para fornecer autenticação, integridade de dados e criptografia de dados
Roteamento	permitir que os roteadores troquem informações de rota, comparem informações de caminho e selecionem o melhor caminho
Descoberta de serviço	usado para a detecção automática de dispositivos ou serviços

Funções de protocolo de rede

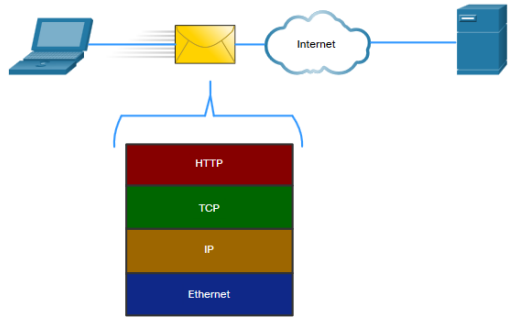
- Os dispositivos usam protocolos acordados para se comunicar.
- Protocolos podem ter uma ou mais funções.



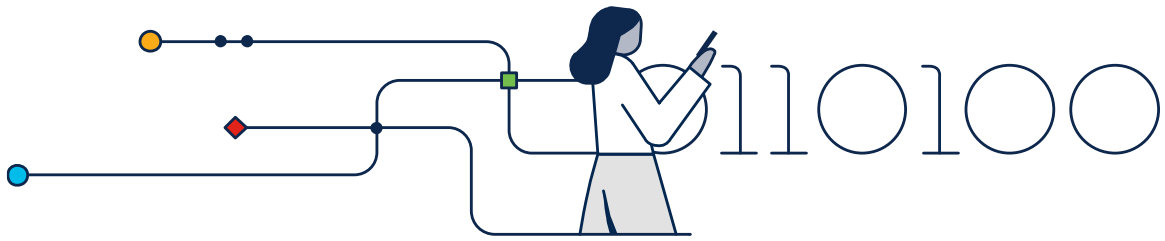
Função	Descrição
Endereçamento	Identificação de remetente e destinatário
Confiabilidade	Fornece entrega garantida
Controle de fluxo	Garante fluxos de dados a uma taxaeficiente
Sequenciamento	Rotula exclusivamente cada segmento de dados transmitido
Detecção de erros	Determina se os dados ficaram corrompidos durante a transmissão
Interface de aplicação	Comunicações de processo a processo entre aplicativos de rede

Interação de protocolos

- As redes exigem o uso de vários protocolos.
- Cada protocolo tem sua própria função e formato.



Protocolos	Função
Protocolo HTTP	▪ Governa a maneira como um servidor da Web e um cliente da Web interagem ▪ Define conteúdo e formato
Protocolo TCP	▪ Gerencia as conversas individuais ▪ Fornece entrega garantida ▪ Gerencia o controle de fluxo
Protocolo IP	Entrega mensagens globalmente do remetente para o receptor
Ethernet	Entrega mensagens de uma NIC para outra NIC na mesma rede local (LAN) Ethernet



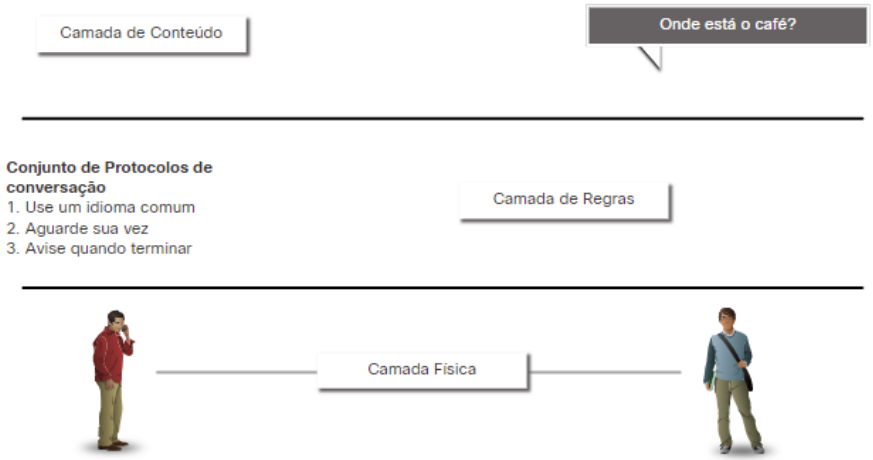
Conjunto de Protocolos

Conjuntos de protocolos de rede

Os protocolos devem ser capazes de funcionar com outros protocolos.

Conjunto de Protocolos:

- Um grupo de protocolos inter-relacionados necessários para executar uma função de comunicação
- Conjuntos de regras que trabalham juntos para ajudar a resolver um problema



Suítes de Protocolos são grupos de regras que funcionam em conjunto para ajudar a resolver um problema.

Os protocolos são visualizados em termos de camadas:

- Camadas Superiores – preocupam com o conteúdo da mensagem
- Camadas Inferiores - preocupado com a movimentação de dados e fornecer serviços para camadas superiores

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Evolução dos conjuntos de protocolos

Existem vários conjuntos de protocolos.

•**Internet Protocol Suite ou TCP/IP**

- O conjunto de protocolos mais comum e mantido pela Internet Engineering Task Force (IETF)

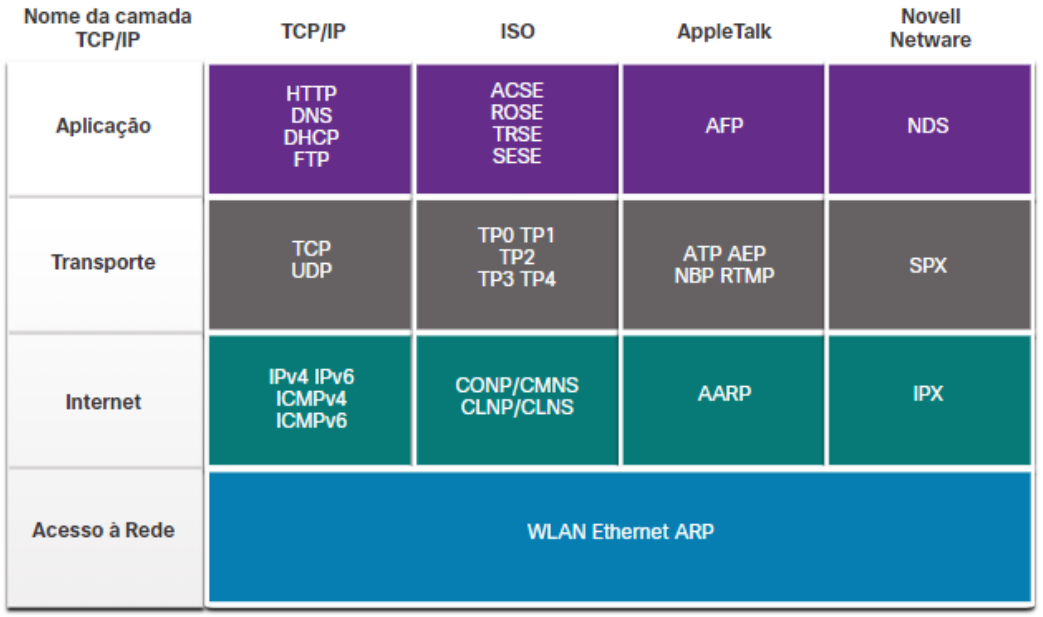
•**Protocolos de Interconexão de Sistemas Abertos (OSI)** - Desenvolvido pela Organização Internacional de Normalização (ISO) e pela União Internacional de Telecomunicações (UIT)

•**AppleTalk**

- Lançamento da suíte proprietária da Apple Inc.

•**Novell NetWare**

- Suíte proprietária desenvolvida pela Novell Inc.



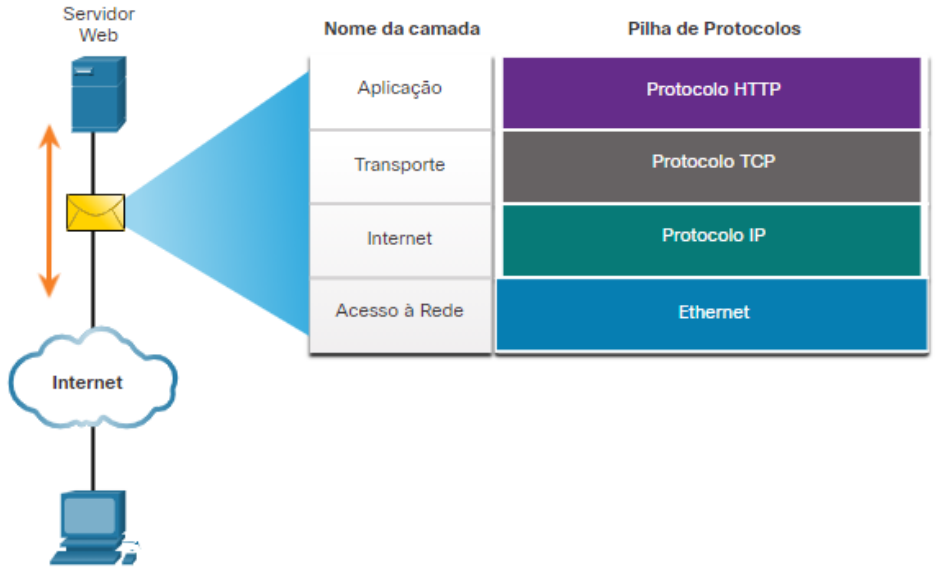
Networking Academy

INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

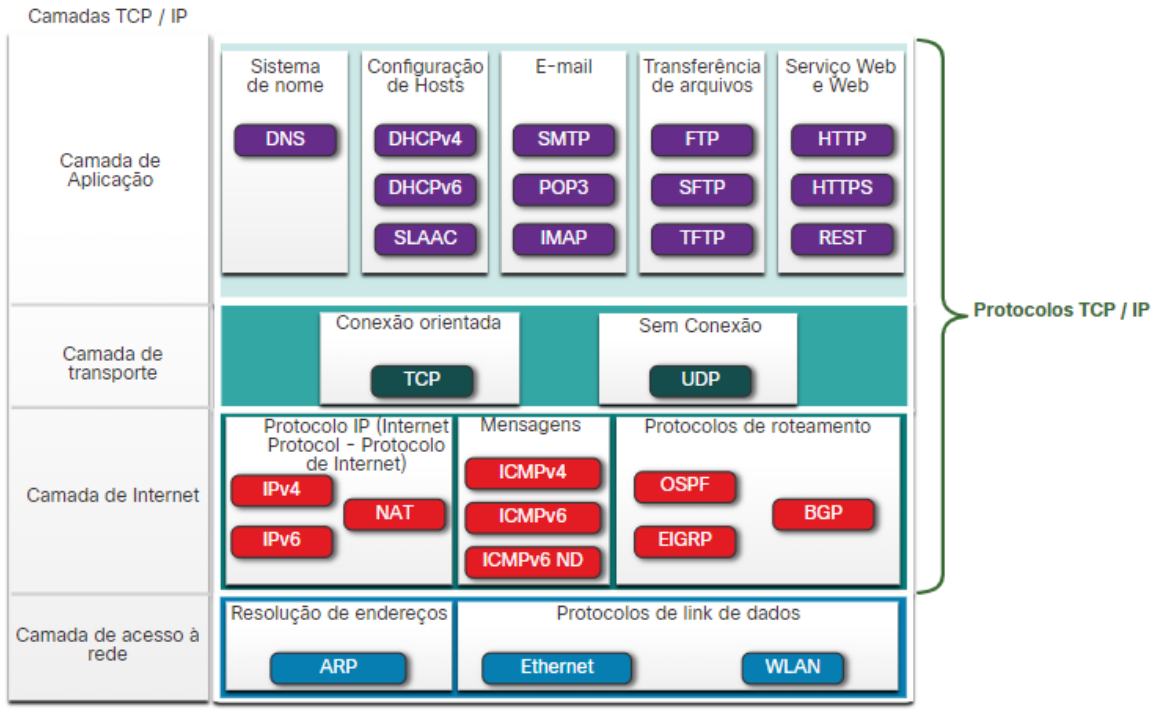
Exemplo de protocolo TCP / IP

- Os protocolos TCP / IP operam nas camadas de aplicação, transporte e Internet.
- Os protocolos LAN de camada de acesso à rede mais comuns são Ethernet e WLAN (LAN sem fio).



Suíte de Protocolos TCP/IP

- TCP/IP é o conjunto de protocolos usado pela internet e inclui muitos protocolos.
- **O TCP/IP é:**
  - Um conjunto de protocolos padrão aberto que está disponível gratuitamente para o público e pode ser usado por qualquer fornecedor
  - Um conjunto de protocolos baseado em padrões que é endossado pelo setor de redes e aprovado por uma organização de padrões para garantir a interoperabilidade

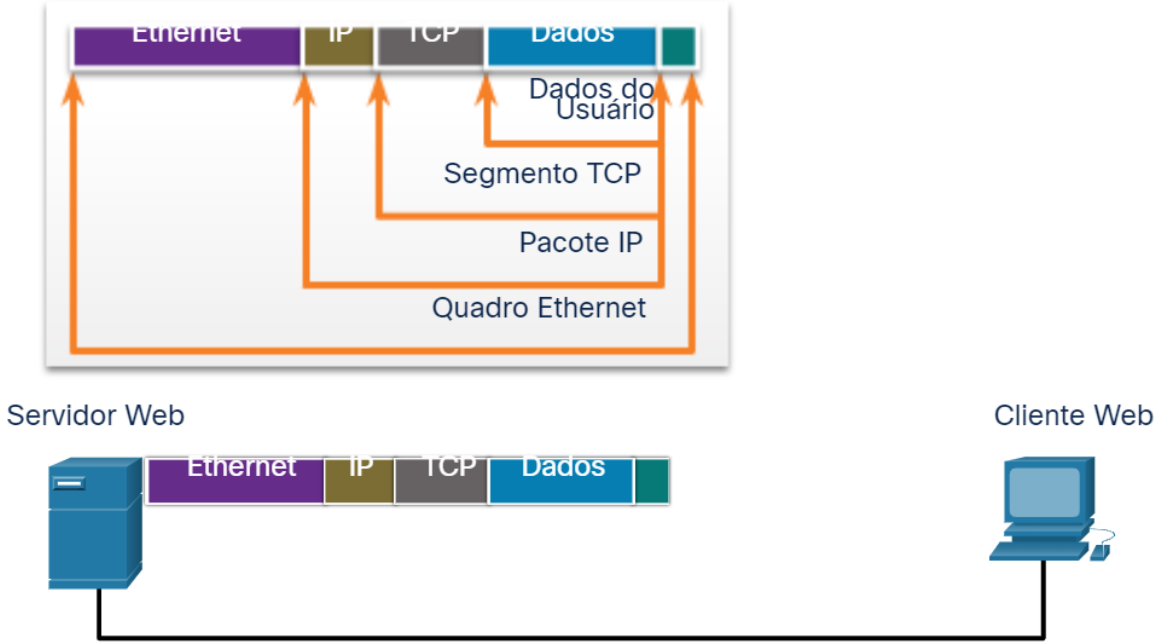


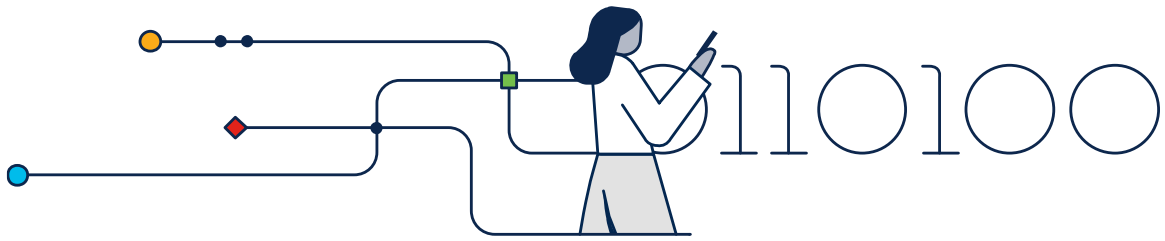
Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Processo de Comunicação TCP/IP

- Um servidor web encapsulando e enviando uma página da Web para um cliente.
- Um cliente desencapsulando a página da Web para o navegador da Web





Empresas de Padrões

Padrões Abertos

As normas abertas incentivam:

- interoperabilidade
- concorrência
- negócios

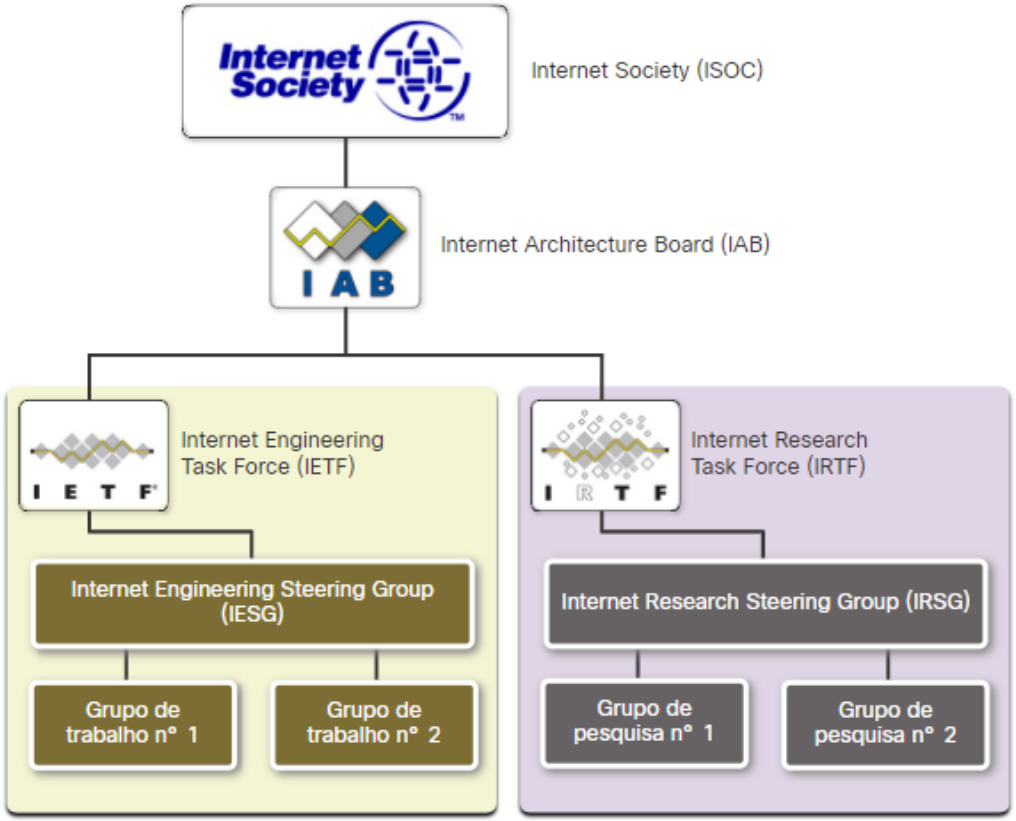
As organizações de padrões são:

- fornecedor neutro
- organizações sem fins lucrativos
- criado para desenvolver e promover o conceito de normas abertas.

CISCO Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Padrões de Internet

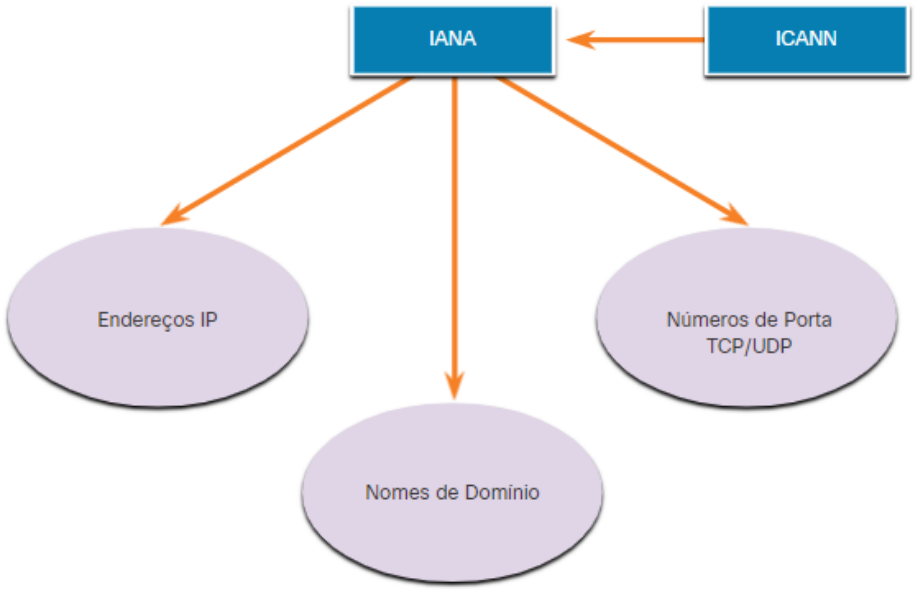


- **Internet Society (ISOC)** - Promove o desenvolvimento aberto e a evolução da Internet
- **Conselho de Arquitetura da Internet (IAB)** - Responsável pelo gerenciamento e desenvolvimento geral dos padrões da Internet.
- **IETF (Internet Engineering Task Force)** - Desenvolve, atualiza e mantém tecnologias de Internet e TCP / IP
- **Força-Tarefa de Pesquisa na Internet (IRTF)** - Focada em pesquisas de longo prazo relacionadas à Internet e aos protocolos TCP / IP

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Padrões de Internet



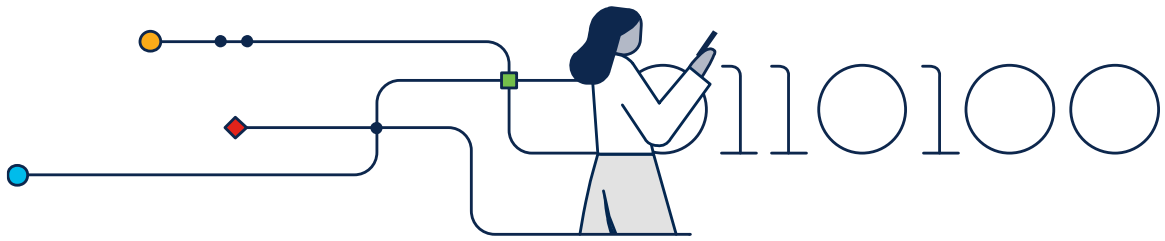
Organizações de padrões envolvidas no desenvolvimento e suporte de TCP / IP

- **Corporação da Internet para nomes e números atribuídos (ICANN)** - Coordena a alocação de endereços IP, o gerenciamento de nomes de domínio e a atribuição de outras informações
- **Autoridade para atribuição de números da Internet (IANA)** - supervisiona e gerencia a alocação de endereços IP, o gerenciamento de nomes de domínio e os identificadores de protocolo da ICANN

Organizações de padrões

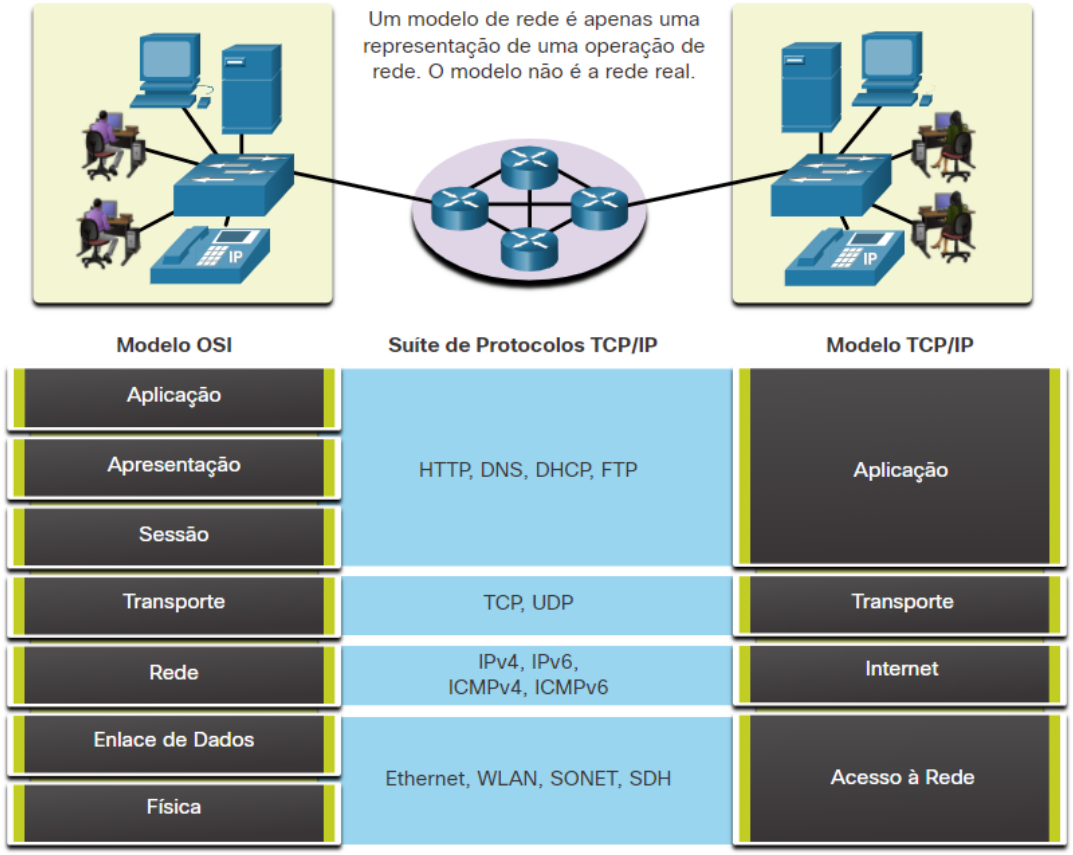
Padrões eletrônicos e de comunicações

- **Instituto de Engenheiros Elétricos e Eletrônicos (IEEE**, pronunciado "I-triple-E") - dedicado à criação de padrões em potência e energia, saúde, telecomunicações e redes
- **Electronic Industries Alliance (EIA)** - desenvolve padrões relacionados à fiação elétrica, conectores e racks de 19 polegadas usados para montar equipamentos de rede
- **Associação da Indústria de Telecomunicações (TIA)** - desenvolve padrões de comunicação em equipamentos de rádio, torres celulares, dispositivos de Voz sobre IP (VoIP), comunicações por satélite e muito mais
- **Setor de padronização de telecomunicações e união internacional de telecomunicações (ITU-T)** - define padrões para compactação de vídeo, IPTV (Internet Protocol Television) e comunicações de banda larga, como uma linha de assinante digital (DSL)



Modelos de Referência

Benefícios de se usar um modelo de camadas



Conceitos complexos, como a forma como uma rede opera, podem ser difíceis de explicar e compreender. Por esse motivo, um modelo em camadas é usado.

Dois modelos em camadas descrevem as operações de rede:

- Modelo de referência OSI (Open System Interconnection)
- Modelo de referência TCP/IP

Cisco Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Benefícios de se usar um modelo de camadas

Estes são os benefícios do uso de um modelo em camadas:

- Auxiliar no projeto de protocolos porque os protocolos que operam em uma camada específica definiram as informações sobre as quais atuam e uma interface definida para as camadas acima e abaixo
- Estimula a competição porque os produtos de diferentes fornecedores podem trabalhar em conjunto
- Impedir que alterações de tecnologia ou capacidade em uma camada afetem outras camadas acima e abaixo
- Fornece um idioma comum para descrever funções e habilidades de rede.

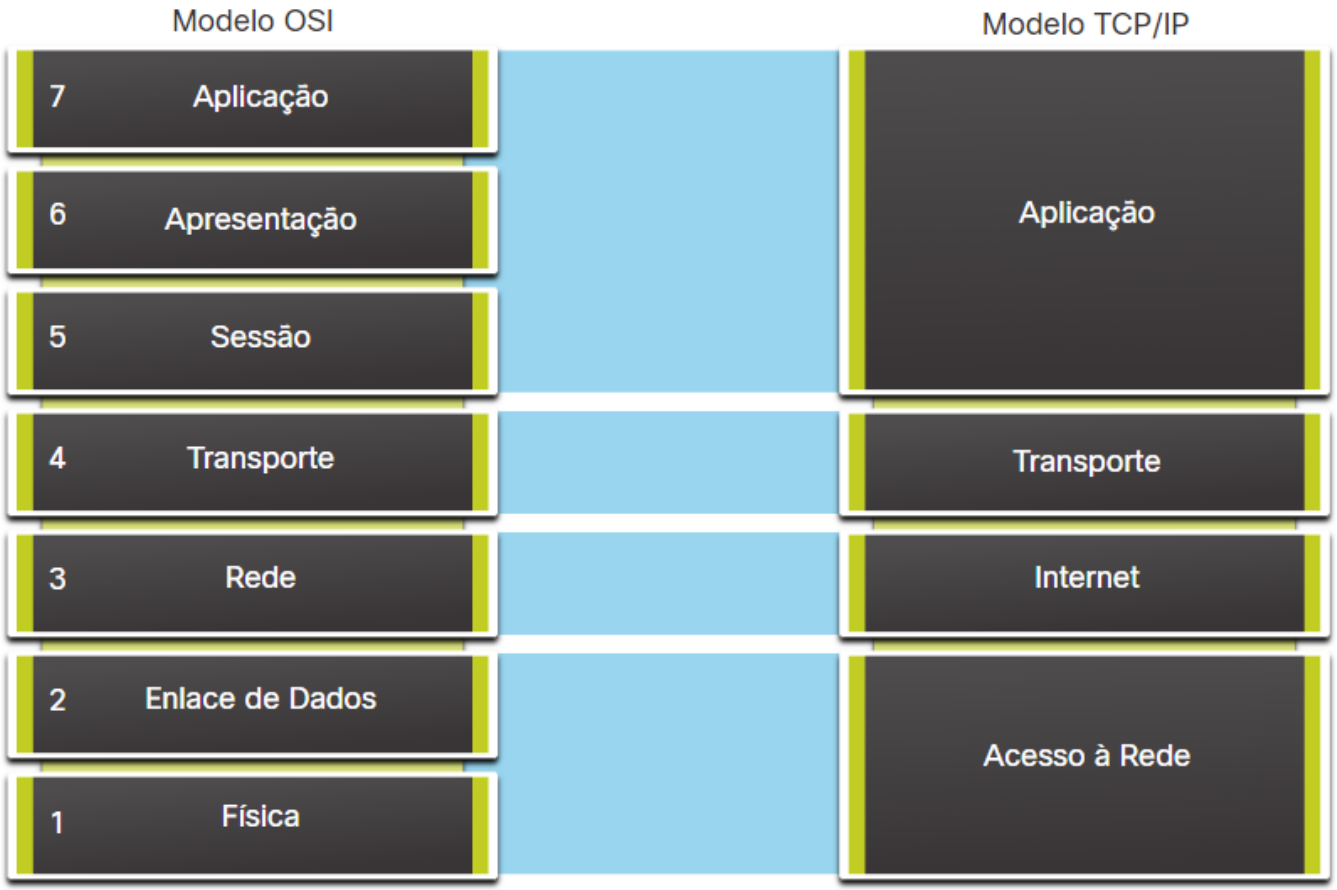
O modelo de referência OSI

Camada de modelo OSI	Descrição
7 - Aplicação	Contém protocolos usados para comunicações processo a processo
6 - Apresentação	Fornece representação comum dos dados transferidos entre os serviços da camada de aplicativo.
5 - Sessão	Fornece serviços para a camada de apresentação e para gerenciar a troca de dados.
4 - Transporte	Define serviços para segmentar, transferir e remontar os dados para comunicações individuais.
3 - Rede	Fornece serviços para troca de dados individuais pela rede.
2 - Link de dados	Descreve métodos para a troca de quadros de dados em uma mídia comum.
1 - Físico	Descreve os meios para ativar, manter e desativar conexões físicas.

O modelo de referência TCP / IP

Camada do modelo TCP/IP	Descrição
Aplicação	Representa dados para o usuário, além do controle de codificação e de diálogo.
Transporte	Permite a comunicação entre vários dispositivos diferentes em redes distintas.
Internet	Determina o melhor caminho pela rede.
Endereço de rede	Controla os dispositivos de hardware e o meio físico que formam a rede.

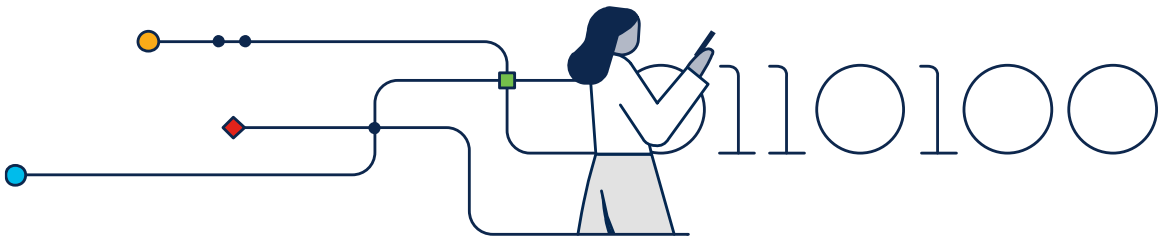
Comparação de modelos OSI e TCP / IP



- O modelo OSI divide a camada de acesso à rede e a camada de aplicação do modelo TCP/IP em várias camadas.
- O conjunto de protocolos TCP/IP não especifica quais protocolos usar ao transmitir por meio de uma mídia física.
- As Camadas 1 e 2 do modelo OSI discutem os procedimentos necessários para acessar a mídia e o meio físico para enviar dados por uma rede.

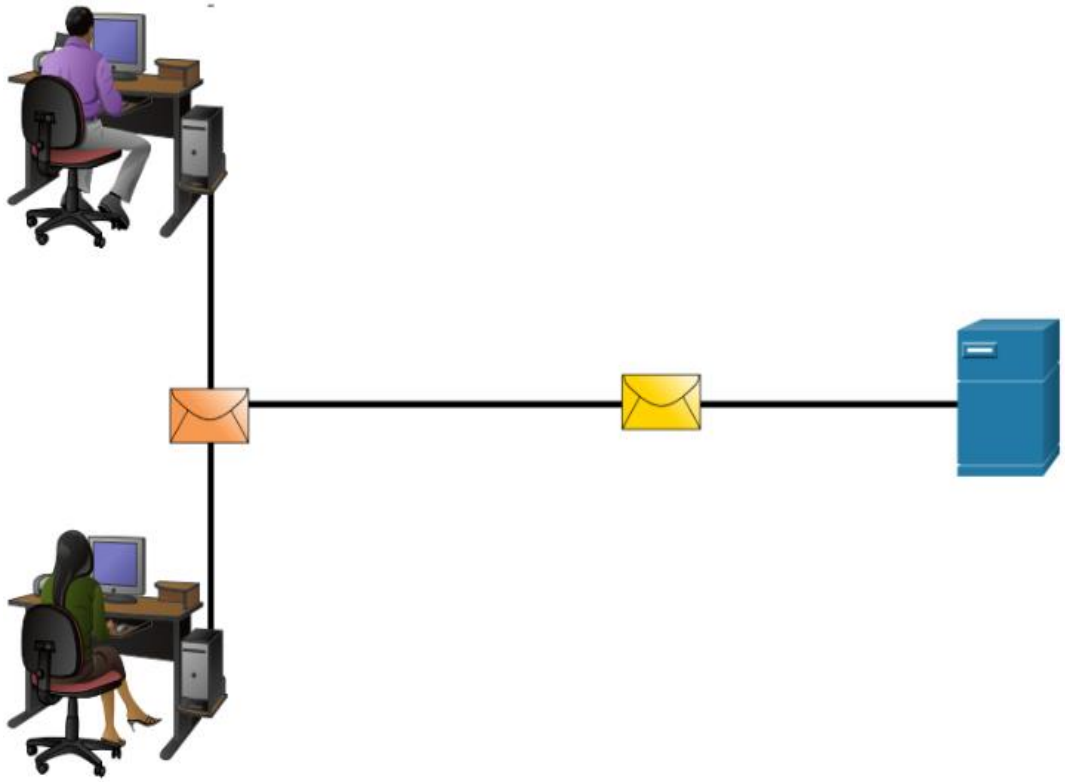
cisco Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT



Encapsulamento de Dados

Segmentação de mensagens

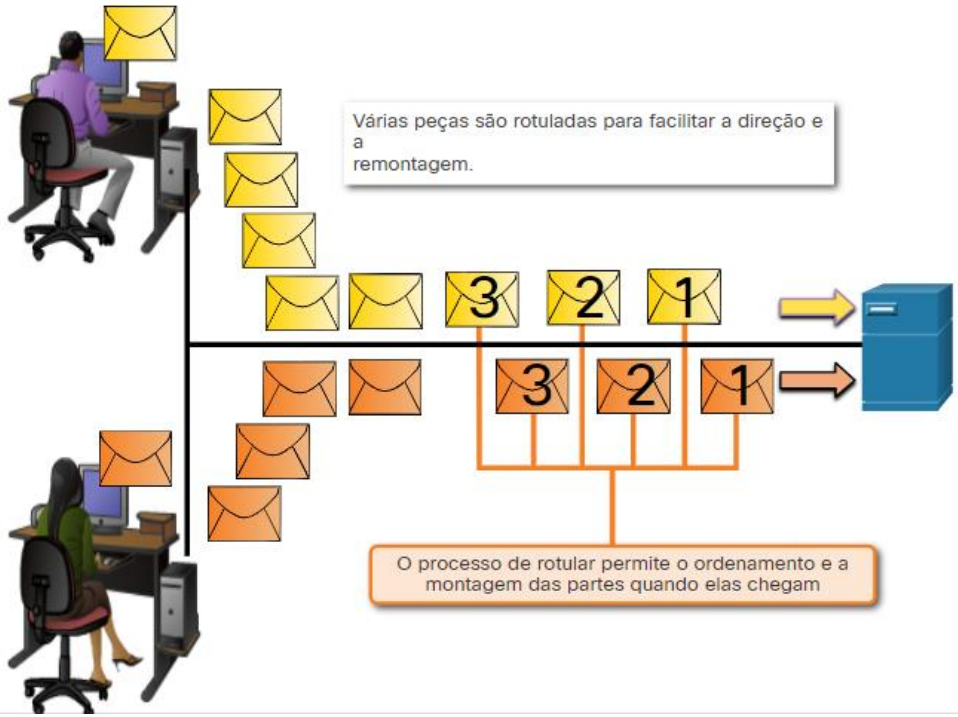


Segmentação é o processo de dividir mensagens em unidades menores. Multiplexação é o processo de tomar vários fluxos de dados segmentados e intercalá-los juntos.

A segmentação de mensagens apresenta dois benefícios principais:

- **Aumenta a velocidade** - É possível enviar grandes quantidades de dados pela rede sem vincular um link de comunicação.
- **Aumenta a eficiência** - Somente segmentos que não conseguem alcançar o destino precisam ser retransmitidos, não todo o fluxo de dados.

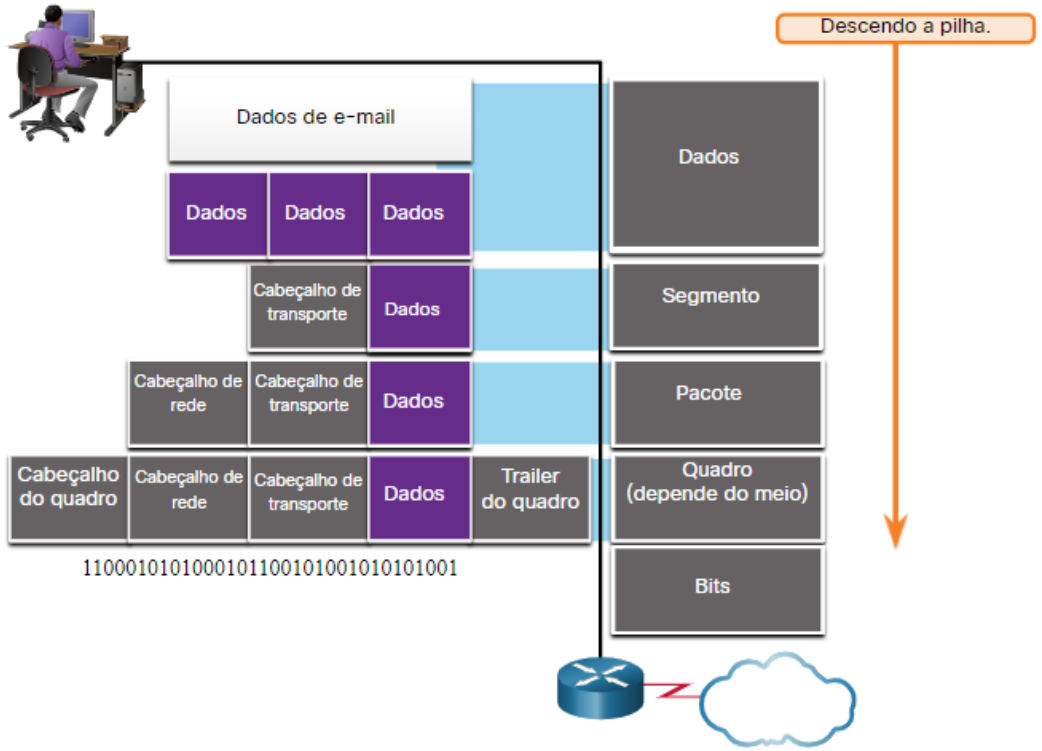
Sequenciamento



Mensagens de sequenciamento é o processo de numeração dos segmentos para que a mensagem possa ser remontada no destino.

O TCP é responsável por sequenciar os segmentos individuais.

Unidades de dados de protocolo



Encapsulamento é o processo em que os protocolos adicionam suas informações aos dados.

- Em cada etapa do processo, uma PDU possui um nome diferente para refletir suas novas funções.
- Não há convenção de nomenclatura universal para PDUs; neste curso, as PDUs são nomeadas de acordo com os protocolos do conjunto TCP / IP.
- PDUs passando a pilha são as seguintes:

1. Dados (fluxo de dados)
2. Segmento
3. Pacote
4. Quadro
5. Bits (Fluxo de Bits)

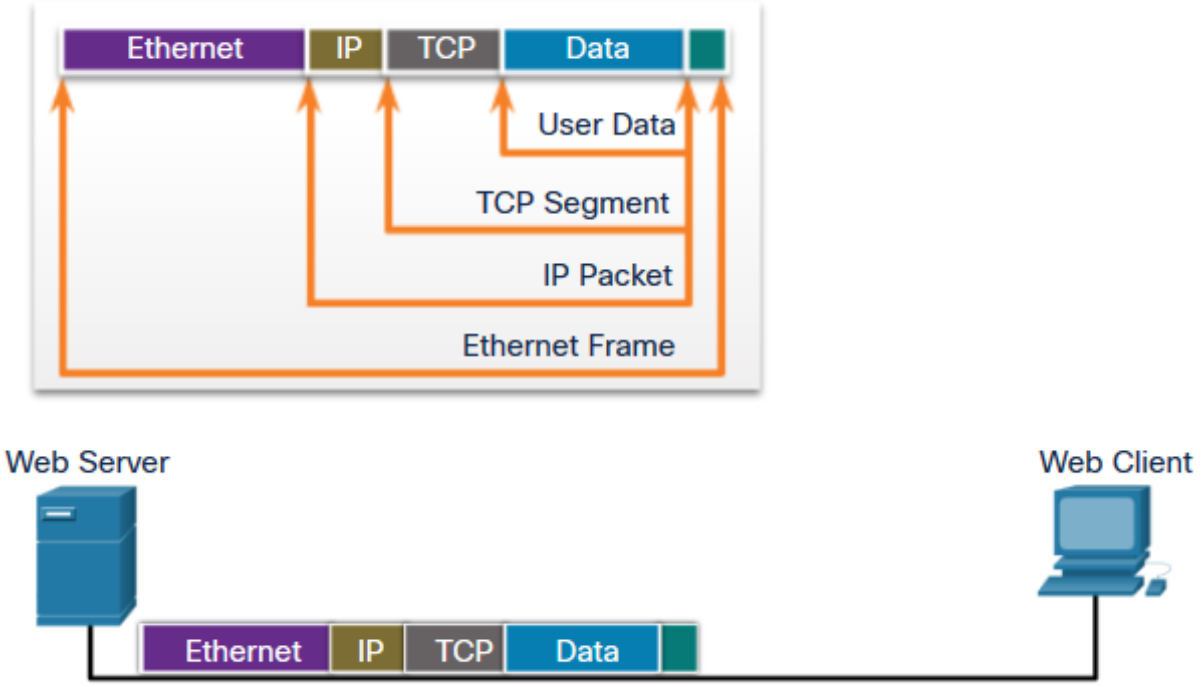
cisco Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Exemplo de encapsulamento

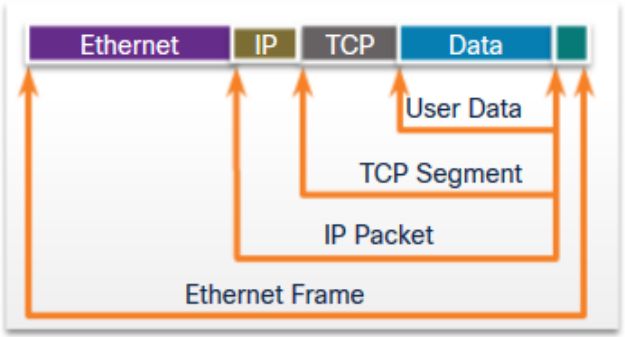
- O encapsulamento é um processo de cima para baixo.
- O nível acima faz o seu processo e, em seguida, passa-o para o próximo nível do modelo.

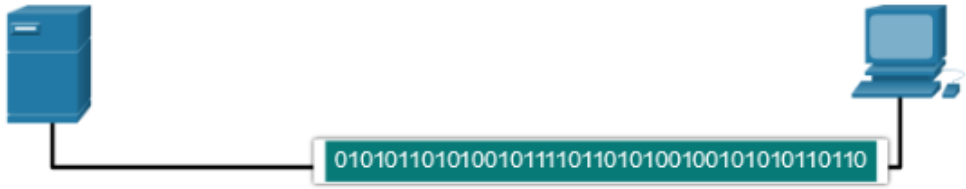
Este processo é repetido por cada camada até que seja enviado como um fluxo de bits.



Exemplo de desencapsulamento

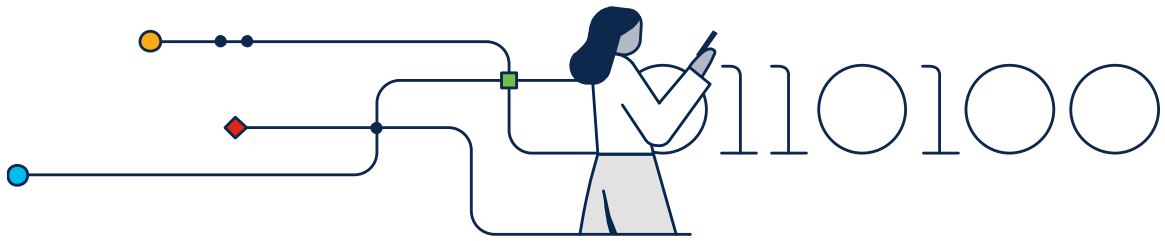
- Os dados são desencapsulados à medida que se move para cima da pilha.
- Quando uma camada completa seu processo, essa camada tira seu cabeçalho e passa para o próximo nível a ser processado. Isso é repetido em cada camada até que seja um fluxo de dados que o aplicativo pode processar.
  1. Recebido como Bits (Fluxo de Bits)
  2. Quadro
  3. Pacote
  4. Segmento
  5. Dados (fluxo de dados)





Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT



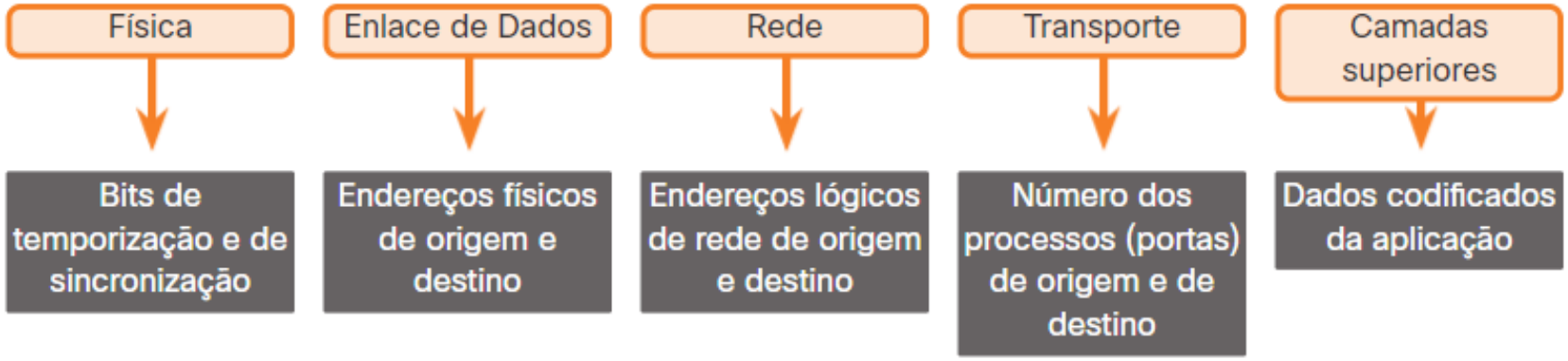
Acesso aos Dados

Endereços

Tanto o link de dados quanto as camadas de rede usam endereçamento para entregar dados da origem ao destino.

Endereços origem e destino da camada de rede - Responsáveis por entregar o pacote IP da origem para o destino final.

Endereços de origem e destino da camada de enlace de dados - Responsável por fornecer o quadro de enlace de dados de uma placa de interface de rede (NIC) para outra NIC na mesma rede.

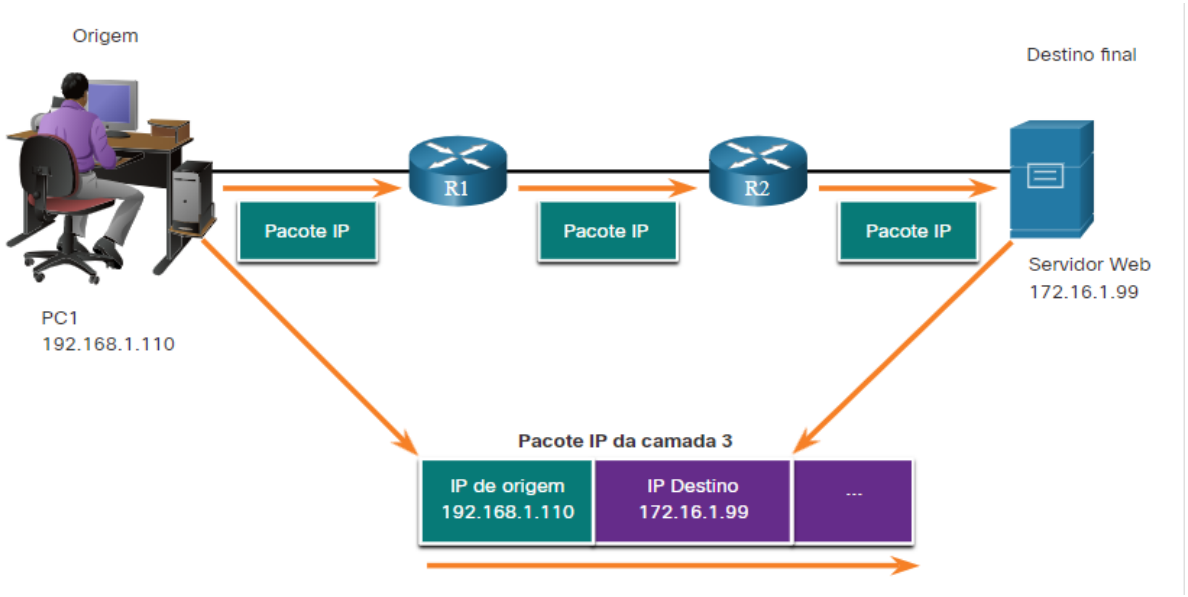


Endereço Lógico da Camada 3

O pacote IP contém dois endereços IP:

- **Endereço IP origem** - O endereço IP do dispositivo emissor, a origem do pacote.
- **Endereço IP de destino** - O endereço IP do dispositivo receptor, o destino final do pacote.

Esses endereços podem estar no mesmo link ou remoto.



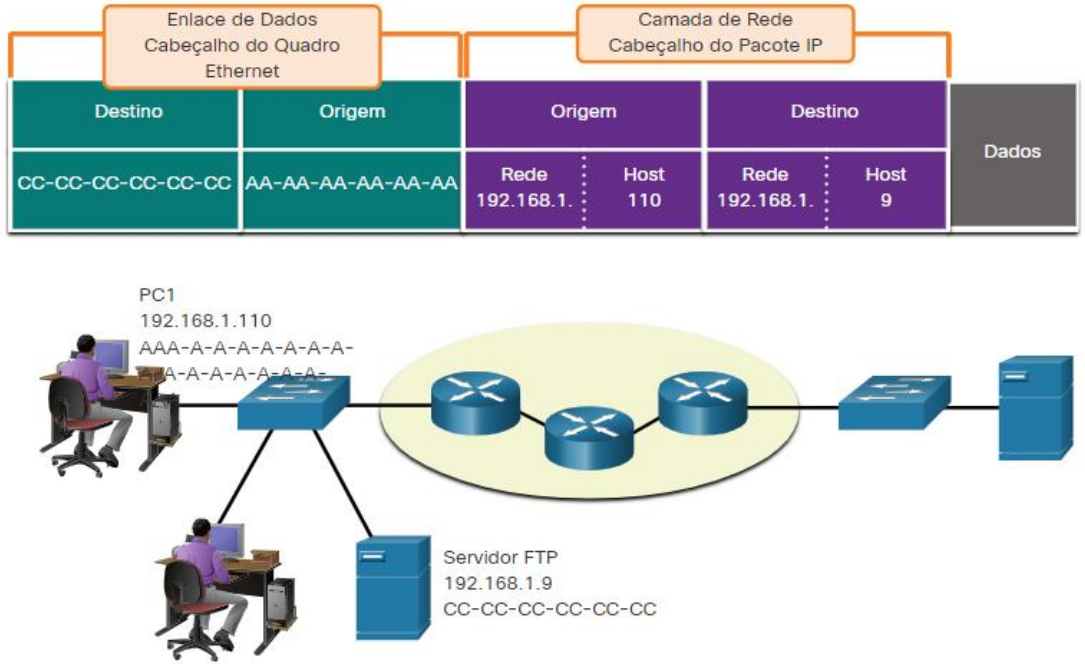
Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Dispositivos na mesma rede

Quando os dispositivos estão na mesma rede, a origem e o destino terão o mesmo número na parte da rede do endereço.

- PC1 — 192.168.1.110
- Servidor FTP — 192.168.1.9

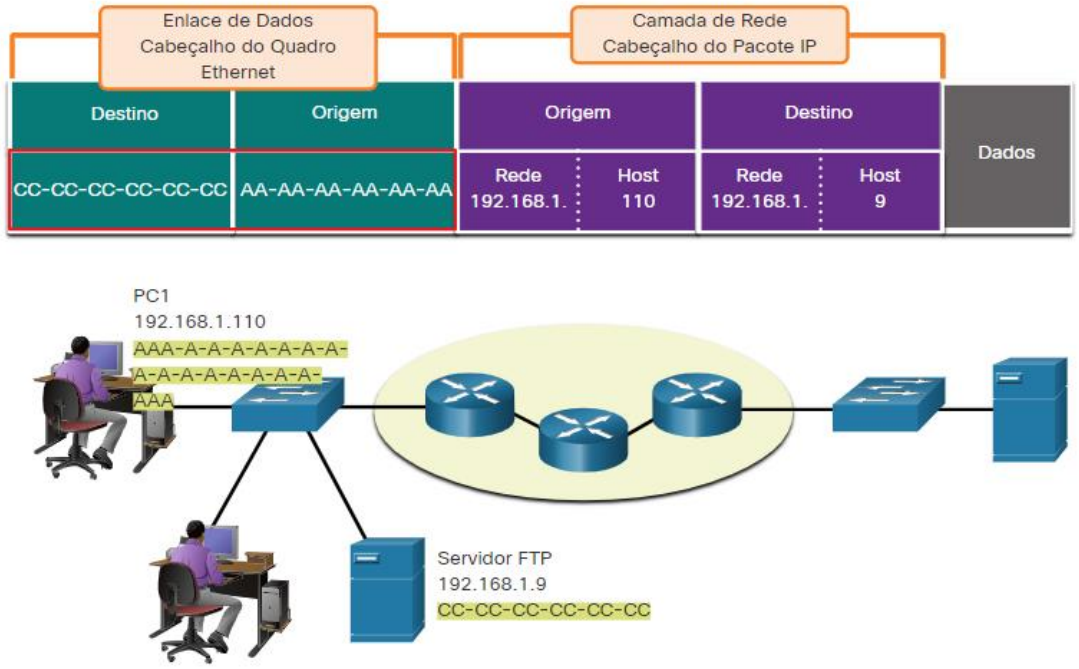


Função de Acesso a Dados dos Endereços da Camada de Link de Dados: Mesma Rede IP

Quando os dispositivos estiverem na mesma rede Ethernet, o quadro do link de dados usará o endereço MAC real da NIC de destino.

Os endereços MAC são fisicamente incorporados à NIC Ethernet e são endereçamento local.

- O endereço MAC de origem será o do originador no link.
- O endereço MAC de destino estará sempre no mesmo link que a origem, mesmo que o destino final seja remoto.

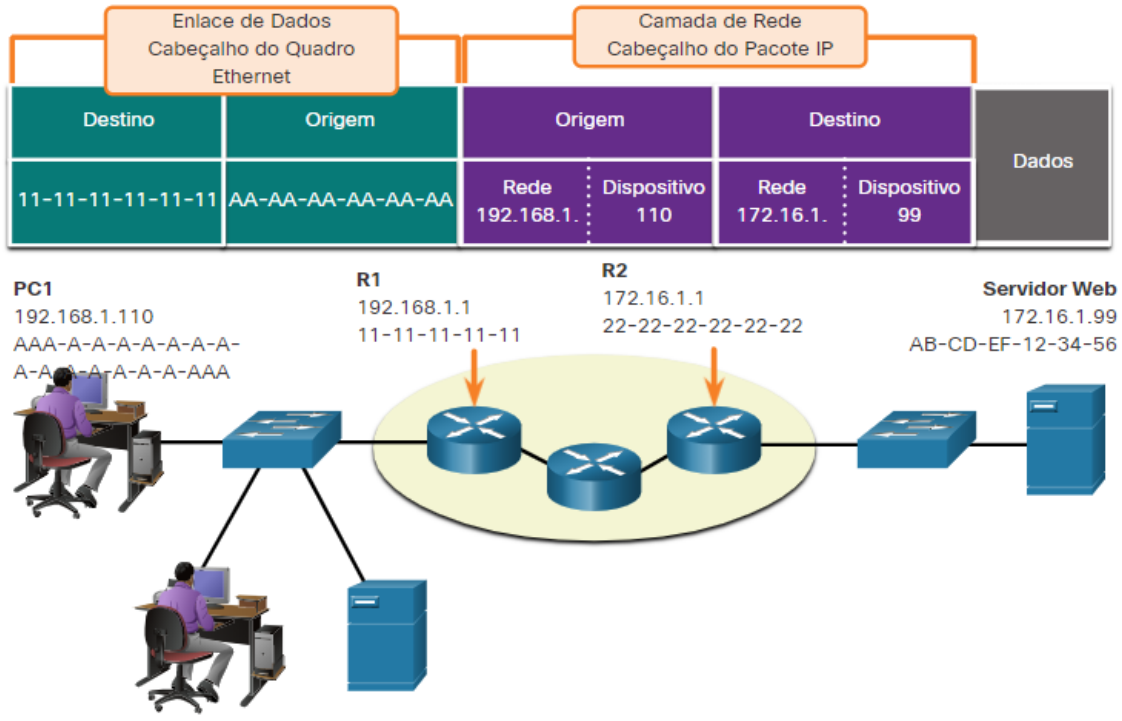


Cisco Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Dispositivos em uma rede remota

- O que acontece quando o destino real (final) não está na mesma LAN e é remoto?
- O que acontece quando PC1 tenta alcançar o servidor Web?
- Isso afeta as camadas de rede e de link de dados?



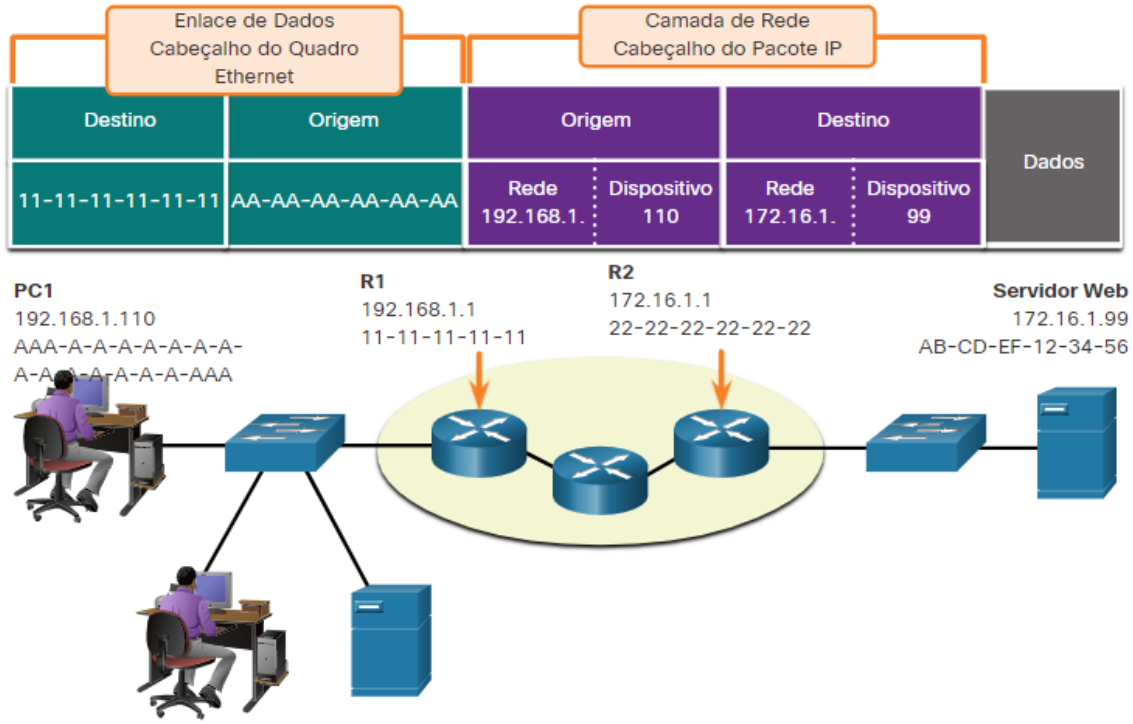
Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Função dos endereços da camada de rede

Quando a origem e o destino têm uma parte de rede diferente, isso significa que eles estão em redes diferentes.

- PC1 — 192.168.1
- Servidor Web — 172.16.1



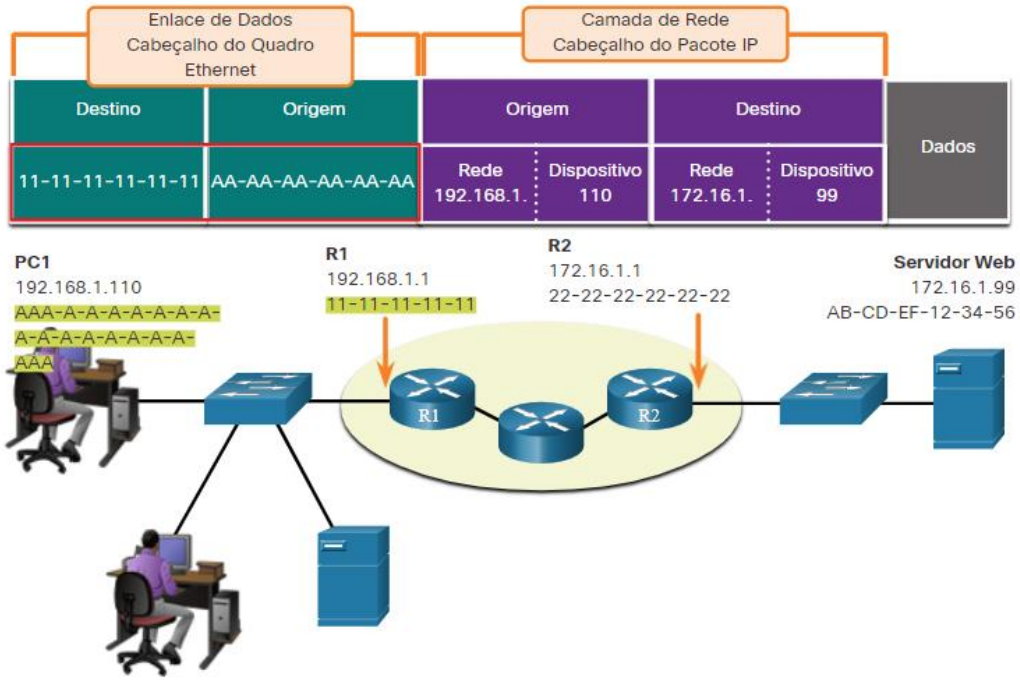
Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Função dos endereços da camada de enlace de dados: redes IP diferentes

Quando o destino final for remoto, a Camada 3 fornecerá à Camada 2 o endereço IP do gateway padrão local, também conhecido como o endereço do roteador.

- O gateway padrão (DGW) é o endereço IP da interface do roteador que faz parte dessa LAN e será a “porta” ou “gateway” para todos os outros locais remotos.
- Todos os dispositivos na LAN devem ser informados sobre esse endereço ou seu tráfego será limitado somente à LAN.
- Depois que a Camada 2 em PC1 for encaminha para o gateway padrão (Roteador), o roteador poderá iniciar o processo de roteamento para obter as informações para o destino real.



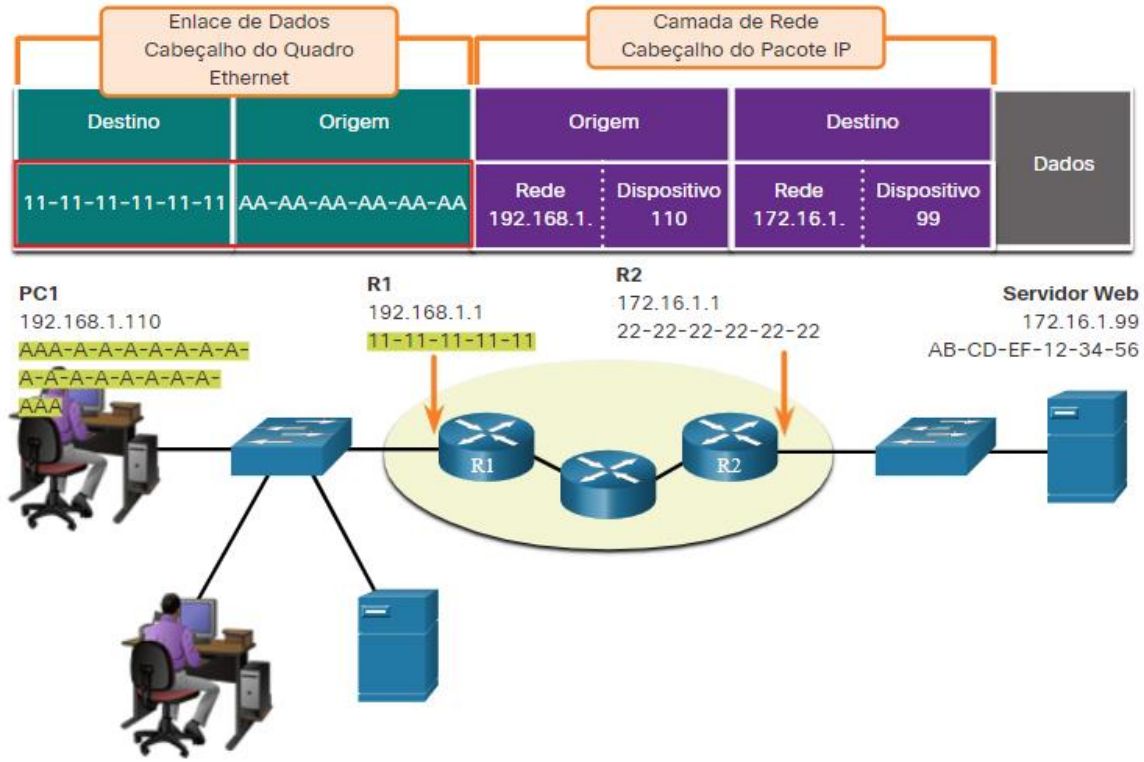
Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Função de Acesso a Dados dos Endereços da Camada de Link de Dados: Redes IP Diferentes

- O endereçamento do link de dados é endereçamento local, portanto, ele terá uma origem e um destino para cada link.
- O endereçamento MAC para o primeiro segmento é:
  - Fonte — AA-AA-AA-AA-AA-AA (PC1) Envia o quadro.
  - Destino — 11-11-11-11-11-11 (R1- MAC de gateway padrão) Recebe o quadro.

Observação: Embora o endereçamento local L2 mude de link para link ou de salto para salto, o endereçamento L3 permanece o mesmo.

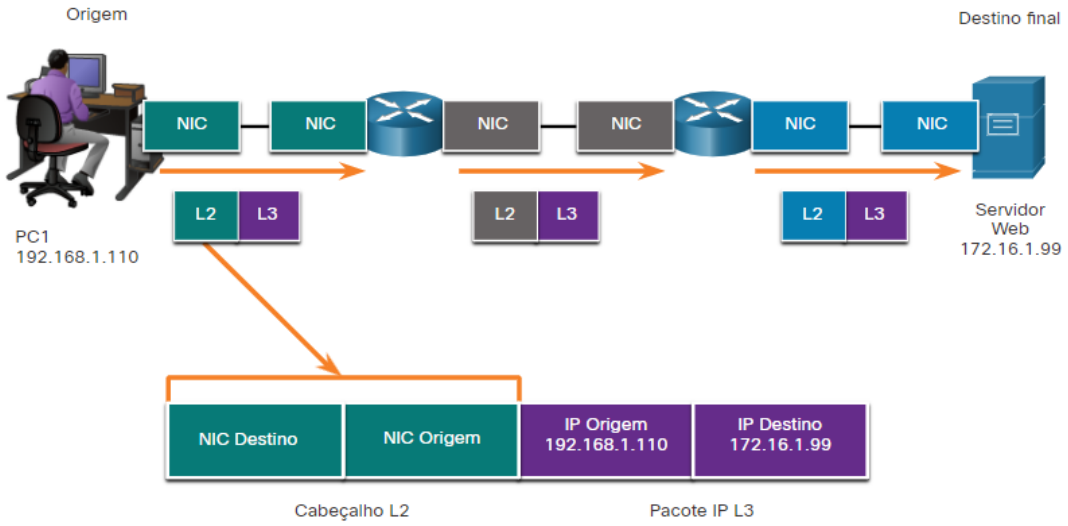


Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Endereços de enlace de dados

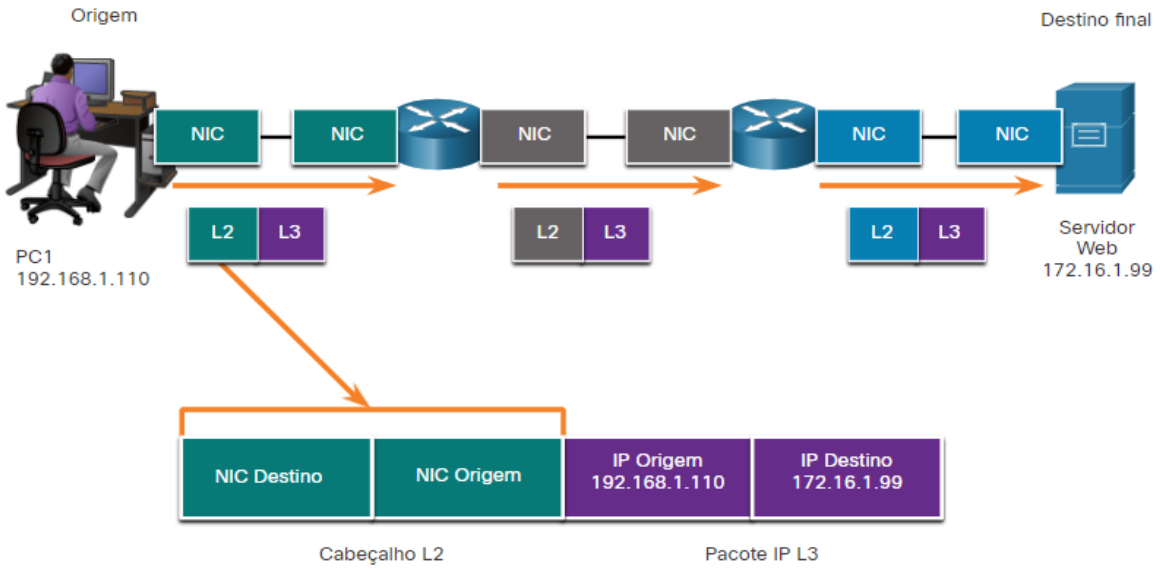
- Como o endereçamento de link de dados é endereçamento local, ele terá uma origem e um destino para cada segmento ou salto da viagem para o destino.
- O endereçamento MAC para o primeiro segmento é:
  - Origem — (NIC PC1) envia quadro
  - Destino — (Primeiro Roteador - Interface DGW) recebe quadro



Endereços de enlace de dados

O endereçamento MAC para o segundo salto é:

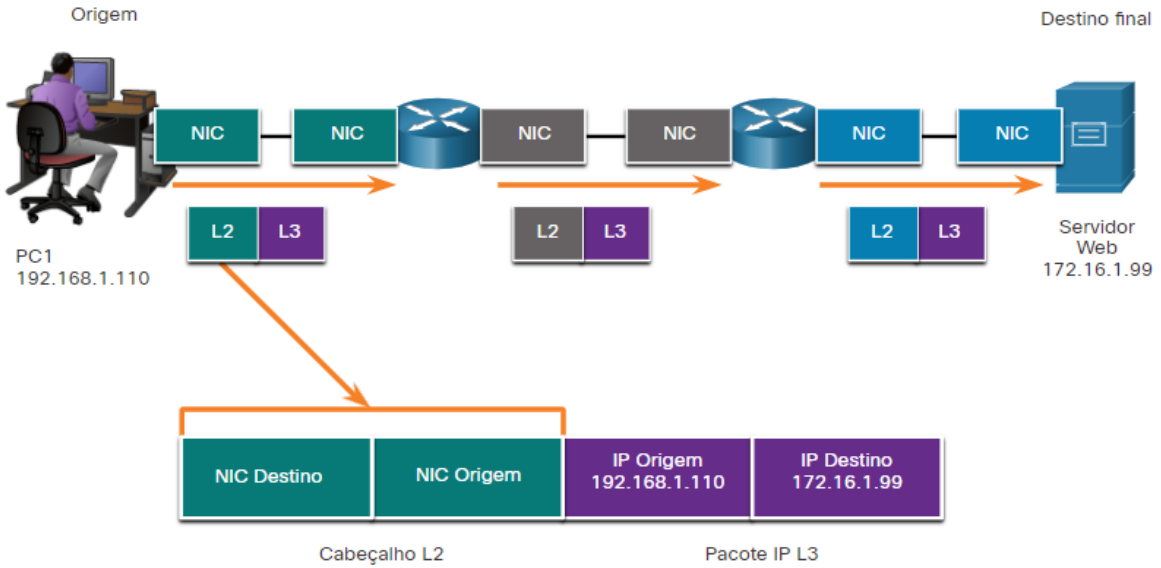
- Origem — (Primeira interface de saída do Roteador) envia quadro
- Destino — (Segundo Roteador) recebe quadro



Endereços de enlace de dados

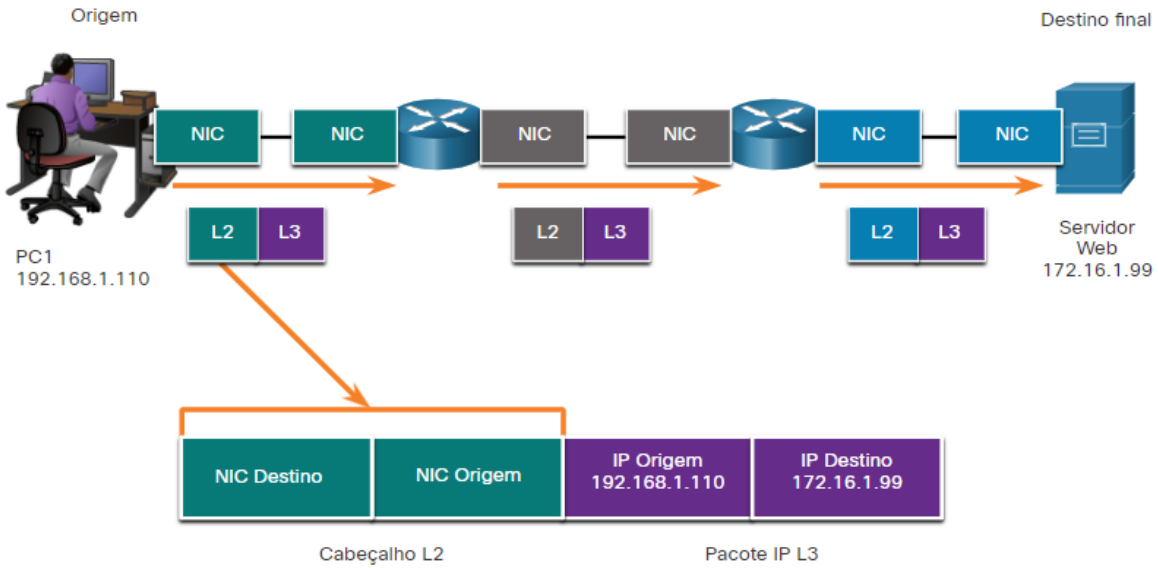
O endereçamento MAC para o último segmento é:

- Origem — (Segunda interface de saída do Roteador) envia quadro
- Destino — (NIC do servidor Web) recebe quadro



Endereços de enlace de dados

- Observe que o pacote não é modificado, mas o quadro é alterado, portanto, o endereçamento IP L3 não muda de segmento para segmento como o endereçamento MAC L2.
- O endereçamento L3 permanece o mesmo, uma vez que é global e o destino final ainda é o servidor Web.



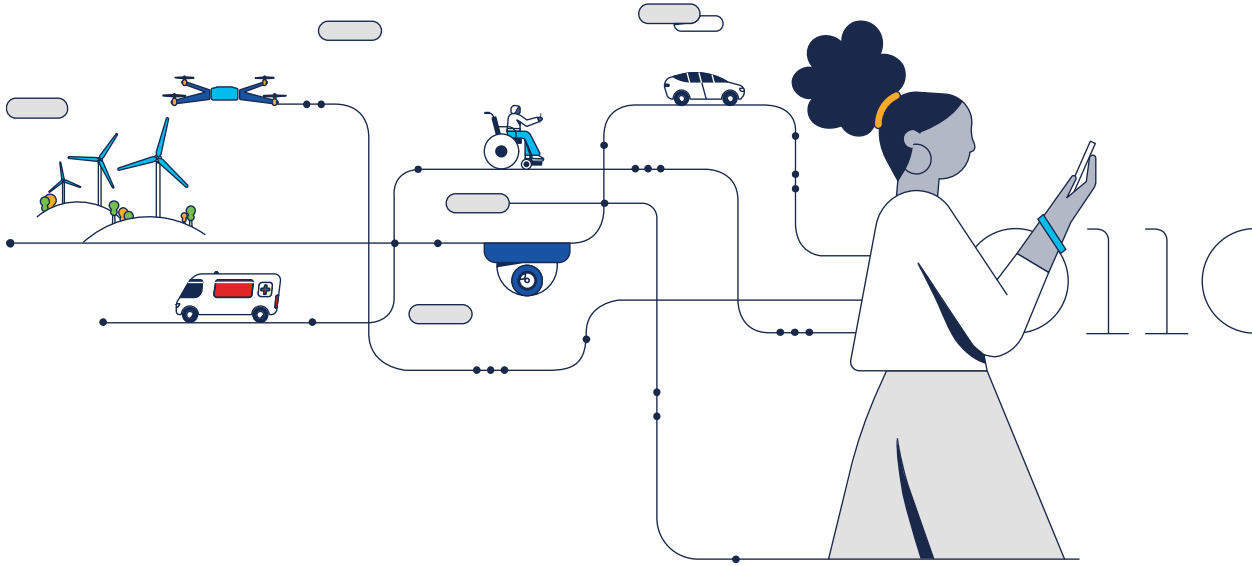
The bridge to possible

Nossos parceiros

TD SYNNEX

WISE
Women in Science
and Engineering
Inclusive Community

cisco
Networking
Academy



INTERNATIONAL
Girls in ICT Day
Brought to you by **WOMEN ROCK-IT**

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

CCNAv7 – ITN – Camada Física

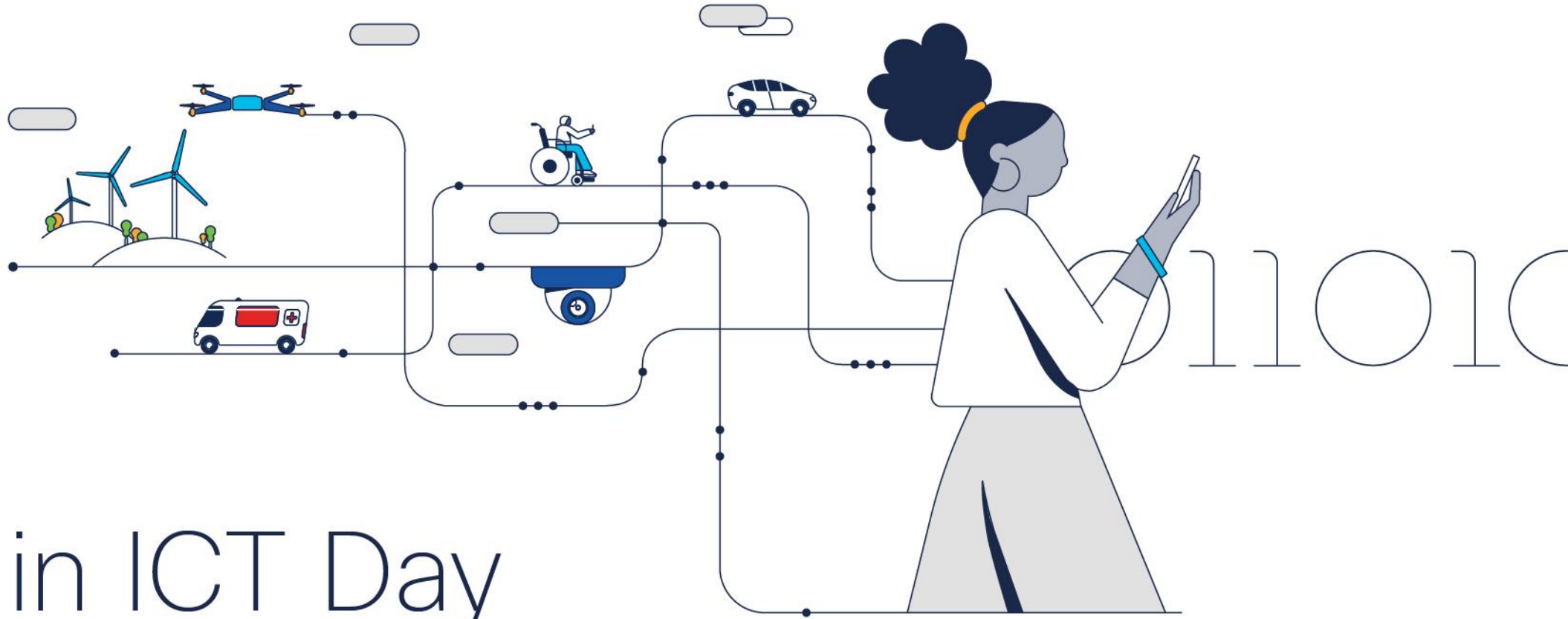
Módulo 4

Embaixadores do Programa 2020, 2021, 2022 & 2023:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

Networking
Academy



INTERNATIONAL

Girls in ICT Day

Brought to you by **WOMEN ROCK-IT**

Propósito

A camada física do modelo OSI fica na parte inferior da pilha.

Faz parte da camada de Acesso à Rede do modelo TCP/IP.

Sem a camada física, você não teria uma rede. Há três maneiras de se conectar à camada física.

Através de uma conexão com fio, onde os dados são transmitidos por meio de um cabo físico a um comutador compartilhado.

Esse tipo de configuração é uma rede conectada.

Nas conexões com fio, os dados são transmitidos usando ondas de rádio. Os dispositivos em uma rede sem fio devem estar conectados a um ponto de acesso sem fio (AP) ou roteador sem fio.

Propósito

Placas de Interface de Rede

As placas de interface de rede (NICs) conectam um dispositivo à rede.

As NICs Ethernet são usadas para uma conexão com fio, enquanto as NICs da rede local sem fio (WLAN) são usadas para a conexão sem fio.

Um dispositivo de usuário final pode incluir um ou os dois tipos de NICs.

Uma impressora de rede, por exemplo, pode só ter uma NIC Ethernet e, portanto, deve ser conectada à rede com um cabo Ethernet.

Outros dispositivos, como tablets e smartphones, só contém uma NIC WLAN e devem usar uma conexão sem fio.

Nem todas as conexões físicas são iguais, em termos de desempenho, durante uma conexão com uma rede.

Camada Física

A camada física do modelo OSI fornece os meios para transportar os bits que formam um quadro da camada de enlace de dados no meio físico de rede.

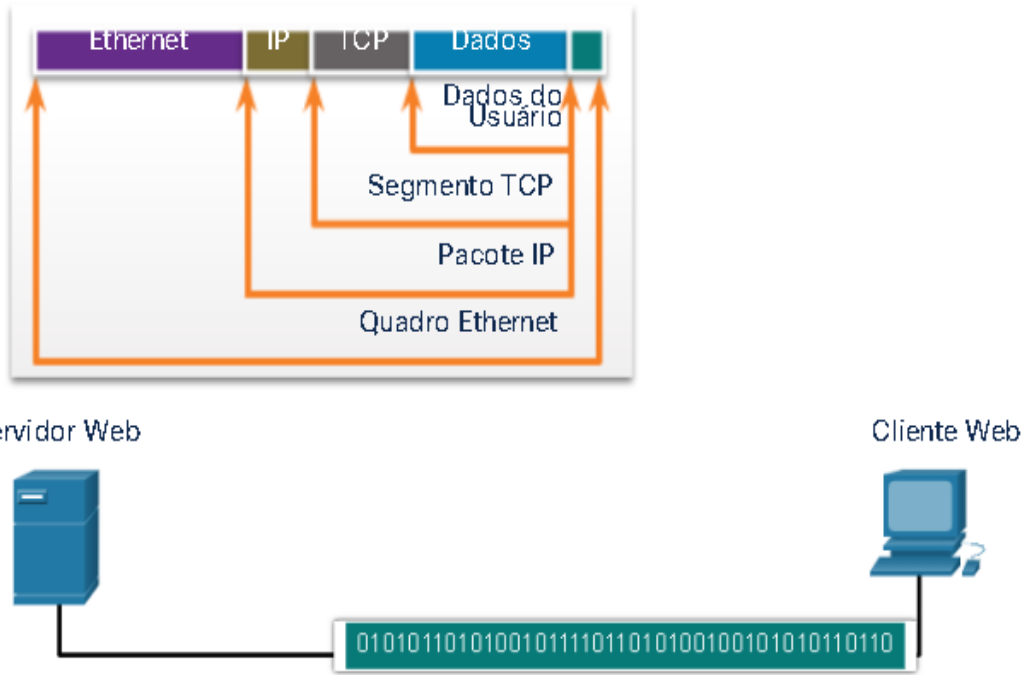
Essa camada aceita um quadro completo da camada de enlace de dados e o codifica como uma série de sinais que são transmitidos à mídia local. Os bits codificados, que formam um quadro, são recebidos por um dispositivo final ou por um dispositivo intermediário.

Processo de encapsulamento.

A camada física codifica os quadros e cria os sinais de onda elétrica, óptica ou de rádio que representam os bits em cada quadro. Esses sinais são então enviados pela mídia, um de cada vez. A última parte deste processo mostra os bits que estão sendo enviados através do meio físico.

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

Princípios da Comunicação



Processo de encapsulamento.

A camada física codifica os quadros e cria os sinais de onda elétrica, óptica ou de rádio que representam os bits em cada quadro.

Esses sinais são então enviados pela mídia, um de cada vez. A última parte deste processo mostra os bits que estão sendo enviados através do meio físico.

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

A camada de enlace, é a segunda camada da base do modelo OSI.

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Características da camada física

Os protocolos e operações das camadas OSI superiores são executados usando software desenvolvido por engenheiros de software e cientistas da computação.

Os serviços e protocolos na suíte TCP/IP são definidos pela Internet Engineering Task Force (IETF).

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

Há muitas organizações nacionais e internacionais diferentes, organizações reguladoras de governo e empresas privadas envolvidas no estabelecimento e na manutenção de padrões da camada física.

Características da camada física

Exemplo de organizações:

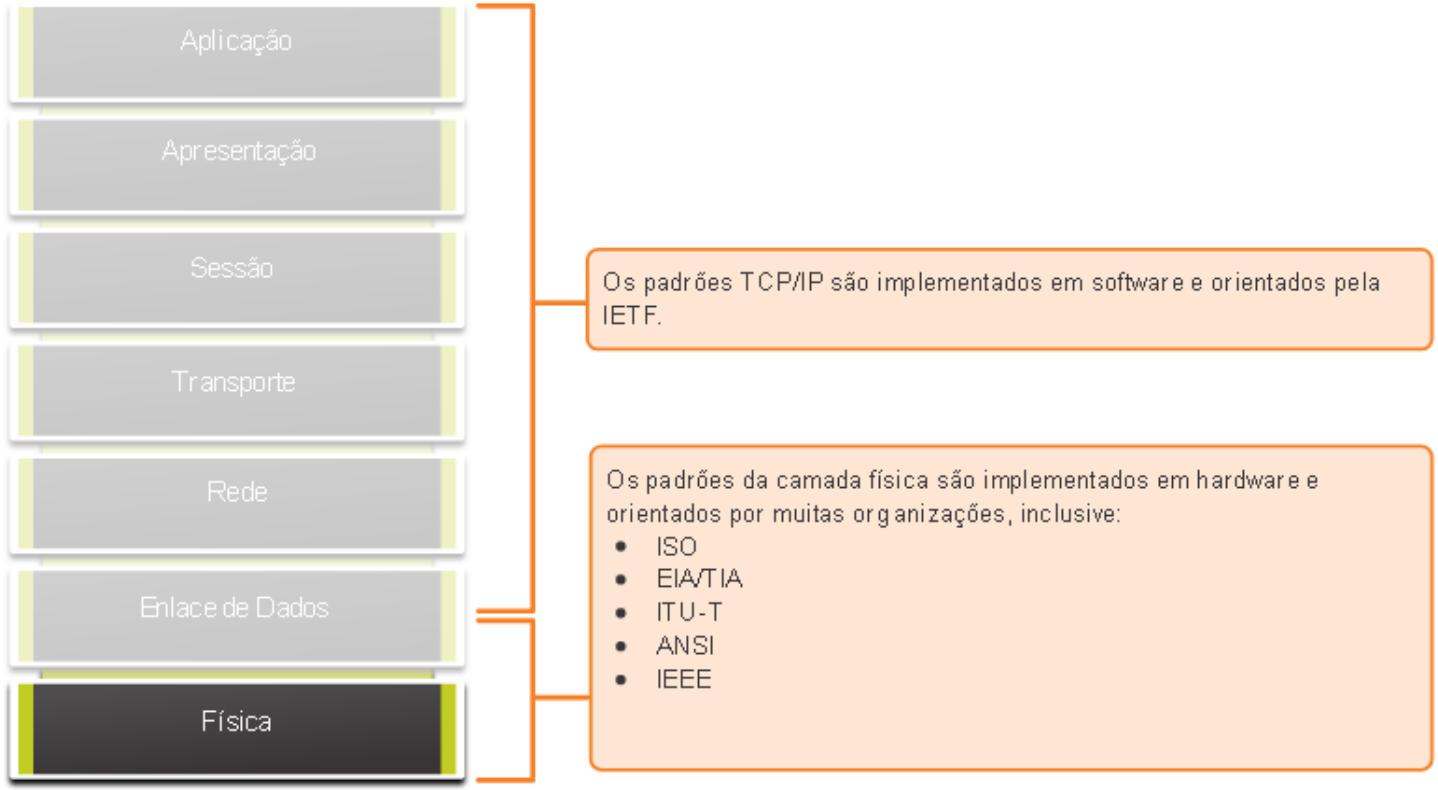
- International Organization for Standardization (ISO).
- Telecommunications Industry Association/Electronic Industries Association (TIA/EIA).
- União Internacional de Telecomunicações (ITU).
- Instituto Nacional de Padronização Americano (ANSI).
- Institute of Electrical and Electronics Engineers (IEEE).

Autoridades reguladoras de telecomunicações nacionais, incluem Federal Communication Commission (FCC) nos EUA e European Telecommunications Standards Institute (ETSI).

Além desses, geralmente existem grupos regionais de padrões de cabeamento, como CSA (Canadian Standards Association), CENELEC (Comitê Europeu de Padronização Eletrotécnica) e JSA / JIS (Japanese Standards Association), que desenvolvem especificações locais.

Características da camada física

Camadas do modelo OSI

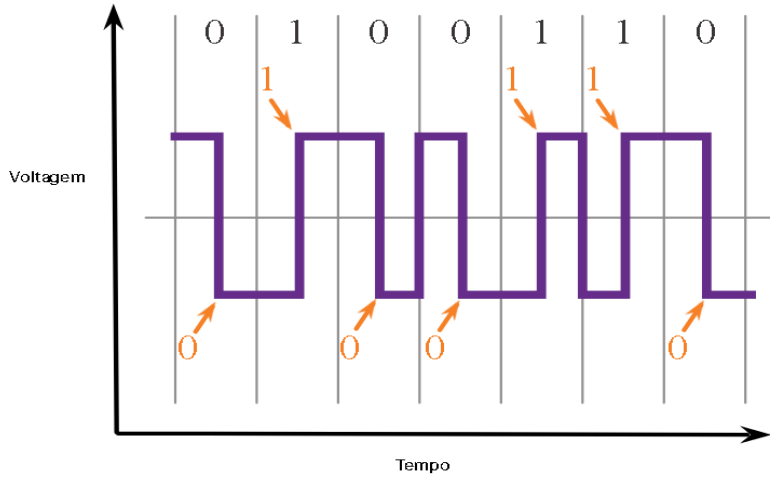


Componentes Físicos

Os padrões da camada física abordam três áreas funcionais:

Componentes Físicos:
São os dispositivos de hardware eletrônico, mídia e outros conectores que transmitem os sinais que representam os bits.
Os componentes de hardware, como NICs, interfaces e conectores, materiais de cabo e projetos de cabo são especificados nos padrões associados à camada física.
As várias portas e interfaces em um roteador também são exemplos de componentes físicos com conectores e conexões específicos decorrentes de padrões.

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



Networking Academy

Componentes Físicos

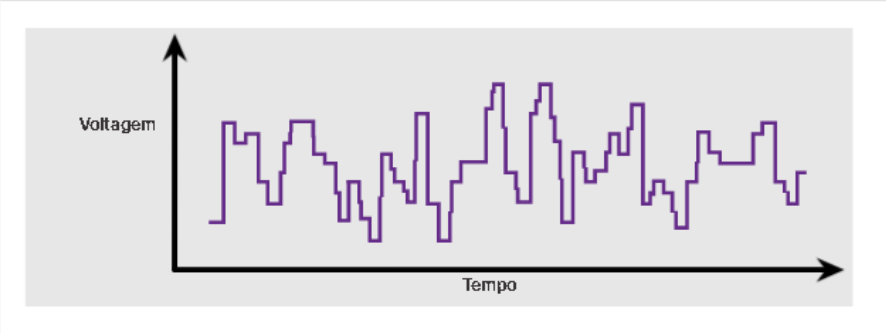
A codificação Manchester representa um bit 0 por uma transição de alta para baixa voltagem, e um bit 1 é representado como uma transição de baixa para alta voltagem.
A transição ocorre no meio de cada período de bit.
Esse tipo de codificação é usado na Ethernet de 10 Mbps. Taxas de dados mais rápidas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

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

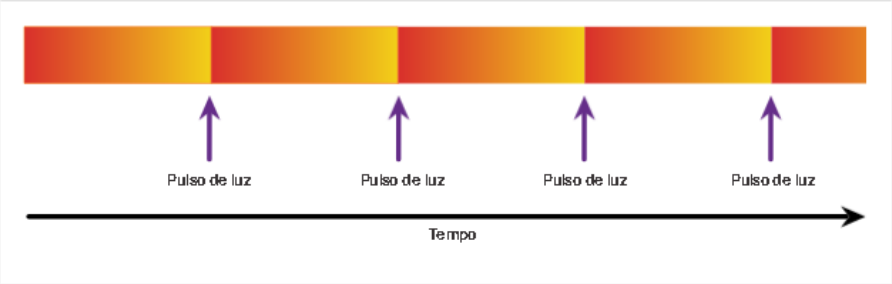
Componentes Físicos

Sinalização para cabo de cobre, cabo de fibra óptica e mídia sem fio.

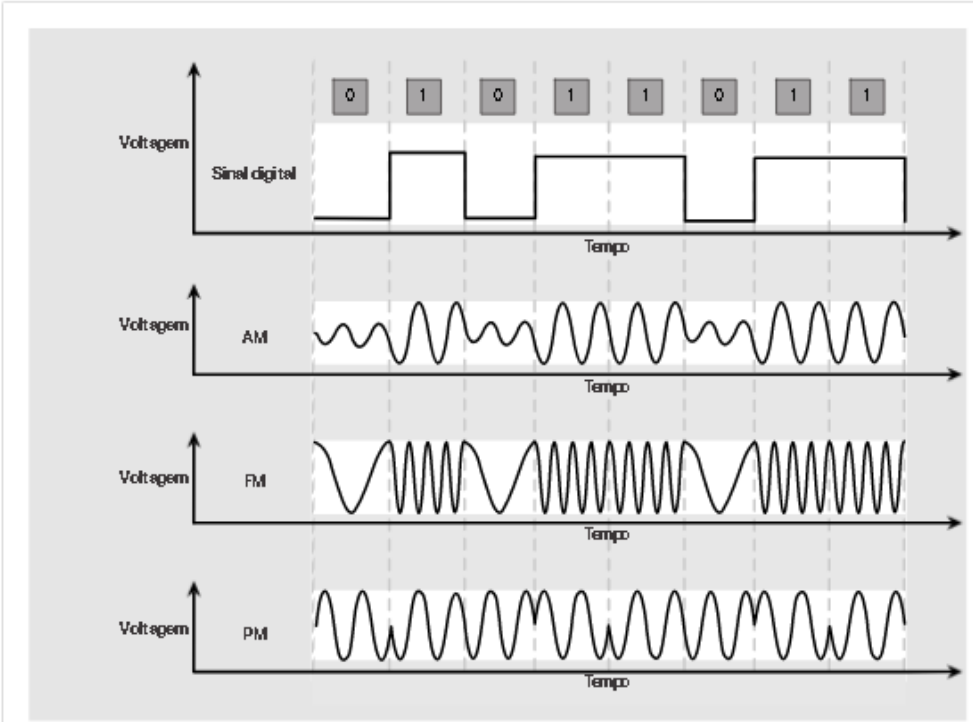
Sinais elétricos em Cabos de Cobre



Pulsos de Luz em Cabos Ópticos



Sinais em microondas sem Fio



Networking Academy

INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Largura de banda

Meios físicos diferentes aceitam a transferência de bits a taxas diferentes.
A transferência de dados é geralmente discutida em termos de largura de banda.
Largura de banda é a capacidade na qual um meio pode transportar dados.
A largura de banda digital mede a quantidade de dados que podem fluir de um lugar para outro durante um determinado tempo.
A largura de banda é normalmente medida em kilobits por segundo (kbps), megabits por segundo (Mbps) ou gigabits por segundo (Gbps).

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

- As propriedades do meio físico
- As tecnologias escolhidas para sinalização e detecção de sinais de rede
- As propriedades do meio físico, as tecnologias atuais e as leis da física desempenham sua função na determinação da largura de banda disponível.

Largura de banda

A tabela mostra as unidades de medida comumente usadas para largura de banda.

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

Terminologia de largura de banda

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

- **Latência**: Refere se ao tempo necessário para os dados viajarem de um ponto a outro, incluindo atrasos.

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

- **Rendimento**: Ou taxa de transferência, é a medida da transferência de bits através da mídia durante um determinado período.

Devido a alguns fatores, geralmente a taxa de transferência não corresponde à largura de banda especificada nas implementações da camada física. A taxa de transferência geralmente é menor que a largura de banda. Existem muitos testes de velocidade on-line que podem revelar a taxa de transferência de uma conexão com a Internet.
Fatores que influenciam a taxa de transferência:

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

Terminologia de largura de banda

- **Dados úteis:**

Sendo uma terceira medida para avaliar a transferência de dados, conhecido como goodput.

Goodput é a medida de dados usáveis transferidos em um determinado período.

Goodput é a taxa de transferência menos a sobrecarga de tráfego para estabelecer sessões, reconhecimentos, encapsulamento e bits retransmitidos.

O goodput é sempre menor que a taxa de transferência, que geralmente é menor do que a largura de banda.

Cabeamento de cobre

É o tipo mais comum de cabeamento usado nas redes hoje em dia.
Existem três tipos diferentes de cabeamento de cobre que são usados em situações específicas.

As redes usam mídia de cobre porque é barata, fácil de instalar e tem baixa resistência à corrente elétrica.
Entretanto, ela é limitada pela distância e interferência de sinal.

Os dados são transmitidos por cabos de cobre como pulsos elétricos.
Um detector na interface de rede de um dispositivo destino tem que receber um sinal que poderá ser decodificado com êxito para corresponder ao sinal enviado.
No entanto, quanto mais o sinal viaja, mais ele se deteriora.
Isso se chama atenuação de sinal. Por isso, todas as mídias de cobre devem seguir limitações de distância rigorosas, conforme especificado nos padrões de orientação.

Cabeamento de cobre

A temporização e a voltagem dos pulsos elétricos também são suscetíveis à interferência de duas fontes:

- **Interferência eletromagnética (EMI) ou interferência de radiofrequência (RFI):**

Os sinais EMI e RFI podem distorcer e corromper os sinais de dados que estão sendo transportados pela mídia de cobre.
Possíveis fontes de EMI e RFI são dispositivos de ondas de rádio e eletromagnéticos, como luzes fluorescentes ou motores elétricos.

- **Diafonia:**

Diafonia é uma perturbação causada pelos campos elétrico ou magnético de um sinal em um fio para o sinal em um fio adjacente.
Nos circuitos de telefone, a diafonia pode fazer com que parte de outra conversa de voz de um circuito adjacente seja ouvida (linha cruzada).
Especificamente, quando uma corrente elétrica flui através de um cabo, ela cria um pequeno campo magnético circular ao redor do cabo, que pode ser captado por um cabo adjacente.

Cabeamento de cobre

Para contrabalançar os efeitos negativos da EMI e da RFI, alguns tipos de cabos de cobre têm proteção metálica e exigem conexões devidamente aterradas.

Para contrabalançar os efeitos negativos do crosstalk, alguns tipos de cabos de cobre têm pares de cabos de circuitos opostos juntos, o que efetivamente cancelam o crosstalk.

A suscetibilidade dos cabos de cobre ao ruído eletrônico também pode ser limitada usando estas recomendações:

- Selecionando a categoria de cabo mais adequado para um determinado ambiente de rede.
- Projetar uma infraestrutura de cabos para evitar fontes conhecidas e potenciais interferências na estrutura do edifício.
- Usando técnicas de cabeamento que incluem o manuseio e a terminação adequados dos cabos.

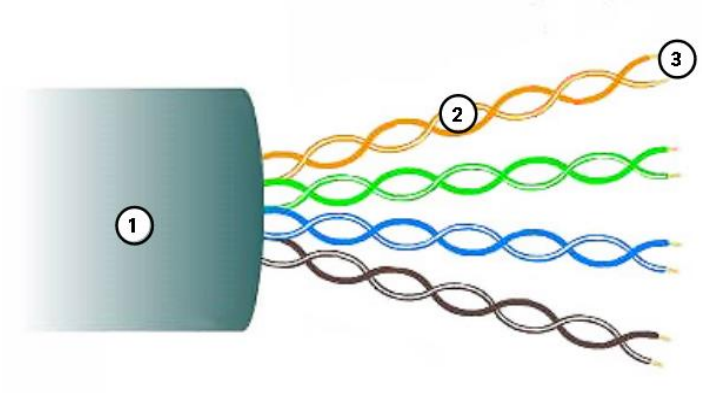
Tipos de cabeamento de cobre

Par trançado não blindado (UTP)

É o meio físico de rede mais comum. Terminado com conectores RJ-45 é usado para interconectar hosts de rede com dispositivos de rede, como comutadores e roteadores.

Consiste em 4 pares de cabos codificados por cores, que foram trançados e depois colocados em uma capa plástica flexível que protege contra danos físicos menores.

O processo de trançar cabos ajuda na proteção contra interferência de sinais de outros cabos.



1. A capa externa protege os fios de cobre contra danos físicos.
2. Os pares trançados protegem o sinal contra interferências.
3. O isolamento plástico com código de cores isola eletricamente os fios um do outro e identifica cada par.

Tipos de cabeamento de cobre

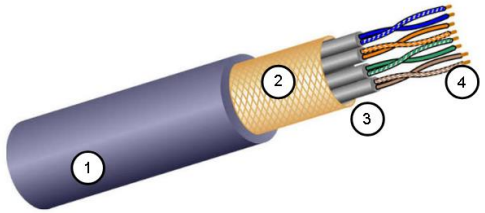
Par trançado blindado (STP)

Oferece maior proteção contra ruído do que o cabeamento UTP. No entanto, é significativamente mais caro e de difícil instalação. Assim como o cabo UTP, o STP usa um conector RJ-45.

Os cabos STP combinam as técnicas de blindagem para contrabalançar a EMI e a RFI, e são trançados para conter o crosstalk. Para aproveitar totalmente a blindagem, os cabos STP são terminados com conectores de dados STP blindados especiais. Se o cabo não estiver devidamente aterrado, a blindagem poderá atuar como uma antena e captar sinais indesejados.

O cabo STP usa quatro pares de cabo, envolvidos em blindagens, que são colocados em uma proteção ou revestimento geral metálico.

1. Revestimento exterior.
2. Escudo trançado ou laminado.
3. Escudos de alumínio.
4. Pares trançados.

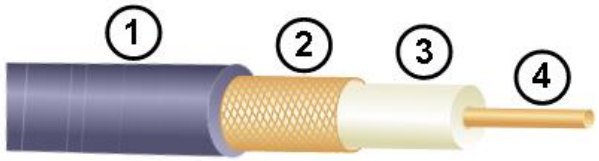


Tipos de cabeamento de cobre

Cabo coaxial

O cabo coaxial, ou coax, recebeu seu nome porque tem dois condutores que compartilham o mesmo eixo.
Consiste de um condutor de cobre é usado para transmitir os sinais eletrônicos.
Uma camada de isolamento plástico flexível que envolve um condutor de cobre.
O material de isolamento é envolvido em uma malha de cobre com tecido, ou uma folha metálica, que atua como o segundo cabo no circuito e uma proteção para o condutor interno.
Essa segunda camada, ou blindagem, também reduz a quantidade de interferência eletromagnética externa.
Todo o cabo é coberto com um revestimento para evitar danos físicos menores.
Há tipos diferentes de conectores utilizados com o cabo coax.

1. Revestimento exterior.
2. Blindagem de cobre trançado.
3. Isolante em plástico.
4. Condutor de cobre.



Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Tipos de cabeamento de cobre

Embora o cabo UTP tenha substituído essencialmente o cabo coaxial nas modernas instalações Ethernet, o design do cabo coaxial é usado nas seguintes situações:

Instalações sem fio:
Conectam antenas a dispositivos sem fio.
O cabo coaxial transporta a energia de radiofrequência (RF) entre as antenas e o equipamento de rádio.

Instalações de Internet a cabo:
Os provedores de serviços a cabo fornecem conectividade à Internet para seus clientes, substituindo partes do cabo coaxial e suportando elementos de amplificação por cabo de fibra óptica.
No entanto, o cabeamento dentro das instalações do cliente ainda é coaxial.

Cabeamento UTP

Consiste em 4 pares de fios de cobre com código de cores, torcidos juntos e depois envoltos em uma bainha de plástico flexível.
Não usa blindagem para contrabalançar os efeitos de EMI e RFI.
Limitando efeito negativo da diafonia através de:

Cancelamento:
Os designers agora emparelham os fios em um circuito.
Quando dois fios de um circuito elétrico são colocados próximos um do outro, seus campos magnéticos serão opostos.
Assim, os dois campos magnéticos cancelam um ao outro e também podem cancelar sinais externos de EMI e RFI.

Variações no número de torções por par de fios:
Aumentam ainda mais o efeito de cancelamento de fios de circuito emparelhados, variando o número de torções de cada par de fios em um cabo.
Deve seguir especificações precisas que orientam quantas tranças são permitidas por metro (3,28 pés) do cabo. O par laranja/laranja e branco é menos trançado do que o par azul/azul e branco.
Cada par colorido é trançado um número de vezes diferente.
Depende exclusivamente do efeito de cancelamento produzido pelos pares de fios trançados para limitar a degradação de sinal e fornecer efetivamente a autoblindagem para cabos trançados na mídia de rede.

Padrões e conectores de cabeamento UTP

O cabeamento de UTP está em conformidade com os padrões estabelecidos conjuntamente pela TIA/EIA, que estipula os padrões de cabeamento comerciais para instalações de LAN e é o padrão mais usado em ambientes de cabeamento de LAN.

Alguns dos elementos definidos são:

- Tipos de cabos;
- Comprimentos do cabo;
- Conectores;
- Terminação de cabo;
- Métodos de teste de cabo.

As características elétricas do cabeamento de cobre são definidas pelo Instituto de Engenharia Elétrica e Eletrônica (IEEE).
O IEEE classifica o cabeamento UTP de acordo com o desempenho. Os cabos são colocados nas categorias, com base na capacidade de transportar taxas de largura de banda mais altas.
Por exemplo, o cabo Categoria 5 é usado normalmente em instalações 100BASE-TX Fast Ethernet. Outras categorias incluem o cabo Categoria 5 aprimorada, Categoria 6 e Categoria 6a.

Padrões e conectores de cabeamento UTP

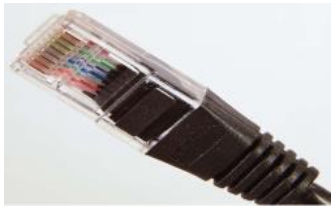
Os cabos em categorias mais altas são desenvolvidos e construídos para suportar taxas de dados mais elevadas.
À medida que novas tecnologias Ethernet de velocidade de gigabit estão sendo desenvolvidas e adotadas, a Categoria 5e é agora o tipo de cabo minimamente aceitável, com a Categoria 6 sendo o tipo recomendado para novas instalações prediais.

- A categoria 3 foi originalmente utilizada para comunicação de voz através de linhas de voz, mas mais tarde utilizada para transmissão de dados.
- As categorias 5 e 5e são utilizadas para a transmissão de dados. Categoria 5 suporta 100Mbps e Categoria 5e suporta 1000 Mbps.
- A categoria 6 tem um separador adicional entre cada par de fios para suportar velocidades mais altas. Categoria 6 suporta até 10 Gbps.
- Categoria 7 também suporta 10 Gbps.
- Categoria 8 suporta 40 Gbps.
- Alguns fabricantes produzem cabos que excedem as especificações da Categoria TIA/EIA 6a e os classificam como Categoria 7.

Padrões e conectores de cabeamento UTP

O cabo UTP geralmente é terminado com um conector RJ-45.
O padrão TIA/EIA-568 descreve os códigos de cores de cabos para atribuições dos pinos (pinagem) para cabos Ethernet.

Plugues UTP RJ-45
O conector RJ-45 é o componente macho, prensado na extremidade do cabo.



Sockets UTP RJ-45
O soquete é o componente feminino de um dispositivo de rede, parede, tomada de partição de cubículo ou painel de conexões. Quando terminado incorretamente, o cabo é uma fonte potencial de degradação do desempenho da camada física.

Cabo UTP mal terminado
Conectores defeituosos possuem fios expostos, sem torção e não totalmente cobertos pela bainha.

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Cabos UTP diretos e cruzados

Situações diversas podem exigir que os cabos UTP sejam conectados de acordo com diferentes convenções de fiação. Isso significa que os fios individuais do cabo precisam ser conectados em ordem diferente para conjuntos diferentes de pinos nos conectores RJ-45.

Estes são os principais tipos de cabo obtidos com o uso de convenções de cabeamento específicos:

Ethernet direto:
O tipo mais comum de cabo de rede. Geralmente é usado para interconectar um host a um switch e um switch a um roteador.

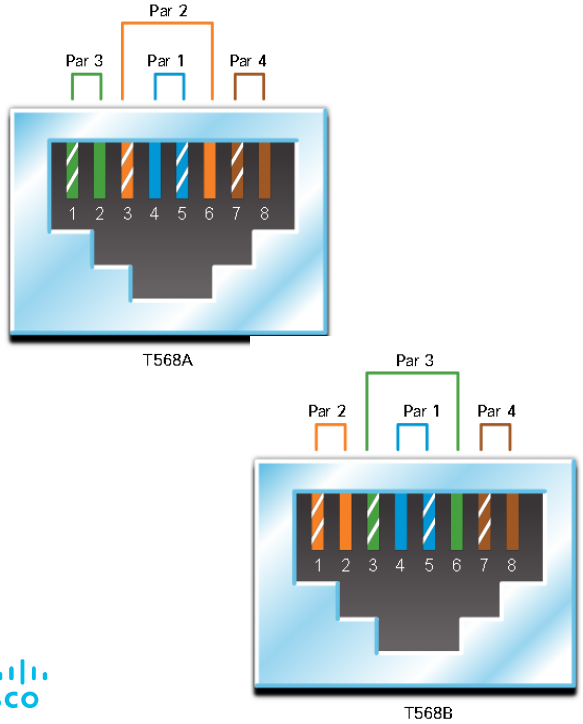
Ethernet Crossover:
Um cabo usado para interconectar dispositivos semelhantes.
Por exemplo, para conectar um switch a um switch, um host a um host ou um roteador a um roteador.
No entanto, os cabos cruzados agora são considerados legados, pois as NICs usam o cruzamento de interface dependente médio (Auto-MDIX) para detectar automaticamente o tipo de cabo e fazer a conexão interna.

Observação: Outro tipo de cabo é um cabo de rollover, que é proprietário da Cisco.
É usado para conectar uma estação de trabalho a uma porta do console do roteador ou do switch.

Cabos UTP diretos e cruzados

O uso incorreto de um cabo crossover ou direto entre dois dispositivos não danifica os dispositivos, mas a conectividade e comunicação entre os dispositivos não será realizada.
Este é um erro comum e verificar se as conexões do dispositivo estão corretas deve ser a primeira ação de solução de problemas se a conectividade não for alcançada.

Diagramas dos padrões de fiação T568A e T568B.



Cada um mostra a pinagem correta para os pares de fios individuais.
Cada par de fios de cor é numerado e consiste em um fio de cor sólida e um fio listrado branco.
O par 1 é azul, o par 2 é laranja, o par 3 é verde e o par 4 é marrom.
Cada padrão alterna entre fios listrados brancos e sólidos.

Para o padrão T568A, o par azul é encerrado nos pinos 4 e 5, o par laranja é terminado nos pinos 3 e 6, o par verde é encerrado nos pinos 1 e 2, e o par marrom é encerrado nos pinos 7 e 8.

Para o padrão T568B, o par azul é encerrado nos pinos 4 e 5, o par laranja é encerrado nos pinos 1 e 2, o par verde é terminada nos pinos 3 e 6, e o par marrom é encerrado nos pinos 7 e 8.

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Cabos UTP diretos e cruzados

Cable Types and Standards

Tipo do Cabo	Padrão	Aplicação
Ethernet Direto	Ambas as extremidades T568A ou T568B	Conecta um host de rede a um dispositivo de rede, como um switch ou hub
Ethernet Cruzado	Uma extremidade é T568A, outra é T568B	Conecta dois hosts de rede Conecta dois dispositivos intermediários de rede (alternar para switch ou roteador para roteador)
Rollover	Proprietário da Cisco	Conecta uma porta serial da estação de trabalho a uma porta do console do roteador, usando um adaptador

Cabeamento de Fibra Óptica

- O cabo de fibra óptica transmite dados por longas distâncias e a larguras de banda mais altas do que qualquer outra mídia de rede.
- Pode transmitir sinais com menos atenuação e é completamente imune à interferência de EMI e RFI.
- Comumente usada para interconectar dispositivos de rede.
- É um fio flexível, extremamente fino e transparente de vidro muito puro, não muito maior do que um fio de cabelo humano. Os bits são codificados na fibra como pulsos de luz. O cabo de fibra óptica atua como um guia de onda, ou “tubo de luz”, para transmitir luz entre as duas extremidades com o mínimo de perda do sinal.

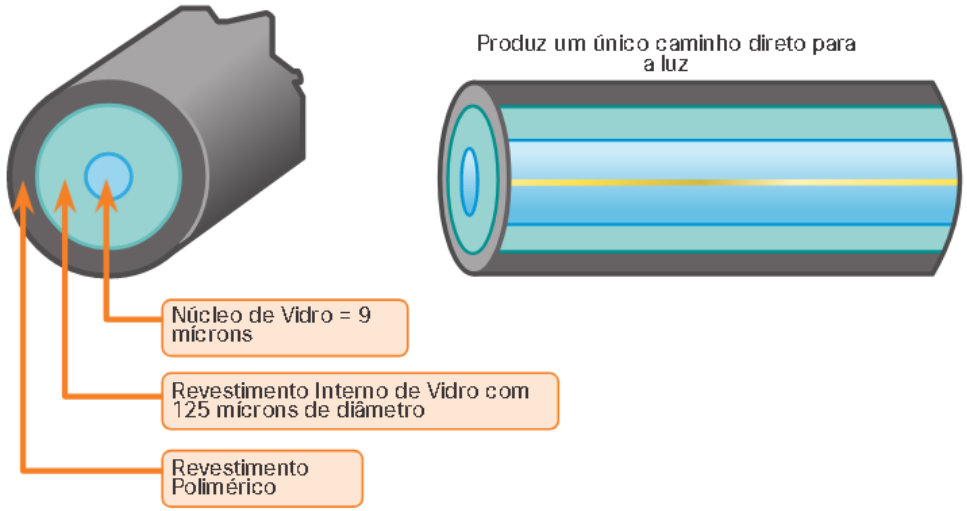
Considere um rolo de papel toalha vazio com o interior revestido como um espelho.
Ele tem mil metros de comprimento e um pequeno ponteiro laser é usado para enviar sinais de código Morse na velocidade da luz.
Basicamente, é assim que o cabo de fibra óptica funciona, só que tem um diâmetro menor e usa tecnologias de luz sofisticadas.

Tipos de fibra

- **Fibra monomodo (SMF):**

O SMF consiste em um núcleo muito pequeno e usa a tecnologia laser cara para enviar um único raio de luz.

O SMF é popular em situações de longa distância que se estendem por centenas de quilômetros, como os exigidos em aplicações de telefonia de longo curso e TV a cabo.



Networking Academy

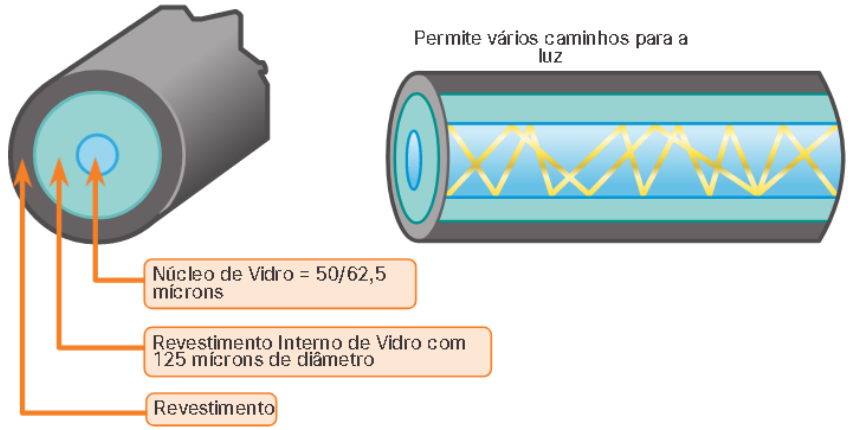
INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Tipos de fibra

- **Fibra multimodo (MMF)**

O MMF consiste em um núcleo maior e usa emissores de LED para enviar pulsos de luz. Especificamente, a luz de um LED entra na fibra multimodo em diferentes ângulos, como mostrado na figura. Popular nas LANs porque pode ser acionada por LEDs de baixo custo.
Ela fornece largura de banda até 10 Gb/s por links de até 550 metros.



Uma das diferenças destacadas entre MMF e SMF é a quantidade de dispersão.
O termo dispersão se refere ao espalhamento do pulso de luz com o tempo.
Maior dispersão significa aumento da perda de força do sinal. MMF tem uma dispersão maior do que SMF.
É por isso que o MMF só pode viajar até 500 metros antes da perda de sinal.

Uso de cabeamento de fibra óptica

Usado em quatro setores:

Redes corporativas:
Usadas para aplicativos de cabeamento de backbone e dispositivos de infraestrutura de interconexão.

FTTH (Fiber-to-the-Home):
Usado para fornecer serviços de banda larga sempre ativos para residências e pequenas empresas.

Redes de longo cursO:
Utilizadas por provedores de serviços para conectar países e cidades.

Redes de cabos submarinos:
Utilizadas para fornecer soluções confiáveis de alta velocidade e alta capacidade, capazes de sobreviver em ambientes submarinos adversos até distâncias transoceânicas.
Pesquise na internet por “mapa de telegeografia de cabos submarinos” para visualizar vários mapas on-line.
Nosso foco neste curso é o uso de fibra dentro da empresa.

Conectores de fibra óptica

As principais diferenças entre os tipos de conectores são as dimensões e os métodos de acoplamento. As empresas decidem os tipos de conectores que serão usados, com base no seu equipamento.
Alguns switches e roteadores têm portas que suportam conectores de fibra óptica por meio de um transceptor SFP (Small Form Factor Pluggable).

- **Conectores de ponta reta ST -** Um dos primeiros tipos de conectores usados. Trava firmemente com um mecanismo do tipo baioneta "Twist-on / twist-off".
- **Conectores de Assinante SC -** Às vezes chamados de conector quadrado ou conector padrão. São um conector LAN e WAN amplamente adotado que usa um mecanismo push-pull para garantir uma inserção positiva. É usado com fibra multimodo e monomodo.
- **Conectores LC simplex -** Versão menor do conector SC. Às vezes chamados de conectores pequenos ou locais e estão crescendo rapidamente em popularidade devido ao seu tamanho menor.
- **Conector LC multimodo duplex -** É semelhante a um conector LC simples, mas usa um conector duplex.

Até recentemente, a luz só podia viajar em uma direção sobre fibra óptica.
Duas fibras foram necessárias para suportar a operação full duplex.
Portanto, os cabos de conexão de fibra óptica agrupam dois cabos de fibra óptica e os terminam com um par de conectores padrão de fibra única. Alguns conectores de fibra aceitam fibras de transmissão e de recepção em um único conector, conhecido como conector duplex.
Padrões BX, como 100BASE-BX, usam comprimentos de onda diferentes para enviar e receber através de uma única fibra.

Cabos de conexão de fibra

Os cabos de fibra são necessários para interconectar dispositivos da infraestrutura.
O uso das cores diferencia entre cabos monomodo e multimodo.
A cor amarela indica cabos de fibra monomodo e o laranja é para cabos de fibra multimodo.

- **Cabo Multimodo SC-SC**
- **Cabo Monomodo LC-LC**
- **Cabo Multimodo ST-LC**
- **Cabo Monomodo SC-ST**

Os cabos de fibra devem ser protegidos com uma pequena tampa de plástico quando não estiverem em uso.

Fibra versus Cobre

Há muitas vantagens de usar cabos de fibra óptica em comparação com os cabos de cobre. A tabela destaca algumas dessas diferenças.

Atualmente, na maioria dos ambientes empresariais, a fibra óptica é usada principalmente como cabeamento de backbone para conexões ponto a ponto de alto tráfego entre instalações de distribuição de dados.
Ele também é usado para a interconexão de edifícios em campus multi-construção.
Como os cabos de fibra ótica não conduzem eletricidade e têm uma baixa perda de sinal, eles são adequados para esses usos.

UTP and Fiber-Optic Cabling Comparison

Problemas de Implementação	Cabeamento UTP	Cabeamento de fibra óptica
Largura de banda suportada	10 Mb/s - 10 Gb/s	10 Mb/s - 100 Gb/s
Distância	Relativamente curto (1 a 100 metros)	Relativamente longo (1 - 100.000 metros)
Imunidade a interferência eletromagnética e de frequências de rádio	Baixa	Alto (totalmente imune)
Imunidade a perigos elétricos	Baixa	Alto (totalmente imune)
Custos da mídia e dos conectores	Menor	Mais alta
Habilidades necessárias para a instalação	Menor	Mais alta
Precauções de segurança	Menor	Mais alta

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Meios sem fio

É o terceiro meio de comunicação de camada física de uma rede.
Transporta sinais eletromagnéticos que representam os dígitos binários de comunicações de dados usando frequências de rádio ou de micro-ondas.
Com melhores opções de mobilidade de todas as mídias.
Atualmente o principal meio de comunicação dos usuários.

Algumas de suas limitações são:

Área de cobertura:
Funcionam bem em ambientes abertos.
No entanto, alguns materiais de construção utilizados em prédios e estruturas, e o terreno local, limitarão a eficácia da cobertura.

Interferência:
Suscetível a interferências e pode ser interrompida por dispositivos comuns, como telefones sem fio domésticos, alguns tipos de luzes fluorescentes, fornos de microondas e outras comunicações sem fio.

Meios sem fio

Segurança:
Não requer acesso a uma parte física da mídia.
Portanto, os dispositivos e usuários que não estão autorizados a acessar a rede podem obter acesso à transmissão.
A segurança da rede é o principal componente da administração de uma rede sem fio.

AS WLANs e os meios compartilhados:
Operam em half-duplex, o que significa que apenas um dispositivo pode enviar ou receber por vez.
É compartilhado com todos os usuários sem fio resultando em largura de banda reduzida para cada usuário.

Embora esteja aumentando em popularidade na conectividade de desktop, cobre e fibra são as mídias de camada física mais populares para a implantação de dispositivos de rede intermediários, como roteadores e switches.

Tipos de Meio Físico Sem Fio

O IEEE e os padrões do setor abrangem as camadas física e de enlace de dados.

As especificações da camada física são aplicadas a áreas que incluem o seguinte:

- Codificação de dados para sinal de rádio;
- Frequência e potência de transmissão;
- Requisitos de recepção e decodificação de sinal;
- Projeto e construção de antenas.

Os padrões sem fio são:

Wi-Fi (IEEE 802.11) - Tecnologia de LAN sem fio (WLAN) ou Wi-Fi. Usa um protocolo baseado em contenção conhecido como acesso múltiplo / detecção de colisão de portadora (CSMA / CA).
A NIC sem fio deve ouvir primeiro, antes de transmitir, para determinar se o canal de rádio está limpo. Se houver outro dispositivo sem fio transmitindo, a NIC deverá esperar até o canal estar limpo. Wi-Fi é uma marca comercial registrada da Wi-Fi Alliance.
O Wi-Fi é usado com dispositivos WLAN certificados com base nos padrões IEEE 802.11.

Tipos de Meio Físico Sem Fio

Bluetooth (IEEE 802.15):
Padrão de rede pessoal sem fio (WPAN), conhecido como “Bluetooth”.
Usa um processo de emparelhamento de dispositivo para se comunicar em distâncias de 1 a 100 metros.

WiMAX (IEEE 802:16):
Conhecido como Interoperabilidade mundial para acesso por microondas (WiMAX), esse padrão sem fio usa uma topologia ponto a multiponto para fornecer acesso à banda larga sem fio.

Zigbee (IEEE 802.15.4):
Uma especificação usada para comunicações de baixa taxa de dados e baixa potência.
Destina-se a aplicações que exigem taxas de dados de curto alcance, baixas e longa duração da bateria.
Usado para ambientes industriais e de Internet das Coisas (IoT), como interruptores de luz sem fio e coleta de dados de dispositivos médicos.

Observação: Outras tecnologias sem fio, como comunicações celulares e via satélite, também podem fornecer conectividade de rede de dados.
No entanto, essas tecnologias sem fio estão fora do escopo deste módulo.

Lan sem fio

Uma implementação de dados sem fio permite que dispositivos se conectem sem fio por meio de uma LAN.
Uma WLAN requer os seguintes dispositivos de rede:

Ponto de acesso sem fio (AP):
Concentram os sinais sem fio dos usuários e se conectam à infraestrutura de rede existente baseada em cobre, como Ethernet.
Os roteadores sem fio domésticos e de pequenas empresas integram as funções de um roteador, comutador e ponto de acesso em um dispositivo, conforme mostrado na figura.

Adaptadores de NIC sem fio:
Fornecem recursos de comunicação sem fio para hosts de rede.
Como a tecnologia se desenvolveu, vários padrões baseados na Ethernet WLAN surgiram.
Ao comprar dispositivos sem fio, garanta compatibilidade e interoperabilidade.

Os benefícios das tecnologias da comunicação de dados sem fio são evidentes, especialmente a economia nos custos de fiação local e a conveniência da mobilidade de host.
Os administradores de rede devem desenvolver e aplicar políticas e processos de segurança rigorosos para proteger as WLANs contra acesso e danos não autorizados.

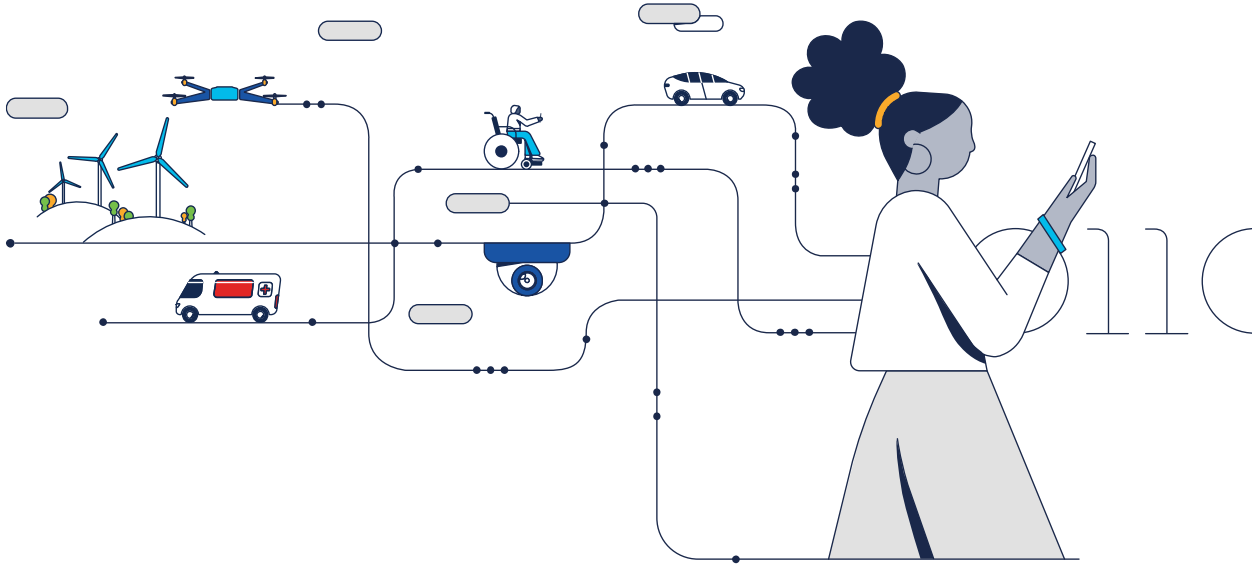
The bridge to possible

Nossos parceiros

TD SYNNEX

WISE
Women in Science
and Engineering
Inclusive Community

cisco
Networking
Academy



INTERNATIONAL
Girls in ICT Day
Brought to you by **WOMEN ROCK-IT**

Cisco Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

CCNAv7 – ITN –Sistema de Números

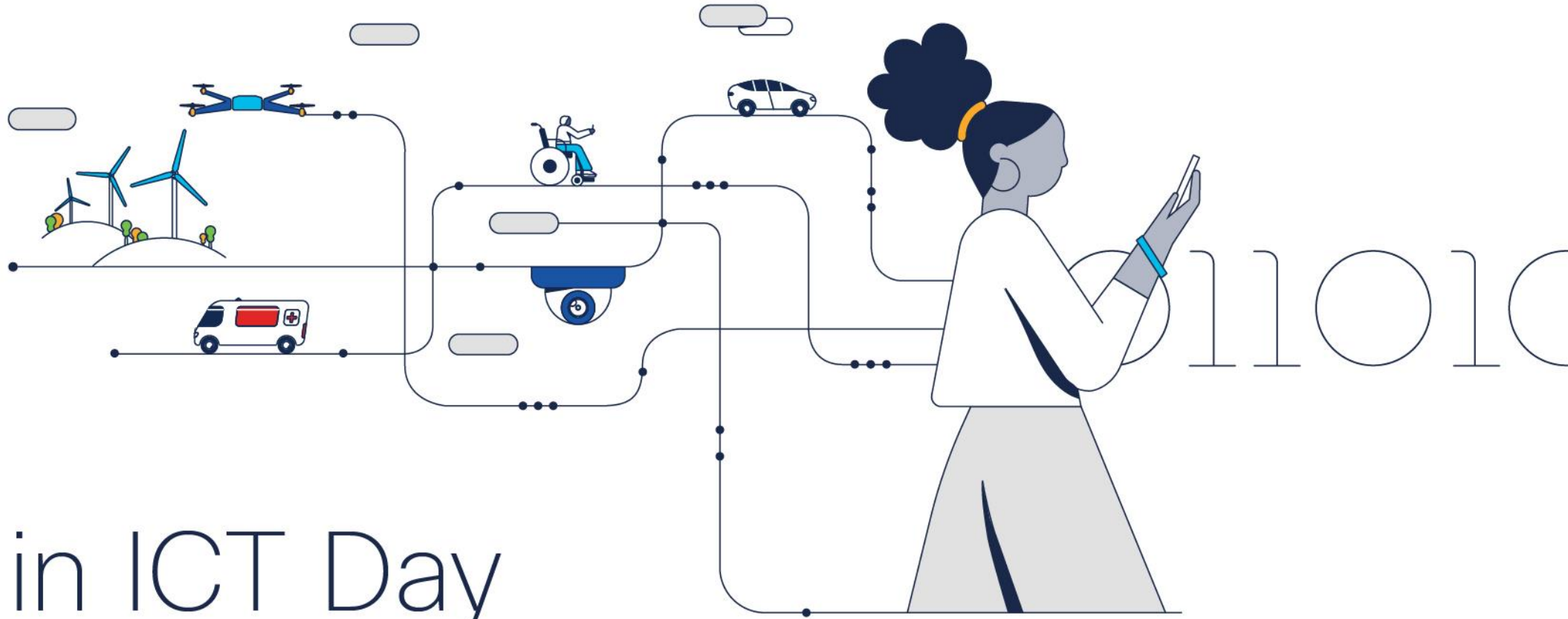
Módulo 5

Embaixadores do Programa 2020, 2021, 2022 & 2023:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

Networking
Academy



INTERNATIONAL

Girls in ICT Day

Brought to you by **WOMEN ROCK-IT**

Agenda

Como converter endereços binários em endereços decimais pontilhados e decimais em binários.

*Novos truques com Atividade **Jogo Binário***

Título do módulo: **Sistemas de números**

Objetivo do módulo: **Calcular números entre sistemas decimal, binário e hexadecimal.**

Título do Tópico	Objetivo do Tópico
Sistema Binário de Numeração	Calcular números entre sistemas decimal e binário.
Sistema de numeração hexadecimal	Calcular números entre sistemas decimal e hexadecimal.

Networking Academy

INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

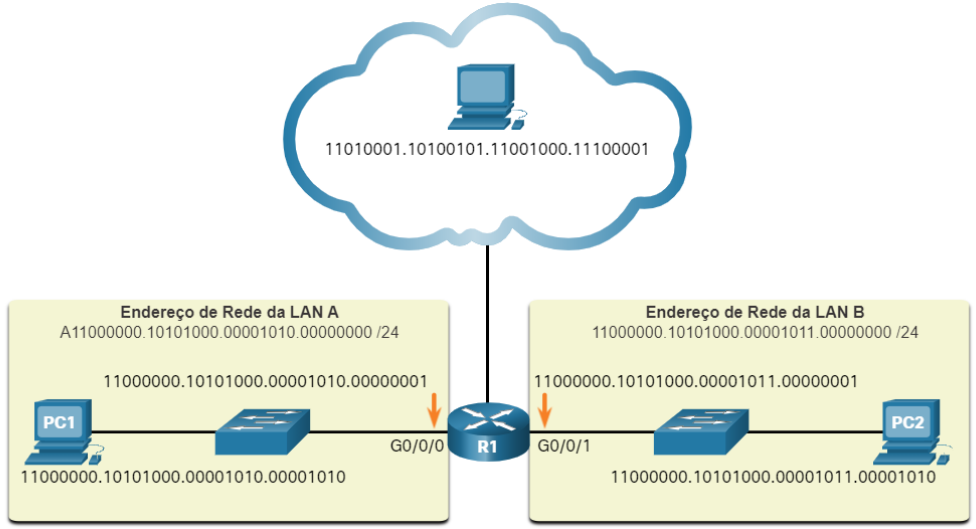
Sistemas de Numeração Binários

Endereços Binários e IPv4

- Os endereços IPV4 são binários, utilizando um sistema matemático compostos pelo algarismos 0 e 1.

São difíceis de gerenciar, por isso Administradores de Rede o convertem para decimal.

- Binário é um sistema de numeração 0 e 1 chamados bits.
- Decimal consiste em 10 dígitos, consistindo nos dígitos de 0 a 9.



Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Conversão entre Sistemas

Vídeo – Convertendo entre sistemas de numeração binária e decimal

NOTAÇÃO POSICIONAL BINÁRIA

https://contenthub.netacad.com/f5af14ac-f6c8-4d89-8e41-3f191aef5139

Raiz	10	10	10	10
Posição no número	3	2	1	0
Cáculo	(10^3)	(10^2)	(10^1)	(10^0)
Valor da posição	1000	100	10	1

- Exemplo: Número Decimal 1234

	Milhar	Centena	Dezena	Unidade
Valor Posicional	1000	100	10	1
Número decimal (1234)	1	2	3	4
Cálculo	1 x 1000	2 x 100	3 x 10	4 x 1
Junte-os...	1000	+ 200	+ 30	+ 4
Resultado	**1.234**			

Conversão entre Sistemas

- Por outro lado, a notação posicional binária opera como descrito na tabela.

Raiz	2	2	2	2	2	2	2	2
Posição no número	7	6	5	4	3	2	1	0
Cáculo	(2^7)	(2^6)	(2^5)	(2^4)	(2^3)	(2^2)	(2^1)	(2^0)
Valor da posição	128	64	32	16	8	4	2	1

- O exemplo na tabela ilustra como um número binário 11000000 corresponde ao número 192.

Se o número binário fosse 10101000, o decimal correspondente seria 168

Valor Posicional	128	64	32	16	8	4	2	1
Número binário (11000000)	1	1	0	0	0	0	0	0
Cáculo	1 x 128	1 x 64	0 x 32	0 x 16	0 x 8	0 x 4	0 x 2	0 x 1
Adicione-os..	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Resultado	**192**							

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Converter binário para decimal

11000000.10101000.00001011.00001010

Divida o IPv4 em 4 octetos de 8 bits.

Aplique o valor posicional binário ao primeiro octeto do número binário e calcule de acordo.

Utilize o mesmo processo com o seguintes Octetos

Valor Posicional	128	64	32	16	8	4	2	1
Número binário (11000000)	1	1	0	0	0	0	0	0
Cáculo	128	64	32	16	8	4	2	1
Adicionar...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Resultado	**192**							

Fig1. Primeiro Octeto

Valor Posicional	128	64	32	16	8	4	2	1
Número binário (10101000)	1	0	1	0	1	0	0	0
Cáculo	128	64	32	16	8	4	2	1
Adicionar...	128	+ 0	+ 32	+ 0	+ 8	+ 0	+ 0	+ 0
Resultado	**168**							

Fig2. Segundo Octeto

Valor Posicional	128	64	32	16	8	4	2	1
Número Binário (00001011)	0	0	0	0	1	0	1	1
Cálculo	128	64	32	16	8	4	2	1
Adicionar...	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 1
Resultado	**11**							

Fig3. Terceiro Octeto

Valor Posicional	128	64	32	16	8	4	2	1
Número binário (00001010)	0	0	0	0	1	0	1	0
Cáculo	128	64	32	16	8	4	2	1
Adicionar...	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 0
Resultado	**10**							

Fig4. Quarto Octeto

Networking Academy

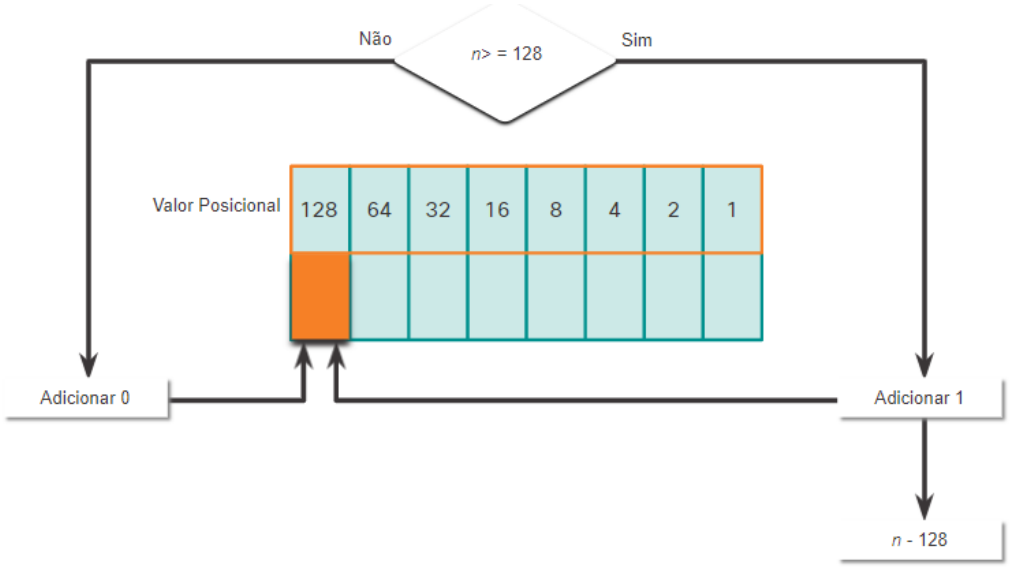
INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Conversão de decimal para binário

Utilize a tabela de valores posicionais binários

128	64	32	16	8	4	2	1



O número decimal do octeto (n) é igual ou superior ao bit mais significativo (**128**)?

- Se sim insira o binario **0** ao valor **128**.
- Se não insira o binario **1** ao valor **128** e subtraia **128** do numero decimal.

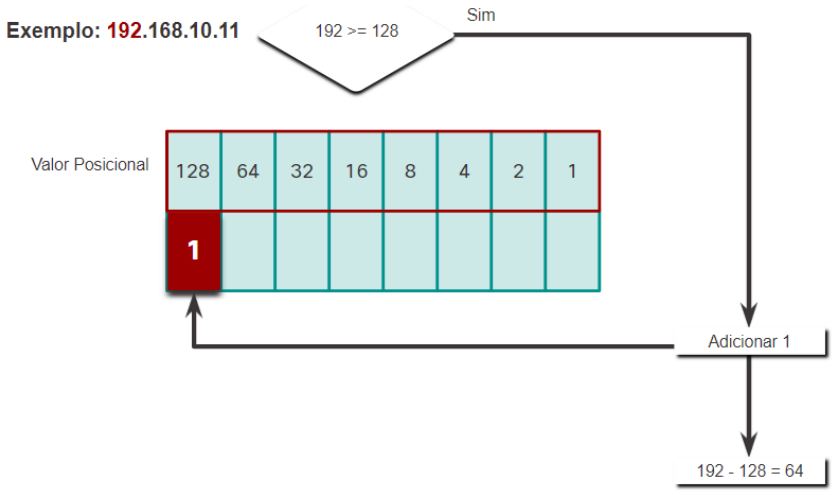
Networking Academy

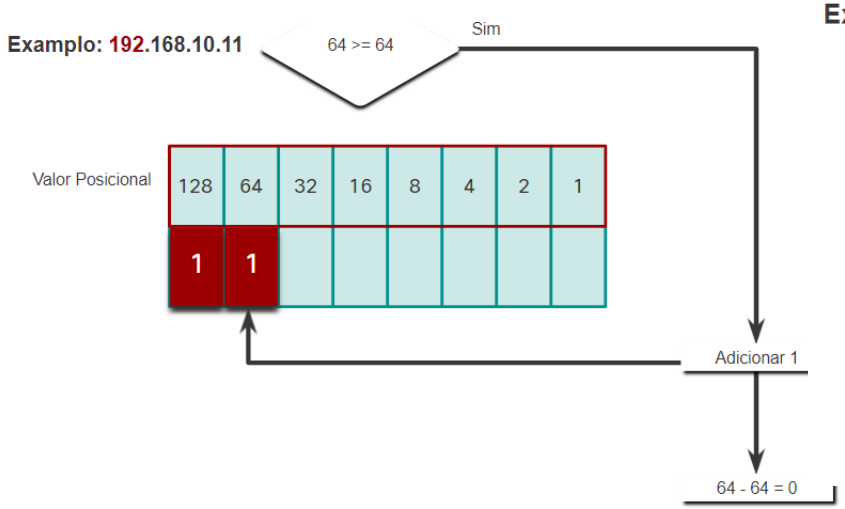
INTERNATIONAL Girls in ICT Day
Brought to you by **WOMEN ROCK-IT**

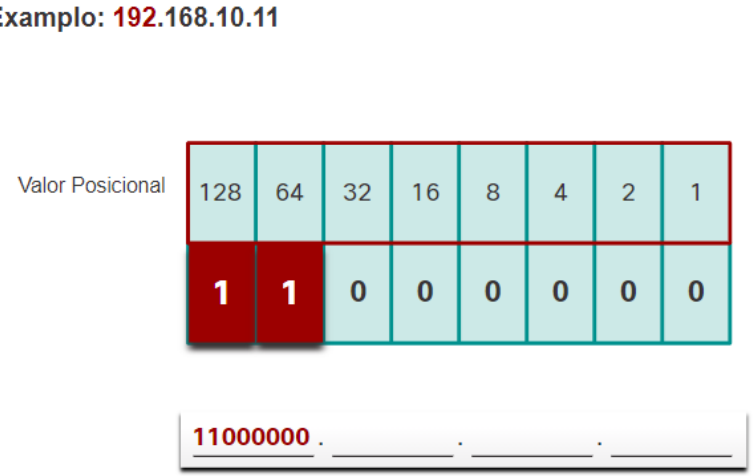
Exemplo de Conversão de Decimal para Binário

192.168.11.10

Converter primeiro octeto para binário







Exemplo de Conversão de Decimal para Binário

192.168.11.10

Converter segundo octeto para binário

Valor Posicional	128	64	32	16	8	4	2	1
	1	0	**1**	0	**1**	0	0	0

11000000 . **10101000** . _____ . _____

Converter terceiro octeto para binário

Valor Posicional	128	64	32	16	8	4	2	1
	0	0	0	0	**1**	0	**1**	0

11000000 . 10101000 . **00001010** . _____

Converter quarto octeto para binário

Valor Posicional	128	64	32	16	8	4	2	1
	0	0	0	0	**1**	0	**1**	**1**

11000000 . 10101000 . 00001010 . **00001011**

Networking Academy

INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Jogo Binário

Esta é uma maneira divertida de aprender números binários para redes.

Game Link: https://learningnetwork.cisco.com/docs/DOC-1803

Acesso pelo login no **cisco.com** para usar este link.

Será necessário criar uma conta se você ainda não tiver uma.

Networking Academy

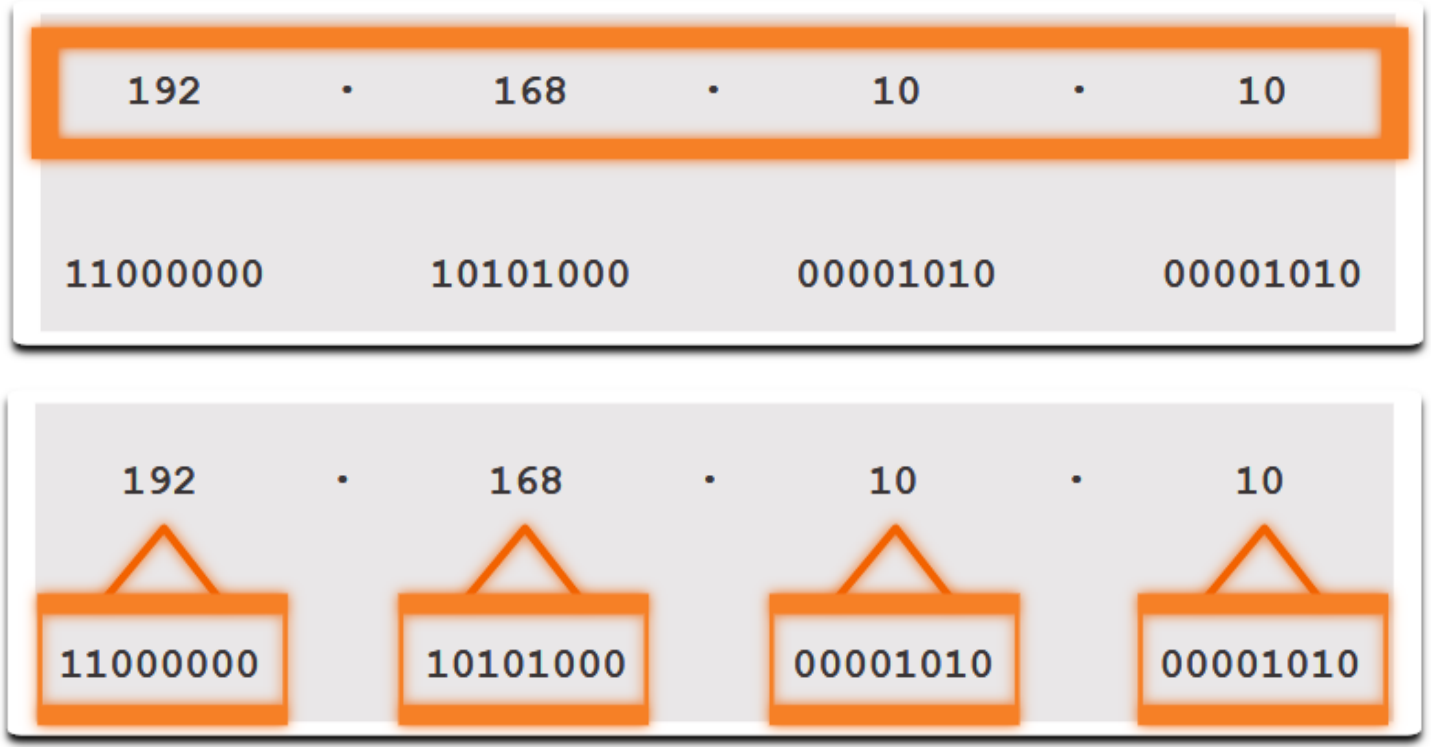
INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Endereços IPV4

Roteadores e computadores utilizam binários.

Humanos trabalham em decimal.



IP – Computador

Composto por quatro octetos diferentes

Networking Academy

INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Sistema de numeração hexadecimal

Para converter **decimal** em **hexadecimal**, você também deve primeiro converter o **decimal** para **binário**.

Assim como **decimal** é um sistema numérico de base **dez**, **hexadecimal** é um sistema de **dezesseis** bases.

O sistema numérico de dezesseis base usa os dígitos 0 a 9 e as letras A a F.

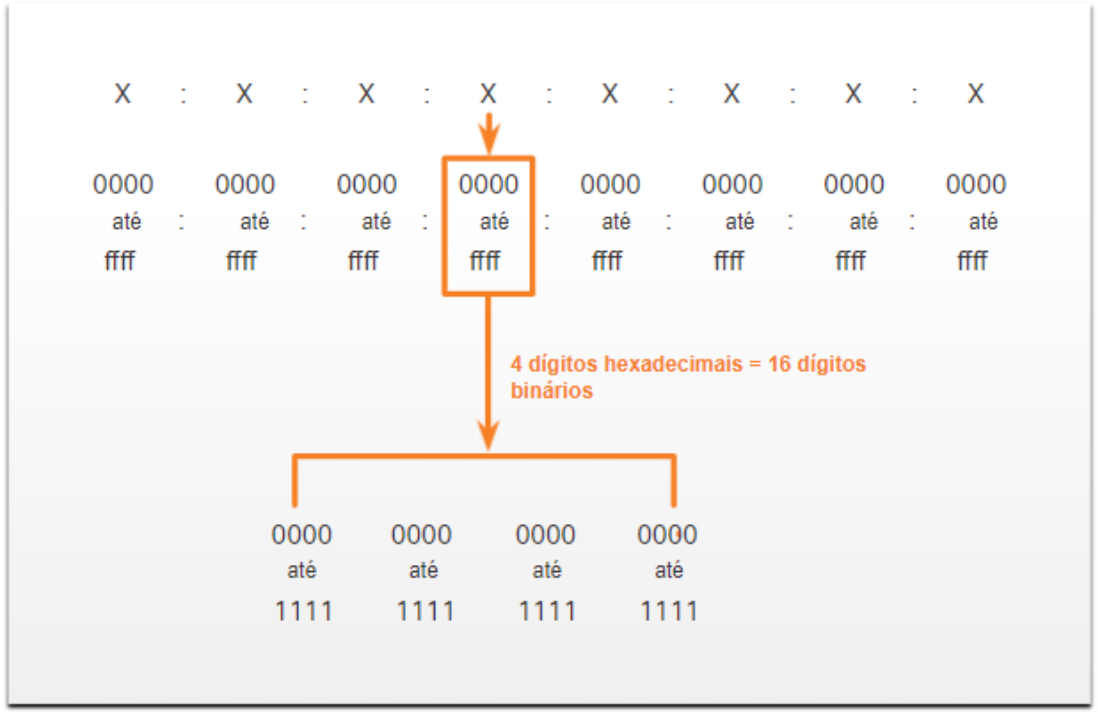
O sistema de numeração **hexadecimal** é usado em rede para representar endereços **IPv6** e endereços **MAC** Ethernet.

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

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

Sistema de numeração hexadecimal

- Cada "x" é um único hextet, 16 bits ou quatro dígitos hexadecimais.



Sistema de numeração hexadecimal

Endereços hexadecimais e IPv6

Para Converter números decimais em valores hexadecimais é simples:

1. **Converta** o número decimal para strings binárias de 8 bits.
2. **Divida** as cadeias binárias **em grupos de quatro** a partir da posição mais à direita.
3. **Converta** cada quatro números binários em seu dígito **hexadecimal** equivalente.

Para Converter números hexadecimais em valores decimais também é simples:

1. **Converta** o número **hexadecimal** em cadeias **binárias** de 4 bits.
2. **Crie agrupamento binário de 8 bits** a partir da posição mais à direita.
3. **Converta** cada agrupamento binário de 8 bits em seu dígito decimal equivalente.

Conversão decimal para hexadecimal

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

Por exemplo, 168 convertidos em hexadecimal usando o processo de três etapas:

1. **168** em binário é **10101000**
2. **10101000** em dois grupos de quatro dígitos binários é **1010** e **1000**.
3. **1010** é hexadecimal **A**
   1000 é hexadecimal **8**.

Responda: **168** é **A8** em **hexadecimal**.

Tabela de valores decimais e hexadecimais equivalentes para os binários 0000 a 1111.

Conversão decimal para hexadecimal

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

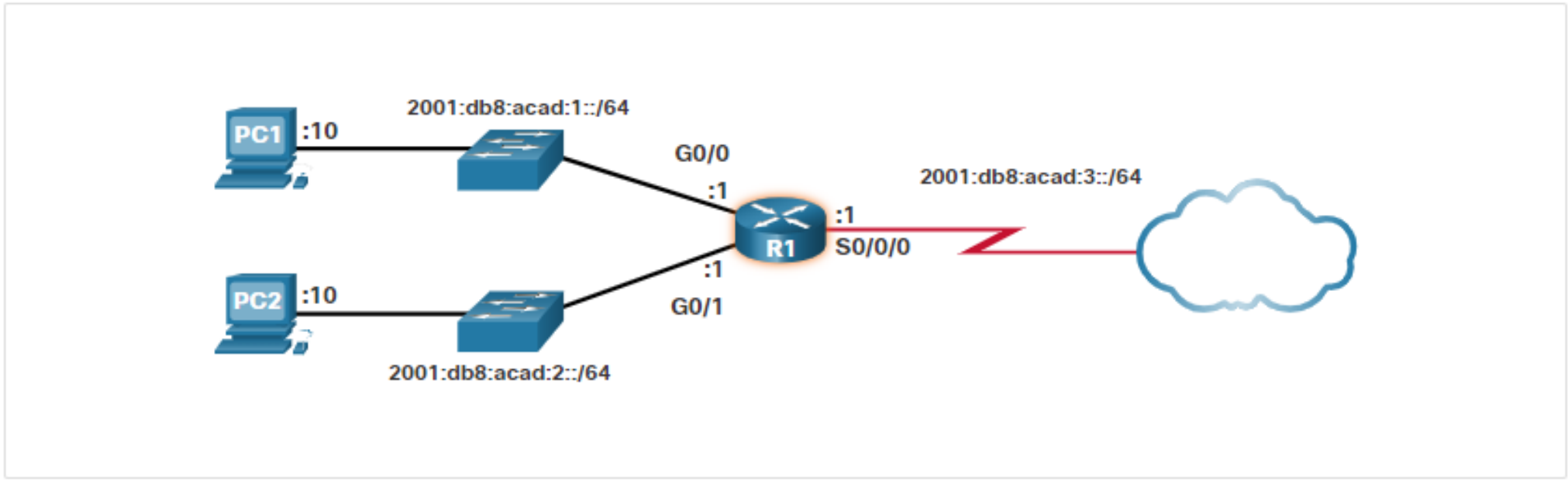
Por exemplo, Hexadecimal **D2** para **decimal**:

1. **D2** em cadeias binárias de 4 bits é **1101** e **0010**.
2. **1101** e **0010** é **11010010** em um agrupamento de 8 bits (**binário**).
3. **11010010** em **binário** é equivalente a **210** em **decimal**.

Responda: **D2** em hexadecimal é **210** em decimal.

Tabela de valores decimais e hexadecimais equivalentes para os binários 0000 a 1111.

Exemplo Topologia IPv6



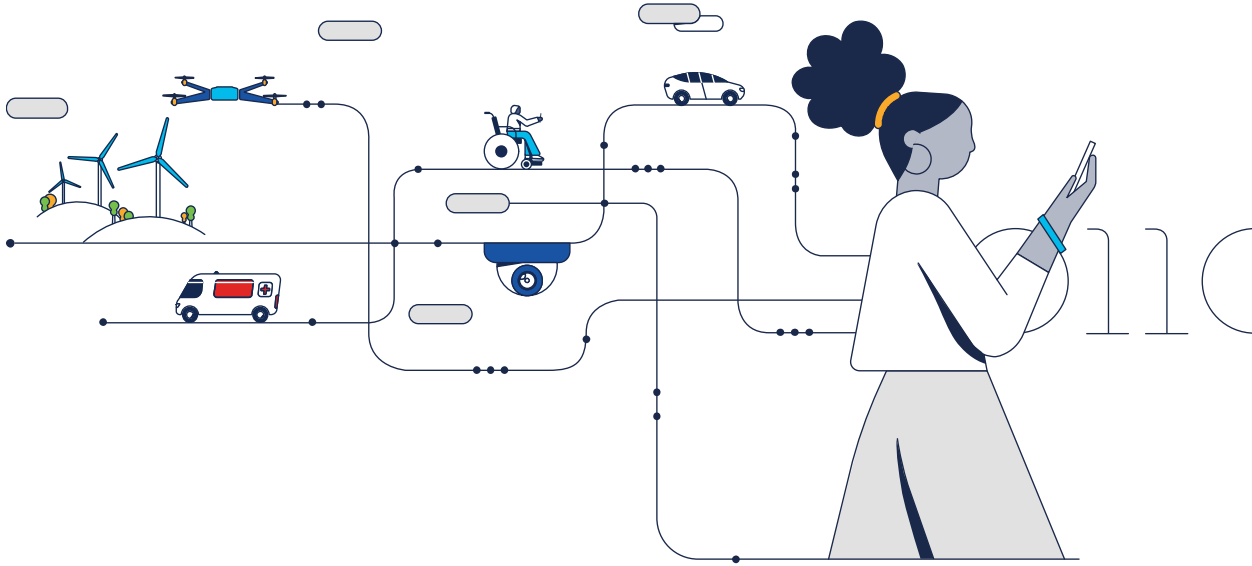
The bridge to possible

Nossos parceiros

TD SYNNEX

WISE
Women in Science
and Engineering
Inclusive Community

cisco
Networking
Academy



INTERNATIONAL
Girls in ICT Day
Brought to you by **WOMEN ROCK-IT**

Cisco Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

CCNAv7 – ITN – Camada Enlace de Dados

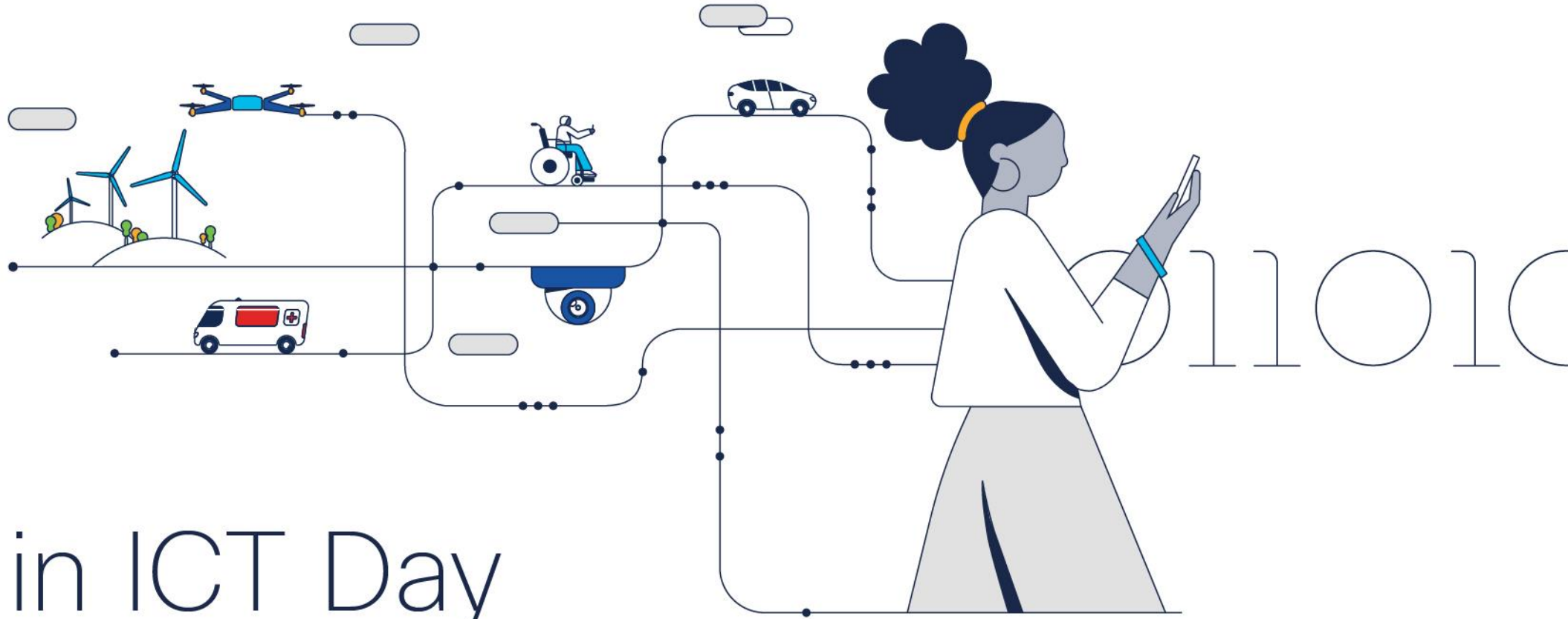
Módulo 6

Embaixadores do Programa 2020, 2021, 2022 & 2023:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

Networking
Academy



INTERNATIONAL

Girls in ICT Day

Brought to you by **WOMEN ROCK-IT**

Camada de enlace

A camada de enlace de dados do modelo OSI (Camada 2) prepara os dados da rede para a rede física (Camada 1).

É responsável pela comunicação da placa de rede (NIC) e realiza as seguintes atividades:

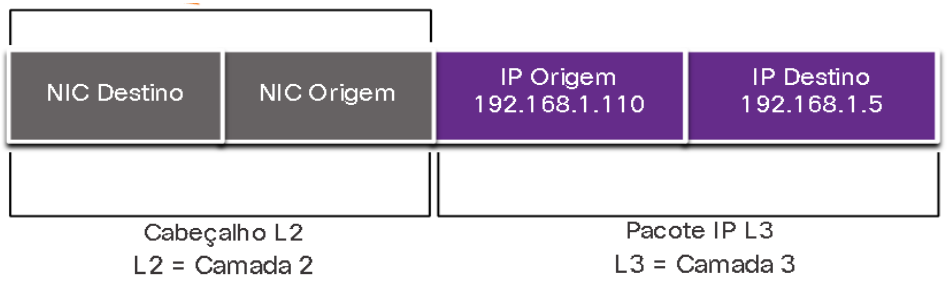
- Permite que as camadas superiores acessem a mídia, pois as camadas superiores não estão cientes do tipo de mídia que é usado para encaminhar os dados.
- Aceita dados, geralmente pacotes de Camada 3 (ou seja, IPv4 ou IPv6), e os encapsular em quadros da Camada 2.
- Controla como os dados são colocados e recebidos na mídia.
- Troca quadros entre pontos de extremidade através da mídia de rede.
- Recebe dados encapsulados, geralmente pacotes de Camada 3, e os direciona para o protocolo de camada superior apropriado.
- Executa a detecção de erros e rejeita qualquer quadro corrompido.

Camada de enlace

Um nó pode ser um dispositivo final, como um laptop ou telefone celular, ou um dispositivo intermediário, como um switch Ethernet, que pode receber, criar, armazenar ou encaminhar dados ao longo de um caminho de comunicação.

Sem a camada de enlace de dados, um protocolo de camada de rede, como o IP, teria de estar preparado para se conectar a cada tipo de meio físico que poderia existir ao longo do caminho. Além disso, toda vez que uma nova tecnologia ou meio de rede fosse desenvolvido, o IP teria que se adaptar.

A camada de link(ou enlace) de dados adiciona informações de destino Ethernet da Camada 2 e NIC de origem a um pacote da Camada 3.
Em seguida, ele converte essa informação para um formato suportado pela camada física (ou seja, Camada 1).



Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

SUBCAMADAS DE ENLACE

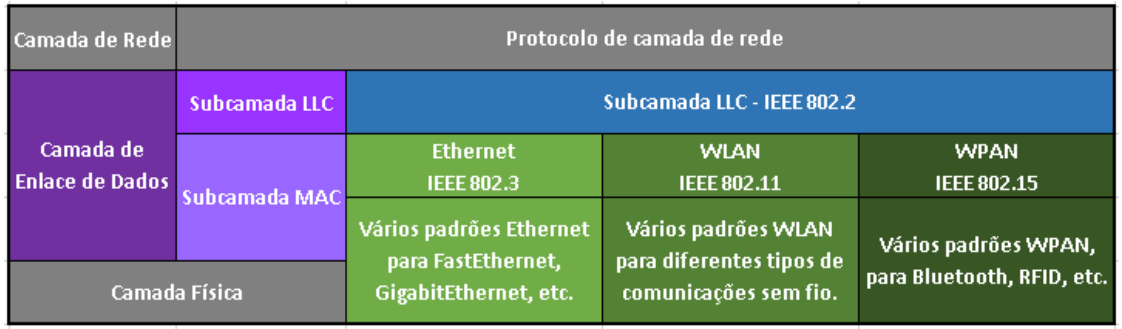
IEEE 802 LAN/MAN

Os padrões IEEE 802 LAN/MAN são específicos para LANs Ethernet, LANs sem fio (WLAN), redes pessoais sem fio (WPAN) e outros tipos de redes locais e metropolitanas. E, consiste em 2 subcamadas:

Logical Link Control (LLC) (IEEE 802.2): Essa subcamada comunica entre o software de rede nas camadas superiores e o hardware do dispositivo nas camadas inferiores. Ela pega os dados do protocolo de rede, como um pacote IPv4 ou IPv6, e adiciona informações de controle da camada 2 para ajudar a entregar o pacote ao nó de destino, usando a mesma interface de rede e mídia.

Controle de Acesso a Mídia (MAC): Implementa a subcamada (**IEEE 802.3**, **802.11** ou **802.15**) no hardware.

É responsável pelo encapsulamento de dados e controla a NIC e outro hardware responsável pelo envio e recebimento de dados no meio LAN/MAN, com ou sem fio.
Fornece endereçamento de camada de enlace e é integrado com várias tecnologias de camada física.



Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

SUBCAMADAS DE ENLACE

IEEE 802 LAN/MAN

A subcamada MAC fornece encapsulamento de dados:

- **Delimitação de quadros -** O processo de enquadramento fornece delimitadores importantes para identificar campos dentro de um quadro.
  Esses bits de delimitação promovem a sincronização entre os nós de transmissão e de recepção.
- **Endereçamento -** Fornece endereçamento de origem e destino para transportar o quadro da Camada 2 entre dispositivos na mesma mídia compartilhada.
- **Detecção de erro -** Inclui um trailer usado para detectar erros de transmissão.

A subcamada MAC também fornece controle de acesso a mídia, permitindo que vários dispositivos se comuniquem através de uma mídia compartilhada (half-duplex). As comunicações full-duplex não exigem controle de acesso.

Fornecimento de Acesso ao Meio Físico

Cada ambiente de rede pode ter diferentes características. Em uma LAN Ethernet geralmente consiste em muitos hosts que disputam o acesso ao meio físico para envio de dados.
A subcamada MAC resolve isso.

Em interfaces seriais, para se conectar à WAN, o método de acesso consiste em uma conexão direta entre apenas dois dispositivos, geralmente dois roteadores.
Portanto, eles não exigem as técnicas empregadas pela subcamada MAC IEEE 802.

À medida que as interfaces do roteador encapsulam o pacote no quadro apropriado, um método adequado de controle de acesso ao meio físico é usado para acessar cada link.
Em cada salto um roteador irá executará essas funções da Camada 2:

1. Aceita um quadro de um meio;
2. Desencapsula o quadro, para a PDU de Camada 3;
3. Encapsula novamente o pacote em um novo quadro;
4. Encaminha o novo quadro apropriado para o meio físico desse segmento da rede física.

Padrões da camada de enlace

Os protocolos da camada de enlace de dados geralmente não são definidos por RFCs (Request for Comments), ao contrário dos protocolos das camadas superiores do conjunto TCP / IP.
A Internet Engineering Task Force (IETF) mantém os protocolos e serviços funcionais do conjunto de protocolos TCP / IP nas camadas superiores, mas eles não definem as funções e a operação da camada de acesso à rede TCP / IP.

As organizações de engenharia que definem padrões abertos e protocolos que se aplicam à camada de acesso à rede (ou seja, as camadas físicas e de link de dados OSI) incluem o seguinte:

- Institute of Electrical and Electronics Engineers (IEEE)
- International Telecommunication Union (ITU)
- International Organization for Standardization (ISO)
- Instituto Nacional Americano de Padronização (ANSI)

Topologias físicas e lógicas

A camada de link de dados prepara os dados da rede para a rede física. Para isso ela deve conhecer a topologia lógica de uma rede para poder determinar o que é necessário para transferir quadros de um dispositivo para outro.

Existem dois tipos de topologias usadas ao descrever redes LAN e WAN:

- **Topologia física:** Identifica as conexões físicas e como os dispositivos finais e intermediários são interconectados. A topologia também pode incluir a localização específica do dispositivo, como o número do quarto e a localização no rack do equipamento. As topologias físicas são geralmente ponto a ponto ou estrela.
- **Topologia lógica:** É à maneira como uma rede transfere quadros de um nó para o outro. Esta topologia identifica conexões virtuais usando interfaces de dispositivo e esquemas de endereçamento IP da Camada 3.

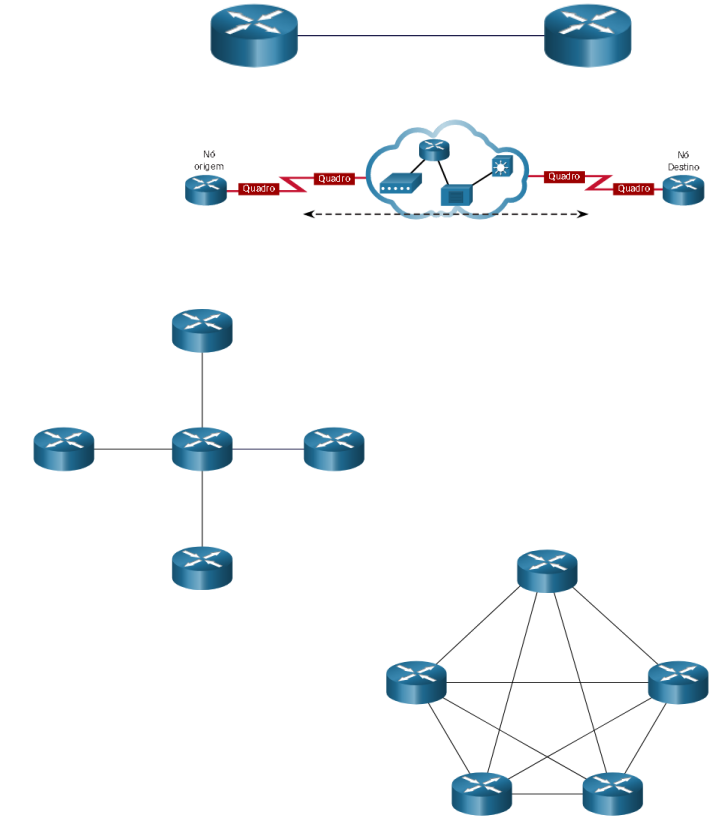
A camada de enlace de dados “vê” a topologia lógica da rede quando controla o acesso de dados ao meio físico. É a topologia lógica que influencia o tipo de enquadramento de rede e o controle de acesso ao meio usado.

Topologias WAN

Ponto a Ponto: Mais simples e comum. Consiste em uma ligação permanente entre 2 pontos finais, que não compartilham o meio físico com outros hosts. Usando um protocolo de comunicação serial como o PPP, um nó não precisa determinar se um quadro de entrada é destinado a ele ou a outro nó. Sendo os protocolos de enlace muito simples, pois todos os quadros no meio físico podem trafegar apenas para os 2 nós ou a partir deles.
Quando conectados por alguma distancia geográfica, usando vários dispositivos físicos intermediários, a topologia logica ponto a ponto não será alterada.

Estrela: Consiste em um site central interconectando sites de filiais através do uso de links ponto a ponto. Os sites de filiais não trocam dados com outras filiais sem passar pelo site central.

Malha: Fornece alta disponibilidade, todos os sistemas finais são interconectados entre si. Os custos administrativos e físicos podem ser significativos. Cada link é essencialmente um link ponto a ponto.



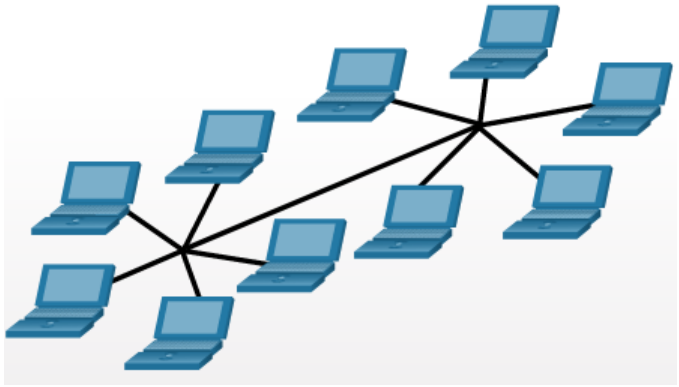
Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Topologias LAN

Em LANs multiacesso, os hosts são interligados usando **topologia estrela** ou **estrela estendida.**
Neste tipo de topologia, os dispositivos finais são conectados a um dispositivo intermediário central, neste caso, um switch Ethernet.
As topologias em estrela estendidas, estende essa topologia interconectando vários switches Ethernet.
São fáceis de instalar, escalonáveis e fáceis de solucionar problemas.

Às vezes, pode haver apenas dois roteadores conectados na LAN Ethernet.
Este seria um exemplo de Ethernet usado em uma **topologia ponto a ponto**.



Comunicação Duplex

A comunicação duplex é se refere à direção da transmissão de dados entre dois dispositivos.
Existem dois modos comuns de duplex.

Comunicação Half-duplex: O half-duplex restringe a troca de dados a uma direção de cada vez.
Permite que apenas um dispositivo envie ou receba por vez na mídia compartilhada.
WLANs e topologias de barramento herdadas com hubs Ethernet usam o modo half-duplex.

Comunicação Full-duplex: O modo full-duplex permite o envio e o recebimento simultâneos de dados na mídia compartilhada.
A camada de enlace de dados supõe que o meio físico está disponível para transmissão para ambos os nós a qualquer momento.
Os comutadores Ethernet operam no modo full-duplex por padrão, mas podem operar no modo half-duplex se estiverem conectados a um dispositivo como um hub Ethernet.

As interfaces interconectadas, como uma NIC de host e uma interface em switch Ethernet, devem usar o mesmo modo duplex. Caso contrário, haverá uma incompatibilidade de duplex que criará ineficiência e latência no link.

Métodos de Controle de Acesso

Métodos de controle de acesso controlam como dois, ou mais dispositivos, tentando acessar a rede simultaneamente, compartilham o meio físico.

São dois os métodos:

1. Acesso baseado em Contenção: Os nós operam em half-duplex, competindo pelo uso do meio. Podem ser controlados por 2 métodos de acesso baseados em contenção:

- **CSMA/CD (Carrier Sense Multiple Access with Collision Detection):** Usado em LAN sem fio e LAN Ethernet legadas. Se dois dispositivos transmitirem simultaneamente, ocorre uma colisão.
  Ambos os dispositivos detectam a colisão na rede. A NIC compara os dados transmitidos com os dados recebidos.
  Os dados enviados por ambos serão corrompidos e precisarão ser reenviados.
- **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):** Usado em LANs sem fio (WLANs IEEE 802.11). Não detecta colisões, tenta evitá-las aguardando antes de transmitir. Ao transmitir, o nó informa o tempo necessário para a transmissão.
  Todos os dispositivos sem fio recebem essas informações para saber quanto tempo a mídia ficará indisponível.
  Após o envio, o receptor retorna uma confirmação para que o remetente saiba que o quadro chegou.

Métodos de Controle de Acesso

2. Acesso Controlado: Cada nó tem seu próprio tempo para usar o meio. São ineficientes porque um dispositivo deve aguardar sua vez para acessar o meio. Usada em topologia legada, anel de token.

Observações:

- Quer se trate de uma LAN Ethernet que use hubs, ou uma WLAN, os sistemas baseados em contenção não escalam bem sob uso intenso.

- As LANs Ethernet que usam comutadores não usam um sistema baseado em contenção porque o comutador e a NIC do host operam no **modo full-duplex.**

Quadro de enlace de dados

A camada de enlace, prepara os dados encapsulados para o transporte pela mídia local, encapsulando-o com um cabeçalho e um trailer para criar um quadro.
Cada tipo de quadro tem três partes básicas:

- Cabeçalho;
- Dados;
- Trailer.

Todos os protocolos da camada de enlace de dados encapsulam os dados dentro do campo de dados do quadro.
No entanto, a estrutura do quadro e os campos contidos no cabeçalho e trailer, variam de acordo com o protocolo e as necessidades de todo transporte de dados através de todos os tipos de mídia.
Dependendo do ambiente, a quantidade de informações de controle necessária no quadro varia para corresponder às exigências de controle de acesso ao meio físico e à topologia lógica.
Por exemplo, um quadro WLAN deve incluir procedimentos para evitar colisões e, portanto, requer informações de controle adicionais quando comparado a um quadro Ethernet.

Os campos de cabeçalho e de trailer aumentam à medida que mais informações de controle são necessárias.

Campos do Quadro

O enquadramento quebra o fluxo em agrupamentos decifráveis, com a informação de controle inserida no cabeçalho e trailer como valores em diferentes campos. Esse formato fornece aos sinais físicos uma estrutura reconhecida por nós e decodificada em pacotes no destino. Nem todos os protocolos incluem todos os campos.
Os padrões para um protocolo de enlace de dados específico definem o formato real do quadro.

Os campos de quadro incluem:

Sinalizadores de início e fim do quadro: Identificando os limites de início e fim do quadro.

Endereçamento: Indica os nós de origem e destino na mídia.

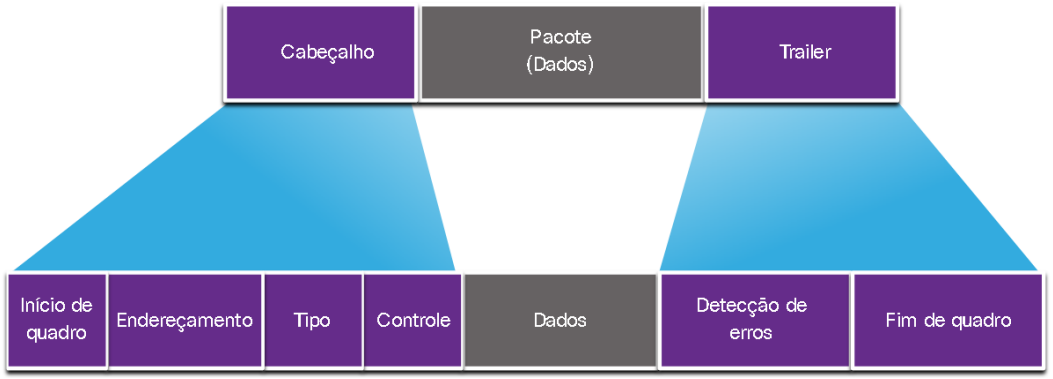
Tipo: Identifica o protocolo da camada 3 no campo de dados.

Controle: Identifica serviços especiais de controle de fluxo, como qualidade de serviço (QoS). A QoS dá prioridade ao encaminhamento para certos tipos de mensagens. Por exemplo, os quadros de voz sobre IP (VoIP) normalmente recebem prioridade porque são sensíveis ao atraso.

Dados: Contém a carga útil do quadro (ou seja, cabeçalho do pacote, cabeçalho do segmento e os dados).

Detecção de Erro: Incluído após os dados para formar o trailer.

Campos do Quadro



Em um pacote de dados encapsulado por um cabeçalho de link de dados e um trailer de link de dados.
O cabeçalho do link de dados é dividido em 4 campos: início do quadro, endereçamento, tipo e controle.
O trailer do link de dados é dividido em dois campos: Detecção de erro e parada de quadros.

Os protocolos de enlance acrescentam um trailer ao final de cada quadro, com um matemático dos bits.
Em um processo chamado detecção de erros, o trailer determina se o quadro chegou sem erros.
Isso se faz necessário porque os sinais na mídia podem estar sujeitos a interferências, distorções ou perdas que alterariam os valores de bits que esses sinais representam.

Um nó de transmissão cria um resumo lógico dos conteúdos do quadro, conhecido como valor de verificação de redundância cíclica (cyclic redundancy check - CRC) Este valor é colocado no campo FCS (Sequência de Verificação de Quadro) para exibição ou conteúdo do quadro. No trailer Ethernet, o FCS fornece um método para o nó de recebimento determinar se o quadro apresentou erros de transmissão.

Endereços de camada 2

Os endereços de dispositivos na camada 2 são chamados de endereços físicos.
O endereçamento está contido no cabeçalho do quadro e especifica o nó de destino do quadro.
Normalmente, ele está no início do quadro, portanto, a NIC pode determinar rapidamente se ela corresponde ao seu próprio endereço de Camada 2 antes de aceitar o restante do quadro.
O cabeçalho do quadro também pode conter o endereço de origem do quadro.

Os endereços físicos não indicam em qual rede o dispositivo está localizado.
Trata se de um endereço exclusivo do dispositivo. Um dispositivo ainda funcionará com o mesmo endereço físico da Camada 2, mesmo que o dispositivo se mova para outra rede ou sub-rede. Portanto, os endereços de Camada 2 são usados apenas para conectar dispositivos dentro da mesma mídia compartilhada, na mesma rede IP.

Conforme o pacote IP viaja do host para o roteador, de roteador para roteador e de roteador para host, em cada ponto ao longo do caminho, o pacote IP é encapsulado em um novo quadro de enlace de dados.

Atualizando o endereço de link de dados de origem da NIC que está enviando o quadro e o endereço de link de dados de destino da NIC que está recebendo o quadro a cada salto.

O endereçamento IP permanece inalterado.

Quadros de LAN e WAN

Os endereços de dispositivos na camada 2 são chamados de endereços físicos.
O endereçamento está contido no cabeçalho do quadro e especifica o nó de destino do quadro.
Normalmente, ele está no início do quadro, portanto, a NIC pode determinar rapidamente se ela corresponde ao seu próprio endereço de Camada 2 antes de aceitar o restante do quadro.
O cabeçalho do quadro também pode conter o endereço de origem do quadro.

Os endereços físicos não indicam em qual rede o dispositivo está localizado.
Trata se de um endereço exclusivo do dispositivo. Um dispositivo ainda funcionará com o mesmo endereço físico da Camada 2, mesmo que o dispositivo se mova para outra rede ou sub-rede. Portanto, os endereços de Camada 2 são usados apenas para conectar dispositivos dentro da mesma mídia compartilhada, na mesma rede IP.

Conforme o pacote IP viaja do host para o roteador, de roteador para roteador e de roteador para host, em cada ponto ao longo do caminho, o pacote IP é encapsulado em um novo quadro de enlace de dados.

Atualizando o endereço de link de dados de origem da NIC que está enviando o quadro e o endereço de link de dados de destino da NIC que está recebendo o quadro a cada salto.
O endereçamento IP permanece inalterado.

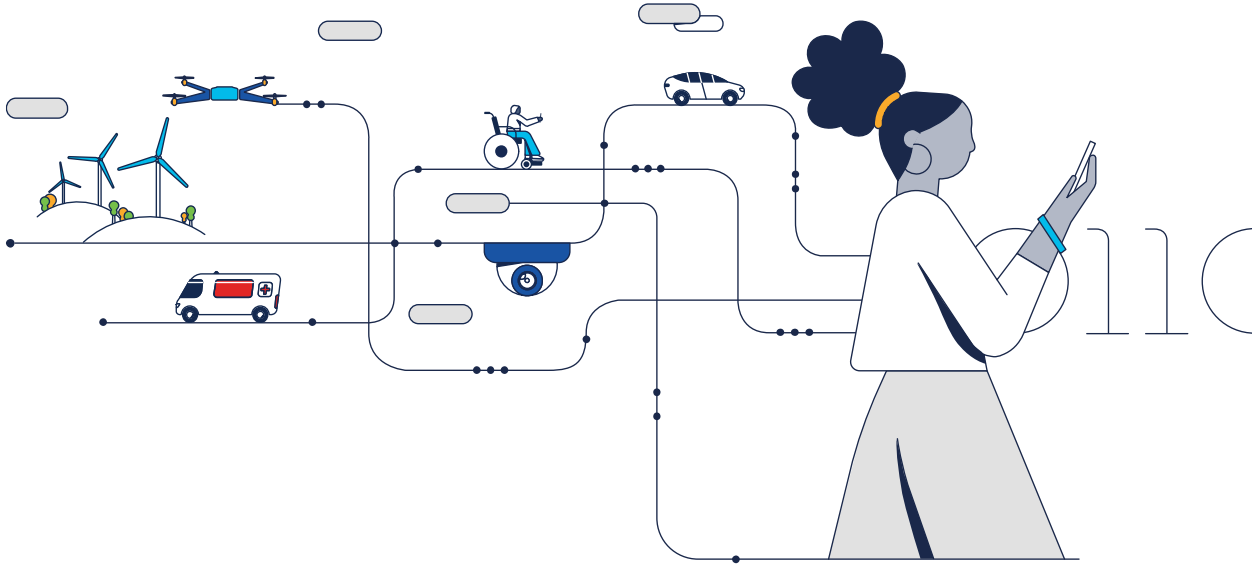
The bridge to possible

Nossos parceiros

TD SYNNEX

WISE
Women in Science
and Engineering
Inclusive Community

cisco
Networking
Academy



INTERNATIONAL
Girls in ICT Day
Brought to you by **WOMEN ROCK-IT**

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

CCNAv7 – ITN – Switching Ethernet

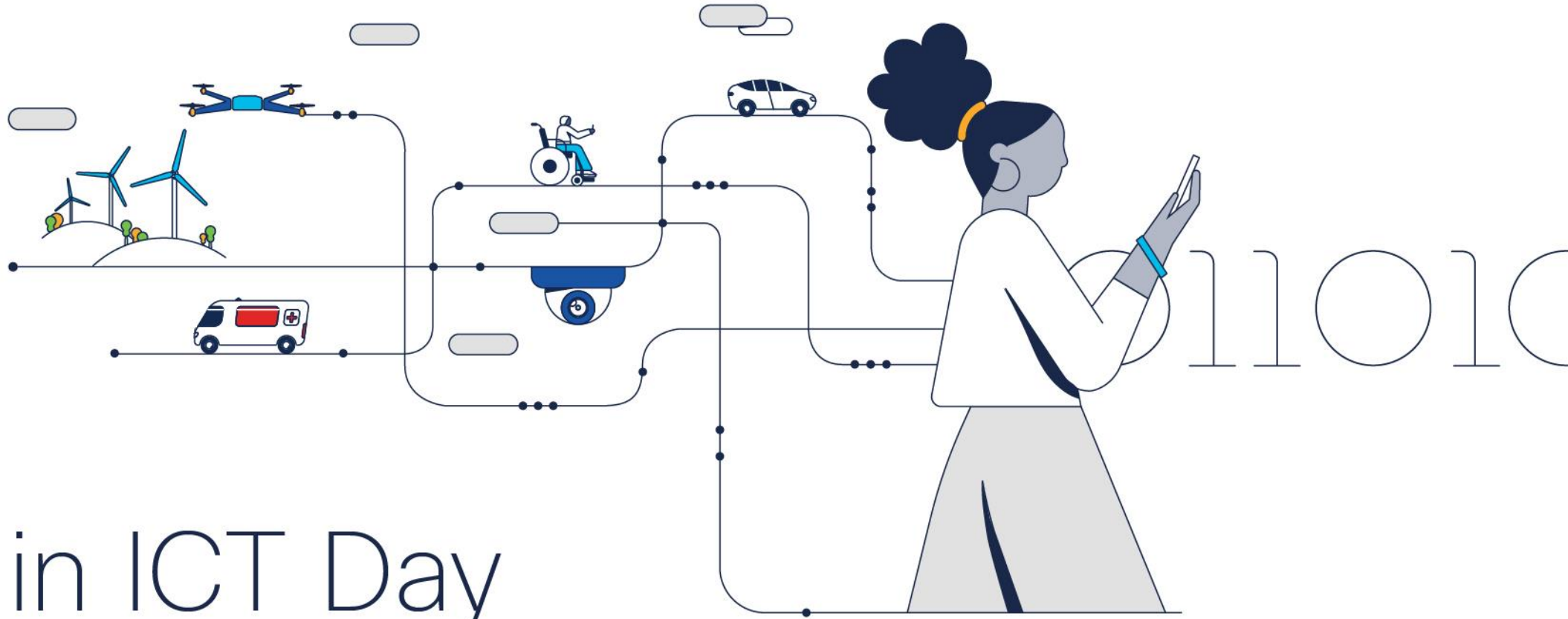
Módulo 7

Embaixadores do Programa 2020, 2021, 2022 & 2023:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

Networking
Academy



INTERNATIONAL

Girls in ICT Day

Brought to you by **WOMEN ROCK-IT**

Quadros Ethernet

A Ethernet é uma das duas tecnologias de LAN usadas atualmente, sendo a outra LANs sem fio (WLANs).
A Ethernet utiliza comunicações com fios, incluindo par trançado, ligações de fibra óptica e cabos coaxiais. Opera na camada de enlace de dados e na camada física.
É uma família de tecnologias de rede definidas nos padrões IEEE 802.2 e 802.3. A Ethernet suporta as seguintes larguras de banda:

- 10 Mbps
- 100 Mbps
- 1000 Mbps (1 Gbps)
- 10,000 Mbps (10 Gbps)
- 40,000 Mbps (40 Gbps)
- 100,000 Mbps (100 Gbps)

Os padrões Ethernet definem os protocolos da camada 2 e as tecnologias da camada 1.

Quadros Ethernet

Protocolos IEEE 802 LAN/MAN, incluindo Ethernet, usam as seguintes duas subcamadas separadas da camada de link de dados para operar.
Eles são o controle de link lógico (LLC) e o controle de acesso de mídia (MAC).

Subcamada LLC Sublayer - Essa subcamada IEEE 802.2 se comunica entre o software de rede nas camadas superiores e o hardware do dispositivo nas camadas inferiores.
Ela coloca a informação no quadro que identifica qual protocolo de camada de rede está sendo usado para o quadro.
Essas informações permitem que vários protocolos da camada 3, como IPv4 e IPv6, usem a mesma interface de rede e mídia.

Subcamada MAC - Esta subcamada (IEEE 802.3, 802.11 ou 802.15 por exemplo) é implementada em hardware e é responsável pelo encapsulamento de dados e controle de acesso a mídia.
Ele fornece endereçamento de camada de link de dados e é integrado com várias tecnologias de camada física.

Quadros Ethernet

A subcamada MAC é responsável pelo encapsulamento de dados e acesso à mídia.

O encapsulamento de dados IEEE 802.3 inclui o seguinte:

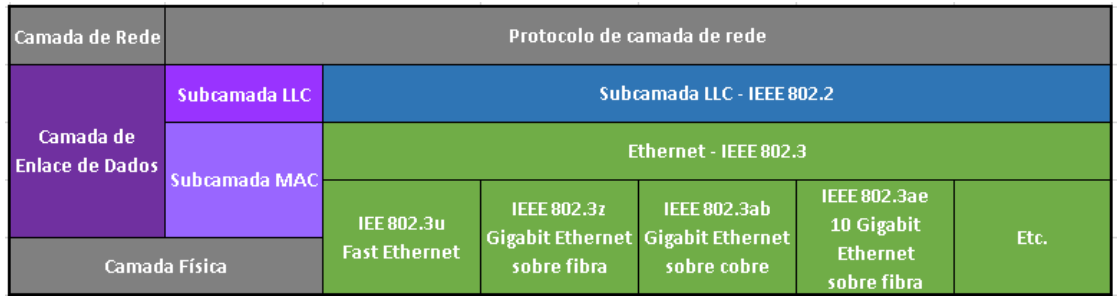
Quadro Ethernet - Esta é a estrutura interna do quadro Ethernet.

Endereçamento Ethernet - O quadro Ethernet inclui um endereço MAC de origem e de destino para fornecer o quadro Ethernet da NIC Ethernet para a NIC Ethernet na mesma LAN.

Detecção de erro Ethernet - O quadro Ethernet inclui um trailer de sequência de verificação de quadros (FCS) usado para detecção de erros.

A subcamada MAC IEEE 802.3 inclui as especificações para diferentes padrões de comunicações Ethernet em vários tipos de mídia, incluindo cobre e fibra.

As LANs Ethernet de hoje usam switches que operam em full-duplex.
As comunicações full-duplex com switches Ethernet não exigem controle de acesso através do CSMA/CD.



Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

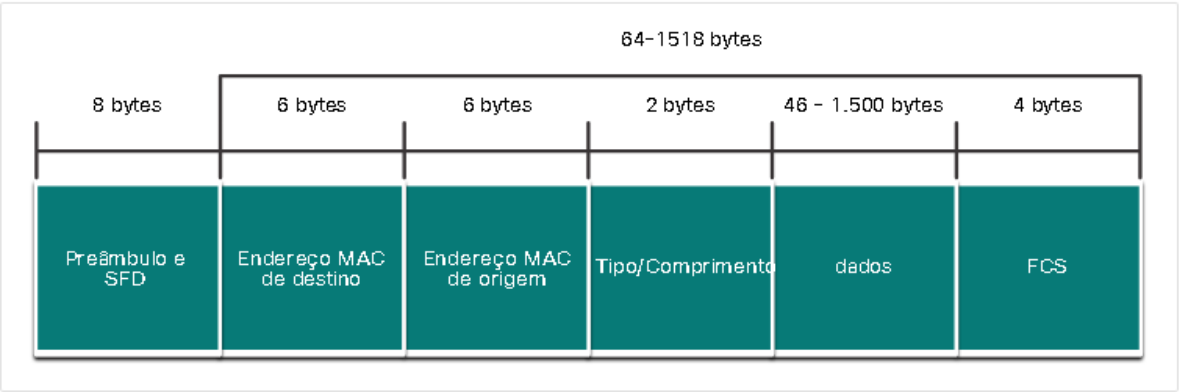
Campos de Quadro Ethernet

O tamanho mínimo de quadro Ethernet é 64 bytes e o máximo é 1518 bytes. Isso inclui todos os bytes do campo de endereço MAC de destino através do campo FCS (Frame Check Sequence).
O campo de preâmbulo não é incluído ao descrever o tamanho do quadro.

Qualquer quadro com comprimento menor que 64 bytes é considerado um "fragmento de colisão" ou um "quadro desprezível" e é automaticamente descartado pelas estações receptoras.
Quadros com mais de 1.500 bytes de dados são considerados “jumbo” ou “baby giant”.

Se o tamanho de um quadro transmitido for menor que o mínimo ou maior que o máximo, o dispositivo receptor descarta o quadro.
É provável que quadros perdidos sejam resultado de colisões ou outros sinais indesejados.
Eles são considerados inválidos.
Os quadros jumbo geralmente são suportados pela maioria dos switches e NICs Fast Ethernet e Gigabit Ethernet.

Campos do quadro Ethernet



Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Campos de Quadro Ethernet

Campo	Descrição
Campos Preâmbulo e Delimitador Início de Quadro	O Preâmbulo (7 bytes) e o Delimitador de Quadro Inicial (SFD), também chamado de Início do Frame (1 byte), os campos são usados para sincronização entre o dispositivos de envio e recepção. Estes primeiros oito bytes do quadro são usado para chamar a atenção dos nós de recepção. Essencialmente, o primeiro poucos bytes informam aos receptores para se prepararem para receber um novo quadro.
Campo Endereço MAC de Destino	Este campo de 6 bytes é o identificador do destinatário desejado. Como você , esse endereço é usado pela Camada 2 para auxiliar dispositivos no determinar se um quadro é endereçado a eles. O endereço no quadro é em comparação com o endereço MAC no dispositivo. Se houver uma correspondência, o aceita o quadro. Pode ser unicast, multicast ou broadcast endereço:
Campo Endereço MAC de Origem	Esse campo de 6 bytes identifica a NIC ou interface de origem do quadro.
Tipo/Comprimento	Este campo de 2 bytes identifica o protocolo da camada superior encapsulado em o quadro Ethernet. Os valores comuns são, em hexadecimal, 0x800 para IPv4, 0x86DD para IPv6 e 0x806 para ARP. **Nota**: Você também pode ver este campo referido como EtherType, Tipo ou Comprimento.
Campo Dados	Este campo (46 - 1500 bytes) contém os dados encapsulados de um camada superior, que é uma PDU de Camada 3 genérica, ou mais comumente, um IPv4 pacote. Todos os quadros devem ter pelo menos 64 bytes. Se um pequeno pacote for encapsulado, bits adicionais chamados pad são usados para aumentar o tamanho do quadro para este tamanho mínimo.
Campo Sequência de Verificação de Quadro	O campo FCS (Frame Check Sequence) (4 bytes) é usado para detectar erros em um quadro. Ele utiliza uma verificação de redundância cíclica (CRC). O dispositivo de envio inclui os resultados de um CRC no campo FCS do quadro. A O dispositivo receptor recebe o quadro e gera um CRC para procurar erros. Se o cálculo corresponder, significa que não houve erro. Cálculos que não coincidem são uma indicação de que os dados foram alterados; Portanto, o quadro é descartado. Uma alteração nos dados pode ser o resultado de um interrupção dos sinais elétricos que representam os bits.

Endereços MAC Ethernet

Os endereços IPv4 são representados usando o sistema de dez números base decimal e o sistema de números de base binária 2.

Endereços IPv6 e endereços Ethernet são representados usando o sistema hexadecimal base dezesseis números.

O sistema de numeração hexadecimal usa os números de 0 a 9 e as letras de A a F.

Um endereço MAC Ethernet consiste em um valor binário de 48 bits.
Hexadecimal é usado para identificar um endereço Ethernet porque um único dígito hexadecimal representa quatro bits binários.
Portanto, um endereço MAC Ethernet de 48 bits pode ser expresso usando apenas 12 valores hexadecimais.

Equivalentes decimais e binários de 0 a F Hexadecimal

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

Endereços MAC Ethernet

Equivalentes decimais, binários e hexadecimais selecionados

Decimal	Binário	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

Dado que 8 bits (um byte) é um agrupamento binário comum, os binários 00000000 a 11111111 podem ser representados em hexadecimal como o intervalo de 00 a FF.

Ao usar hexadecimal, os zeros à esquerda são sempre exibidos para concluir a representação de 8 bits. Por exemplo, na tabela, o valor binário 0000 1010 é mostrado em hexadecimal como 0A.

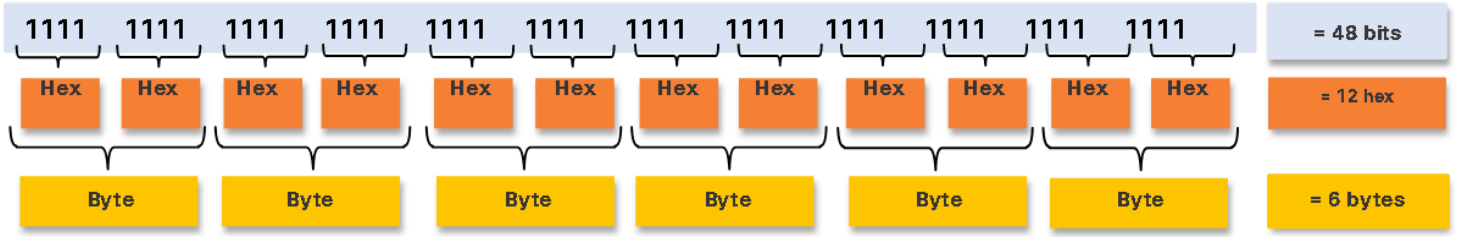
Números hexadecimais são frequentemente representados pelo valor precedido por 0x (por exemplo, 0x73) para distinguir entre valores decimal e hexadecimais na documentação.

O hexadecimal também pode ser representado por um subscript 16, ou o número hexadecimal seguido por um H (por exemplo, 73H).

Talvez seja necessário converter entre valores decimal e hexadecimais. Se tais conversões forem necessárias, converta o valor decimal ou hexadecimal em binário e, em seguida, converta o valor binário em decimal ou hexadecimal, conforme apropriado.

Endereços MAC Ethernet

Um endereço MAC Ethernet é um endereço de 48 bits expresso usando 12 dígitos hexadecimais.
Como um byte é igual a 8 bits, também podemos dizer que um endereço MAC tem 6 bytes de comprimento.
O endereço MAC são compostos de 48 bits total. Estes 48 bits podem ser divididos em doze agrupamentos de 4 bits, ou 12 dígitos hexadecimais.
Combinar dois dígitos hexadecimais juntos faz um byte, portanto os 48 bits também são equivalentes a 6 bytes.



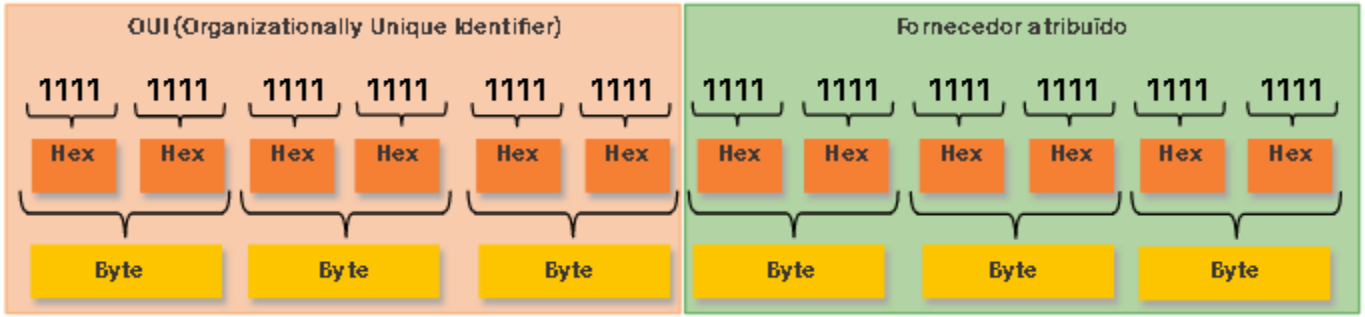
Todos os endereços MAC devem ser exclusivos do dispositivo Ethernet ou da interface Ethernet.
Para garantir isso, todos os fornecedores que vendem dispositivos Ethernet devem se registrar no IEEE para obter um código hexadecimal exclusivo de 6 (ou seja, 24 bits ou 3 bytes) chamado identificador exclusivo organizacionalmente (OUI).

Endereços MAC Ethernet

Quando um fornecedor atribui um endereço MAC a um dispositivo ou interface Ethernet, o fornecedor deve:

- Usar sua OUI atribuída como os primeiros 6 dígitos hexadecimais.
- Atribuir um valor exclusivo nos últimos 6 dígitos hexadecimais.

Os primeiros seis dígitos hexadecimais de um endereço MAC (os primeiros 6 dígitos hexadecimais ou 3 primeiros bytes) é o identificador exclusivo organizacional e os últimos seis dígitos hexadecimais são atribuídos pelo fornecedor.



É da responsabilidade do fornecedor garantir que nenhum de seus dispositivos seja atribuído o mesmo endereço MAC. No entanto, é possível que endereços MAC duplicados existam devido a erros cometidos durante a fabricação, erros cometidos em alguns métodos de implementação de máquinas virtuais ou modificações feitas usando uma das várias ferramentas de software. Em qualquer caso, será necessário modificar o endereço MAC com uma nova NIC ou fazer modificações via software.

Processamento de quadros

Às vezes, o endereço MAC é referido como endereço gravado de fábrica (BIA, burned-in-address) porque o endereço é codificado na memória somente leitura (ROM) na NIC.
Isso significa que o endereço é codificado no chip da ROM permanentemente.

Observação: Nos modernos sistemas operacionais de PC e NICs, é possível alterar o endereço MAC no software. Isso é útil para tentar obter acesso a uma rede que filtre com base no BIA. Consequentemente, a filtragem ou o controle de tráfego com base no endereço MAC não é mais tão seguro.

Quando o computador é inicializado, a NIC copia seu endereço MAC da ROM para a RAM. Quando um dispositivo está encaminhando uma mensagem para uma rede Ethernet, o cabeçalho Ethernet inclui:

- **Endereço MAC de origem -** Este é o endereço MAC da NIC do dispositivo de origem.
- **Endereço MAC de destino -** Este é o endereço MAC da NIC do dispositivo de destino.

Processamento de quadros

No processo de encaminhamento, quando uma NIC recebe um quadro Ethernet, examina o endereço MAC de destino para verificar se corresponde ao endereço MAC físico armazenado na RAM. Se não houver correspondência, o dispositivo descartará o quadro.
Caso haja, ele passará o quadro para cima nas camadas OSI, onde o processo de desencapsulamento ocorre.

Note: As NICs Ethernet também aceitarão quadros se o endereço MAC de destino for uma transmissão ou um grupo multicast do qual o host é membro.

Qualquer dispositivo que seja a origem ou o destino de um quadro Ethernet terá uma NIC Ethernet e, portanto, um endereço MAC.
Isso inclui estações de trabalho, servidores, impressoras, dispositivos móveis e roteadores.

Endereço MAC Unicast

Na Ethernet, são utilizados diferentes endereços MAC para comunicação unicast, broadcast e multicast da Camada 2.

Um endereço MAC de unicast é o endereço exclusivo usado quando um quadro é enviado de um único dispositivo de transmissão para um único dispositivo de destino.

No processamento de um quadro unicast, para que um pacote unicast seja enviado e recebido, um endereço IP de destino deve estar no cabeçalho do pacote IP.
Um endereço MAC de destino correspondente também deve estar presente no cabeçalho do quadro Ethernet. O endereço IP e o endereço MAC se combinam para entregar dados a um host de destino específico.

O processo que um host de origem usa para determinar o endereço MAC de destino associado a um endereço IPv4 é conhecido como ARP (Address Resolution Protocol). O processo que um host de origem usa para determinar o endereço MAC de destino associado a um endereço IPv6 é conhecido como ND (Neighbour Discovery Discovery).

Observação: O endereço MAC de origem deve ser sempre unicast.

Endereço MAC Broadcast

Um quadro de transmissão Ethernet é recebido e processado por cada dispositivo na LAN Ethernet.
Os recursos de uma transmissão Ethernet são os seguintes:

Possui um endereço MAC de destino de FF-FF-FF-FF-FF-FF em hexadecimal (48 números binários (sendo eles no valor de 0 ou 1)).

É inundada todas as portas de switch Ethernet, exceto a porta de entrada.

Ele não é encaminhado por um roteador.

Se os dados encapsulados forem um pacote de transmissão IPv4, isso significa que o pacote contém um endereço IPv4 de destino que possui todos os 1s na parte do host.
Essa numeração no endereço significa que todos os hosts naquela rede local (domínio de broadcast) receberão e processarão o pacote.
No processamento de um quadro de broadcast, o endereço MAC de destino e o endereço IP de destino são ambos endereços de broadcast.
O switch então encaminha o quadro para todas as suas interfaces, exceto aquela conectada a entrada. Quando um host de origem envia um pacote IPv4 broadcast a todos os dispositivos de sua rede.
O pacote IPv4 broadcast é encapsulado no quadro Ethernet, o endereço MAC de destino é o endereço MAC de broadcast FF-FF-FF-FF-FF-FF em hexadecimal (48 uns em binário). DHCP para IPv4 é um exemplo de um protocolo que usa endereços de broadcast Ethernet e IPv4. No entanto, nem todas os broadcasts Ethernet carregam um pacote IPv4. Por exemplo, as Solicitações ARP não usam IPv4, mas a mensagem ARP é enviada como um broadcast Ethernet.

Endereço MAC Multicast

Um quadro de multicast Ethernet é recebido e processado por um grupo de dispositivos que pertencem ao mesmo grupo de multicast. Os recursos multicast Ethernet são:

- Há um endereço MAC de destino 01-00-5E quando os dados encapsulados são um pacote multicast IPv4 e um endereço MAC de destino de 33-33 quando os dados encapsulados são um pacote multicast IPv6.
- Há outros endereços MAC de destino multicast reservados para quando os dados encapsulados não são IP, como STP (Spanning Tree Protocol) e LLDP (Link Layer Discovery Protocol).
- São inundadas todas as portas de switch Ethernet, exceto a porta de entrada, a menos que o switch esteja configurado para espionagem multicast.
- Ele não é encaminhado por um roteador, a menos que o roteador esteja configurado para rotear pacotes multicast.

Os dispositivos que pertencem a um grupo multicast recebem um endereço IP do grupo multicast. O intervalo de endereços multicast IPv4 é 224.0.0.0 a 239.255.255.255. O intervalo de endereços multicast IPv6 começa com ff00::/8. Como os endereços multicast representam um grupo de de hosts, eles só podem ser utilizados como destino de um pacote. A origem sempre será um endereço unicast.
Assim como nos endereços unicast e broadcast, o endereço IP multicast requer um endereço MAC multicast correspondente para entregar quadros em uma rede local. O endereço MAC multicast está associado e usa informações de endereçamento do endereço multicast IPv4 ou IPv6. Protocolos de roteamento e outros protocolos de rede usam endereçamento multicast. Aplicativos como software de vídeo e imagem também podem usar endereçamento multicast, embora aplicativos multicast não sejam tão comuns.

A tabela de endereços MAC

Se um switch apenas encaminhasse cada quadro recebido de todas as portas, sua rede ficaria tão congestionada que provavelmente chegaria a uma parada completa.

Um switch Ethernet da camada 2 usa endereços MAC da camada 2 para tomar decisões de encaminhamento. Desconhece completamente os dados (protocolo) que estão sendo transportados na parte de dados do quadro, como um pacote IPv4, uma mensagem ARP ou um pacote ND IPv6.
O switch toma suas decisões de encaminhamento com base apenas nos endereços MAC Ethernet da camada 2.

Um switch Ethernet examina sua tabela de endereços MAC para tomar uma decisão de encaminhamento para cada quadro.

Observação: A tabela de endereços MAC às vezes é chamada de tabela de memória de conteúdo endereçável (CAM).

A tabela de endereços MAC

O switch cria a tabela de endereços MAC dinamicamente examinando o endereço MAC de origem dos quadros recebidos em uma porta. O switch encaminha os quadros procurando uma correspondência entre o endereço MAC de destino no quadro e uma entrada na tabela de endereços MAC.
Todo quadro que entra em um switch é verificado quanto ao aprendizado de novas informações. Isso é feito examinando o endereço MAC de origem do quadro e o número da porta em que o quadro entrou.
Se o endereço MAC de origem não existe, é adicionado à tabela juntamente com o número da porta de entrada. Se o endereço MAC de origem existir, o switch atualizará o cronômetro de atualização para essa entrada na tabela. Por padrão, a maioria dos switches Ethernet mantém uma entrada na tabela por 5 minutos.

Nota: Se o endereço MAC de origem existir na tabela, mas em uma porta diferente, o switch tratará isso como uma nova entrada. A entrada é substituída usando o mesmo endereço MAC, mas com o número de porta mais atual.

Se o endereço MAC de destino for um endereço unicast, o switch procurará uma correspondência entre o endereço MAC de destino do quadro e uma entrada em sua tabela de endereços MAC. Se o endereço MAC de destino estiver na tabela, ele encaminhará o quadro pela porta especificada. Se o endereço MAC de destino não estiver na tabela, o switch encaminhará o quadro por todas as portas, exceto a de entrada. Isso é chamado de unicast desconhecido.

Nota: Se o endereço MAC de destino for um broadcast ou multicast, o quadro também inundará todas as portas, exceto a porta de entrada.

A tabela de endereços MAC

A medida que um switch recebe quadros de dispositivos diferentes, ele é capaz de preencher sua tabela de endereços MAC examinando o endereço MAC de origem de cada quadro. Quando a tabela de endereços MAC do switch contém o endereço MAC de origem, ele atualiza o temporizador para a entrada de endereço MAC a porta associada.
Quando a tabela de endereços MAC do switch contém o endereço MAC de destino, ele pode filtrar o quadro e encaminhar uma única porta.

Um switch pode ter vários endereços MAC associados a uma única porta.
Isso é comum quando o switch está conectado a outro switch.
O switch terá uma entrada separada na tabela de endereços MAC para cada quadro recebido com um endereço MAC de origem diferente.

Quando um dispositivo tem um endereço IP em uma rede remota, o quadro Ethernet não pode ser enviado diretamente para o dispositivo de destino.
Em vez disso, o quadro Ethernet é enviado ao endereço MAC do gateway padrão, o roteador.

Métodos de encaminhamento e velocidades de switches

Os switches usam suas tabelas de endereço MAC para determinar qual porta usar para encaminhar quadros. Com os switches Cisco, existem dois métodos de encaminhamento de quadros e há boas razões para usar um em vez do outro, dependendo da situação.

Os switches usam um dos seguintes métodos de encaminhamento para o switching de dados entre suas interfaces de rede:

- **Switching store-and-forward :** Método de encaminhamento de quadros recebe o quadro inteiro e calcula o CRC. O CRC usa uma fórmula matemática, baseada no número de bits (valores 1) no quadro, para determinar se o quadro recebido apresenta erro. Se o CRC é válido, o switch procura o endereço de destino, que determina a interface de saída. Em seguida, o quadro é encaminhado para fora da porta correta.
- **Switching cut-through:** Método de encaminhamento de quadros encaminha o quadro antes de ser totalmente recebido. Pelo menos o endereço de destino do quadro deve ser lido para que o quadro possa ser encaminhado.

Uma grande vantagem da troca de armazenamento e encaminhamento é que ele determina se um quadro tem erros antes de propagar o quadro. Quando um erro é detectado em um quadro, o switch o descarta. O descarte de quadros com erros reduz o consumo de largura de banda por dados corrompidos. O switch store-and-forward é necessário para a análise de qualidade de serviço (QoS) em redes convergentes onde a classificação de quadros para priorização de tráfego é necessária. Por exemplo, os fluxos de dados de voz sobre IP (VoIP) precisam ter prioridade sobre o tráfego de navegação na web.

Métodos de encaminhamento e velocidades de switches

No switching cut-through, o switch atua nos dados assim que eles são recebidos, mesmo que a transmissão não tenha sido concluída. O switch armazena em buffer apenas o quadro suficiente para ler o endereço MAC de destino, para que possa determinar para qual porta deve encaminhar os dados. O endereço MAC de destino está localizado nos primeiros 6 bytes do quadro após o preâmbulo. O switch consulta o endereço MAC de destino na tabela de switching, determina a porta da interface de saída e encaminha o quadro ao seu destino pela porta de switch designada. O switch não realiza nenhuma verificação de erros no quadro. Há duas formas de switching cut-through:

- **Comutação Fast-forward:** Oferece o menor nível de latência e encaminha imediatamente um pacote depois de ler o endereço de destino. Por começar o encaminhamento antes de receber todo o pacote, alguns pacotes podem ser retransmitidos com erros. Isso ocorre com pouca freqüência e a NIC de destino descarta o pacote com defeito após o recebimento. A latência é medida do primeiro bit recebido até o primeiro bit transmitido. É o método cut-through típico de switching.
- **Comutação Fragment-free:** O switch armazena os primeiros 64 bytes do quadro antes de encaminhar, pois a maioria dos erros e das colisões de rede ocorre durante os primeiros 64 bytes. Essa forma pode ser encarada como um compromisso entre o switching store-and-forward e o switching fast-forward. O switching fragment-free tenta melhorar o switching fast-forward executando uma pequena verificação de erros nos primeiros 64 bytes do quadro para garantir que não ocorra uma colisão antes de encaminhar o quadro. É um compromisso entre a alta latência e a alta integridade do switching store-and-forward e a baixa latência e a integridade reduzida do switching fast-forward.

Alguns switches são configurados para executar o switching cut-through por porta até que um limite de erro definido pelo usuário seja atingido e, depois, mudam automaticamente para store-and-forward. Quando a taxa de erros fica abaixo do limite, a porta retorna automaticamente para o switching cut-through.

Métodos de encaminhamento e velocidades de switches

Um switch Ethernet pode usar uma técnica de armazenamento de quadros em buffers antes de enviá-los. O buffer também pode ser usado quando a porta de destino está ocupada devido ao congestionamento. O switch armazena o quadro até que ele possa ser transmitido.

Existem dois métodos de buffer de memória:

Método	Descrição
Memória por porta	• Os quadros são armazenados em filas vinculadas a entradas e portas de saída. • Um quadro é transmitido para a porta de saída somente quando todos os quadros à frente na fila foram transmitidos com sucesso. • É possível para um único quadro atrasar a transmissão de todos os os quadros na memória devido a uma porta de destino ocupada. • Esse atraso ocorre mesmo que os outros quadros possam ser transmitidos para portas de destino abertas.
Memória compartilhada	• Deposita todos os quadros em um buffer de memória comum compartilhado por todos os switches e a quantidade de memória de buffer necessária por uma porta é alocados dinamicamente. • Os quadros no buffer são vinculados dinamicamente ao destino permitindo que um pacote seja recebido em uma porta e, em seguida, transmitida em outra porta, sem movê-la para uma fila diferente.

O buffer de memória compartilhada também resulta na capacidade de armazenar quadros maiores com potencialmente menos quadros descartados. Isso é importante com a comutação assimétrica, que permite taxas de dados diferentes em portas diferentes, como ao conectar um servidor a uma porta de switch de 10 Gbps e PCs a portas de 1 Gbps.

Métodos de encaminhamento e velocidades de switches

Duas das configurações mais básicas em um switch são as configurações de largura de banda e duplex para cada porta do switch individual.
É fundamental a correspondência dessas configurações na porta do switch e nos dispositivos conectados, como um computador ou outro switch.

Há dois tipos de configurações duplex usadas para comunicação em uma rede Ethernet:

- **Full-duplex -** As duas extremidades da conexão podem enviar e receber simultaneamente.
- **Half-duplex -** Somente uma extremidade da conexão pode enviar por vez.

A negociação automática é uma função opcional encontrada na maioria dos switches Ethernet e das placas de interface de rede (NICs).
Ele permite que dois dispositivos negociem automaticamente as melhores capacidades de velocidade e duplex. Full-duplex será escolhido se os dois dispositivos o tiverem para a largura de banda mais alta comum entre eles.

Observação: A maioria dos switches Cisco e NICs Ethernet é padronizada para negociação automática para velocidade e duplex. Portas Gigabit Ethernet só operam em full-duplex.

Métodos de encaminhamento e velocidades de switches

Duas das configurações mais básicas em um switch são as configurações de largura de banda e duplex para cada porta do switch individual.
É fundamental a correspondência dessas configurações na porta do switch e nos dispositivos conectados, como um computador ou outro switch.

Há dois tipos de configurações duplex usadas para comunicação em uma rede Ethernet:

- **Full-duplex -** As duas extremidades da conexão podem enviar e receber simultaneamente.
- **Half-duplex -** Somente uma extremidade da conexão pode enviar por vez.

A negociação automática é uma função opcional encontrada na maioria dos switches Ethernet e das placas de interface de rede (NICs).
Ele permite que dois dispositivos negociem automaticamente as melhores capacidades de velocidade e duplex. Full-duplex será escolhido se os dois dispositivos o tiverem para a largura de banda mais alta comum entre eles.

Observação: A maioria dos switches Cisco e NICs Ethernet é padronizada para negociação automática para velocidade e duplex. Portas Gigabit Ethernet só operam em full-duplex.

Métodos de encaminhamento e velocidades de switches

A incompatibilidade duplex é uma das causas mais comuns de problemas de desempenho nos links Ethernet 10/100 Mbps.
Ocorre quando uma porta no link opera em half-duplex, enquanto a outra porta opera em full-duplex.

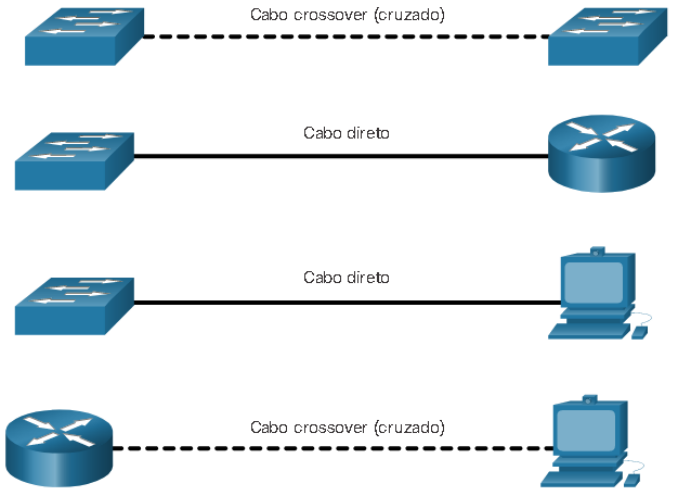
A incompatibilidade duplex ocorre quando uma ou ambas as portas em um link são redefinidas e o processo de negociação automática não resulta nos dois parceiros de link com a mesma configuração.
Também pode ocorrer quando os usuários reconfiguram um lado de um link e esquecem de reconfigurar o outro.
Os dois lados de um link devem estar ambos com a negociação automática ligada ou desligada.
A prática recomendada é configurar ambas as portas de switch Ethernet como full-duplex.

Métodos de encaminhamento e velocidades de switches

As conexões entre dispositivos exigiram uma vez o uso de um cabo cruzado ou direto.
O tipo de cabo necessário dependia do tipo de dispositivos de interconexão.

A maioria dos dispositivos de switch agora suporta o recurso de (Auto-MDIX) interface dependente automática. Quando ativado, o switch detecta automaticamente o tipo de cabo conectado à porta e configura as interfaces de acordo.
Com isso, você pode utilizar um cabo cruzado ou direto para conexões a uma porta 10/100/1000 de cobre no switch, seja qual for o tipo de dispositivo na outra extremidade da conexão.

O recurso auto-MDIX é ativado por padrão em switches que executam o Cisco IOS Release 12.2 (18) SE ou posterior. No entanto, o recurso pode ser desativado. Por esse motivo, você sempre deve usar o tipo de cabo correto e não confiar no recurso Auto-MDIX. O Auto-MDIX pode ser reativado usando o comando de configuração de mdix auto interface.



Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

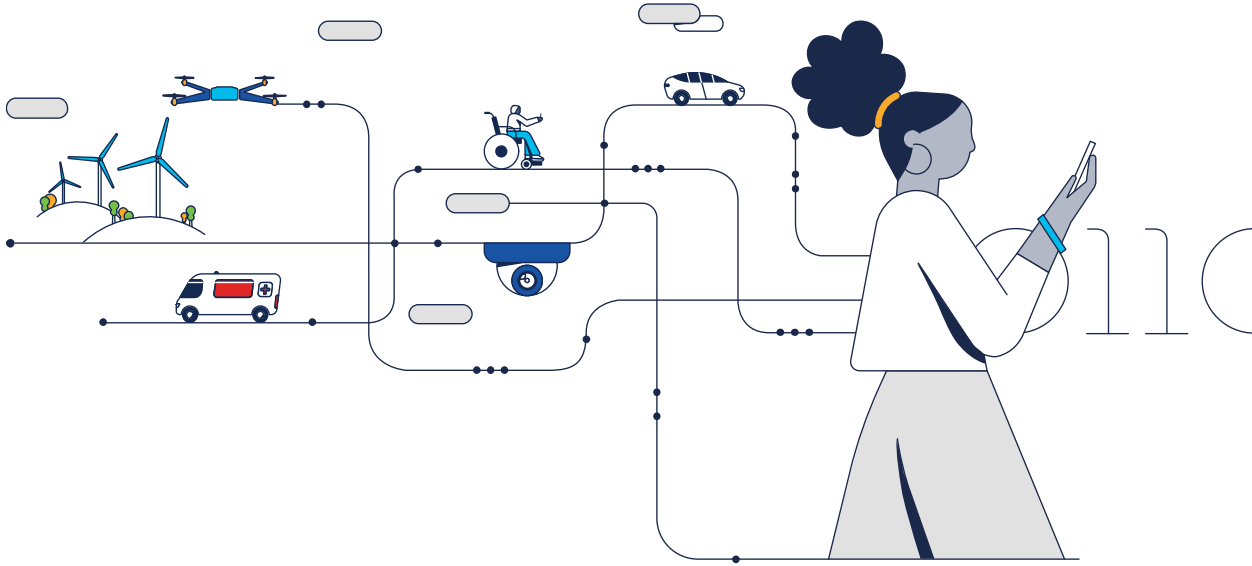
The bridge to possible

Nossos parceiros

TD SYNNEX

WISE
Women in Science
and Engineering
Inclusive Community

cisco
Networking
Academy



INTERNATIONAL
Girls in ICT Day
Brought to you by **WOMEN ROCK-IT**

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

CCNAv7 – ITN – Camada de Rede

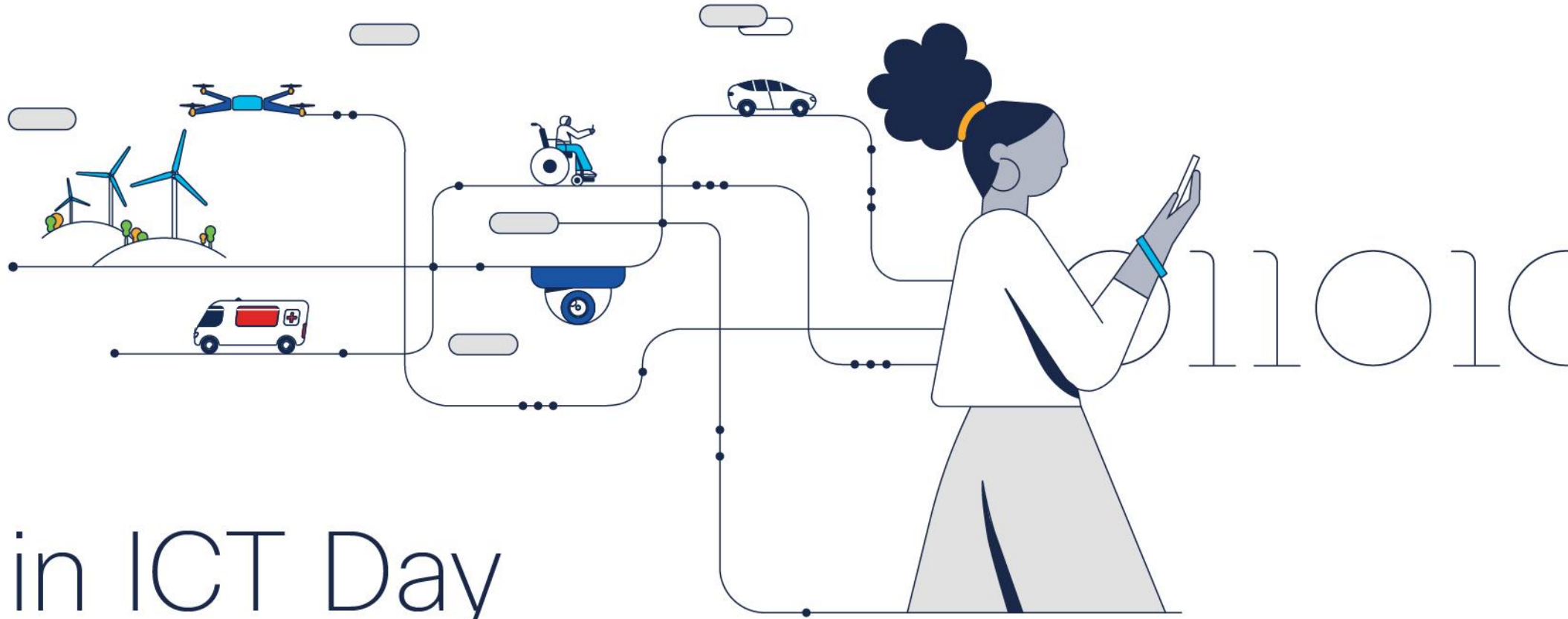
Módulo 8

Embaixadores do Programa 2020, 2021, 2022 & 2023:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

Networking
Academy



INTERNATIONAL

Girls in ICT Day

Brought to you by **WOMEN ROCK-IT**

Características de Camada de Rede

A camada de rede, ou Camada 3 do modelo OSI, fornece serviços que permitem aos dispositivos finais trocarem dados entre redes. Os protocolos IP versão 4 (IPv4) e IP versão 6 (IPv6) são os principais protocolos de comunicação de camada de rede. Outros protocolos de camada de rede incluem protocolos de roteamento, como OSPF (Open Shortest Path First) e protocolos de mensagens, como ICMP (Internet Control Message Protocol). Os protocolos de rede executam quatro operações básicas:

Endereçamento de dispositivos: Todos os dispositivos devem ser configurados com um endereço IP exclusivo para identificação na rede.

Encapsulamento: A camada de rede encapsula a unidade de dados de protocolo (PDU) da camada de transporte em um pacote, adicionando informações de cabeçalho IP, como os endereços IP dos hosts origem (emissor) e destino (receptor). O processo de encapsulamento é executado pela origem do pacote IP.

Roteamento: A camada de rede fornece serviços para direcionar os pacotes para um host de destino em outra rede. Para trafegar para outras redes, o pacote deve ser processado por um roteador. A função do roteador é escolher o melhor caminho e direcionar os pacotes para o host de destino em um processo conhecido como roteamento. Um pacote pode atravessar muitos roteadores antes de chegar ao host de destino. Cada roteador que um pacote atravessa para chegar ao host de destino é chamado de salto.

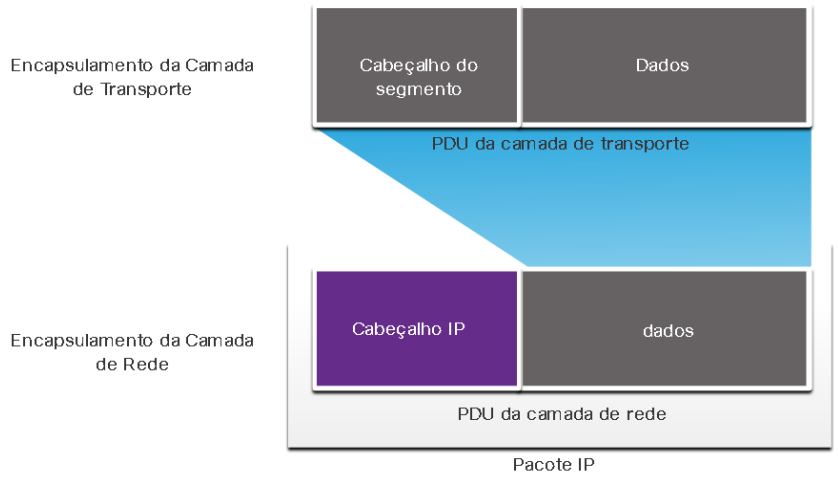
Desencapsulamento - Quando o pacote chega na camada de rede do host de destino, o host verifica o cabeçalho IP do pacote. Se o endereço IP de destino no cabeçalho corresponder ao seu próprio endereço IP, o cabeçalho IP será removido do pacote. Depois que o pacote é desencapsulado pela camada de rede, a PDU resultante da Camada 4 é transferida para o serviço apropriado na camada de transporte. O processo de desencapsulamento é executado pelo host de destino do pacote IP.

Os protocolos de comunicação da camada 3 especificam a estrutura de pacotes e o processamento usado para transportar os dados de um host para outro.

Características de Camada de Rede

O IP encapsula o segmento da camada de transporte (a camada 4 acima da camada de rede) ou outros dados adicionando um cabeçalho IP. O cabeçalho IP é adicionado na frente dos dados para criar o pacote IP que será entregue ao host de destino.

O processo de encapsulamento camada por camada possibilita o desenvolvimento e a expansão dos serviços nas diferentes camadas sem afetar outras camadas. Isso significa que os segmentos da camada de transporte podem ser imediatamente empacotados por
IPv4, IPv6 ou qualquer protocolo que venha a ser desenvolvido no futuro.



O cabeçalho IP é examinado por dispositivos de Camada 3 (ou seja, roteadores e switches de Camada 3) à medida que viaja através de uma rede até seu destino. É importante notar que as informações de endereçamento IP permanecem as mesmas desde o momento em que o pacote sai do host de origem até chegar ao host de destino, exceto quando traduzidas pelo dispositivo que executa a Tradução de Endereços de Rede (NAT) para IPv4.

Os roteadores implementam protocolos de roteamento para rotear pacotes entre redes. O roteamento realizado por esses dispositivos intermediários examina o endereçamento da camada de rede no cabeçalho do pacote. Em todos os casos, a parte de dados do pacote, ou seja, a PDU da camada de transporte encapsulada ou outros dados, permanece inalterada durante os processos da camada de rede.

Características de Camada de Rede

O IP foi desenvolvido como um protocolo com baixa sobrecarga. Ele fornece apenas as funções necessárias para enviar um pacote de uma origem a um destino por um sistema interconectado de redes. O protocolo não foi projetado para rastrear e gerenciar o fluxo de pacotes. Essas funções são realizadas por outros protocolos em outras camadas, principalmente TCP na Camada 4.

Características básicas da IP:

- **Sem conexão -** Não há conexão com o destino estabelecido antes do envio de pacotes de dados. Significa que nenhuma conexão ponto a ponto dedicada é criada pelo IP antes que os dados sejam enviados.
- **Melhor esforço -** o IP é inerentemente não confiável, porque a entrega de pacotes não é garantida. O IP não requer campos adicionais no cabeçalho para manter uma conexão estabelecida. Esse processo reduz bastante a sobrecarga do IP.
- **Independente da mídia -** A operação é independente do meio (ou seja, cobre, fibra ótica ou sem fio) que carrega os dados. A camada de enlace de dados OSI é responsável por pegar um pacote IP e prepará-lo para transmissão pelo meio de comunicação. Isso significa que a entrega de pacotes IP não se limita a nenhum meio específico.

Uma característica que a camada de rede considera nos meios físicos é o tamanho máximo da PDU que cada meio consegue transportar, chamada de unidade máxima de transmissão (maximum transmission unit - MTU). Parte das comunicações de controle entre a camada de enlace de dados e a camada de rede é a definição de um tamanho máximo para o pacote. A camada de enlace de dados passa o valor da MTU para a camada de rede. A camada de rede então determina o tamanho que os pacotes podem ter.

Em alguns casos, um dispositivo intermediário, geralmente um roteador, deve dividir um pacote IPv4 ao encaminhá-lo de um meio para outro com uma MTU menor. Esse processo é chamado fragmentação do pacote ou fragmentação. A fragmentação causa latência. Os pacotes IPv6 não podem ser fragmentados pelo roteador.

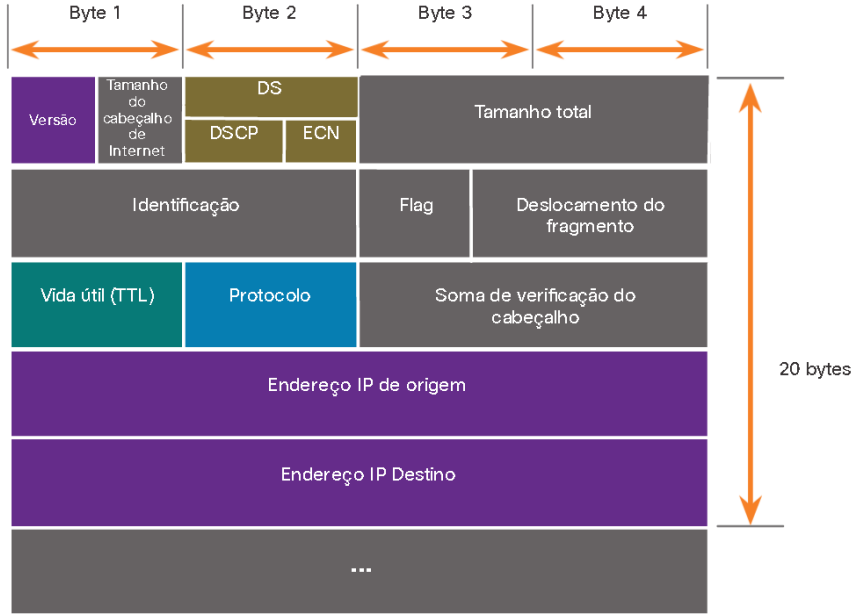
Pacote IPV4

O IPv4 é um dos principais protocolos da camada de rede. O cabeçalho do pacote IPv4 é usado para garantir que esse pacote seja entregue a cada salto até seu destino. Consiste em campos com informações que serão examinados pelo processo da Camada 3.

Os diagramas de cabeçalho de protocolo, são lidos da esquerda para a direita, de cima para baixo e disponibilizam uma visualização para consultar seus campos. Os dois mais referenciados são os endereços IP de origem e destino.

Normalmente, esses endereços não mudam durante a viagem da origem ao destino.

- **Versão:** Valor binário de 4 bits definido como 0100, identifica que este é um pacote IP versão 4.
- **Serviços diferenciados ou DiffServ (DS):** Campo de 8 bits, determina a prioridade de cada pacote. Os seis bits mais significativos do campo DiffServ são os bits do ponto de código de serviços diferenciados (DSCP) e os dois últimos são os bits de notificação de congestionamento explícita (ECN).
- **Checksum de cabeçalho:** Usado para detectar corrupção no cabeçalho IPv4.
- **Tempo de vida (TTL):** Valor binário de 8 bits, usado para limitar a vida útil de um pacote. O dispositivo de origem do pacote IPv4 define o valor TTL inicial. É diminuído em um cada vez que o pacote é processado por um roteador. Quando decrementado até zero, o roteador descartará o pacote e enviará uma mensagem ICMP de tempo excedido para o endereço IP de origem. Como o roteador decrementa o TTL de cada pacote, o roteador também deve recalcular a soma de verificação do cabeçalho.
- **Protocolo:** Identifica o protocolo de próximo nível. O valor binário de 8 bits indica o tipo de carga de dados que o pacote está carregando, o que permite que a camada de rede transfira os dados para o protocolo apropriado das camadas superiores. Valores comuns incluem ICMP (1), TCP (6) e UDP (17).
- **Endereço IP Origem :** Valor binário de 32 bits que representa o endereço IP origem do pacote. É sempre um endereço unicast.
- **Endereço IP Destino:** Valor binário de 32 bits que representa o endereço IP destino do pacote. Pode ser um endereço unicast, multicast, ou broadcast.



Os campos **Tamanho do Cabeçalho de Internet (IHL)**, **Tamanho Total** e **Soma de Verificação do Cabeçalho** servem para identificar e validar o pacote. O pacote IPv4 usa especificamente os campos **Identificação**, **Flags** e **Deslocamento do Fragmento** para organizar pacotes fragmentados. Um roteador precisa fragmentar um pacote IPv4 ao encaminhá-lo de um meio para outro com uma MTU menor. Os campos **Opções** e **Preenchimento** raramente são usados.

Pacote IPV6

O IPv4 ainda está em uso hoje. E, eventualmente será substituído pelo IPv6, devido a três grandes problemas:

•**Esgotamento do endereço IPv4:** Possui um número limitado de endereços públicos exclusivos disponíveis. Embora haja aproximadamente 4 bilhões de endereços IPv4, o número crescente de novos dispositivos habilitados para IP, conexões sempre ativas e o potencial de crescimento de regiões menos desenvolvidas têm aumentado a necessidade de mais endereços.

•**Falta de conectividade ponto a ponto:** Network Address Translation (NAT) é uma tecnologia comumente implementada em redes IPv4. É uma forma de vários dispositivos compartilharem um único endereço IPv4 público. No entanto, como o endereço IPv4 público é compartilhado, o endereço IPv4 de um host de rede interna fica oculto. Isso pode ser problemático para tecnologias que exigem conectividade de ponta a ponta.

•**Maior complexidade da rede:** Embora o NAT tenha ampliado a vida útil do IPv4, ele só se destinava a ser um mecanismo de transição para o IPv6. O NAT em suas várias implementações cria complexidade adicional na rede, criando latência e dificultando a solução de problemas.

No início da década de 90, a Internet Engineering Task Force (IETF) com uma preocupação crescente com os problemas do IPv4, começou a procurar um substituto, o que levou ao desenvolvimento do IP versão 6 (IPv6). Superando as limitações do IPv4, com recursos que atendem às demandas atuais e previsíveis de rede. As melhorias que o IPv6 fornece incluem o seguinte:

- **Espaço de endereço aumentado:** Endereçamento hierárquico de 128 bits, em oposição ao IPv4 com 32 bits.
- **Manipulação aprimorada de pacotes:** O cabeçalho IPv6 foi simplificado com menos campos.
- **Elimina a necessidade de NAT:** Maior numero de endereços IPv6 públicos, eliminando o uso de NAT.

O espaço de 32 bits de um endereço IPv4 fornece aproximadamente 4.294.967.296 endereços exclusivos. O espaço de endereço IPv6 fornece 340.282.366.920.938.463.463.374.607.431.768.211.456, ou 340 undecilhões de endereços.

Pacote IPV6

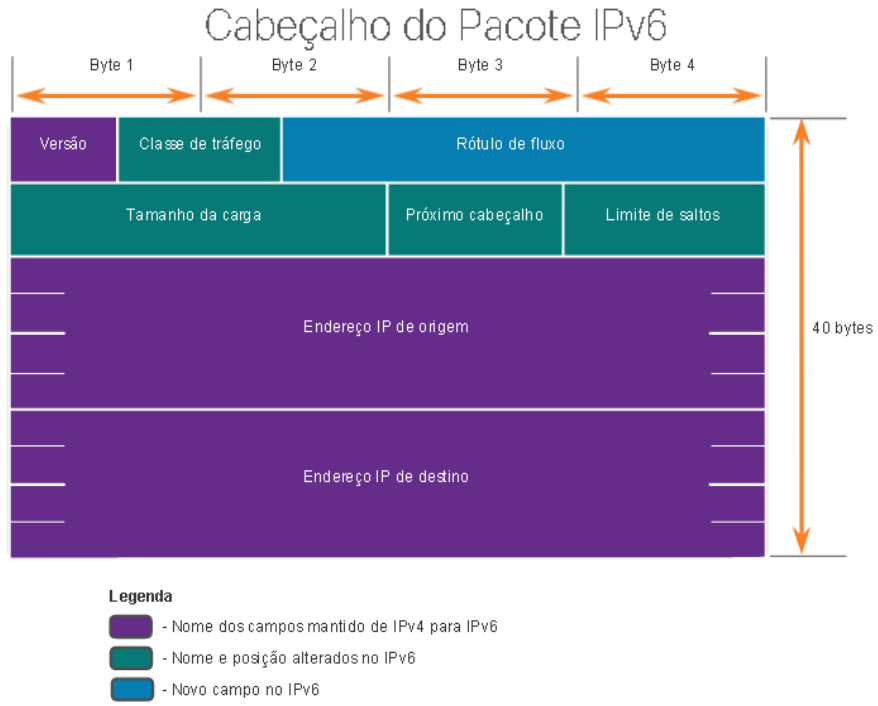
Uma das principais melhorias de design do IPv6 em relação ao IPv4 é o cabeçalho IPv6 simplificado que permite um processamento mais eficiente de cabeçalhos IPv6.

O cabeçalho IPv4 consiste em um cabeçalho de comprimento variável de 20 octetos (até 60 bytes se o campo Opções for usado) e 12 campos de cabeçalho básicos, sem incluir o campo Opções e o campo Preenchimento.

Os campos que mantiveram o mesmo nome no cabeçalho IPv6 são: **versão**, **endereço de origem** e **endereço de destino**. Os campos que alteraram nomes e posição são: **tipo de serviço**, **duração total**, **tempo de vida** e **protocolo**. Os campos que não foram mantidos no IPv6 são: **DIH**, **identificação**, **sinalizadores**, **deslocamento de fragmento**, **soma de verificação de cabeçalho**, **opções** e **preenchimento**.

O cabeçalho simplificado do IPv6 consiste em um cabeçalho de comprimento fixo de 40 octetos (em grande parte devido ao comprimento dos endereços IPv6 de origem e de destino).

Os campos que alteraram nomes e posição no IPv6 são: **classe de tráfego**, **comprimento da carga útil**, **próximo cabeçalho** e **limite de salto**. O campo que é NOVO para IPv6 é **rótulo de fluxo**.



Networking Academy

INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Pacote IPV6

Os campos no cabeçalho do pacote IPv6 incluem o seguinte:

- **Versão:** Valor binário de 4 bits definido como 0110 que identifica isso como um pacote IP versão 6.
- **Classe de tráfego:** Campo de 8 bits, equivalente ao campo DSv (Serviços diferenciados de IPv4).
- **Etiqueta de fluxo:** Campo de 20 bits sugere que todos os pacotes com a mesma etiqueta de fluxo recebam o mesmo tipo de manipulação pelos roteadores.
- **Comprimento da carga útil:** Campo de 16 bits, indica o comprimento da parte dos dados ou da carga útil do pacote IPv6. Isso não inclui o comprimento do cabeçalho IPv6, que é um cabeçalho fixo de 40 bytes.
- **Próximo cabeçalho:** Campo de 8 bits, equivalente ao campo Protocolo IPv4.
- **Limite de salto:** Campo de 8 bits, substitui o campo TTL IPv4. Esse valor é subtraído de um por cada roteador que encaminha o pacote. Quando o contador atinge 0, o pacote é descartado e uma mensagem de ICMPv6 com tempo excedido é encaminhada para o host de envio. Isso indica que o pacote não atingiu seu destino porque o limite de salto foi excedido. Ao contrário do IPv4, o IPv6 não inclui uma soma de verificação do cabeçalho IPv6, porque esta função é executada nas camadas inferior e superior. Isso significa que a soma de verificação não precisa ser recalculada por cada roteador quando diminui o campo Limite de Hop, o que também melhora o desempenho da rede.
- **Endereço IPv6 de origem:** Campo de 128 bits identifica o endereço IPv6 do host de envio.
- **Endereço IPv6 de destino:** Campo de 128 bits identifica o endereço IPv6 do host de recebimento.

Um pacote IPv6 pode conter também **cabeçalhos de extensão (EH)**, que fornecem informações de camada de rede. Opcionais, os cabeçalhos de extensão ficam posicionados entre o cabeçalho IPv6 e a carga. Eles são usados para fragmentação, segurança, suporte à mobilidade e muito mais.

Ao contrário de IPv4, os roteadores não fragmentam os pacotes IPv6 roteados.

Decisão de Encaminhamento do host

Com IPv4 e IPv6, os pacotes são sempre criados no host de origem. O host de origem deve ser capaz de direcionar o pacote para o host de destino. Para fazer isso, os dispositivos finais do host criam sua própria tabela de roteamento.
Outra função da camada de rede é direcionar pacotes entre hosts. Um host pode enviar um pacote para:

- **Si mesmo:** Um host pode executar ping em si mesmo enviando um pacote para o endereço IPv4 127.0.0.1 ou para o endereço IPv6 ::1, que é referido como a interface de loopback. O ping na interface de loopback testa a pilha de protocolos do TCP/IP no host.
- **Host local:** Host de destino que está na mesma rede local que o host de envio. Os hosts de origem e destino compartilham o mesmo endereço de rede.
- **Host remoto:** Host de destino em uma rede remota. Os hosts não compartilham o mesmo endereço de rede.

Se um pacote é destinado a um host local ou remoto é determinado pelo dispositivo final de origem, que verifica se o endereço IP de destino está na mesma rede em que o dispositivo de origem ou não. O método de determinação varia de acordo com a versão IP:

- **Em IPv4:** O dispositivo de origem usa sua máscara de sub-rede juntamente com seu endereço IPv4 e o endereço IPv4 de destino para fazer essa determinação.
- **Em IPv6:** O roteador local anuncia o endereço de rede local (prefixo) para todos os dispositivos na rede.

Os dispositivos que estão além do segmento de rede local são conhecidos como hosts remotos. Quando um dispositivo de origem envia um pacote a um dispositivo de destino remoto, é necessária a ajuda de roteadores e do roteamento.
O roteamento é o processo de identificação do melhor caminho até um destino. O roteador conectado ao segmento de rede local é conhecido como gateway padrão (default gateway).

Introdução ao Roteamento

Quando um host envia um pacote para outro host, ele consulta sua tabela de roteamento para determinar para onde enviar o pacote. Se o host de destino estiver em uma rede remota, o pacote será encaminhado para o gateway padrão, que geralmente é o roteador local. O roteador, desencapsula o cabeçalho Ethernet da camada 2 e o trailer, examina o endereço IP de destino do pacote e pesquisa sua tabela de roteamento para determinar para onde encaminhar o pacote. A tabela de roteamento contém uma lista de todos os endereços de rede conhecidos (prefixos) e para onde encaminhar o pacote. Essas entradas são conhecidas como entradas de rota ou rotas. O roteador encapsula o pacote em um novo cabeçalho e trailer Ethernet e encaminhará o pacote para o próximo salto usando a melhor (mais longa) entrada de rota correspondente.

A tabela de roteamento armazena três tipos de entradas de rota:
Redes conectadas diretamente: São interfaces ativas do roteador. Os roteadores adicionam uma rota diretamente conectada quando uma interface está configurada com um endereço IP e está ativada. Cada interface do roteador está conectada a um segmento de rede diferente.
Redes remotas: São conectadas a outros roteadores. Os roteadores aprendem sobre redes remotas sendo explicitamente configurados por um administrador ou trocando informações de rota usando um protocolo de roteamento dinâmico.
Rota padrão: Uma entrada de rota padrão é um gateway de último recurso. A rota padrão é usada quando não há correspondência melhor na tabela de roteamento IP.

Um roteador pode aprender sobre redes remotas de duas maneiras:

Manualmente: As redes remotas são inseridas manualmente na tabela de rotas usando rotas estáticas.
Dinamicamente: As rotas remotas são aprendidas automaticamente usando um protocolo de roteamento dinâmico.

Introdução ao Roteamento

Rotas estáticas são entradas de rota configuradas manualmente. A rota estática inclui o endereço de rede remota e o endereço IP do roteador de salto seguinte. Se houver uma alteração na topologia da rede, a rota estática não será atualizada automaticamente e deverá ser reconfigurada manualmente, pois ela não se ajusta automaticamente para alterações de topologia. O roteamento estático tem as seguintes características:

- Uma rota estática deve ser configurada manualmente.
- Precisa ser reconfigurada se houver uma alteração na topologia ou a rota estática não for mais viável.
- Uma rota estática é apropriada para uma rede pequena e quando há poucos ou nenhum vínculo redundante.
- Comumente usada com um protocolo de roteamento dinâmico para configurar uma rota padrão.

Um **protocolo de roteamento dinâmico** permite que os roteadores aprendam automaticamente sobre redes remotas, incluindo uma rota padrão, de outros roteadores. Compensam qualquer alteração de topologia sem envolver o administrador da rede. Se houver uma alteração os roteadores compartilham essas informações usando o protocolo de roteamento dinâmico e atualizam automaticamente suas tabelas de roteamento. Os protocolos de roteamento dinâmico incluem OSPF e Enhanced Interior Gateway Routing Protocol (EIGRP). A configuração básica requer que o administrador de rede habilite as redes conectadas diretamente dentro do protocolo de roteamento dinâmico. O protocolo de roteamento dinâmico fará automaticamente o seguinte:

- Descobrir redes remotas;
- Manter as informações de roteamento atualizadas;
- Escolher o melhor caminho para as redes de destino;
- Encontrar um novo melhor caminho se o caminho atual não estiver mais disponível.

Quando um roteador é configurado manualmente com uma rota estática ou aprende sobre uma rede remota dinamicamente usando um protocolo de roteamento dinâmico, o endereço de rede remota e o endereço de próximo salto são inseridos na tabela de roteamento IP.

Introdução ao Roteamento

O comando de modo EXEC privilegiado; **show ip route** é usado para exibir a tabela de roteamento IPv4 em um roteador Cisco IOS. No início de cada entrada de tabela de roteamento é um código que é usado para identificar o tipo de rota ou como a rota foi aprendida. As fontes comuns de rotas (códigos) incluem:

- L - Endereço IP da interface local diretamente conectado
- C - Rede diretamente conectada
- S - A rota estática foi configurada manualmente por um administrador
- O - OSPF
- D - EIGRP

Uma rota diretamente conectada é criada automaticamente quando uma interface do roteador é configurada com informações de endereço IP e é ativada.

Uma rota padrão tem um endereço de rede de todos os zeros. Uma entrada de rota estática na tabela de roteamento começa com um código de **S*.**

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

Cisco Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

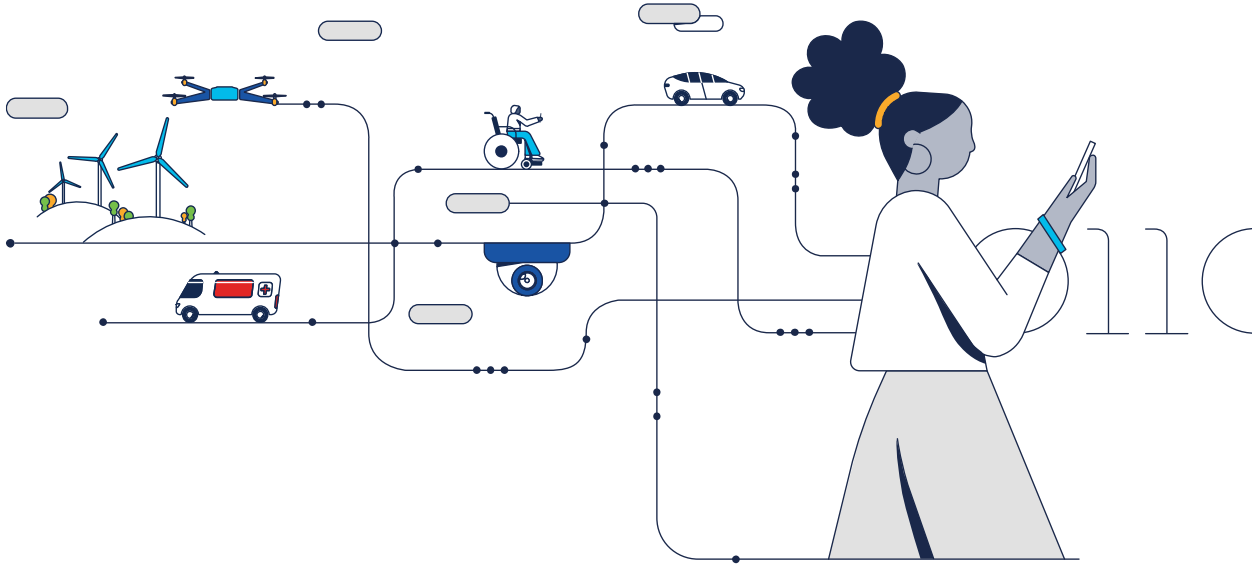
The bridge to possible

Nossos parceiros

TD SYNNEX

WISE
Women in Science
and Engineering
Inclusive Community

cisco
Networking
Academy



INTERNATIONAL
Girls in ICT Day
Brought to you by **WOMEN ROCK-IT**

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

CCNAv7 – ITN – Resolução de endereços

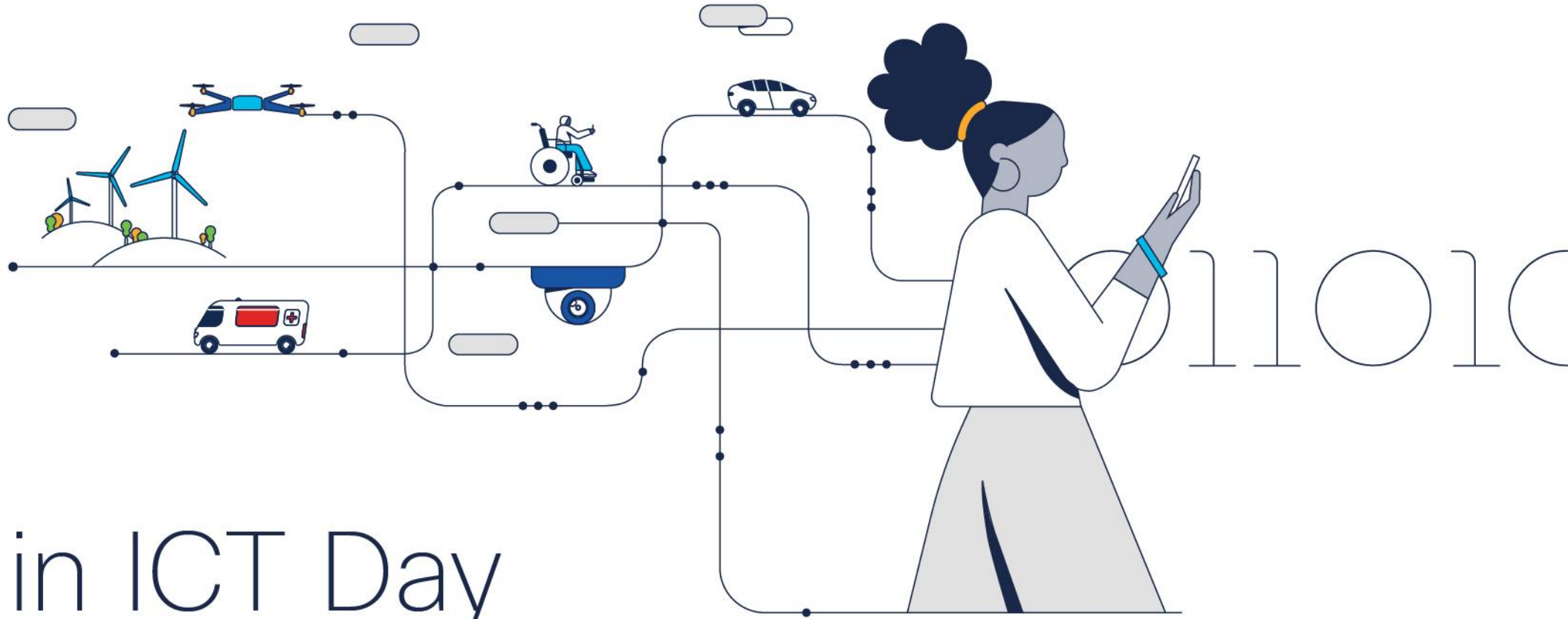
Módulo 9

Embaixadores do Programa 2020, 2021, 2022 & 2023:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

Networking
Academy



INTERNATIONAL

Girls in ICT Day

Brought to you by **WOMEN ROCK-IT**

MAC E IP

Destino na Mesma Rede

A resolução de endereços é usada quando um host ao enviar uma mensagem sabe apenas o endereço IP do dispositivo e necessita saber o endereço de camada 2, MAC desse mesmo dispositivo.

Dois endereços principais são atribuídos a um dispositivo em uma LAN Ethernet;

- **Endereço físico (o endereço MAC)** - Usado para comunicações de NIC para NIC na mesma rede Ethernet.
- **Endereço lógico (o endereço IP)** - Usado para enviar o pacote do dispositivo de origem para o dispositivo de destino. O endereço IP de destino pode estar na mesma rede IP da fonte ou em uma rede remota.

Endereços físicos são usados para entregar o quadro de enlace de dados com o pacote IP encapsulado de uma NIC para outra NIC que está na mesma rede. Se o endereço IP de destino estiver na mesma rede, o endereço MAC de destino será o do dispositivo de destino.

MAC E IP

Destino na Rede Remota

Quando o endereço IP de destino (IPv4 ou IPv6) estiver em uma rede remota, o endereço MAC de destino será o endereço do gateway padrão do host (ou seja, a interface do roteador).

Os roteadores examinam o endereço IPv4 destino para determinar o melhor caminho para encaminhar o pacote IPv4. Quando o roteador recebe o quadro Ethernet, ele desencapsula as informações da Camada 2. Usando o endereço IPv4 de destino, ele determina o dispositivo do próximo salto e, em seguida, encapsula o pacote IPv4 em um novo quadro de link de dados para a interface de saída.

Ao longo de cada link em um caminho, um pacote IP é encapsulado em um quadro. O quadro é específico da tecnologia de link de dados associada a esse link, como Ethernet. Se o dispositivo de salto a seguir para o destino final, o endereço MAC de destino será o NIC Ethernet do dispositivo.

Como os endereços IP dos pacotes IP em um fluxo de dados são associados aos endereços MAC em cada link ao longo do caminho até o destino? Para pacotes IPv4, isso é feito através de um processo chamado **ARP** (**Address Resolution Protocol**). Para pacotes IPv6, o processo é **ICMPv6** Descoberta de vizinhos (**ND**).

ARP

O Protocolo de Resolução de Endereços ou ARP é usado em redes que usam o protocolo IPv4, para mapear endereços IPv4 para endereços MAC.

Cada dispositivo IP em uma rede Ethernet tem um endereço MAC Ethernet exclusivo. Quando um dispositivo envia um quadro Ethernet Layer 2, ele contém estes dois endereços:
Endereço MAC de destino e **Endereço MAC de origem.**

Um dispositivo utiliza o protocolo ARP (Address Resolution Protocol) para determinar o endereço MAC de destino de um dispositivo local quando conhece o endereço IPv4.

O ARP fornece duas funções básicas:

- Resolução de endereços IPv4 em endereços MAC
- Mantendo uma tabela de mapeamentos de endereços IPv4 para MAC

Função ARP

Quando um pacote é enviado à camada de enlace de dados para ser encapsulado em um quadro Ethernet, o dispositivo emissor pesquisará em sua tabela ARP ou cache ARP, armazenada temporariamente na memória RAM, o endereço IPv4 destino correspondente a um endereço MAC.

- Se o endereço IPv4 destino do pacote estiver na mesma rede que o endereço IPv4 origem, o dispositivo pesquisará o endereço IPv4 destino na tabela ARP.
- Se o endereço IPv4 destino do pacote estiver em uma rede diferente do endereço IPv4 origem, o dispositivo pesquisará o endereço IPv4 do gateway padrão na tabela ARP.

Nos dois casos, a pesquisa é por um endereço IPv4 e um endereço MAC correspondente para o dispositivo.

A tabela ARP salva (armazena em cache) temporariamente o mapeamento dos dispositivos da LAN.

Se o dispositivo localizar o endereço IPv4, seu endereço MAC correspondente será usado como endereço MAC de destino no quadro. Se nenhuma entrada for encontrada, o dispositivo enviará uma **requisição ARP.**

Solicitação ARP

A requisição ARP é encapsulada em um quadro Ethernet, sem cabeçalho IPv4, usando as seguintes informações de cabeçalho:

- **Endereço MAC de destino** - Um endereço de broadcast FF-FF-FF-FF-FF-FF, exigindo que todas as NICs Ethernet na LAN aceitem e processem a solicitação ARP.
- **Endereço MAC de origem** - Endereço MAC do remetente da solicitação ARP.
- **Tipo** - As mensagens ARP têm um campo de tipo 0x806. Ele informa à NIC de recebimento que a parte de dados do quadro precisa ser transferida para o processo ARP.

As solicitações de ARP são broadcast, sendo inundadas em todas as portas **pelo switch**, exceto a porta de recebimento. Todas as NICs Ethernet no processo de LAN transmite e devem entregar a solicitação ARP ao seu sistema operacional para processamento. Cada dispositivo deve processar a requisição ARP para ver se o endereço IPv4 destino corresponde ao seu. **Um roteador** não encaminhará broadcasts pelas outras interfaces.

Somente um dispositivo na LAN terá um endereço IPv4 correspondente ao endereço IPv4 na requisição ARP. Nenhum outro dispositivo responderá.

Resposta ARP

Somente o dispositivo com o endereço IPv4 correspondente à solicitação ARP enviará uma **resposta ARP**, encapsulada em um quadro Ethernet usando as seguintes informações de cabeçalho:

- **Endereço MAC de destino** - Endereço MAC do remetente da solicitação ARP.
- **Endereço MAC de origem** - Endereço MAC do remetente da resposta ARP.
- **Tipo** - Campo de tipo 0x806, que informa à NIC que a parte de dados precisa ser transferida para o processo ARP.

Apenas o dispositivo que enviou uma requisição ARP receberá a resposta ARP unicast e adicionará o endereço IPv4 e o endereço MAC correspondentes à sua tabela ARP.

Se nenhum dispositivo responder à requisição ARP, o pacote será descartado.

As entradas na tabela ARP têm carimbo de data/hora (timestamp), que são removidas, caso o dispositivo não receba um quadro de um dispositivo específico antes que o carimbo expire.

Também podemos inserir e remover entradas de mapa estáticas em uma tabela ARP, que não expiram com o tempo.

O IPv6 usa mensagens de requisição e de anúncio de vizinho, conhecido como ND ou NDP, **ICMPv6 Neighbor Discovery Protocol**.

WireShark

APP Link: https://www.wireshark.org/download.html

Cisco Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

Função ARP nas comunicações remotas

Sempre que um dispositivo de origem tiver um pacote com um endereço IPv4 em outra rede, ele encapsulará esse pacote em um quadro usando o endereço MAC de destino do roteador, seu **gateway padrão.**

O endereço IPv4 do gateway padrão é armazenado na configuração IPv4 dos hosts.

Quando um host cria um pacote para um destino, ele compara o endereço IPv4 destino e seu próprio endereço IPv4 para determinar se os dois endereços IPv4 estão localizados na mesma rede de Camada 3.

Se o host de destino não estiver na mesma rede, a origem usará a tabela ARP para obter uma entrada com o endereço IPv4 do gateway padrão. Se não houver uma entrada, ela usará o processo de ARP para determinar um endereço MAC do gateway padrão.

Tabela ARP

Em cada dispositivo, um temporizador da cache ARP remove entradas ARP que não tenham sido usadas durante um determinado período. Os horários diferem dependendo do sistema operacional do dispositivo. Por exemplo, os sistemas operacionais Windows mais recentes armazenam entradas da tabela ARP entre 15 e 45 segundos, conforme ilustrado na figura.

Os comandos também podem ser usados para remover manualmente algumas ou todas as entradas na tabela ARP. Após a remoção de uma entrada, o processo de envio de uma requisição ARP e de recebimento de uma resposta ARP deve ocorrer novamente para inserir o mapa na tabela ARP.

Em um roteador Cisco, use o comando **show ip arp** para exibir a tabela ARP.

Em um PC com Windows 10, use **arp –a** para exibir a tabela ARP.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1           -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225        -   a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226        1   a03d.6fe1.9d91  ARPA   GigabitEthernet0/0/1
R1#
```

Problemas de ARP

As transmissões de ARP podem inundar a mídia local: Como um quadro broadcast, uma requisição ARP é recebida e processada por todos os dispositivos na rede local. Em uma rede corporativa típica, esses broadcasts provavelmente teriam impacto mínimo no desempenho da rede. No entanto, se um grande número de dispositivos precisasse ser ligado e todos começassem a acessar serviços de rede ao mesmo tempo, poderia haver alguma redução no desempenho por um curto período. Depois que os dispositivos enviarem os broadcasts ARP iniciais e tiverem reconhecido os endereços MAC necessários, qualquer impacto na rede será minimizado.

Em alguns casos, o uso do ARP pode levar a um risco potencial à segurança. Um ator de ameaça pode usar **falsificação ARP** para realizar um ataque de envenenamento por ARP. Esta é uma técnica usada por um ator de ameaça para responder a uma solicitação ARP de um endereço IPv4 que pertence a outro dispositivo, como o gateway padrão. O agente da ameaça envia uma resposta ARP com seu próprio endereço MAC. O destinatário da resposta ARP adicionará o endereço MAC errado à sua tabela ARP e enviará esses pacotes ao agente de ameaça. Switches de nível corporativo incluem técnicas de mitigação conhecidas como inspeção dinâmica ARP (DAI). A DAI não faz parte do escopo deste curso.

Descoberta de vizinhos de IPv6

O protocolo ND fornece serviços de resolução de endereço, descoberta de roteador e redirecionamento para IPv6 usando ICMPv6. O ICMPv6 ND usa cinco mensagens ICMPv6 para executar estes serviços:

- Mensagens de solicitação de vizinho;
- Mensagens de anúncio vizinho;
- Mensagens de solicitação de roteador;
- Mensagens de anúncio do roteador;
- Redirecionar mensagem.

As mensagens de solicitação de vizinho e anúncio de vizinho são usadas para mensagens de dispositivo a dispositivo, como resolução de endereço (semelhante ao ARP para IPv4). Os dispositivos incluem computadores e roteadores.

As mensagens de solicitação de roteador e anúncio de roteador são para mensagens entre dispositivos e roteadores. Normalmente, a descoberta de roteador é usada para alocação de endereços dinâmicos e autoconfiguração de endereço sem estado (SLAAC).

Observação: A quinta mensagem ICMPv6 ND é uma mensagem de redirecionamento que é usada para melhor seleção do próximo salto e está além do escopo deste curso.

IPv6 ND é definido no IETF RFC 4861.

IPv6 – Resolução de Endereços

Assim como ARP para IPv4, os dispositivos IPv6 usam IPv6 ND para determinar o endereço MAC de um dispositivo que tem um endereço IPv6 conhecido.

As mensagens **Solicitação de vizinho ICMPv6** e **Anúncio de vizinho** são usadas para a resolução de endereço MAC. Isso é semelhante às Solicitações ARP e Respostas ARP usadas pelo ARP para IPv4.

As mensagens de **solicitação de vizinhos** ICMPv6 são enviadas usando endereços de multicast Ethernet e IPv6 especiais. Isso permite que a NIC Ethernet do dispositivo receptor determine se a mensagem de solicitação de vizinho é para si mesmo sem ter que enviá-la para o sistema operacional para processamento.

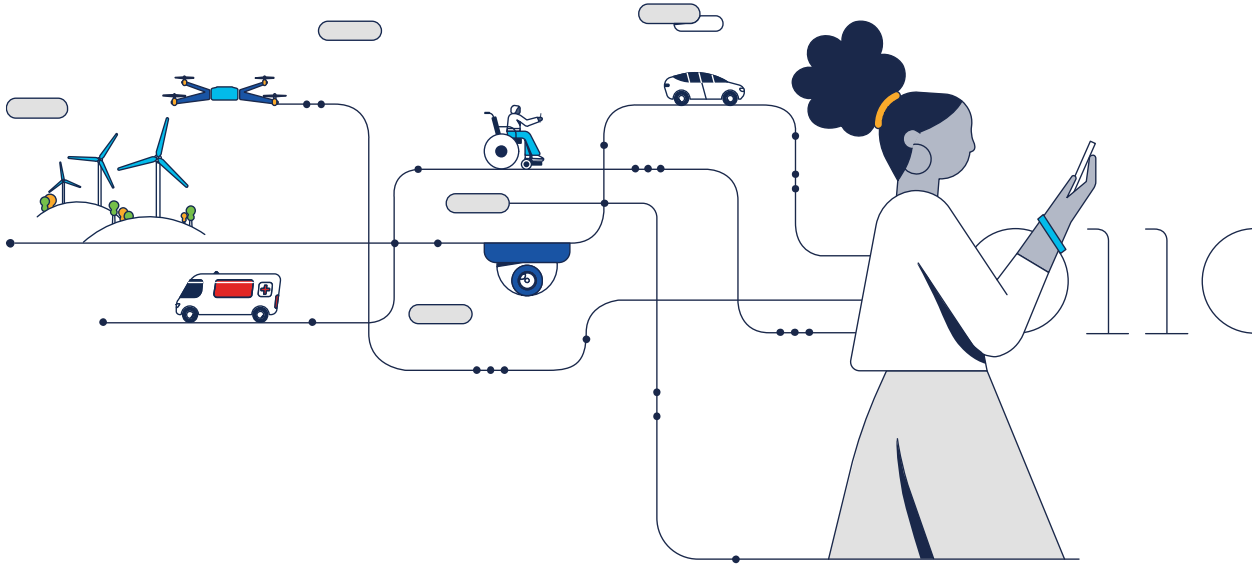
The bridge to possible

Nossos parceiros

TD SYNNEX

WISE
Women in Science
and Engineering
Inclusive Community

cisco
Networking
Academy



INTERNATIONAL
Girls in ICT Day
Brought to you by **WOMEN ROCK-IT**

Networking Academy

INTERNATIONAL Girls in ICT Day
Brought to you by WOMEN ROCK-IT

CCNAv7 – ITN – Configuração básica do roteador

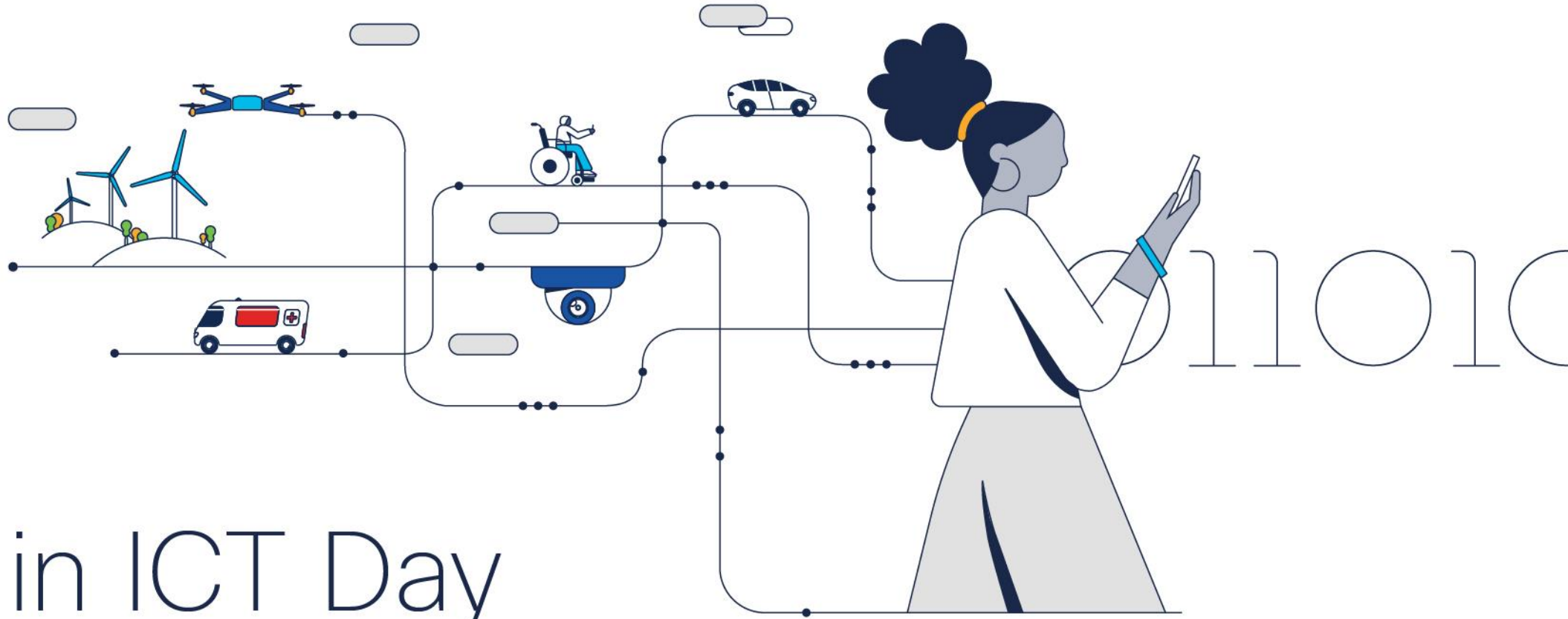
Módulo 10

Embaixadores do Programa 2020, 2021, 2022 & 2023:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

Networking
Academy



INTERNATIONAL

Girls in ICT Day

Brought to you by **WOMEN ROCK-IT**

Configurar definições iniciais do roteador

Configurações iniciais em um roteador	Comandos
1.Configurar o nome do dispositivo.	*Router(config)#* ***hostname hostname***
2. Proteger o modo EXEC privilegiado.	*Router(config)#* ***enable secret password***
3. Proteger o modo EXEC usuário.	*Router(config)#* ***line console 0*** *Router(config-line)#* ***password password*** *Router(config-line)#* ***login***
4. Proteger o acesso remoto Telnet/SSH	*Router(config-line)#* ***line vty 0 4*** *Router(config-line)#* ***password password*** *Router(config-line)#* ***login*** *Router(config-line)#* ***transport input {ssh | telnet}***
5. Proteger todas as senhas do arquivo de configuração.	*Router(config-line)#* ***exit*** *Router(config)#* ***service password-encryption***
6. Apresentar a notificação legal.	*Router(config)#* ***banner motd delimiter message delimiter***
7. Salvar a configuração.	*Router(config)#* ***end*** *Router#* ***copy running-config startup-config***

Exemplo de configuração básica do roteador

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# Login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# Login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)# banner motd #
Digite a mensagem de texto. Termine com uma nova linha e o #
**********************************************
AVISO: O acesso não autorizado é proibido!
**********************************************
#
R1(config)# exit
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Ao configurar o nome do dispositivo observe como o prompt do roteador agora exibe o nome escolhido, R1.

Todo o acesso ao roteador deve ser protegido, o modo EXEC privilegiado, o modo EXEC do usuário, o acesso remoto via telnet e SSH e as senhas de texto simples devem ser criptografadas.

O modo EXEC privilegiado fornece ao usuário acesso completo ao dispositivo e sua configuração. Portanto, é o modo mais importante para proteger.

A notificação legal avisa os usuários de que o dispositivo só deve ser acessado por usuários permitidos.

Se ao configurar o roteador perder a energia acidentalmente, todos os comandos serão perdidos. Por esse motivo, é importante salvar a configuração após realizar as alterações. O comando a seguir salva a configuração na NVRAM.

Configuração de Interfaces

Os roteadores não podem ser acessados por dispositivos finais até que as interfaces estejam configuradas.
Há muitos tipos diferentes de interfaces disponíveis em roteadores Cisco.

```
Router(config)# interface type-and-number
Router(config-if)# description description-text
Router(config-if)# ip address ipv4-address subnet-mask
Router(config-if)# ipv6 address ipv6-address/prefix-length
Router(config-if)# no shutdown
```

O uso do comando **description** é recomendável por ser útil na solução de problemas, fornecendo informações sobre o tipo de rede conectada. O texto da descrição está limitado a 240 caracteres.

O comando **no shutdown** ativa a interface. A interface também deve ser conectada a outro dispositivo, como switch ou roteador, para que a camada física esteja ativa. Ao ativar uma interface, mensagens de informações devem ser exibidas confirmando o link habilitado.

Observação: Em conexões entre roteadores onde não há switch Ethernet, ambas as interfaces de interconexão devem ser configuradas e habilitadas.

Exemplo de configuração de interfaces

```
R1> enable
R1# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# description Link to LAN
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:10::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
*Aug  1 01:43:53.435: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Aug  1 01:43:56.447: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Aug  1 01:43:57.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
```

Verificação da Configuração

Comandos	Descrição
show ip interface brief **show ipv6 interface brief**	A saída exibe todas as interfaces, seus endereços IP e seus status atual. As interfaces configuradas e conectadas devem exibir uma Status de “up” e Protocolo de “up”. Qualquer outra coisa indicaria um problema com a configuração ou O cabeamento.
show ip route **show ipv6 route**	Exibe o conteúdo das tabelas de roteamento IP armazenadas na RAM.
show interfaces	Exibe estatísticas para todas as interfaces no dispositivo. No entanto, este exibirá apenas as informações de endereçamento IPv4.
show ip interfaces	Exibe as estatísticas do IPv4 para todas as interfaces em um roteador.
show ipv6 interface	Exibe as estatísticas do IPv6 para todas as interfaces em um roteador.

Verificação da Configuração

```
R1#  show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 192.168.10.1 YES manual up up
Gigabitethernet0/0/1 209.165.200.225 SIM manual up
Vlan1 unassigned YES unset administratively down down
R1#  show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
    FE80::201:C9FF:FE89:4501
    2001:DB8:ACAD:10::1
GigabitEthernet0/0/1 [up/up]
    FE80::201:C9FF:FE89:4502
    2001:DB8:FEED:224::1
Vlan1 [administratively down/down]
    unassigned
R1#
```

```
R1# show interfaces gig0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4321-2x1GE, address is a0e0.af0d.e140 (bia a0e0.af0d.e140)
  Description: Link to LAN
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 100Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:35, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1180 packets input, 109486 bytes, 0 no buffer
     Received 84 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 1096 multicast, 0 pause input
     65 packets output, 22292 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     11 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     1 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Cisco Networking Academy

INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Verificação da Configuração

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

```
R1# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, a - Application
C 2001:DB8:ACAD:10::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ACAD:10: :1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C 2001:DB8:FEED:224::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L 2001:DB8:FEED:224::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
L FF00::/8 [0/0]
     via Null0, receive
R1#
```

Networking Academy

INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Verificação da Configuração

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP Null turbo vector
  Associated unicast routing topologies:
        Topology "base", operation state is UP
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  IPv4 WCCP Redirect outbound is disabled
  IPv4 WCCP Redirect inbound is disabled
  IPv4 WCCP Redirect exclude is disabled
```

```
R1# show ipv6 interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::868A:8DFF:FE44:49B0
  No Virtual link-local address(es):
  Description: Link to LAN
  Global unicast address(es):
    2001:DB8:ACAD:10::1, subnet is 2001:DB8:ACAD:10::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FF44:49B0
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds
```

Networking Academy

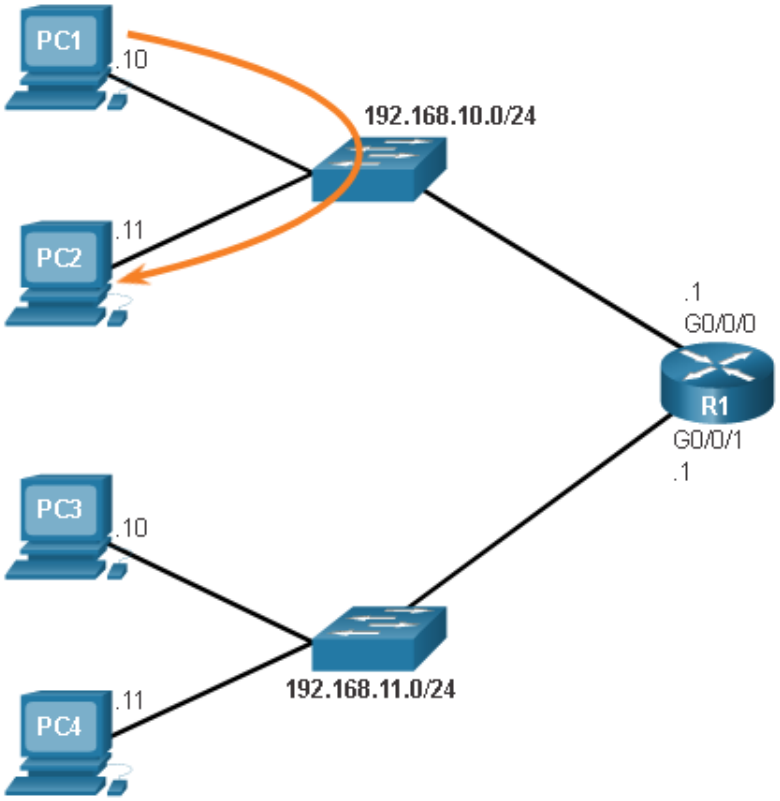
INTERNATIONAL Girls in ICT Day

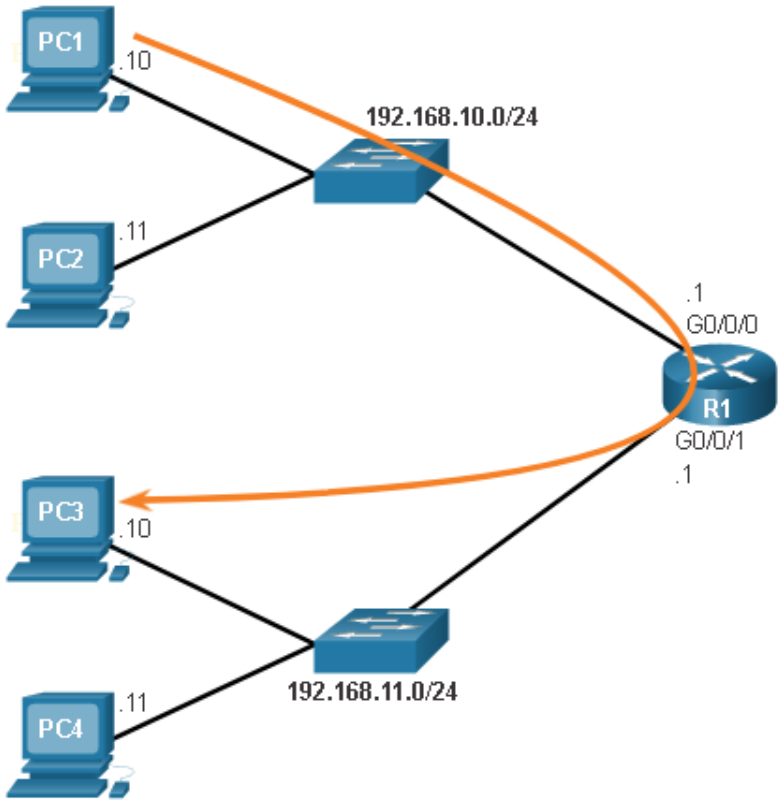
Brought to you by WOMEN ROCK-IT

Gateway Padrão em Host

Se sua rede local tiver apenas um roteador, este será o roteador gateway e todos os hosts e switches da rede deverão ter o endereço deste roteador configurado como gateway padrão.
Se sua rede local tiver vários roteadores, você deverá selecionar um deles para ser o roteador de gateway padrão.
Para que um host se comunique, ele deve ser configurado com um endereço IP e de gateway padrão.
O gateway padrão só é usado quando o host deseja enviar um pacote a um dispositivo em outra rede.
O endereço do gateway padrão geralmente é o endereço da interface do roteador associado à rede local do host.
O endereço IP do dispositivo host e o endereço da interface do roteador devem estar na mesma rede.
Ao enviar um pacote para um host na mesma rede, o gateway padrão não é usado, o pacote é endereçado com o IPv4 do host destino e é encaminhado diretamente.
Ao enviar um pacote para um host em outra rede, o pacote é endereçado com o IPv4 do host destino mas encaminhado para a interface do gateway padrão. O roteador aceita o pacote, acessa sua tabela de roteamento e determina qual a interface apropriada para encaminhar o pacote, com base no endereço de destino e encaminha o pacote para fora da interface de saída para alcançar o host de destino.
O mesmo processo ocorre numa rede IPv6.

Gateway Padrão em Host





Networking Academy

INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

Gateway Padrão em Switch

Um switch que interconecta computadores geralmente é um dispositivo da Camada 2 e não precisa de um endereço IP para funcionar corretamente.

No entanto, para se conectar e gerenciar um switch em uma rede IP local, ele deve ter uma interface virtual de switch (SVI) configurada com um endereço IPv4 e uma máscara de sub-rede na LAN local. O switch também deve ter um endereço de gateway padrão configurado para gerenciar remotamente o switch de outra rede.

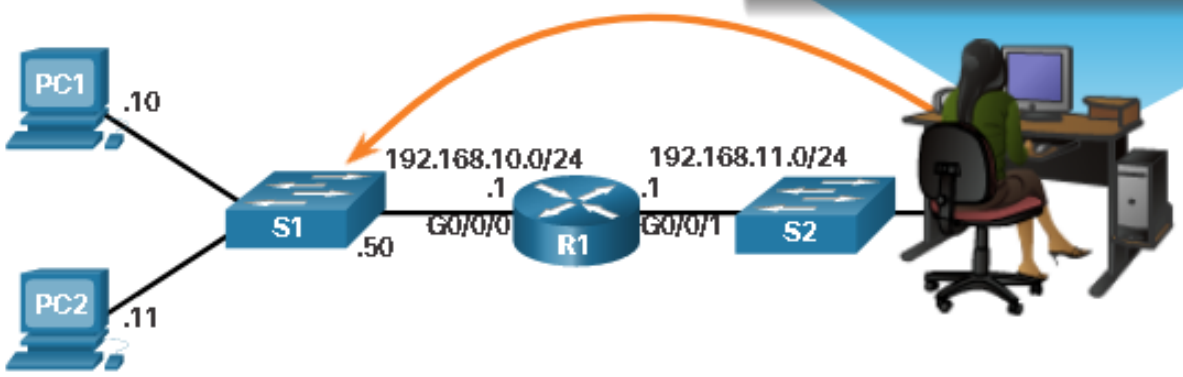
O endereço de gateway padrão geralmente é configurado em todos os dispositivos que se comunicam além da rede local.

O comando de configuração global **ip default-gateway *ip-address*** é usado para configurar um gateway padrão em um switch. O *ip-address* é o endereço IPv4 da interface do roteador local conectada ao switch. Os pacotes provenientes de computadores hosts conectados ao switch já devem ter o endereço do gateway padrão configurado nos sistemas operacionais desses computadores.

Um switch de grupo de trabalho também pode ser configurado com um endereço IPv6 em um SVI. No entanto, o switch não requer que o endereço IPv6 do gateway padrão seja configurado manualmente. O switch receberá automaticamente seu gateway padrão da mensagem de anúncio do roteador ICMPv6 do roteador.

Gateway Padrão em Switch

```
S1# show running-config
Building configuration...
!
<Output Omitted>
service password-encryption
!
hostname S1
!
interface Vlan1
  ip address 192.168.10.50 255.255.255.0
!
<Saída omitida>
!
ip default-gateway 192.168.10.1
<Saída omitida>
```



Networking Academy

INTERNATIONAL Girls in ICT Day

Brought to you by WOMEN ROCK-IT

The bridge to possible