Networking Academy

WOMENROCK-IT

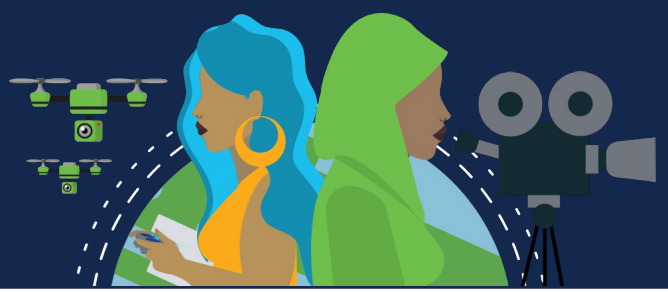
CCNAv7 – ITN – Introduction to Networks

Módulo 1

Embaixadores do Programa 2020, 2021 & 2022:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum



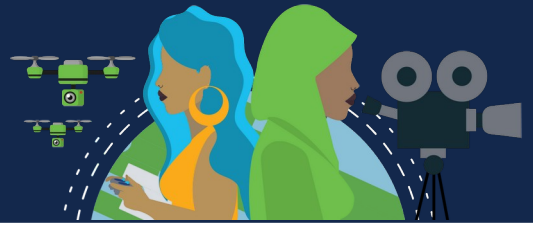
Rede

Rede:

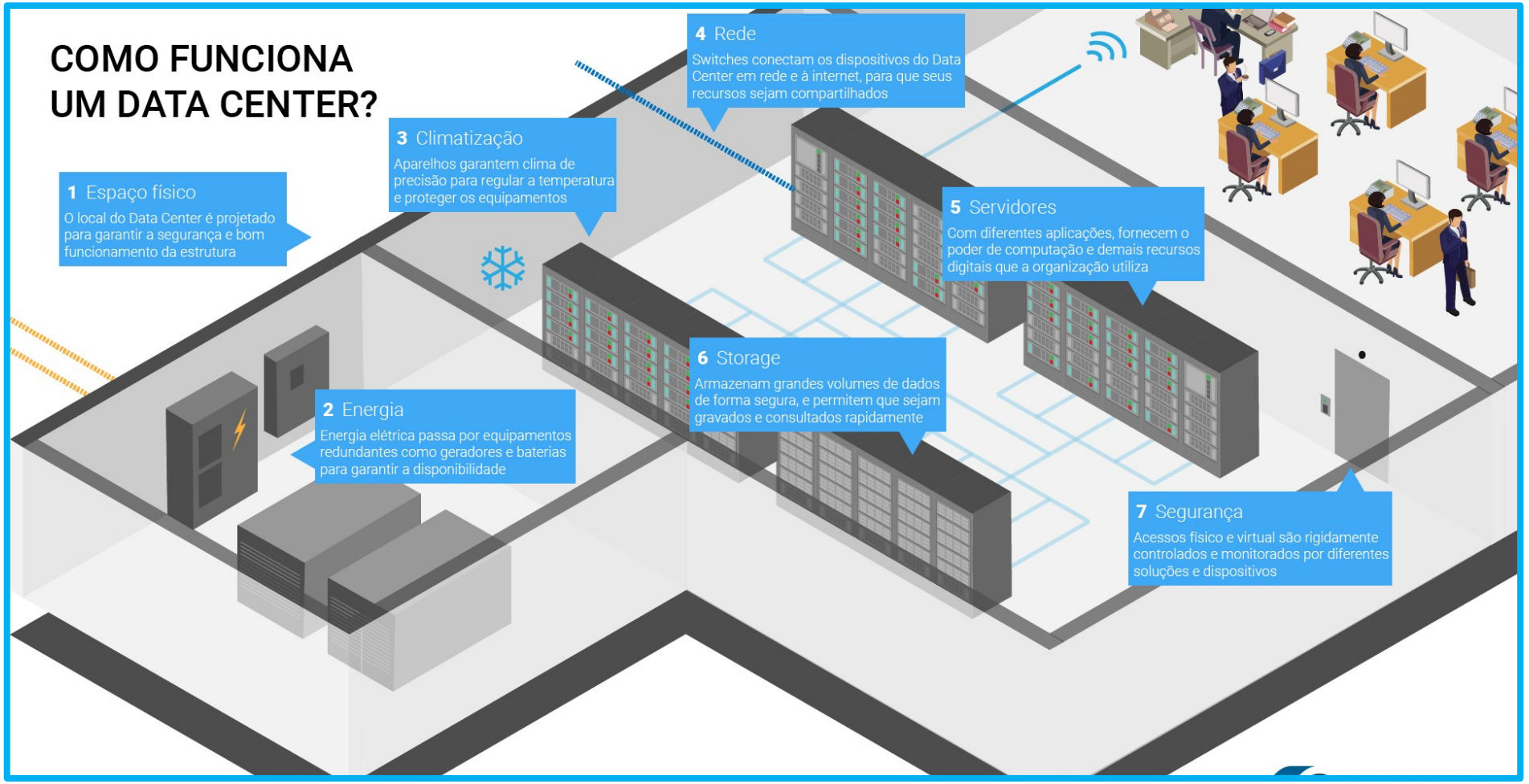
- Conjunto de dispositivos interligados por uma única tecnologia.
- Conjunto de 2 ou mais dispositivos (nós) que usam um conjunto de regras (protocolos) em comum para compartilhar recursos entre si.

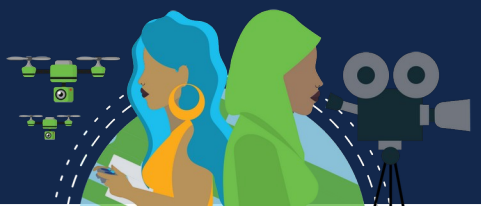
Protocolo:

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

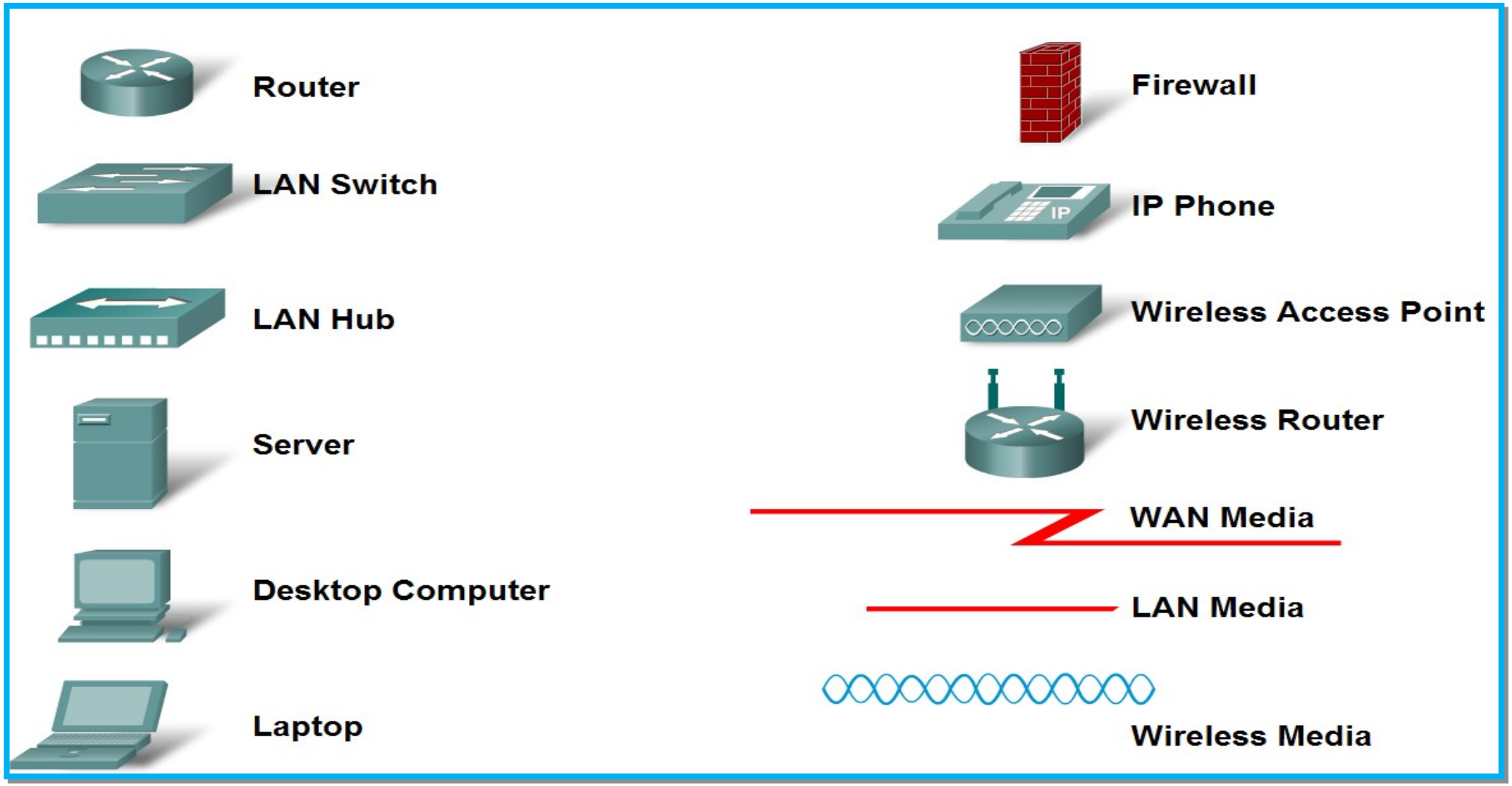


Data Center

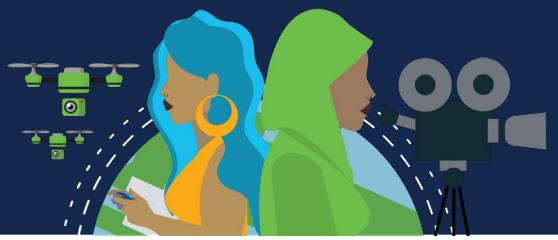

COMO FUNCIONA UM DATA CENTER?
1 Espaço físico
O local do Data Center é projetado para garantir a segurança e bom funcionamento da estrutura
2 Energia
Energia elétrica passa por equipamentos redundantes como geradores e baterias para garantir a disponibilidade
3 Climatização
Aparelhos garantem clima de precisão para regular a temperatura e proteger os equipamentos
4 Rede
Switches conectam os dispositivos do Data Center em rede e à internet, para que seus recursos sejam compartilhados
5 Servidores
Com diferentes aplicações, fornecem o poder de computação e demais recursos digitais que a organização utiliza
6 Storage
Armazenam grandes volumes de dados de forma segura, e permitem que sejam gravados e consultados rapidamente
7 Segurança
Acessos físico e virtual são rigidamente controlados e monitorados por diferentes soluções e dispositivos



Símbolos Comuns de Rede



Fonte: Cisco

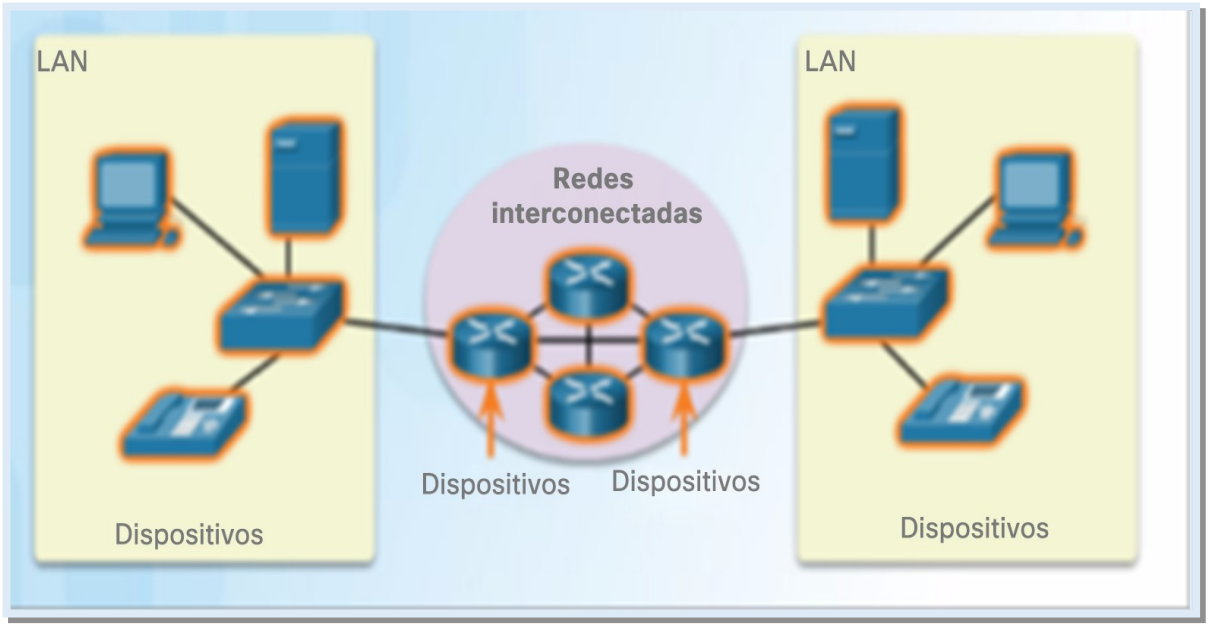


Componentes da Rede

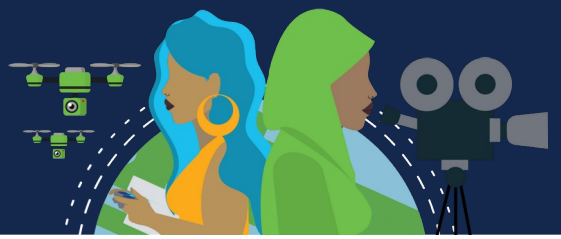
Uma rede pode ser tão simples quanto um único cabo conectando dois computadores ou tão complexa quanto uma coleção de redes que abrangem todo o mundo.

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

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



Fonte: Cisco

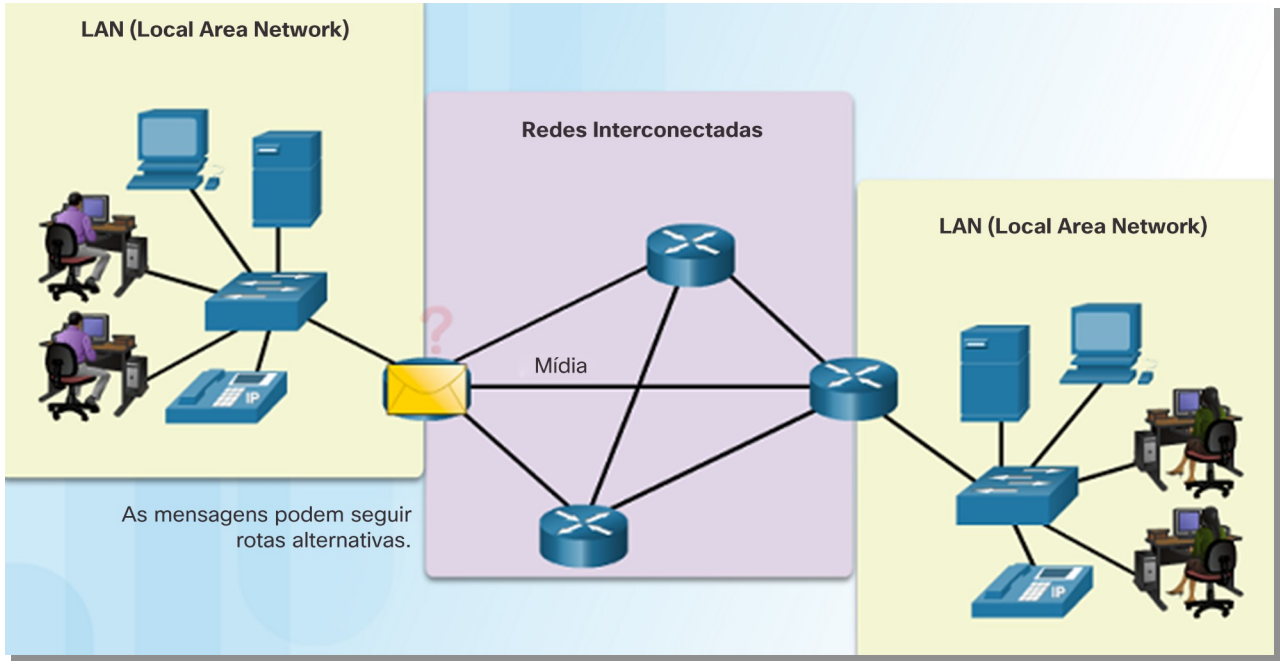


Componentes da Rede

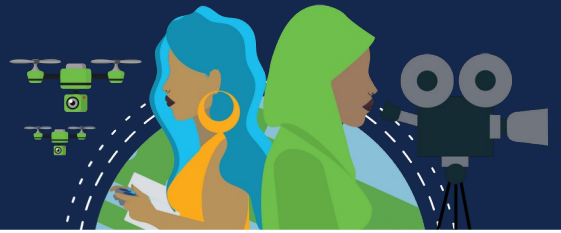
Dispositivos Finais:

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



Fonte: Cisco



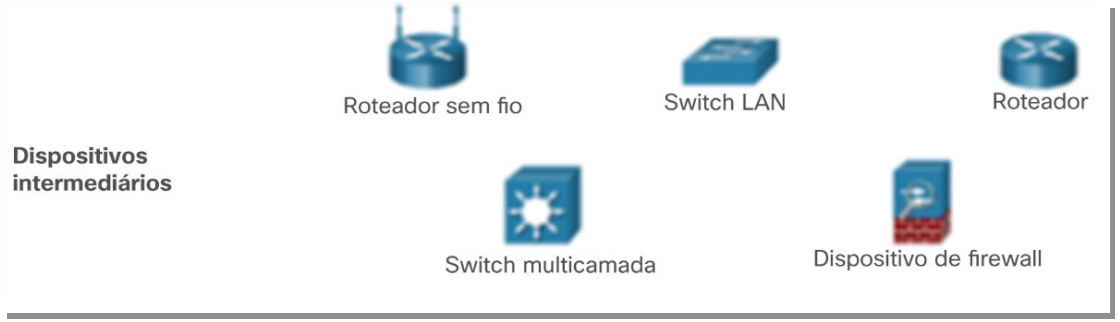
Componentes da Rede

Um dispositivo intermediário interconecta os dispositivos finais em uma rede.

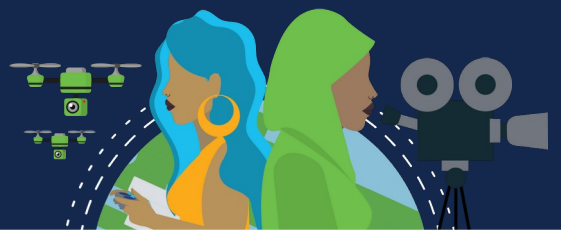
Os exemplos incluem: switches, access points sem fio, roteadores e firewalls.

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.



Fonte: Cisco

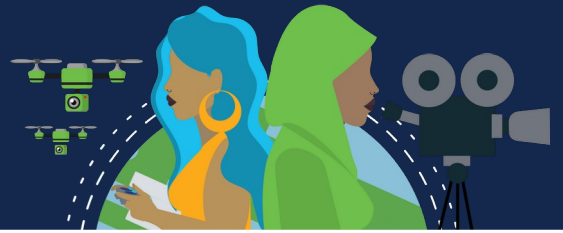


Componentes da Rede

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;

Fonte: Cisco

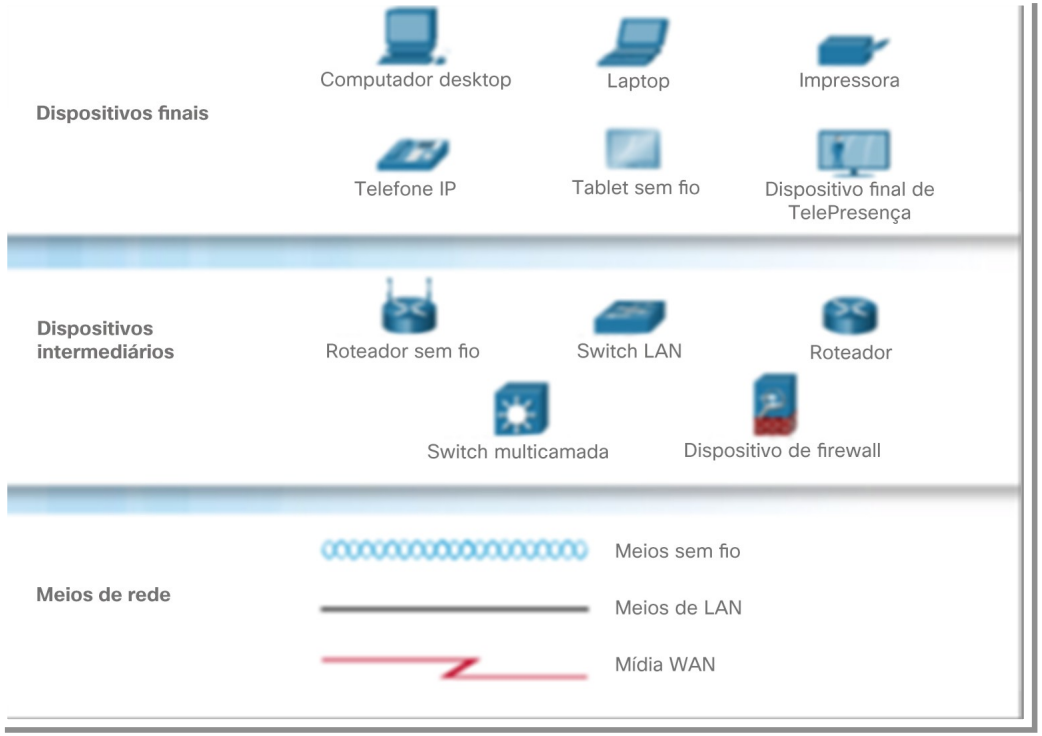


Componentes da Rede

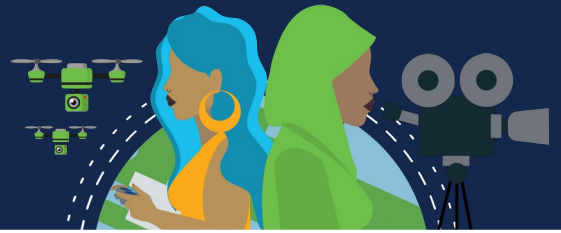
Os diagramas de rede, muitas vezes chamados de diagramas de topologia, usam símbolos para representar os dispositivos na rede.

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

- Placa de rede
- Porta Física
- Interface



Fonte: Cisco



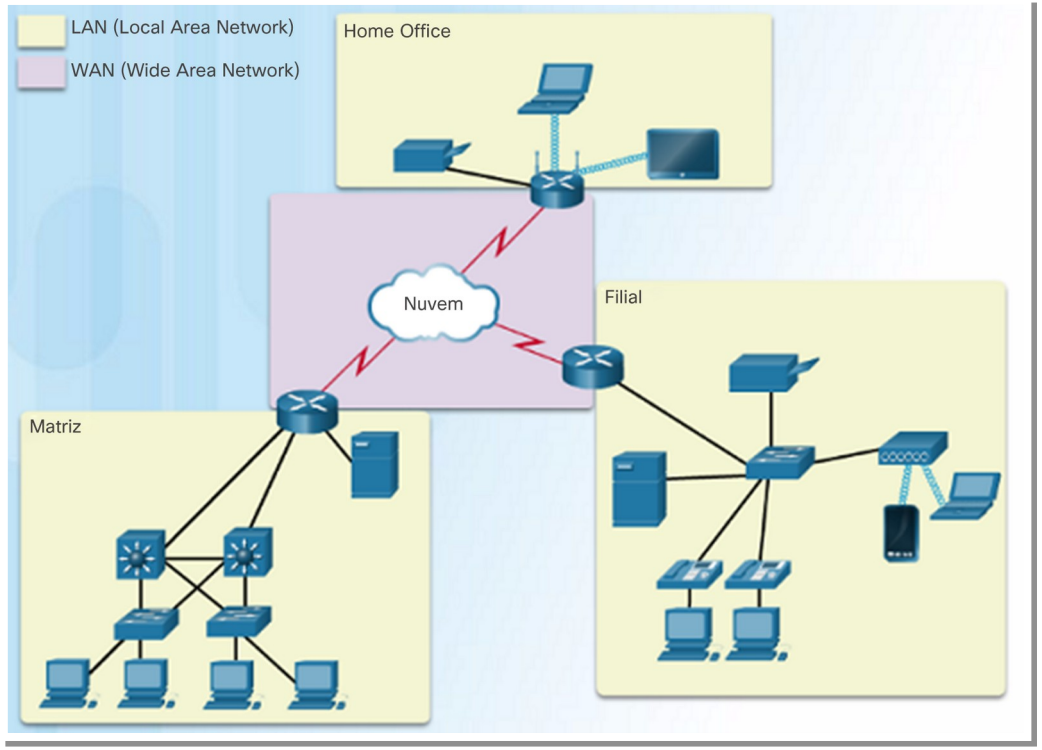
Tipos de Rede

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

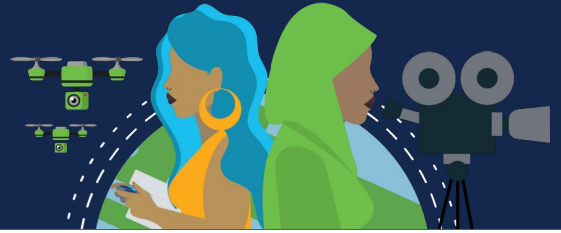
Rede de longa distância (WAN) – abrange uma grande área geográfica, normalmente envolvendo um provedor de serviços de telecomunicações.

<u>Outros tipos de redes incluem:</u>

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



Fonte: Cisco



A Internet

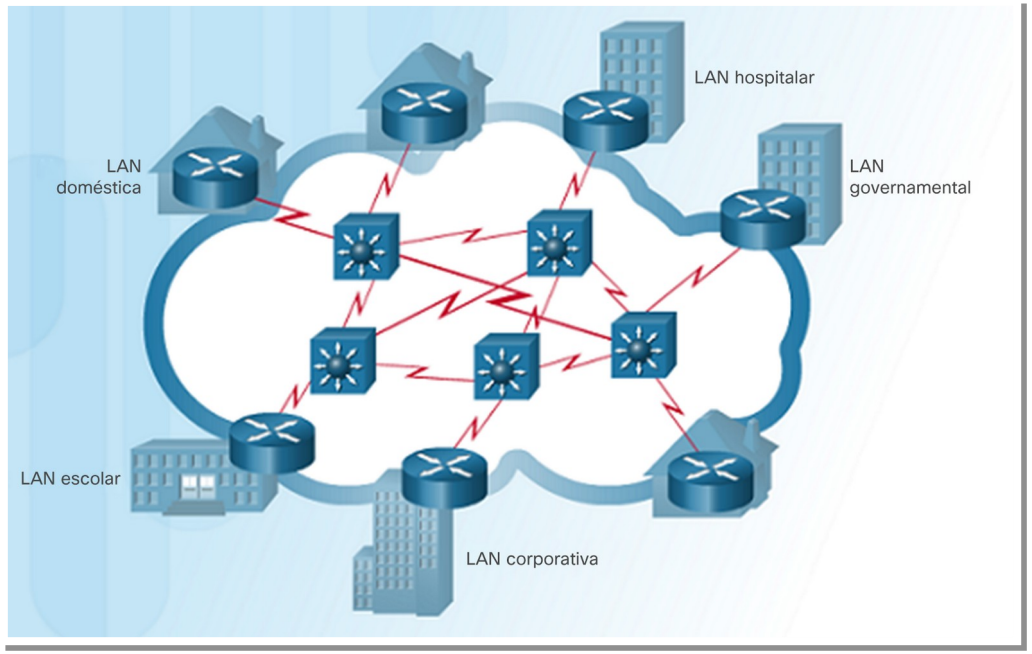
A Internet é um conjunto mundial de LANs e WANs interconectadas.

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.

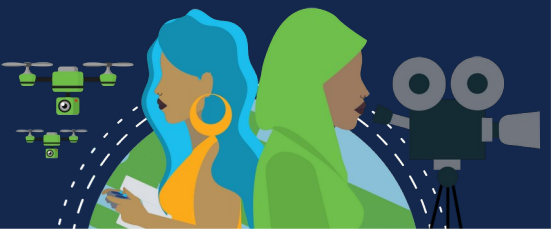
A Internet não pertence a qualquer indivíduo ou grupo, no entanto, os seguintes grupos foram desenvolvidos para ajudar a manter a estrutura:

- IETF
- ICANN
- IAB



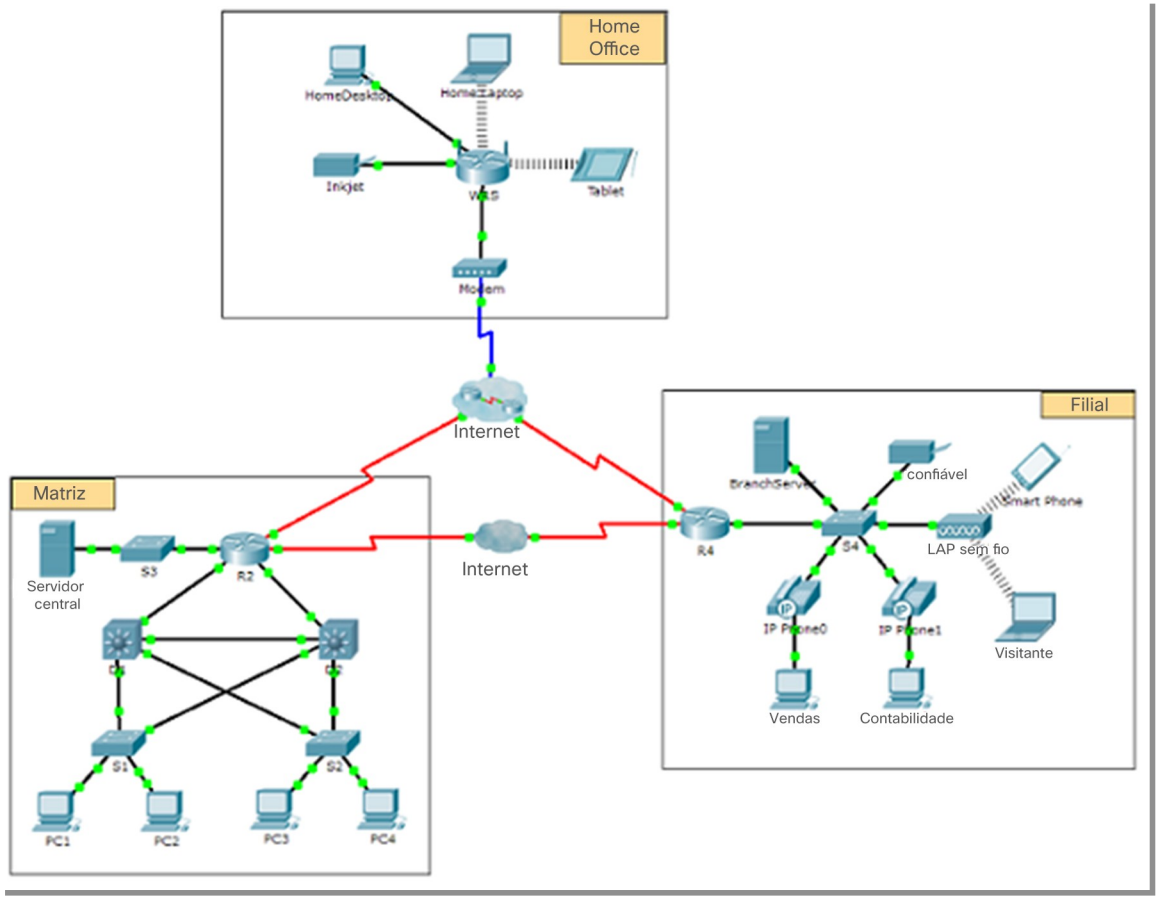
Fonte: Cisco

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?".



Fonte: Cisco

Certificação de Redes

A certificação Cisco Certified Network Associate (CCNA):

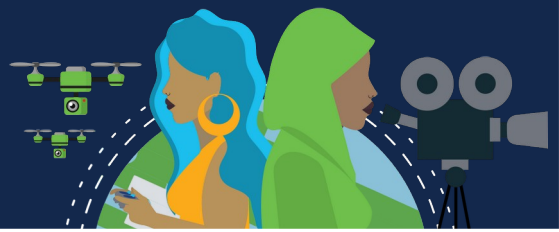
- Demonstra que você tem um conhecimento de tecnologias fundamentais
- Garante que você permaneça relevante com as habilidades necessárias para a adoção de tecnologias de próxima geração.

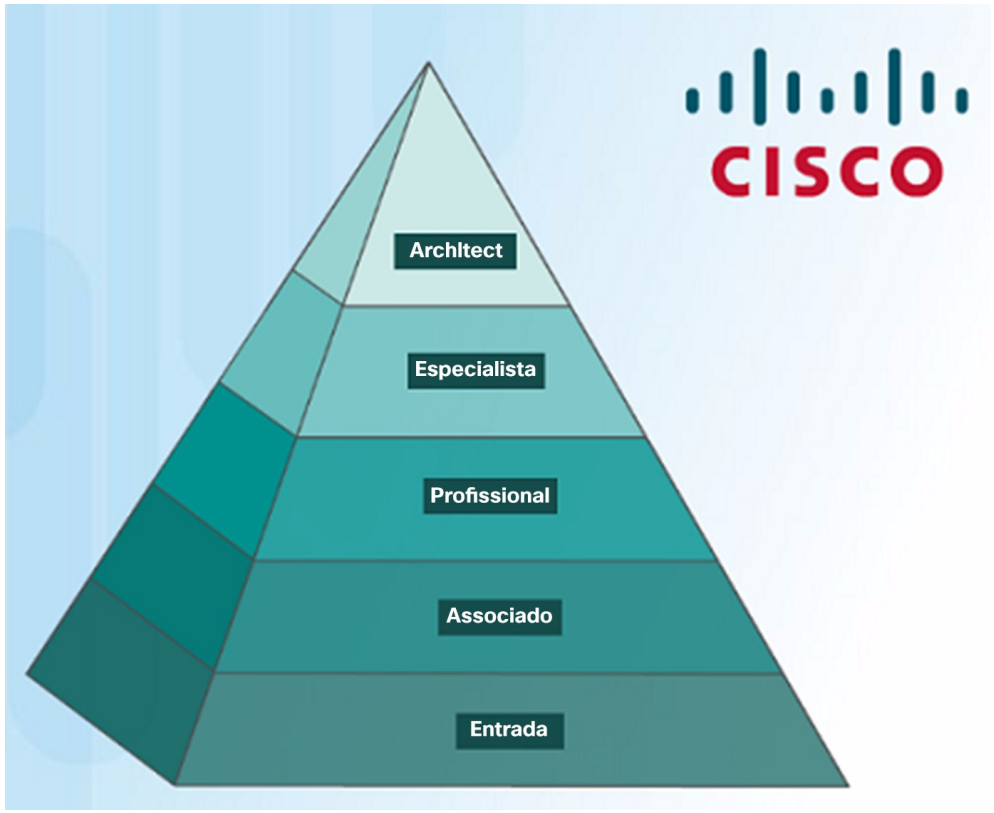
O novo foco da CCNA:

- 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.

Fonte: Cisco

Certificação de Rede





Cisco Certified Network Associate (CCNA)

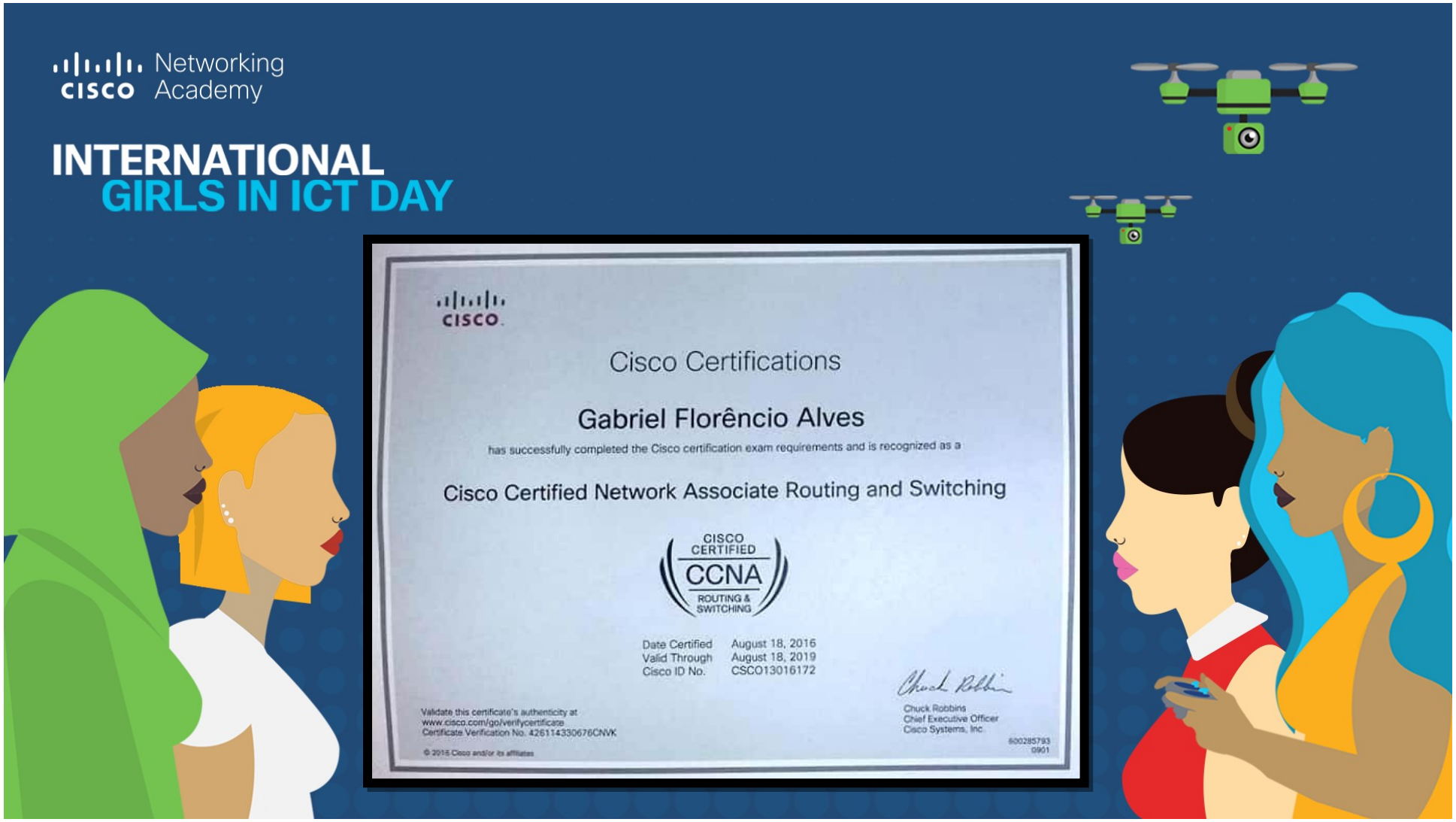
- Certificação de roteamento e switching;
- Você precisa ser aprovado nos dois exames:

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

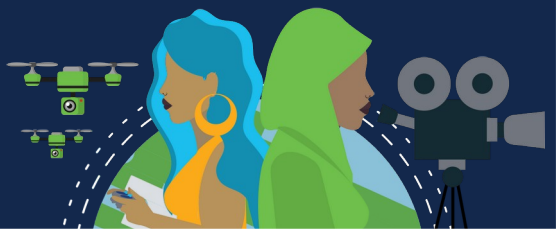
✓ O segundo exame está voltado para as tecnologias WAN e roteamento de IPv4 e IPv6, bem como switching de LAN e infraestrutura de serviços/manutenção.

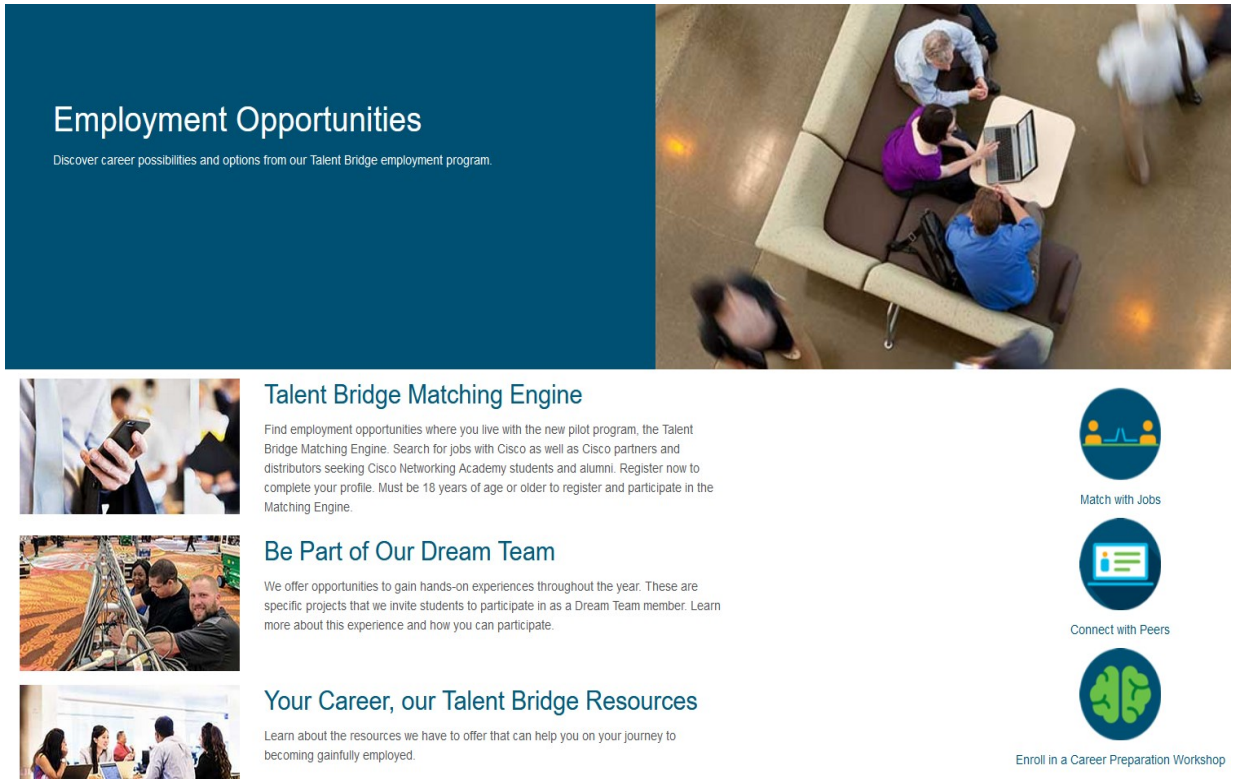
Fonte: Cisco

Apresentação CCNA



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.

Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

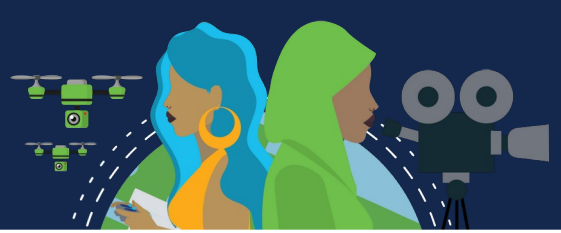
CCNAv7 – ITN – Configuração Básica do Switch e do Dispositivo Final

Módulo 2

Embaixadores do Programa 2020, 2021 & 2022:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum



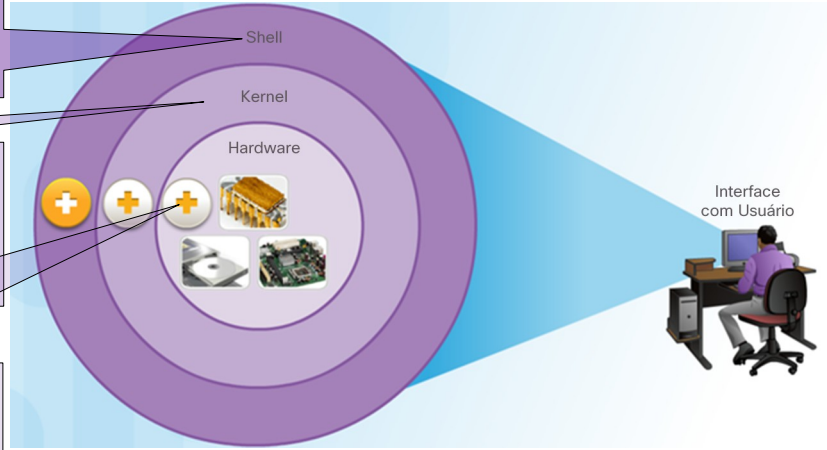
Sistema Operacional

- 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.

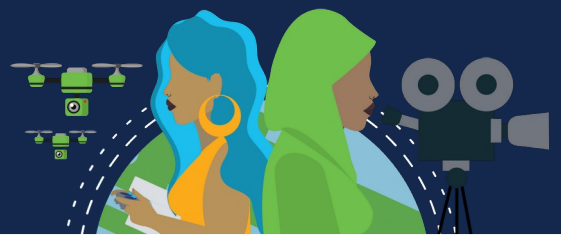
Kernel do sistema operacional
- O kernel do sistema operacional se comunica diretamente com o hardware e gerencia como os recursos de hardware são usados para atender aos requisitos de software.

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.

Fonte: Cisco

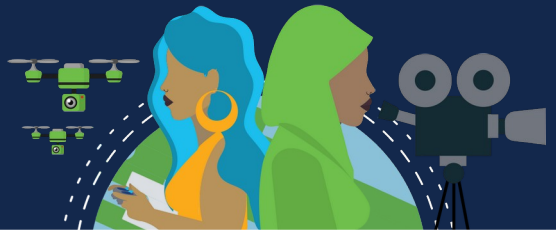


Sistema Operacional

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

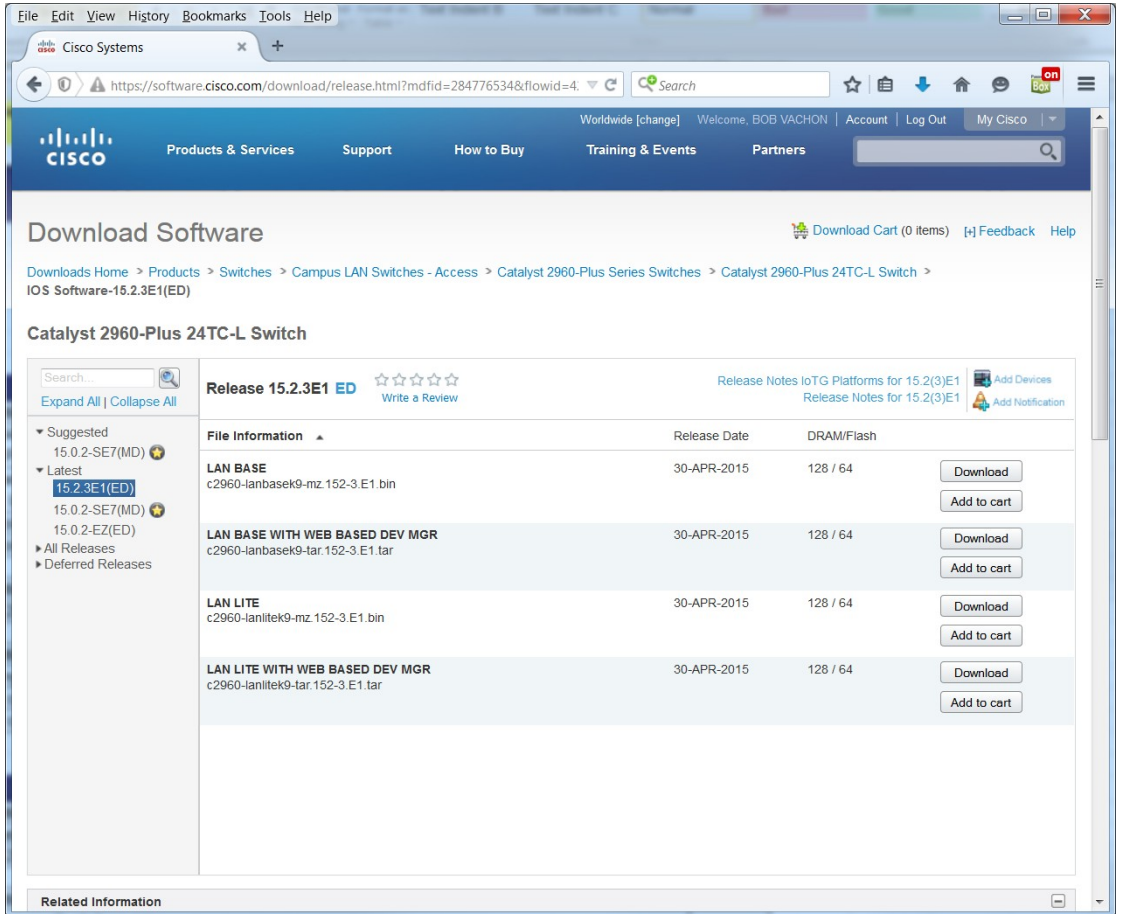
- Utilizar uma CLI em um switch do Cisco IOS ou o roteador permite que um técnico de redes:
  - Use um teclado para executar programas de rede baseados na CLI
  - Use um teclado para inserir texto e comandos baseados em texto

- 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

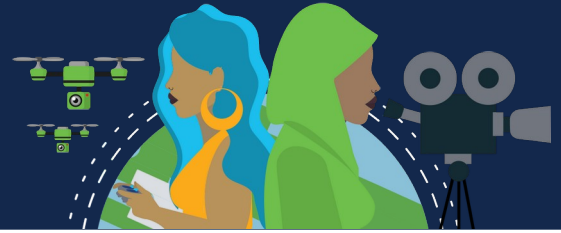


SUBCAMADAS DE ENLACE IEEE 802 LAN/MAN

- 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.



Fonte: Cisco



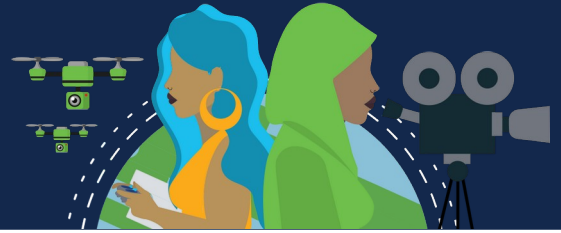
Métodos de Acesso

- 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.

Cisco
Life Changer

Changing the way
the world WORKS!

Fonte: Cisco

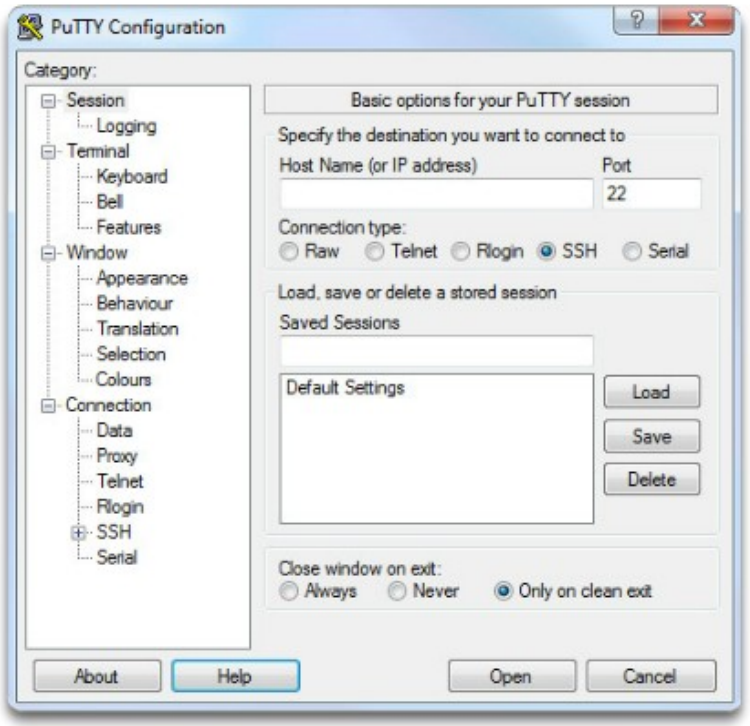


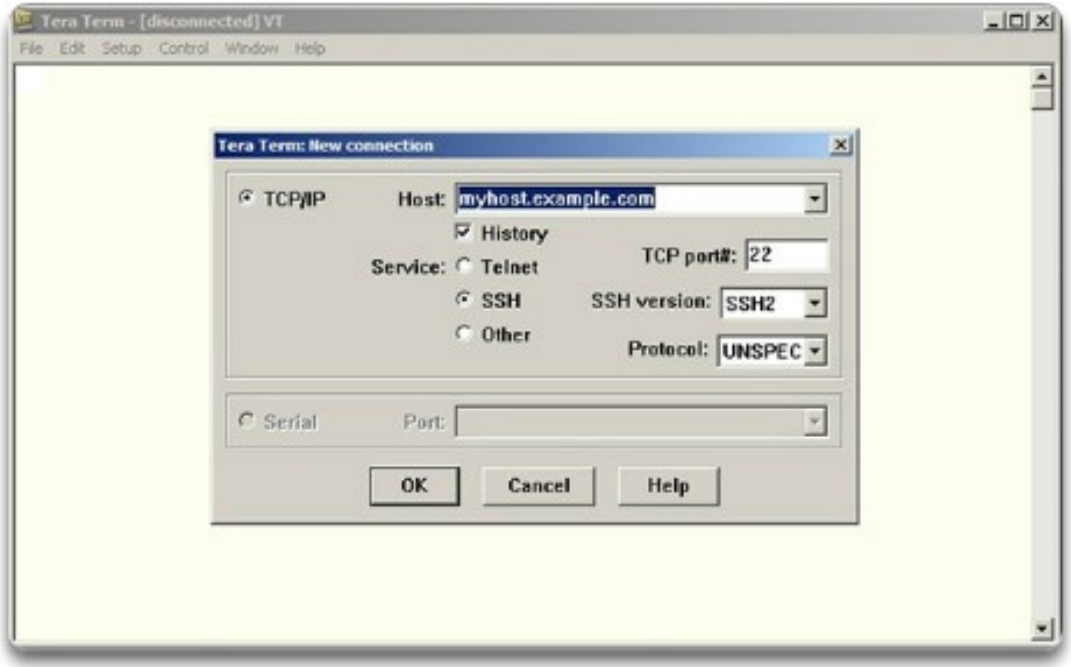
Métodos de Acesso

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

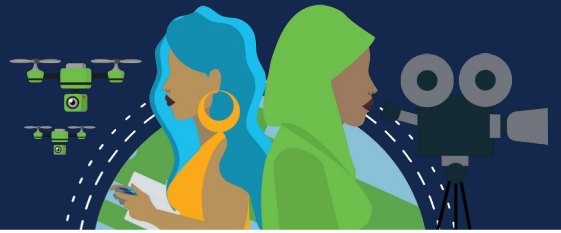
Os programas populares de emulação de terminal incluem PuTTY, Tera Term, SecureCRT e OS X Terminal.

PuTTY





Fonte: Cisco

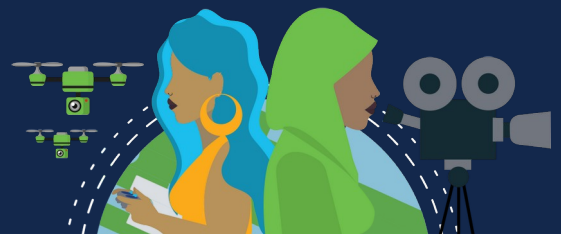


Navegação no IOS

- 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#`

Fonte: Cisco



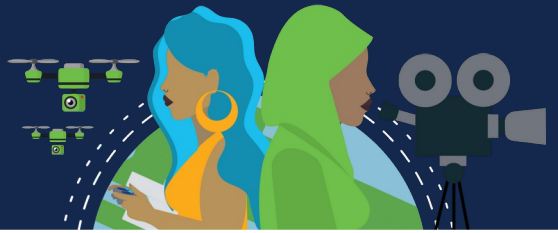
Navegação no IOS

- 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.

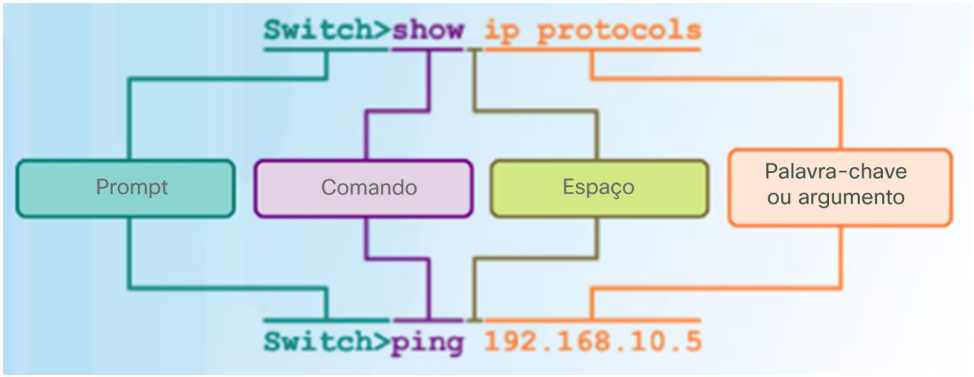
- A seguir há um exemplo da navegação entre os modos do IOS:
  - Entre no modo EXEC privilegiado usando o comando **enable**.
  - Entre no modo de configuração global usando o comando **configure terminal**.
  - Insira o modo de interface sub-config usando o comando **interface fa0/1**.
  - Saia de cada 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**.

Fonte: Cisco



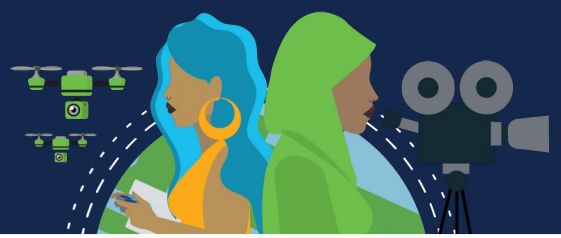
Estrutura de comandos

- 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.

Fonte: Cisco



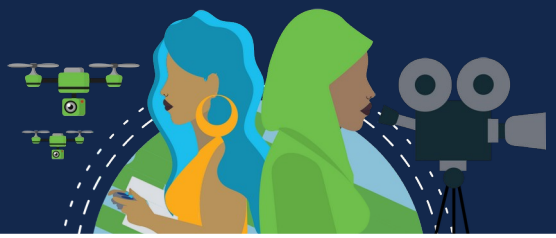
Estrutura de comandos

- 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

Fonte: Cisco

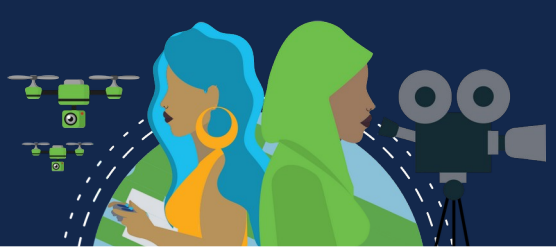


Estrutura de comandos

- 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.

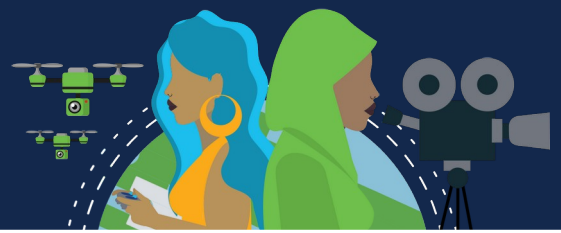
- Por exemplo, o comando **configure** pode ser abreviado para **conf** porque configure é o único comando que se inicia com **conf**.
  - Uma versão ainda mais curta de **con** não dará certo porque mais de um comando se inicia com **con**.
  - Palavras-chave também podem ser abreviadas.

Fonte: Cisco



Estrutura de comandos

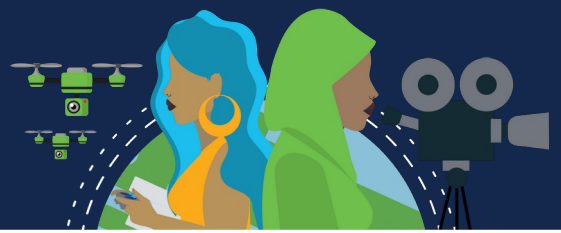
- A CLI do IOS é compatível com as seguintes teclas de acesso:
  - **Seta para baixo** – Permite que o usuário role pelo histórico de comandos.
  - **Seta para cima** – Permite que o usuário role para trás através de comandos anteriores.
  - **Tab** – Conclui o restante do comando parcialmente inserido.
  - **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

Fonte: Cisco

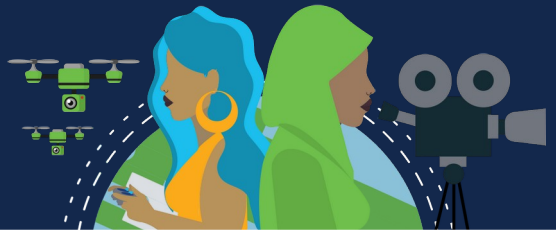


Inicialização

	Memória	Programa / Arquivo	Ação
0s			
	ROM	POST	Diagnóstico do Hardware
	ROM	Bootstrap	Carrega o Inicializador do Sistema
1a Opção	Flash	Imagem do IOS	Localiza e Descomprime o IOS na DRAM
2a Opção	Servidor TFTP	Imagem do IOS	Se Configurado, Localiza e Descomprime o IOS na DRAM
1a Opção	NVRAM	Arquivo Local	Localiza e Carrega Arquivo de Configuração → *copia a startup-config na running-config*
2a Opção	Servidor TFTP	Arquivo Remoto	Se Configurado, Carrega Configuração via Rede
	DRAM (e NVRAM)	Console do IOS	Interação do Usuário e Configurações → *running-config (e/ou startup-config)*

tempo

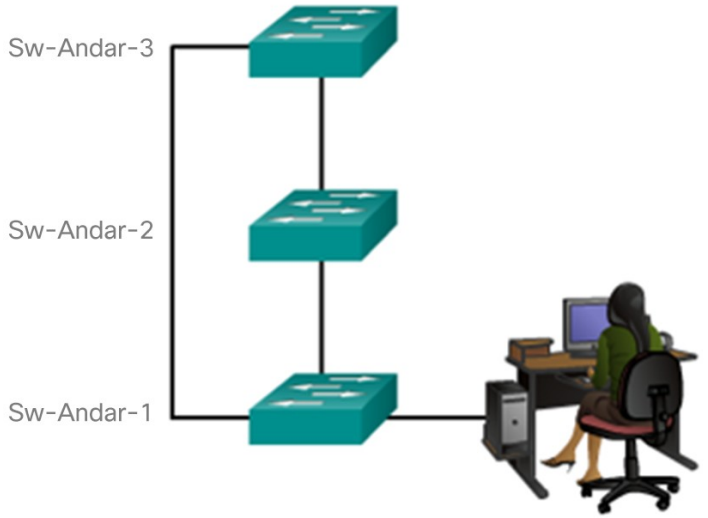
Fonte: labcisco.com.br



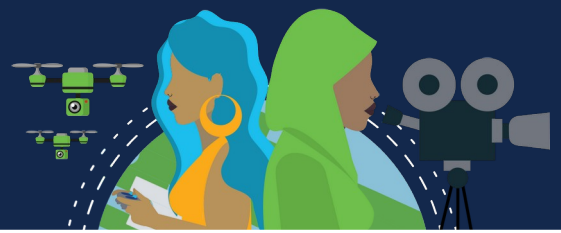
Nomes de Dispositivos

- 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.



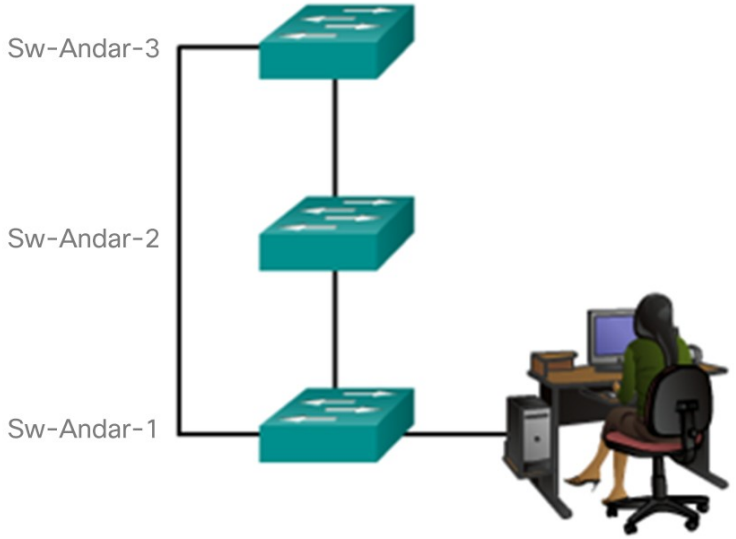
Fonte: Cisco



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.

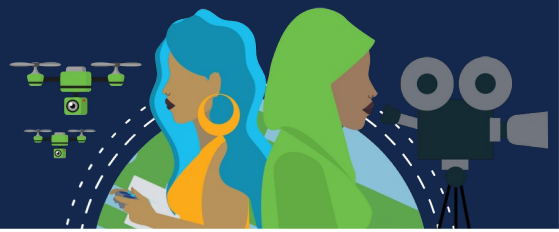
- O comando de configuração global **hostname** name é usado para atribuir um nome.




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

Fonte: Cisco

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

Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

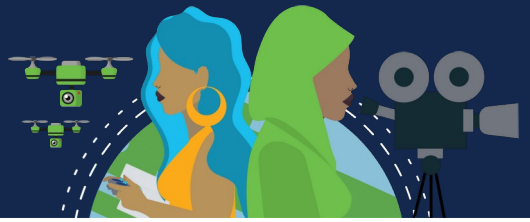
CCNAv7: Aula 3 – Protocolos e Modelos

Módulo 3

Embaixadores do Programa 2020, 2021 & 2022:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum



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.

WOMENROCK-IT

Brasil 2021

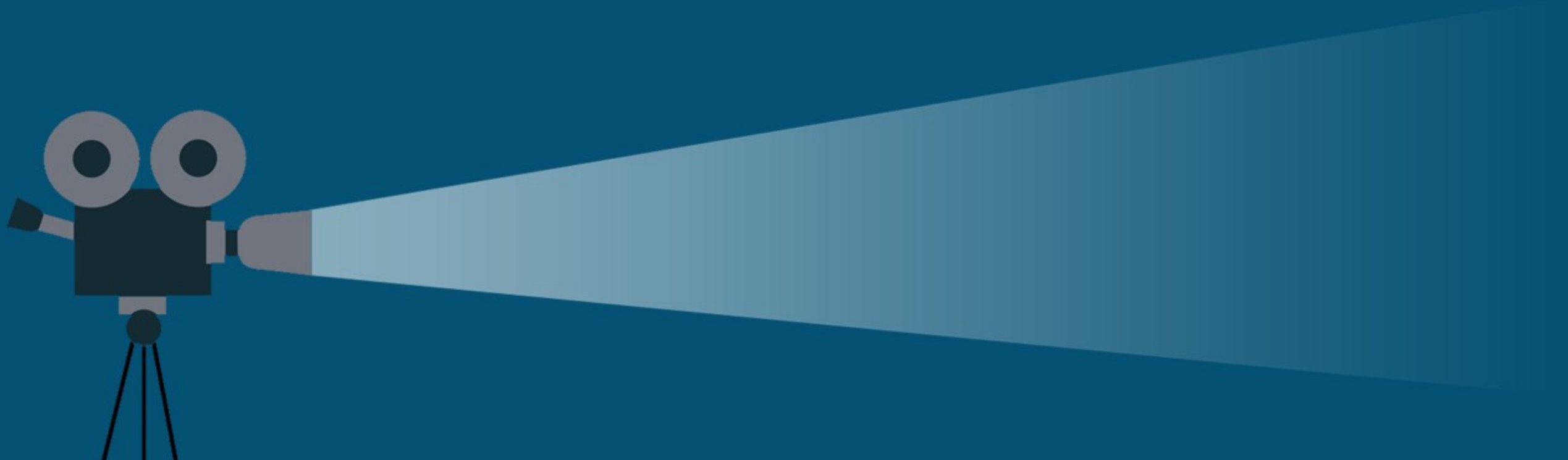
Networking Academy

REGRAS

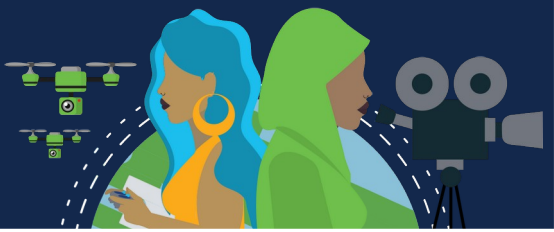
O vídeo de regras

- Dispositivos em uma bolha

Este vídeo explicará os protocolos que os dispositivos usam para ver seu lugar na rede e se comunicar com outros dispositivos.



Princípios da comunicação



As redes podem variar em tamanho e complexidade.

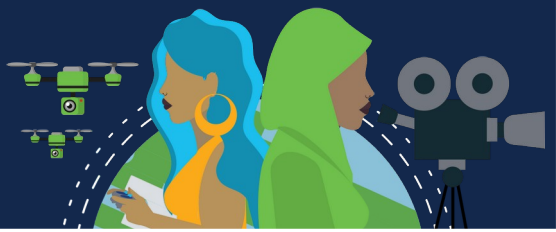
Não é suficiente ter uma conexão, os dispositivos devem concordar em “como” se comunicar.

Há três elementos para qualquer comunicação:

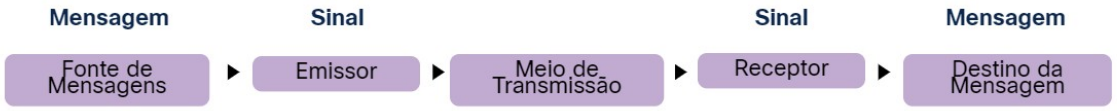
- Haverá uma fonte (remetente).
- Haverá um destino (receptor).
- Haverá um canal (mídia) que prevê o caminho das comunicações para ocorrer.

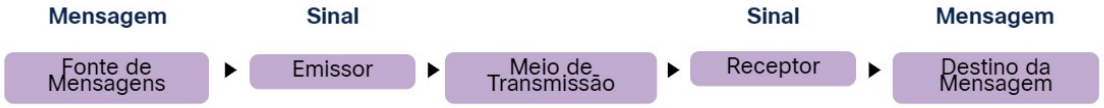
Fonte: Cisco

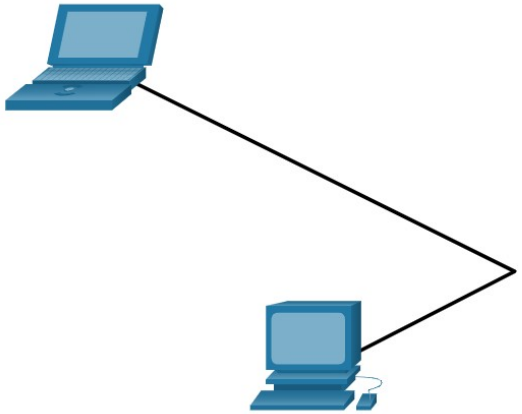
Protocolos de comunicações



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

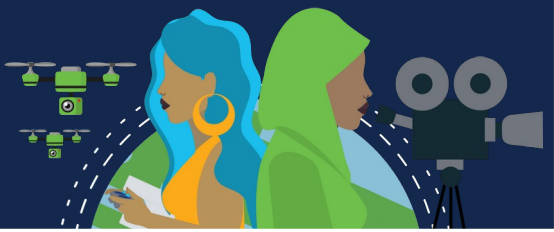






Fonte: Cisco

Estabelecimento de regras



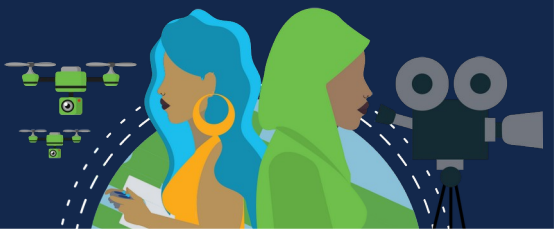
- Os indivíduos devem usar regras ou acordos estabelecidos para governar a conversa.
- A primeira mensagem é difícil de ler porque não está formatada corretamente. A segunda mostra a mensagem formatada corretamente

```
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.
```

Fonte: Cisco

Estabelecimento de regras

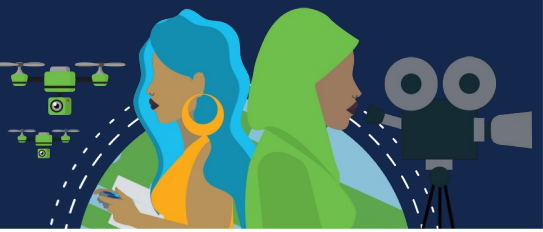


Os protocolos devem ter os seguinte requisitos para entregar com êxito uma mensagem:

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

Fonte: Cisco

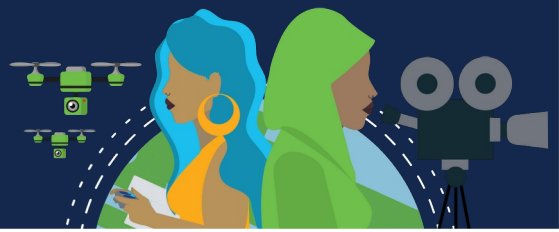
Requisitos do protocolo de rede



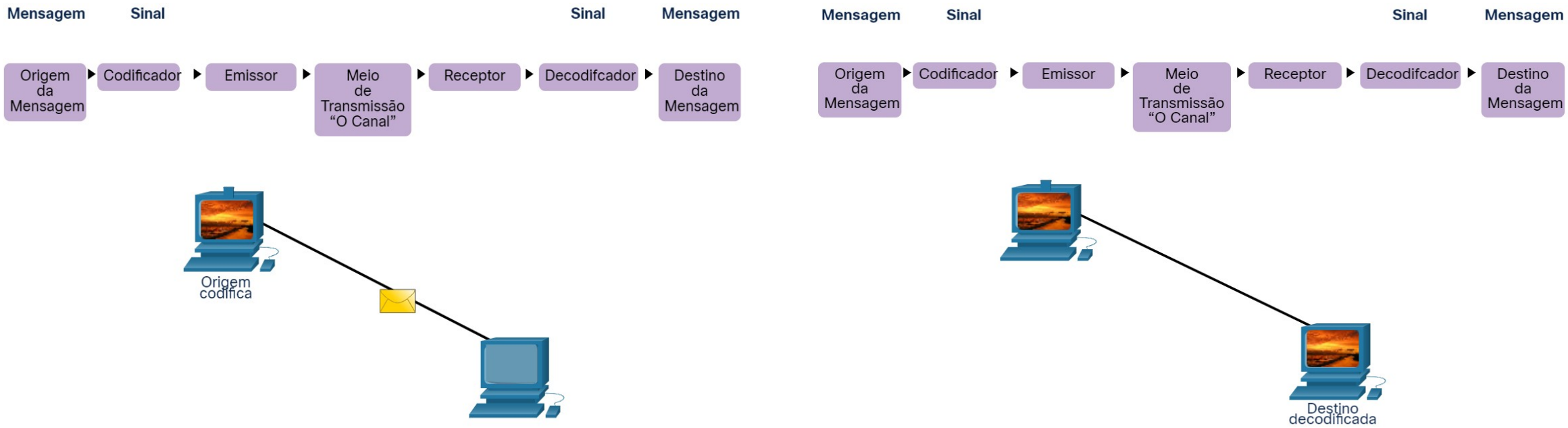
Protocolos de computador comuns devem estar de acordo e incluir os seguintes requisitos:

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

Codificação da mensagem

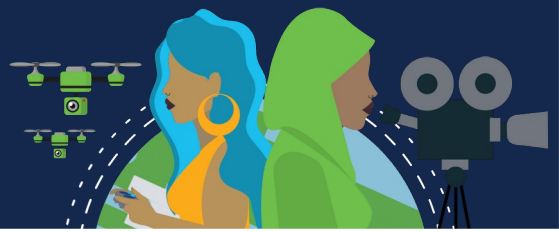


- A codificação é o processo de conversão de informações em outra forma aceitável para a transmissão.
- A decodificação reverte esse processo para interpretar como informações.

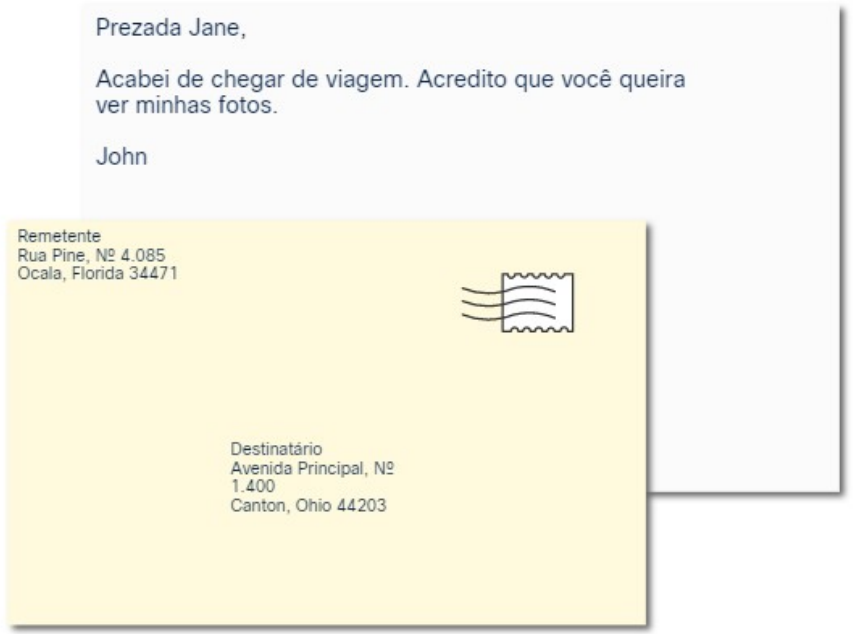


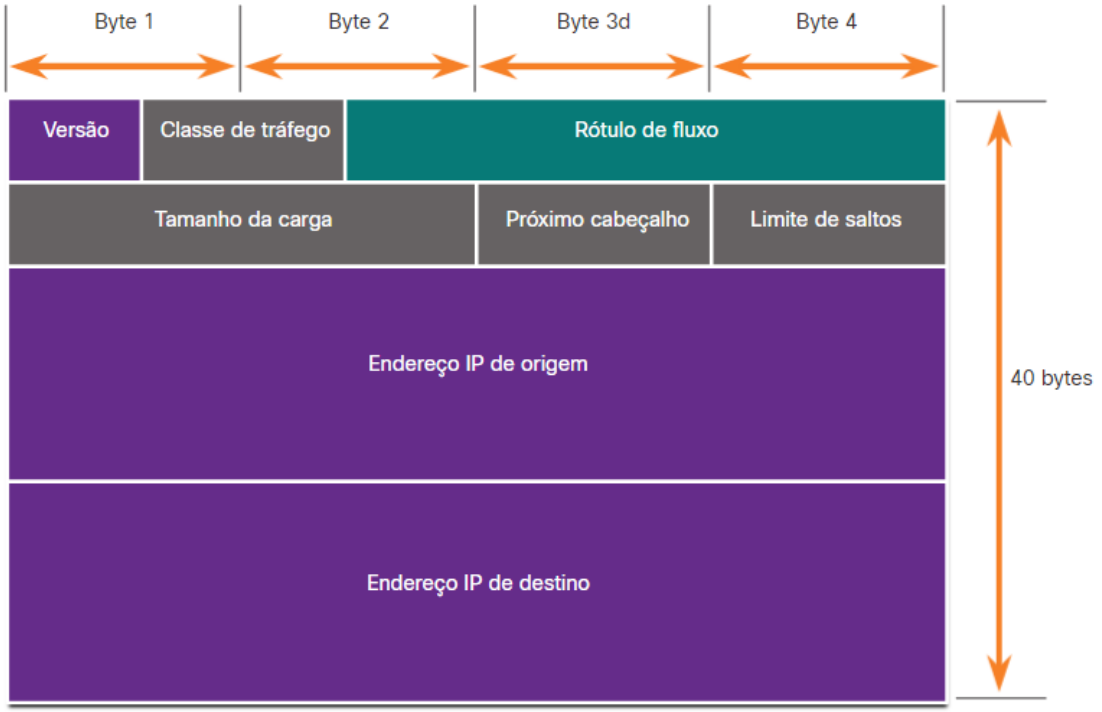
Fonte: Cisco

Formatação e encapsulamento da mensagem



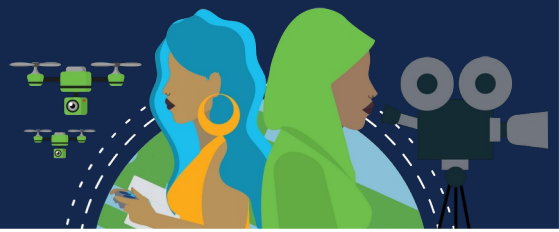
- Quando uma mensagem é enviada, ela deve usar um formato ou estrutura específica.
- Os formatos da mensagem dependem do tipo de mensagem e do canal usado para entregá-la.





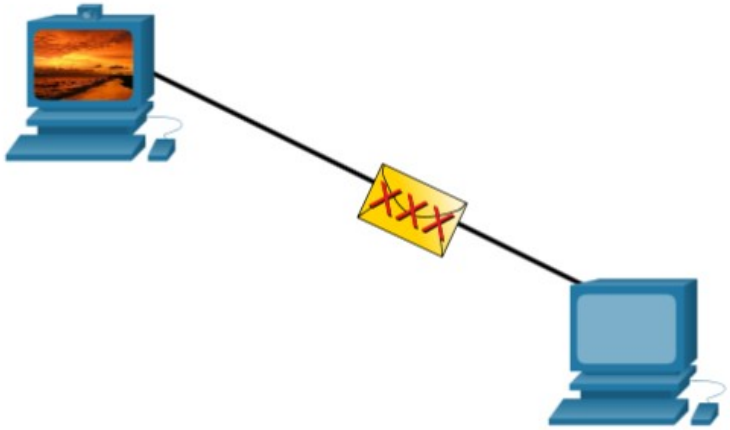
Fonte: Cisco

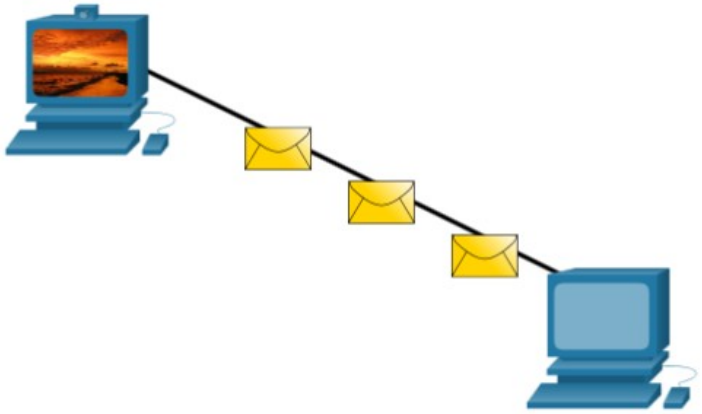
Tamanho da mensagem



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

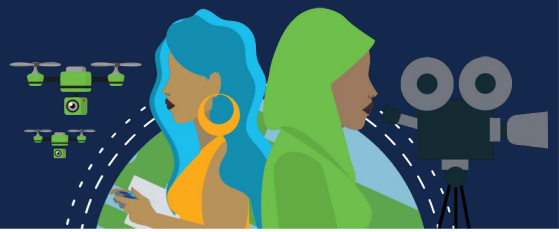
- As mensagens enviadas pela rede são convertidas em bits
- Os bits são codificados em um padrão de luz, som ou impulsos elétricos.
- O host de destino deve decodificar os sinais para interpretar a mensagem.





Fonte: Cisco

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.

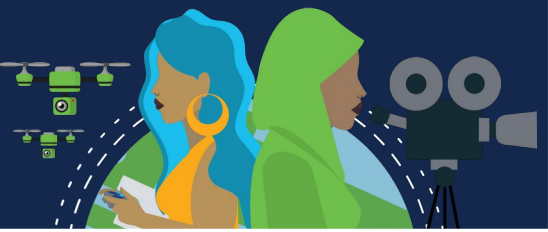
Tempo limite de resposta — gerencia o tempo que um dispositivo espera quando não ouve uma resposta do destino.

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.

Fonte: Cisco

Opções de entrega da mensagem



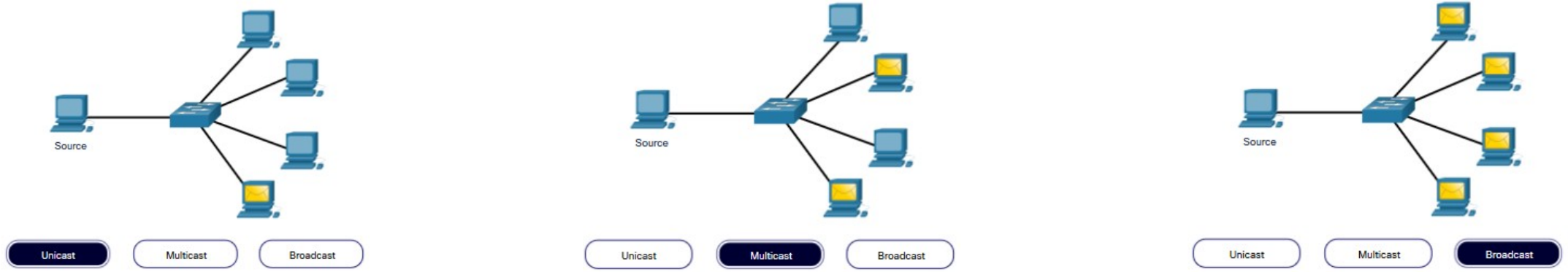
A entrega de mensagens pode ser um dos seguintes métodos:

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.



Fonte: Cisco

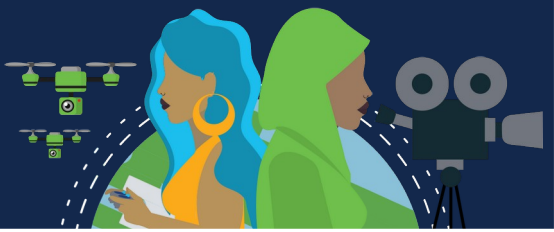
WOMENROCK-IT

Brasil 2021

Networking Academy

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

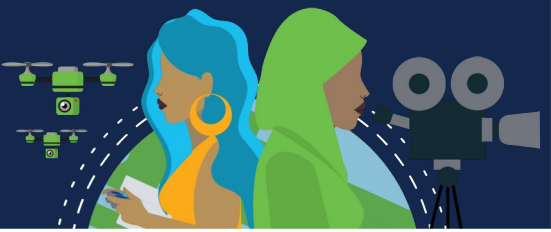
Cada protocolo tem sua própria:

- 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

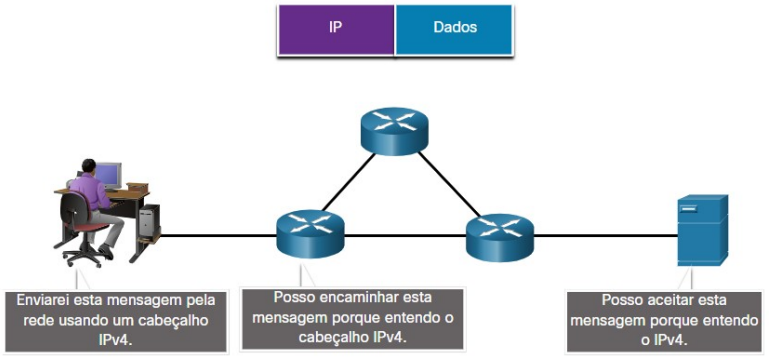
Fonte: Cisco

Funções de protocolo de rede



- Os dispositivos usam protocolos acordados para se comunicar.

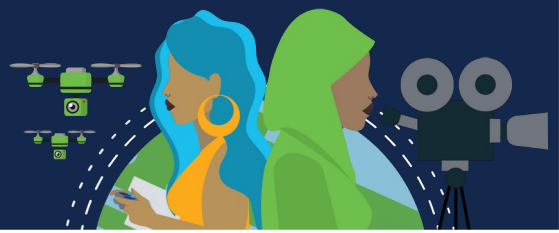
- Protocolos podem ter uma ou mais funções.



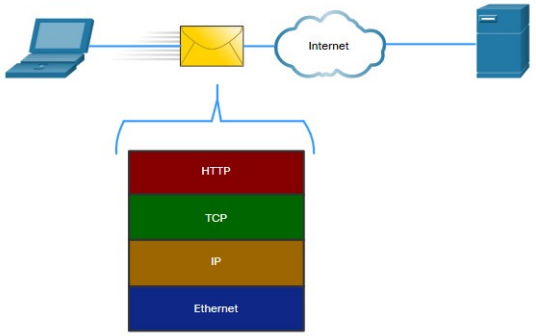
Função	Descrição
Endereçamento	Identificação de remetente e destinatário
Confiabilidade	Fornece entrega garantida
Controle de fluxo	Garante fluxos de dados a uma taxaeficiente
Sequenciamento	Rotula exclusivamente cada segmento de dados transmitido
Detecção de erros	Determina se os dados ficaram corrompidos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

Fonte: Cisco

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

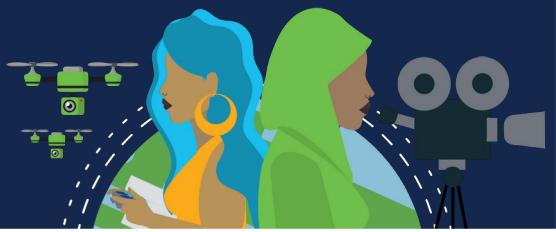
Fonte: Cisco

WOMENROCK-IT
Brasil 2021

Networking Academy

CONJUNTO DE PROTOCOLOS

Conjuntos de protocolos de rede



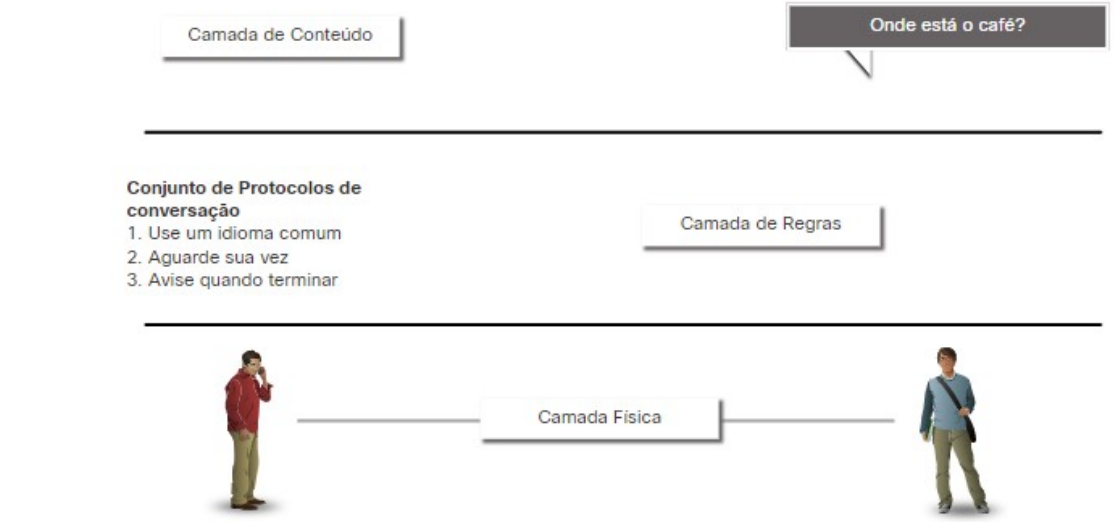
Os protocolos devem ser capazes de funcionar com outros protocolos.

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

Os protocolos são visualizados em termos de camadas:

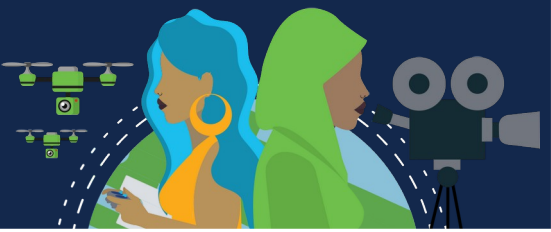
- Camadas Superiores – preocupam com o conteúdo da mensagem
- Camadas Inferiores - preocupado com a movimentação de dados e fornecer serviços para camadas superiores



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

Fonte: Cisco

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.

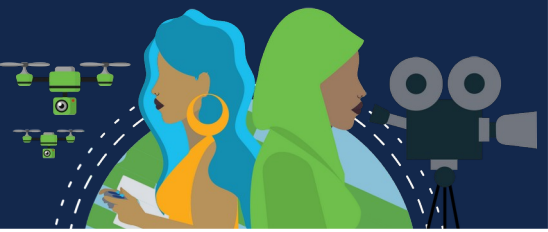
- **Novell NetWare**

- Suíte proprietária desenvolvida pela Novell Inc.

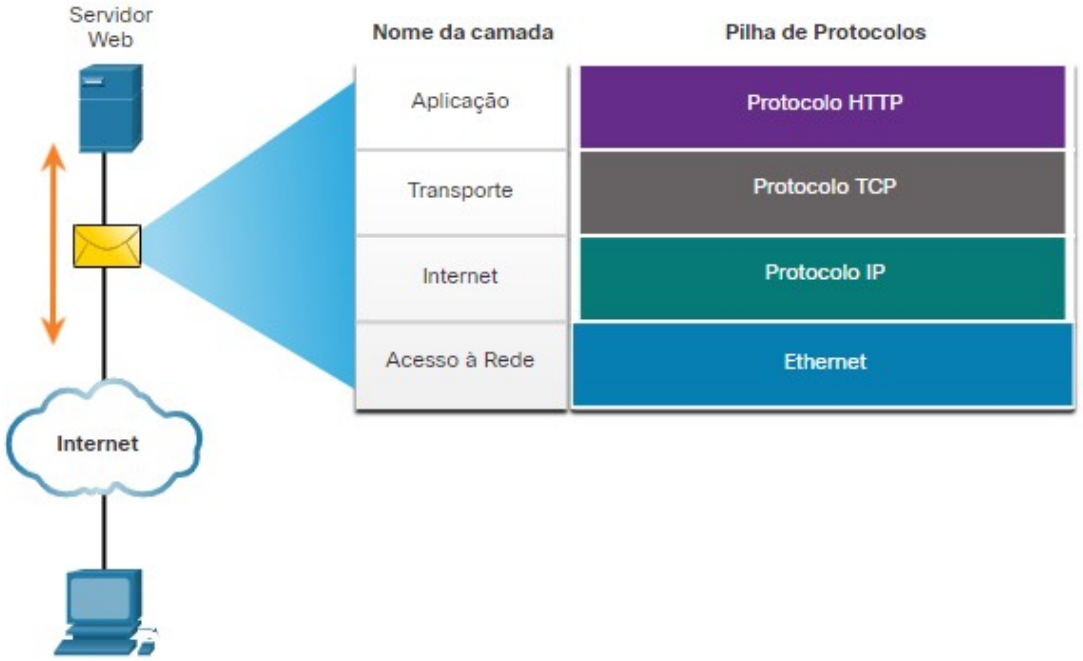
Nome da camada TCP/IP	TCP/IP	ISO	AppleTalk	Novell Netware
Aplicação	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
Transporte	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Acesso à Rede	WLAN Ethernet ARP			

Fonte: Cisco

Exemplo de protocolo TCP / IP

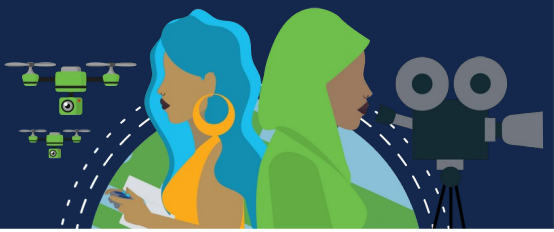


- Os protocolos TCP / IP operam nas camadas de aplicação, transporte e Internet.
- Os protocolos LAN de camada de acesso à rede mais comuns são Ethernet e WLAN (LAN sem fio).

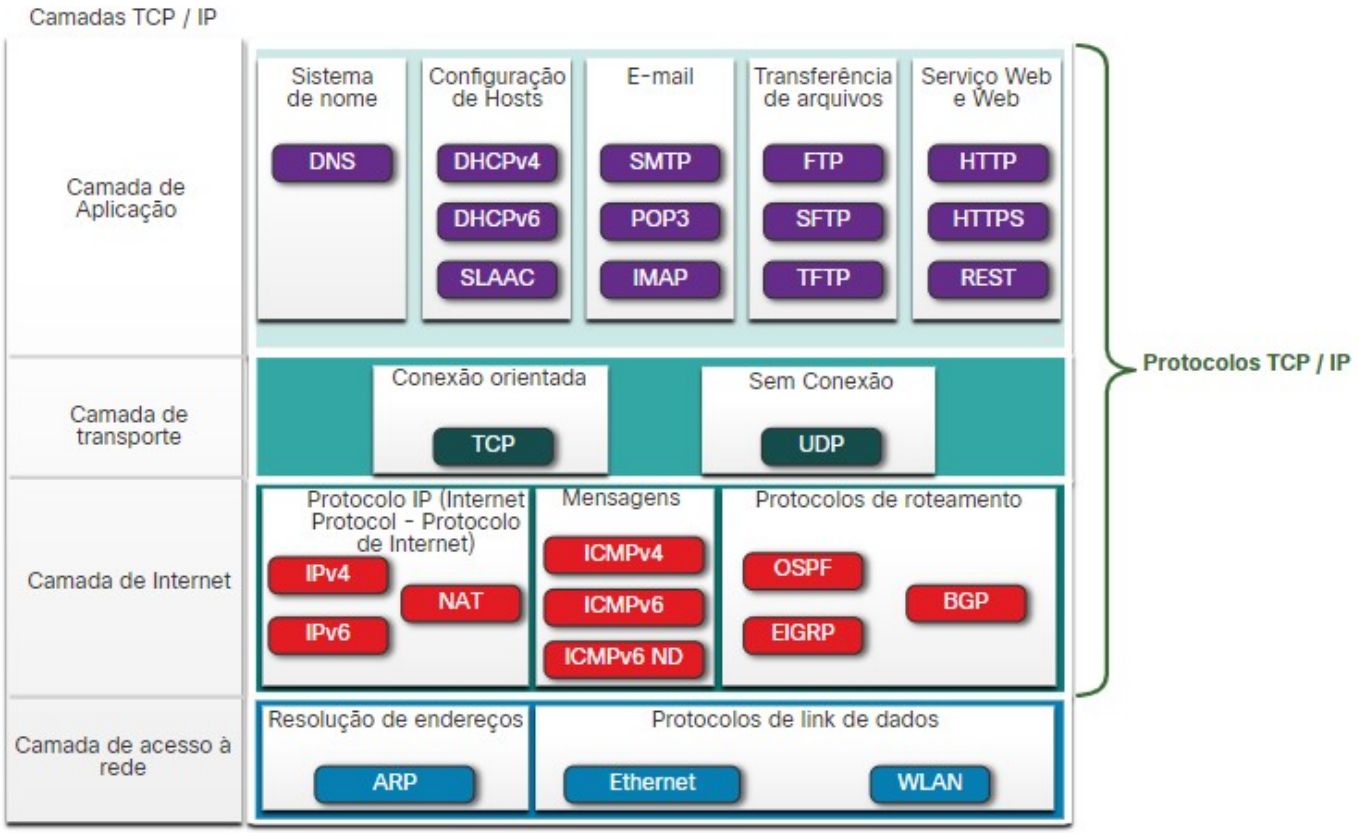


Fonte: Cisco

Suíte de Protocolos TCP/IP

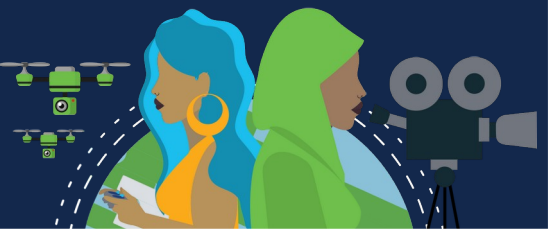


- TCP/IP é o conjunto de protocolos usado pela internet e inclui muitos protocolos.
- **O TCP/IP é:**
  - Um conjunto de protocolos padrão aberto que está disponível gratuitamente para o público e pode ser usado por qualquer fornecedor
  - Um conjunto de protocolos baseado em padrões que é endossado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

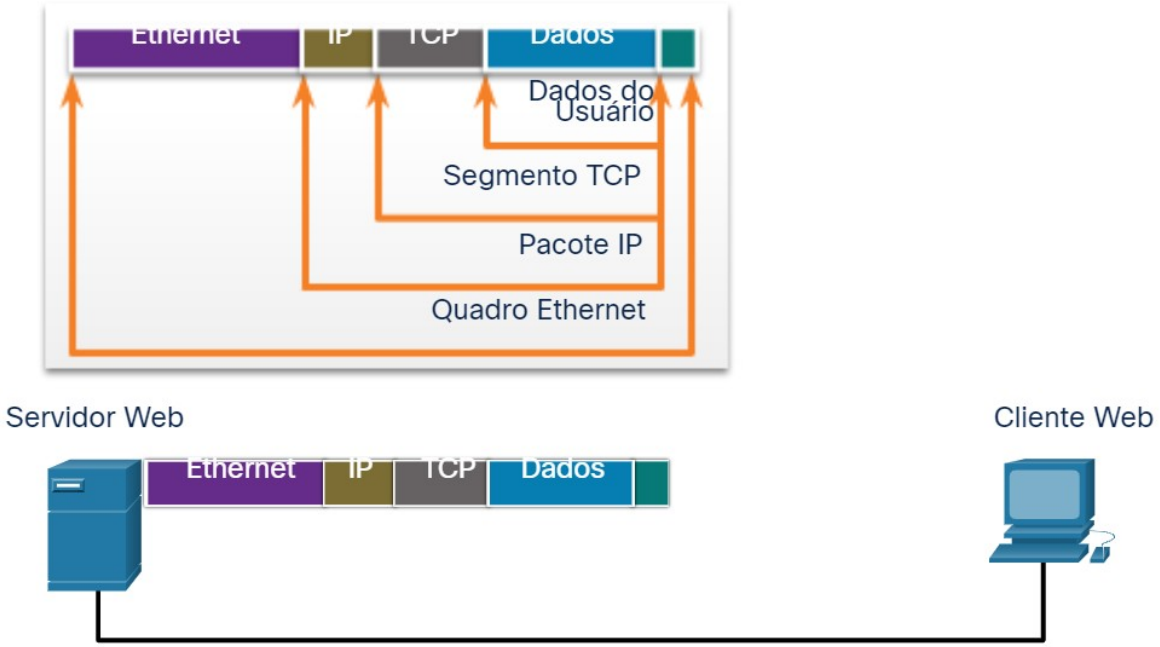


Fonte: Cisco

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



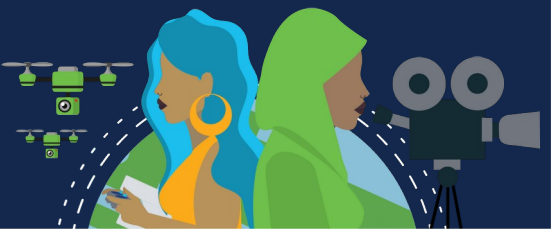
Fonte: Cisco

WOMENROCK-IT
Brasil 2021

Networking Academy

EMPRESAS DE PADRÕES

Padrões abertos



As normas abertas incentivam:

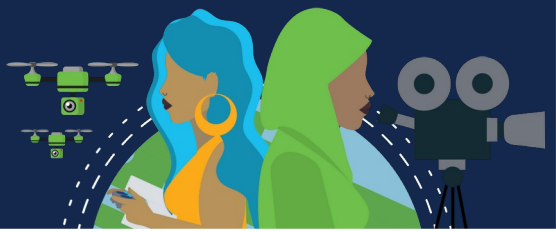
- interoperabilidade
- concorrência
- negócios

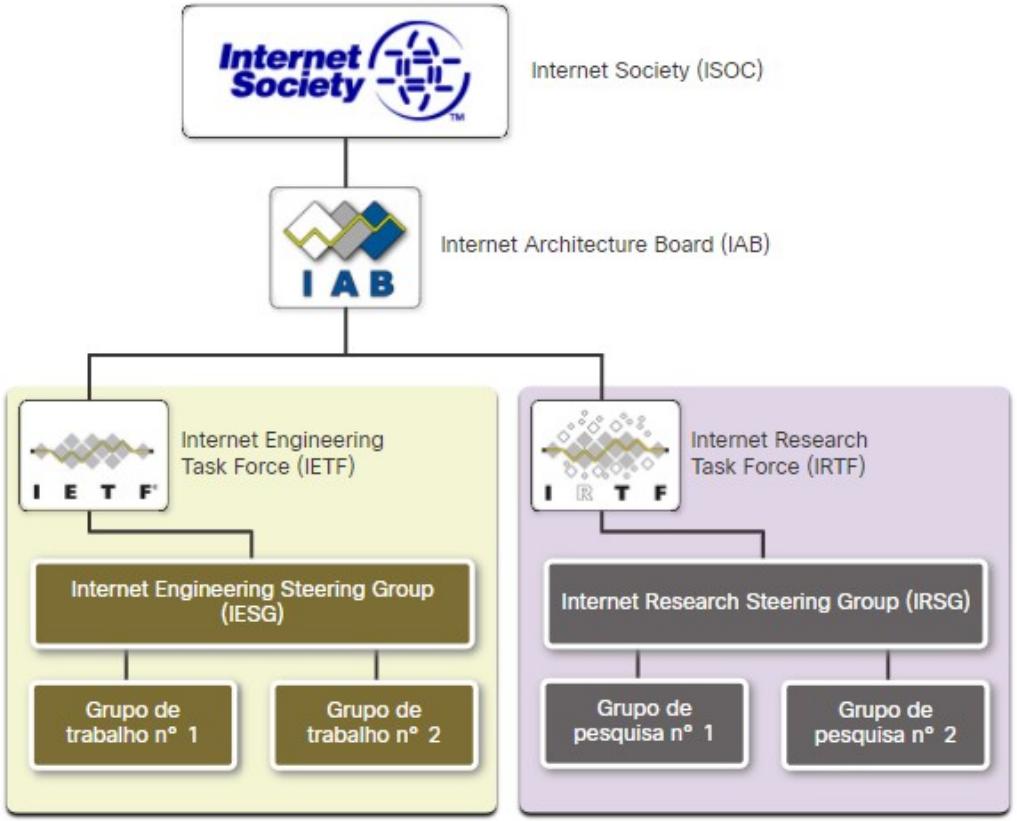
As organizações de padrões são:

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

Fonte: Cisco

Padrões de Internet

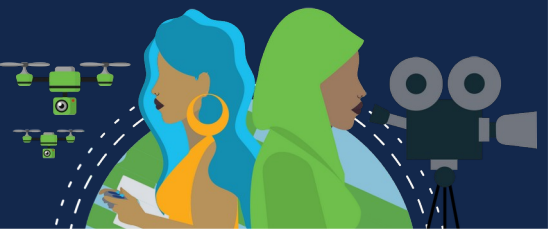


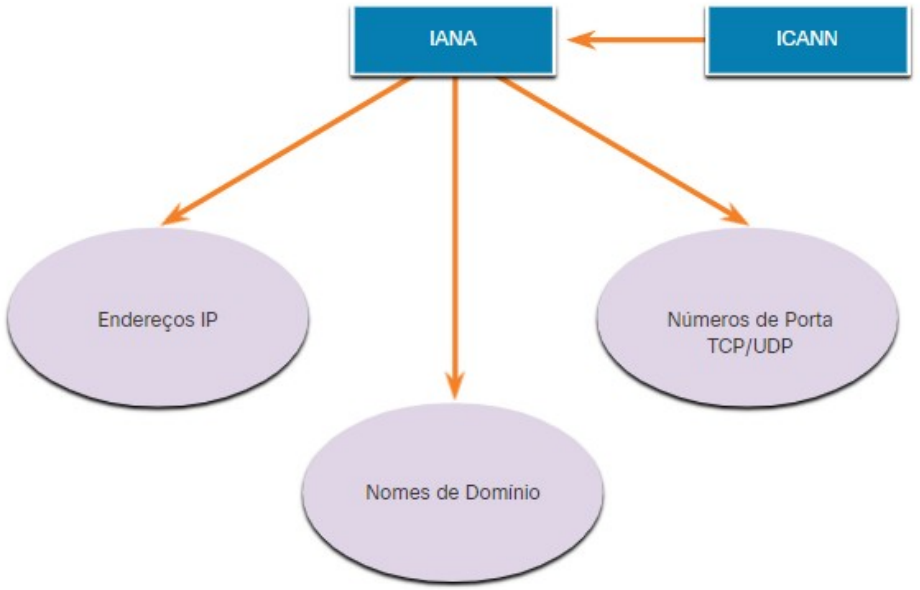


- **Internet Society (ISOC)** - Promove o desenvolvimento aberto e a evolução da Internet
- **Conselho de Arquitetura da Internet (IAB)** - Responsável pelo gerenciamento e desenvolvimento geral dos padrões da Internet.
- **IETF (Internet Engineering Task Force)** - Desenvolve, atualiza e mantém tecnologias 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

Fonte: Cisco

Padrões de Internet



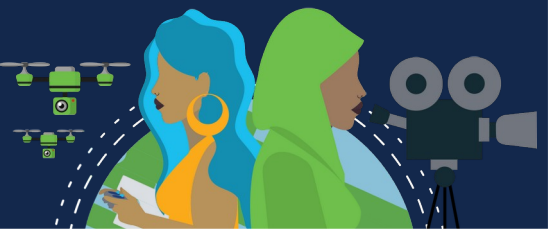


Organizações de padrões envolvidas no desenvolvimento e suporte de TCP / IP

- **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

Fonte: Cisco

Padrões eletrônicos e de comunicações



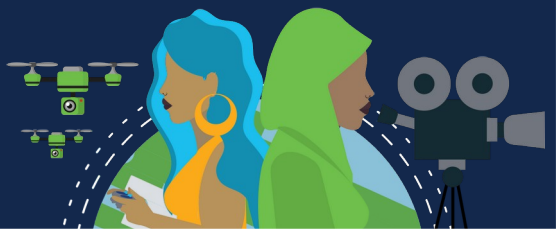
- **Instituto de Engenheiros Elétricos e Eletrônicos (IEEE**, pronunciado "I-triple-E") - dedicado à criação de padrões em potência e energia, saúde, telecomunicações e redes
- **Electronic Industries Alliance (EIA)** - desenvolve padrões relacionados à fiação elétrica, conectores e racks de 19 polegadas 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)

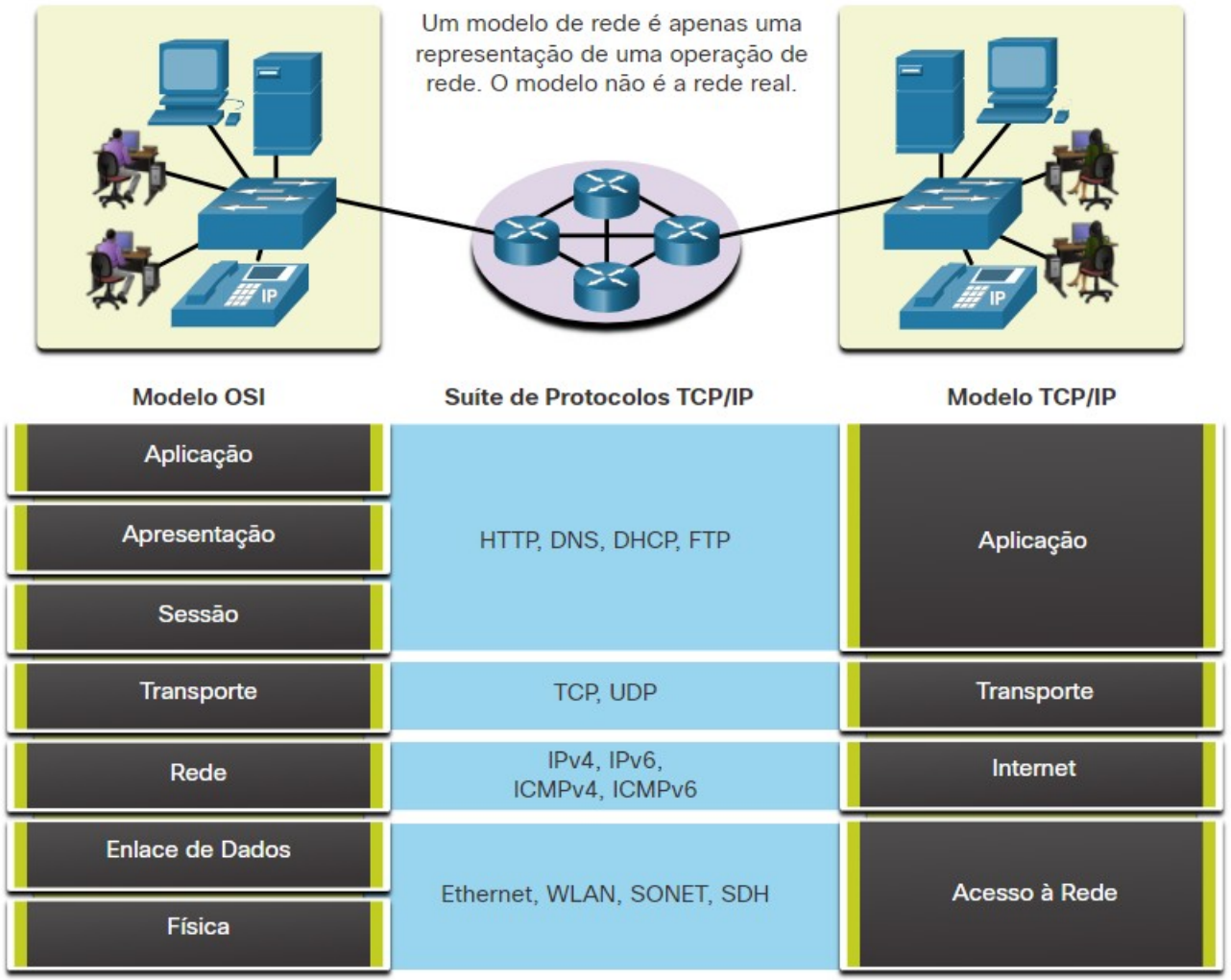
WOMENROCK-IT
Brasil 2021

Networking Academy
CISCO

MODELOS DE REFERÊNCIA

Benefícios de se usar um modelo de camadas





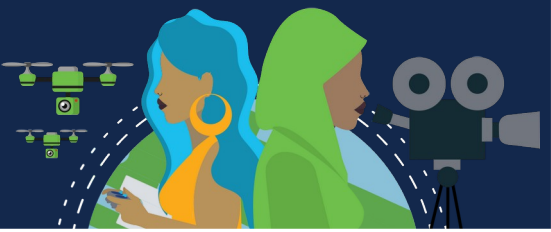
Conceitos complexos, como a forma como uma rede opera, podem ser difíceis de explicar e compreender. Por esse motivo, um modelo em camadas é usado.

Dois modelos em camadas descrevem as operações de rede:

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

Fonte: Cisco

Benefícios de se usar um modelo de camadas

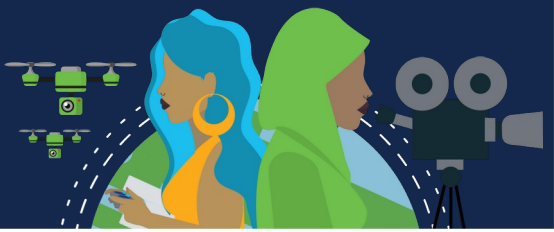


Estes são os benefícios do uso de um modelo em camadas:

- 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.

Fonte: Cisco

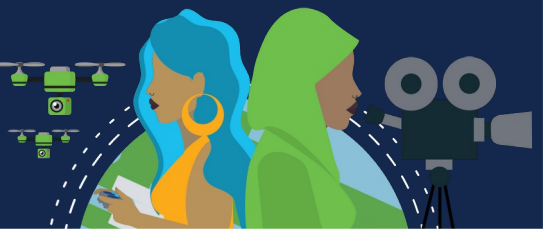
O modelo de referência OSI



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.

Fonte: Cisco

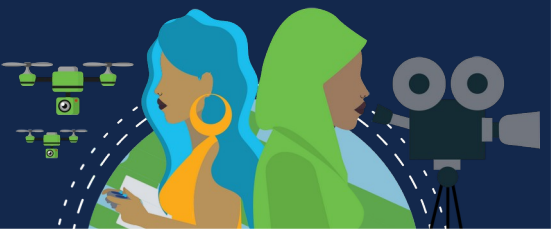
O modelo de referência TCP / IP

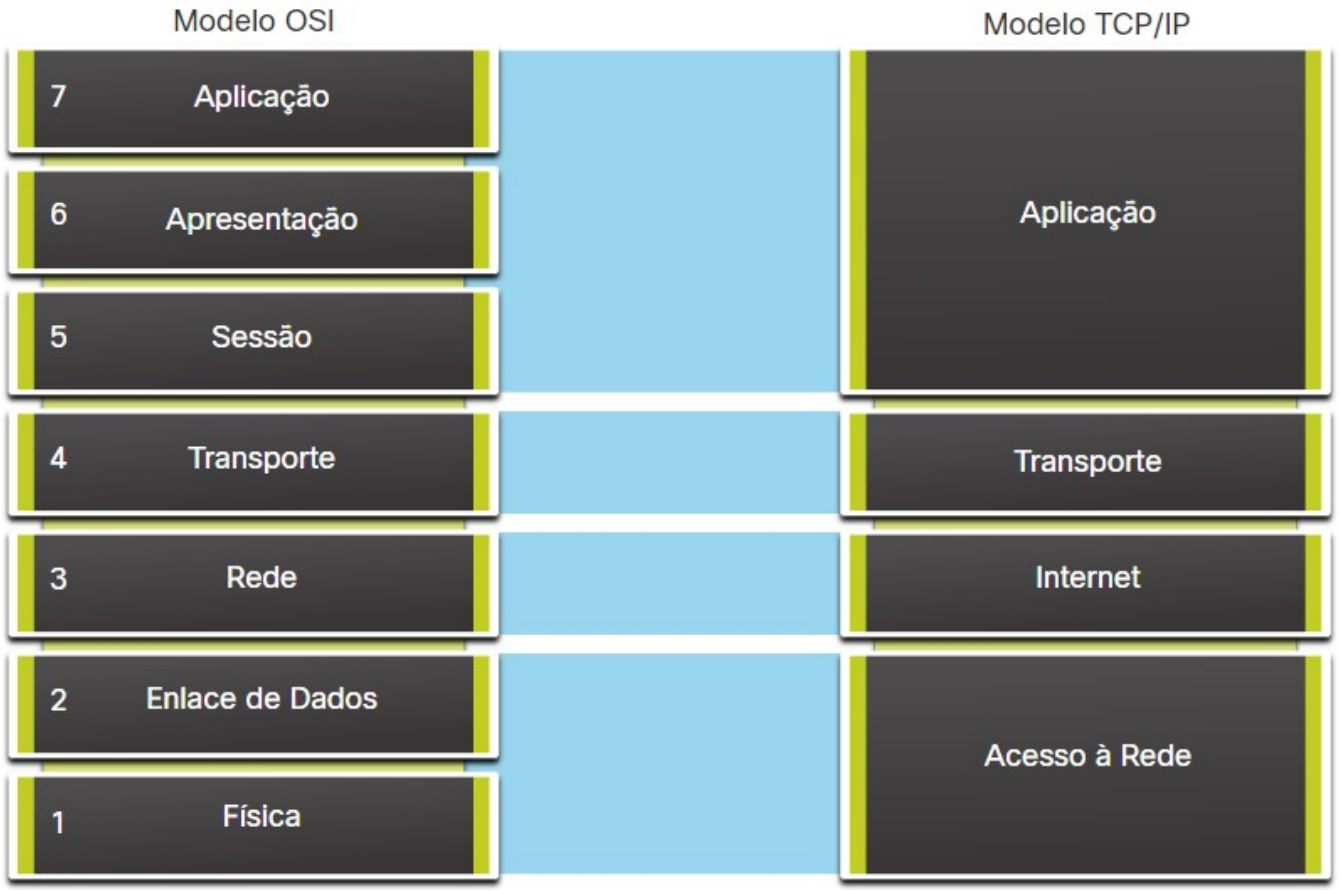


Camada do modelo TCP/IP	Descrição
Aplicação	Representa dados para o usuário, além do controle de codificação e de diálogo.
Transporte	Permite a comunicação entre vários dispositivos diferentes em redes distintas.
Internet	Determina o melhor caminho pela rede.
Endereço de rede	Controla os dispositivos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

Fonte: Cisco

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.

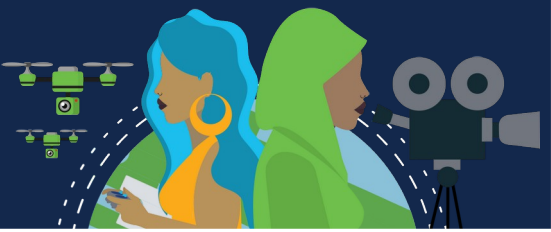
Fonte: Cisco

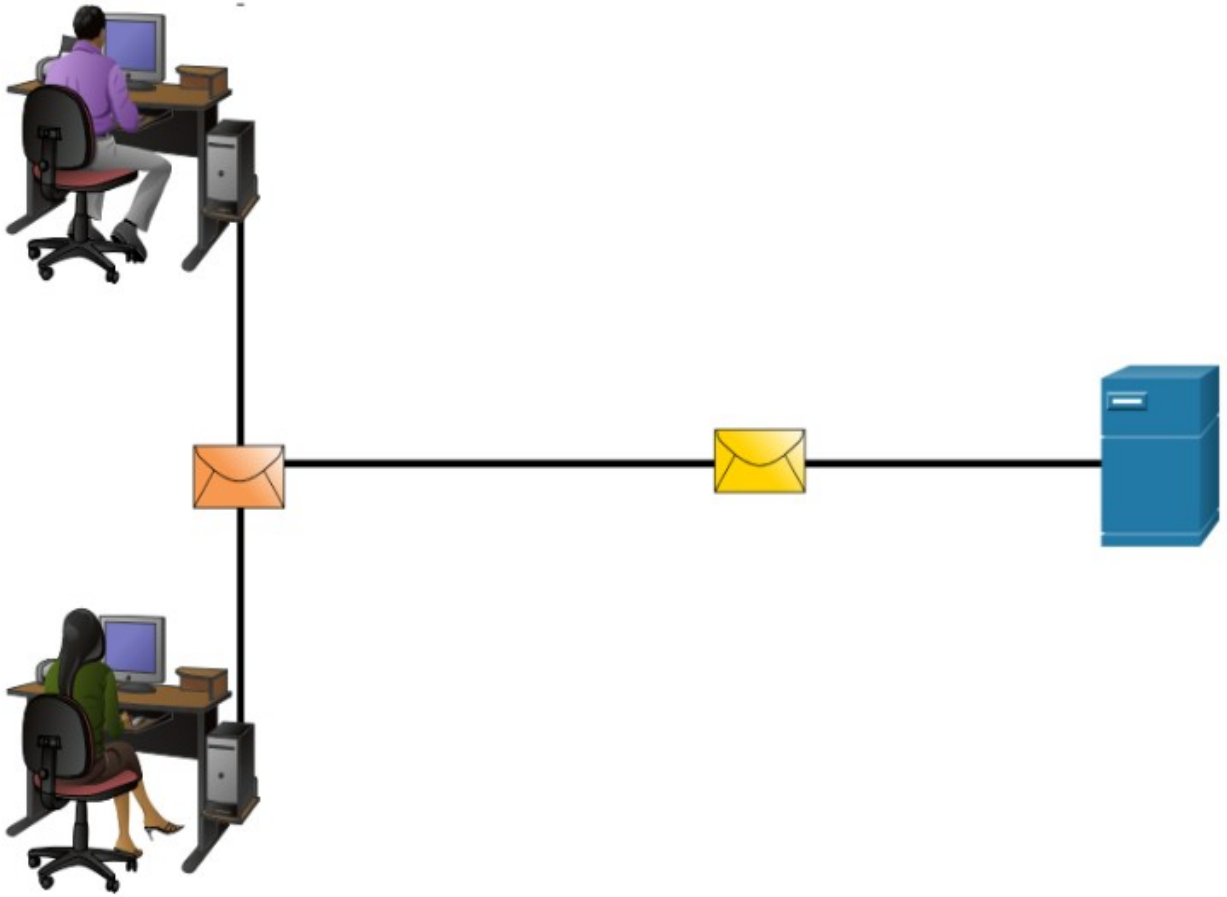
WOMENROCK-IT
Brasil 2021

Networking Academy

ENCAPSULAMENTO DE DADOS

Segmentação de mensagens





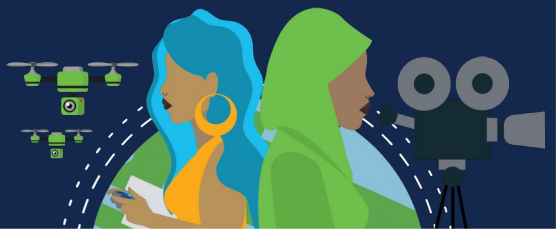
Segmentação é o processo de dividir mensagens em unidades menores. Multiplexação é o processo de tomar vários fluxos de dados segmentados e intercalá-los juntos.

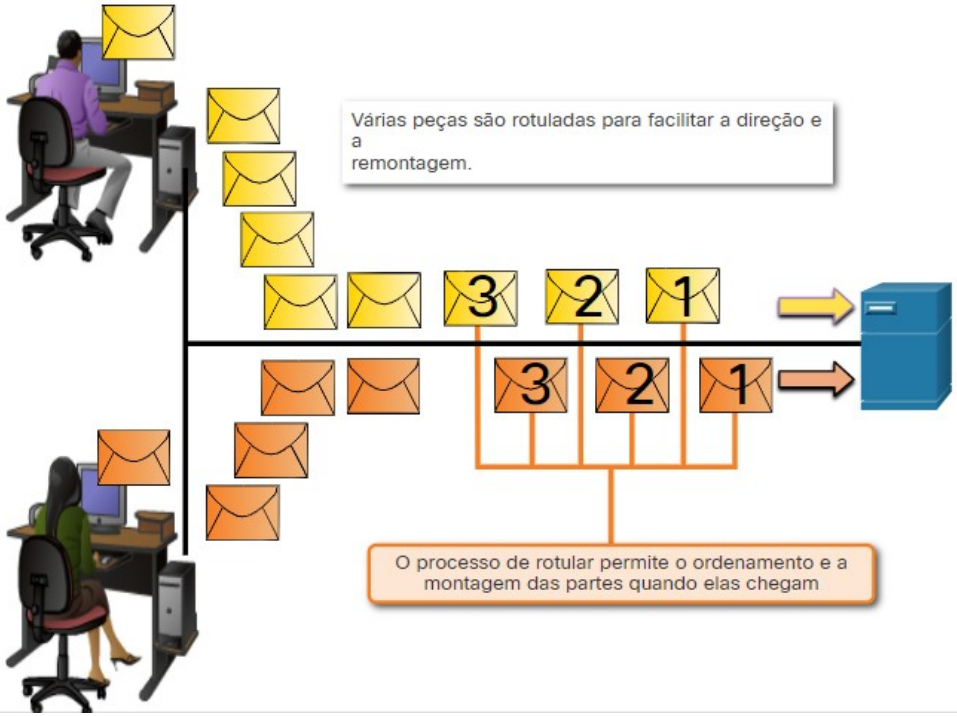
A segmentação de mensagens apresenta dois benefícios principais:

- **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.

Fonte: Cisco

Sequenciamento



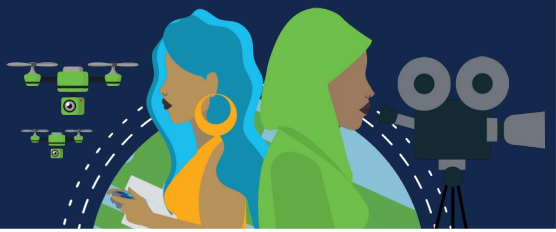


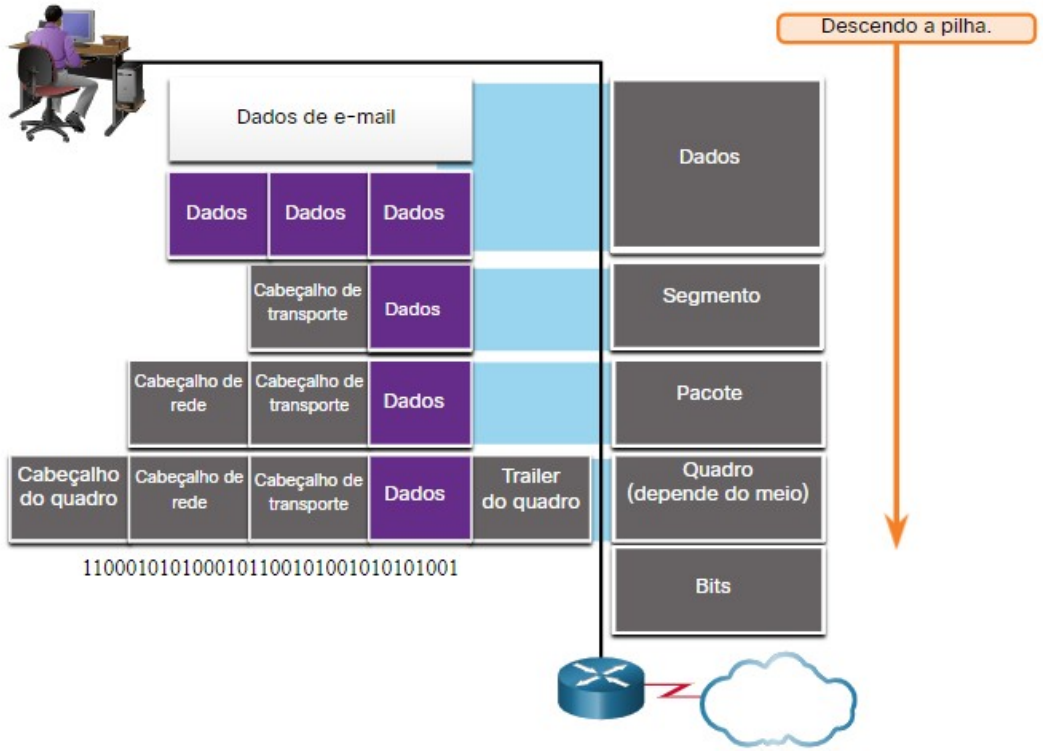
Mensagens de sequenciamento é o processo de numeração dos segmentos para que a mensagem possa ser remontada no destino.

O TCP é responsável por sequenciar os segmentos individuais.

Fonte: Cisco

Unidades de dados de protocolo





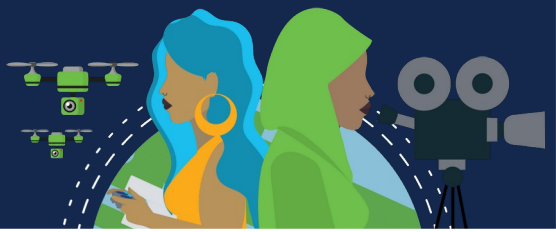
Encapsulamento é o processo em que os protocolos adicionam suas informações aos dados.

- 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)

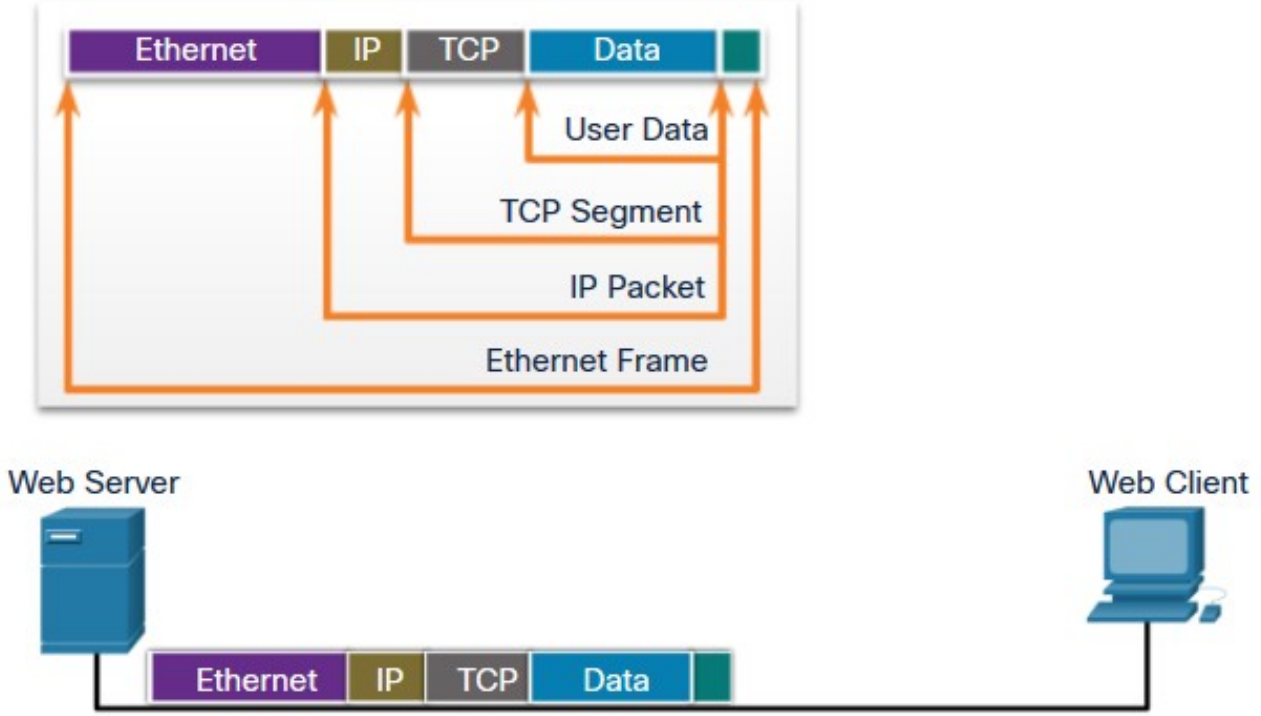
Fonte: Cisco

Exemplo de encapsulamento



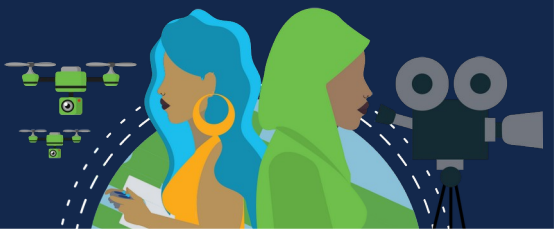
- O encapsulamento é um processo de cima para baixo.
- O nível acima faz o seu processo e, em seguida, passa-o para o próximo nível do modelo.

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

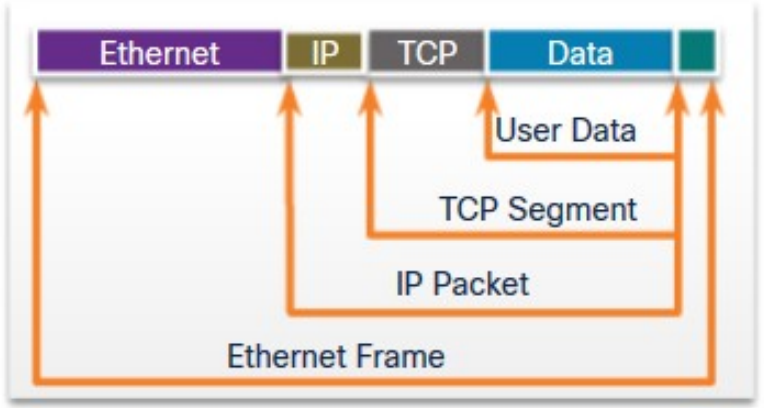


Fonte: Cisco

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)



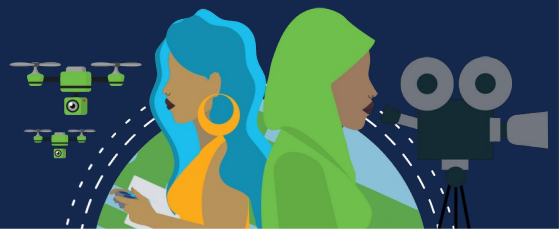
Fonte: Cisco

WOMENROCK-IT
Brasil 2021

Networking Academy

ACESSO AOS DADOS

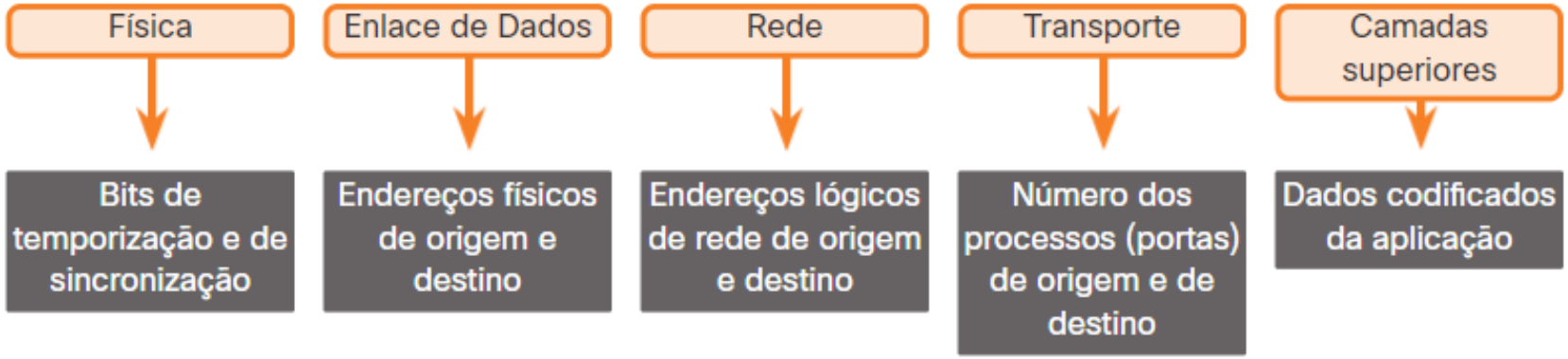
Endereços



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

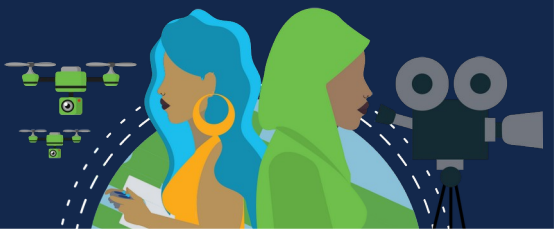
Endereços origem e destino da camada de rede - Responsáveis por entregar o pacote IP da origem para o destino final.

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.



Fonte: Cisco

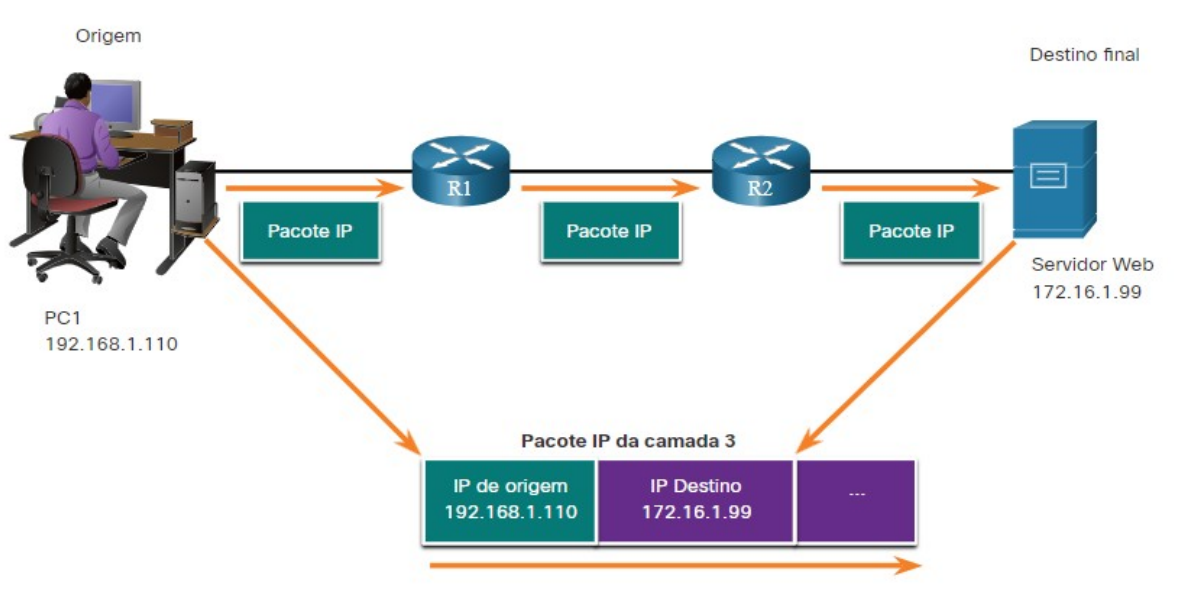
Endereço Lógico da Camada 3



O pacote IP contém dois endereços IP:

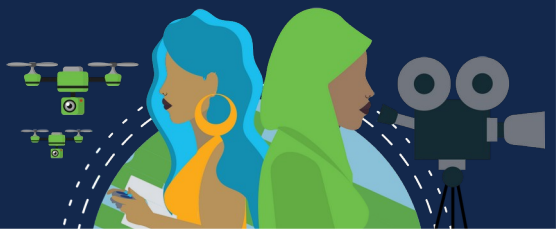
- **Endereço IP origem** - O endereço IP do dispositivo emissor, a origem do pacote.
- **Endereço IP de destino** - O endereço IP do dispositivo receptor, o destino final do pacote.

Esses endereços podem estar no mesmo link ou remoto.



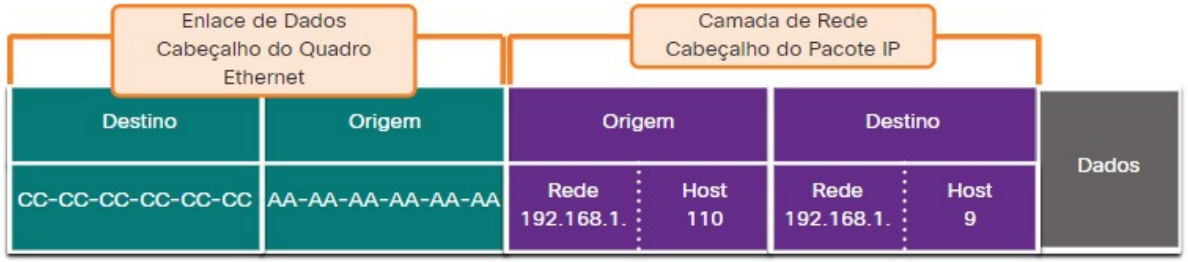
Fonte: Cisco

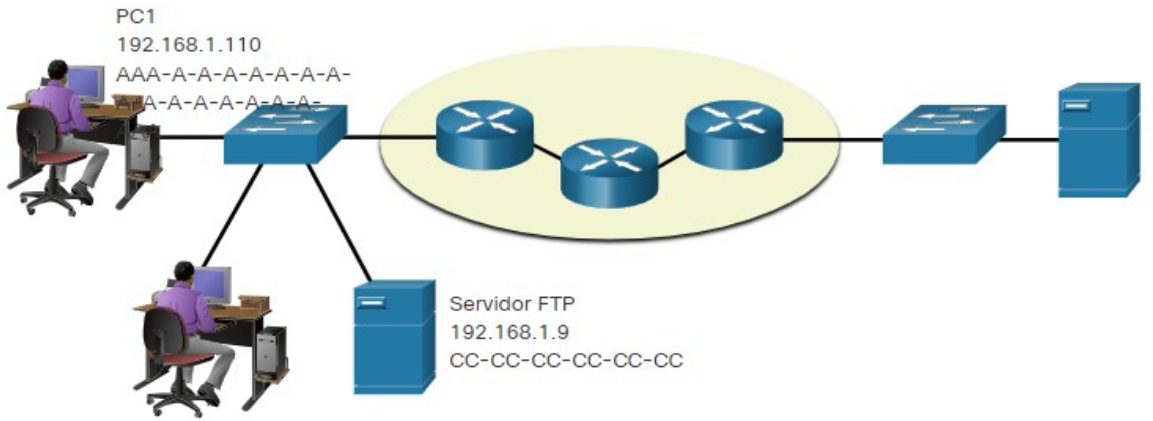
Dispositivos na mesma rede



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

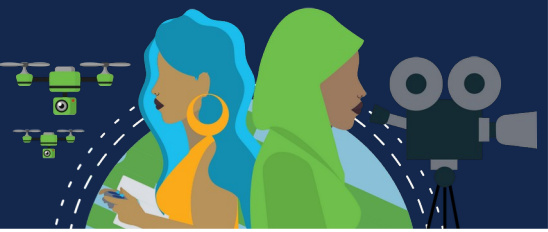
- PC1 — 192.168.1.110
- Servidor FTP — 192.168.1.9





Fonte: Cisco

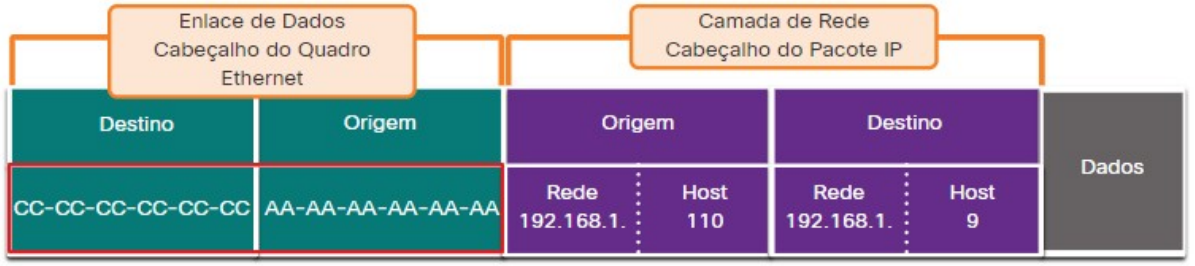
Função de Acesso a Dados dos Endereços da Camada de Link de Dados: Mesma Rede IP

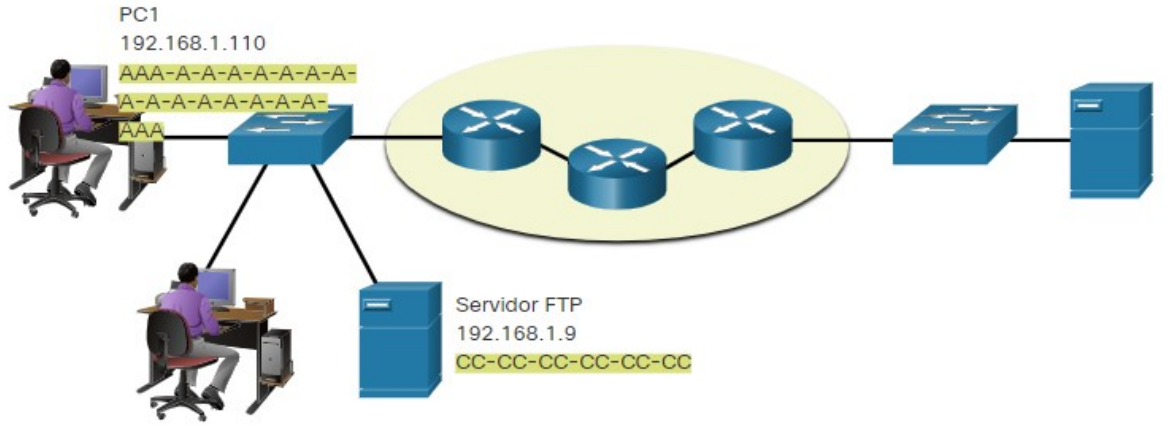


Quando os dispositivos estiverem na mesma rede Ethernet, o quadro do link de dados usará o endereço MAC real da NIC de destino.

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

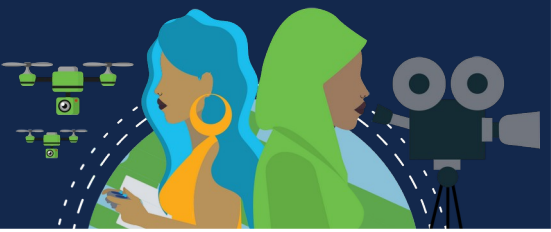
- O endereço MAC de origem será o do originador no link.
- O endereço MAC de destino estará sempre no mesmo link que a origem, mesmo que o destino final seja remoto.



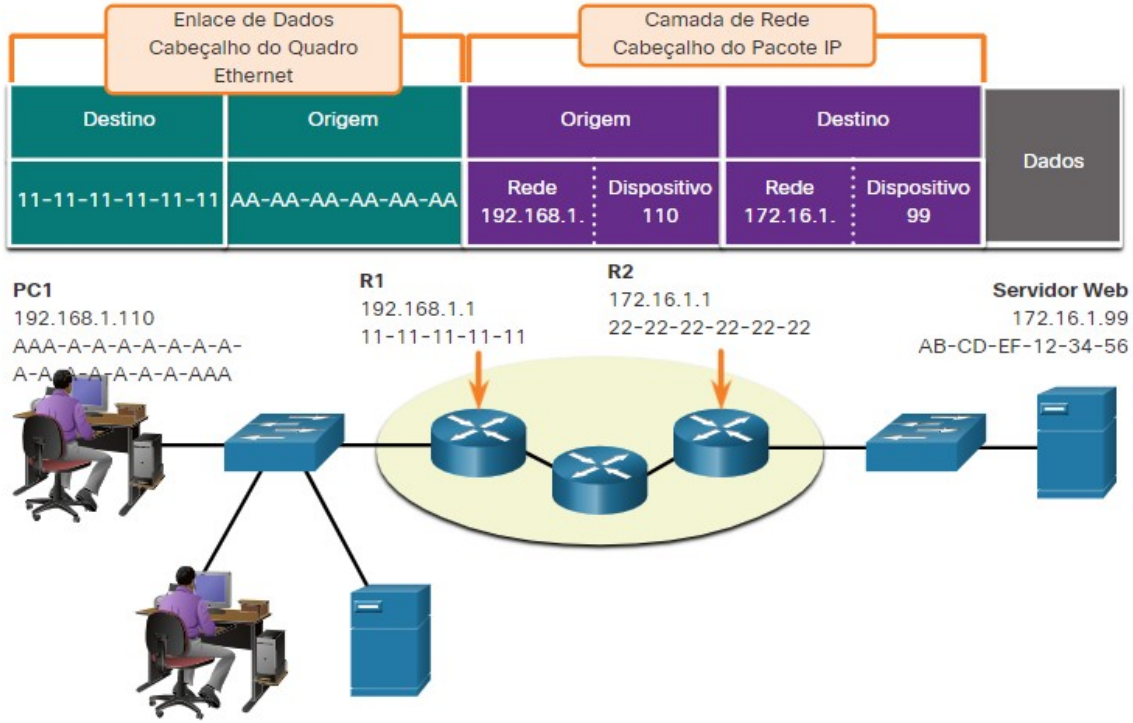


Fonte: Cisco

Dispositivos em uma rede remota

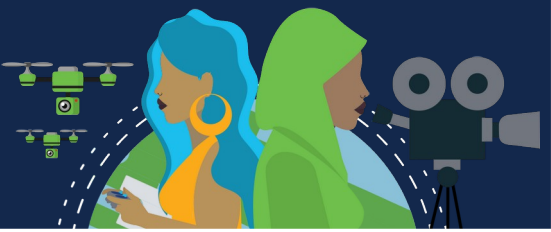


- O que acontece quando o destino real (final) não está na mesma LAN e é remoto?
- O que acontece quando PC1 tenta alcançar o servidor Web?
- Isso afeta as camadas de rede e de link de dados?



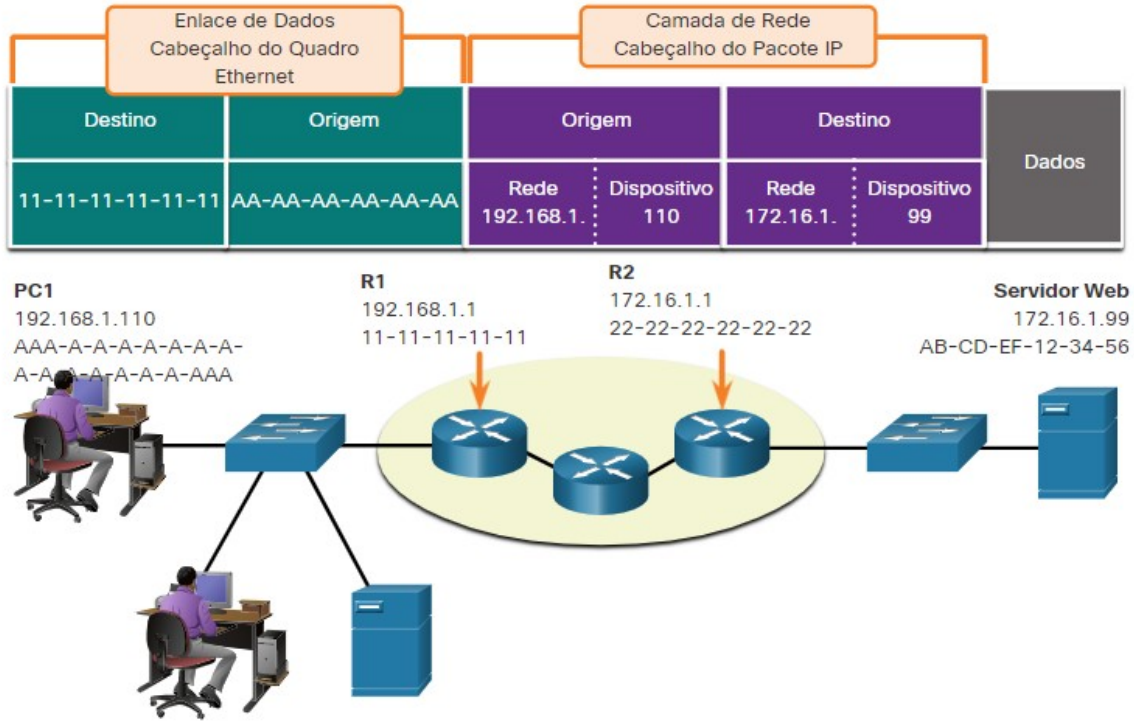
Fonte: Cisco

Função dos endereços da camada de rede



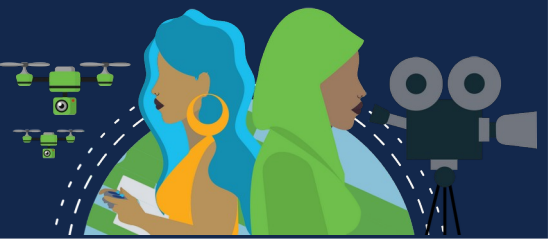
Quando a origem e o destino têm uma parte de rede diferente, isso significa que eles estão em redes diferentes.

- PC1 — 192.168.1
- Servidor Web — 172.16.1



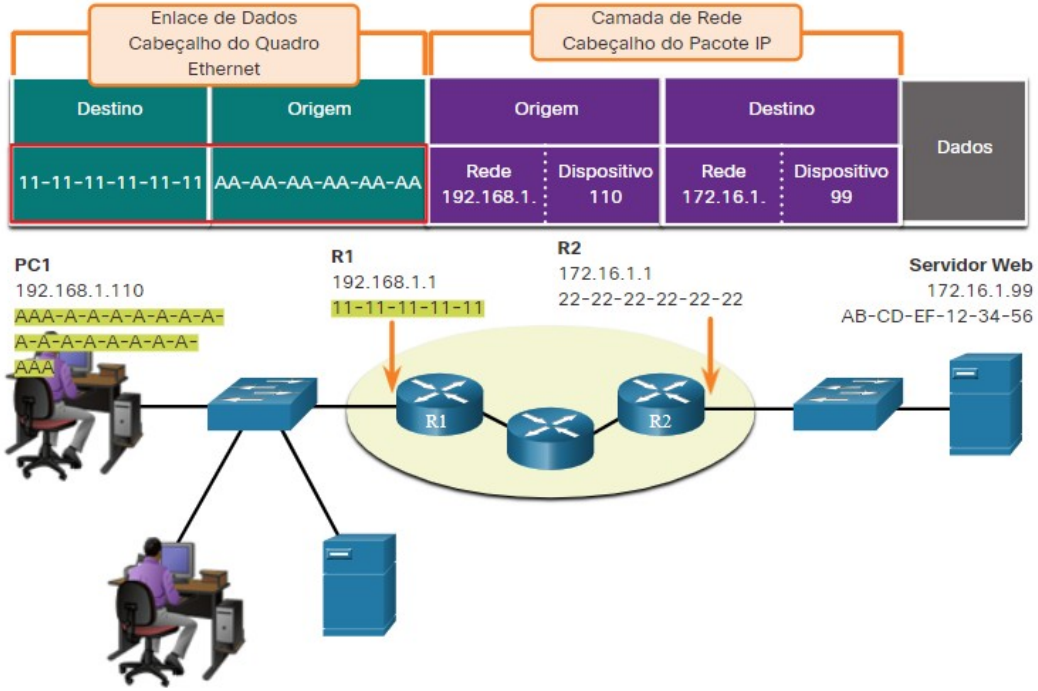
Fonte: Cisco

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



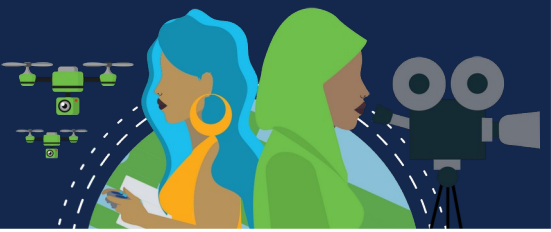
Quando o destino final for remoto, a Camada 3 fornecerá à Camada 2 o endereço IP do gateway padrão local, também conhecido como o endereço do roteador.

- 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.



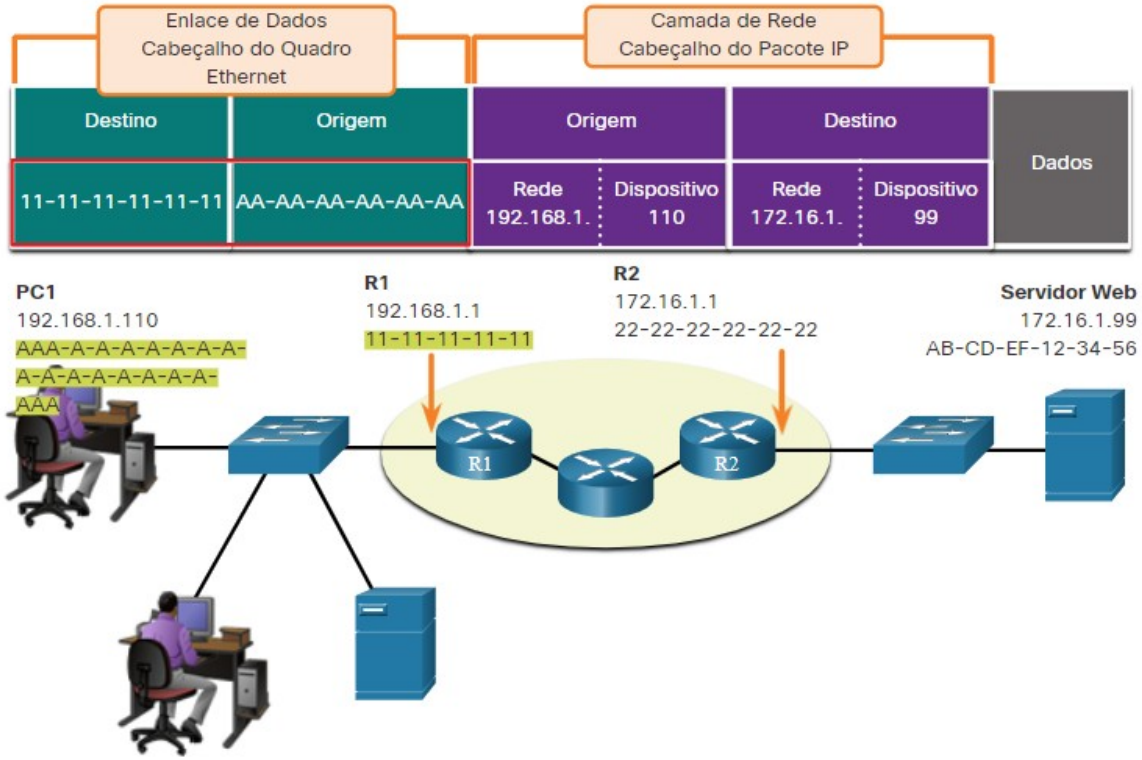
Fonte: Cisco

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



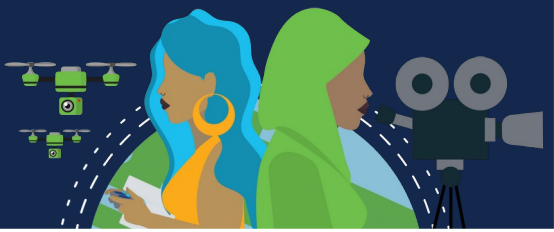
- O endereçamento do link de dados é endereçamento local, portanto, ele terá uma origem e um destino para cada link.
- O endereçamento MAC para o primeiro segmento é:
  - Fonte — AA-AA-AA-AA-AA-AA (PC1) Envia o quadro.
  - Destino — 11-11-11-11-11-11 (R1- MAC de gateway padrão) Recebe o quadro.

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

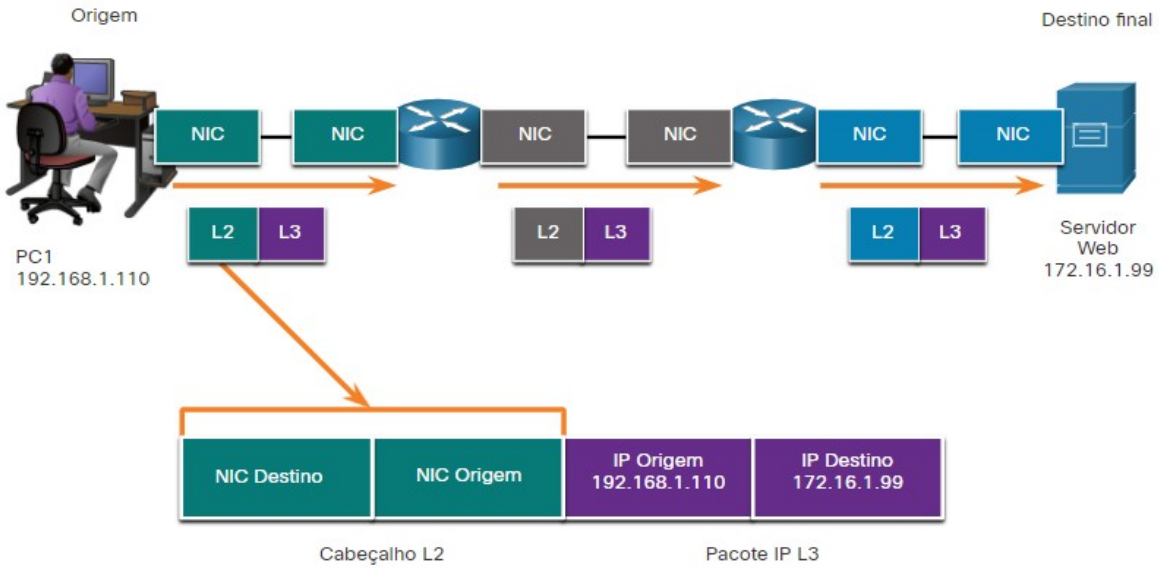


Fonte: Cisco

Endereços de enlace de dados

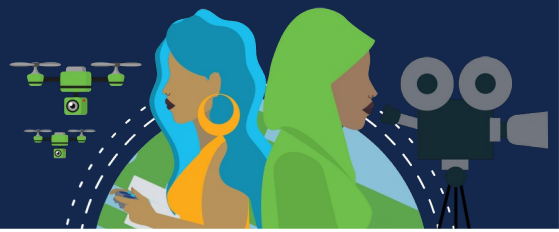


- Como o endereçamento de link de dados é endereçamento local, ele terá uma origem e um destino para cada segmento ou salto da viagem para o destino.
- O endereçamento MAC para o primeiro segmento é:
  - Origem — (NIC PC1) envia quadro
  - Destino — (Primeiro Roteador - Interface DGW) recebe quadro



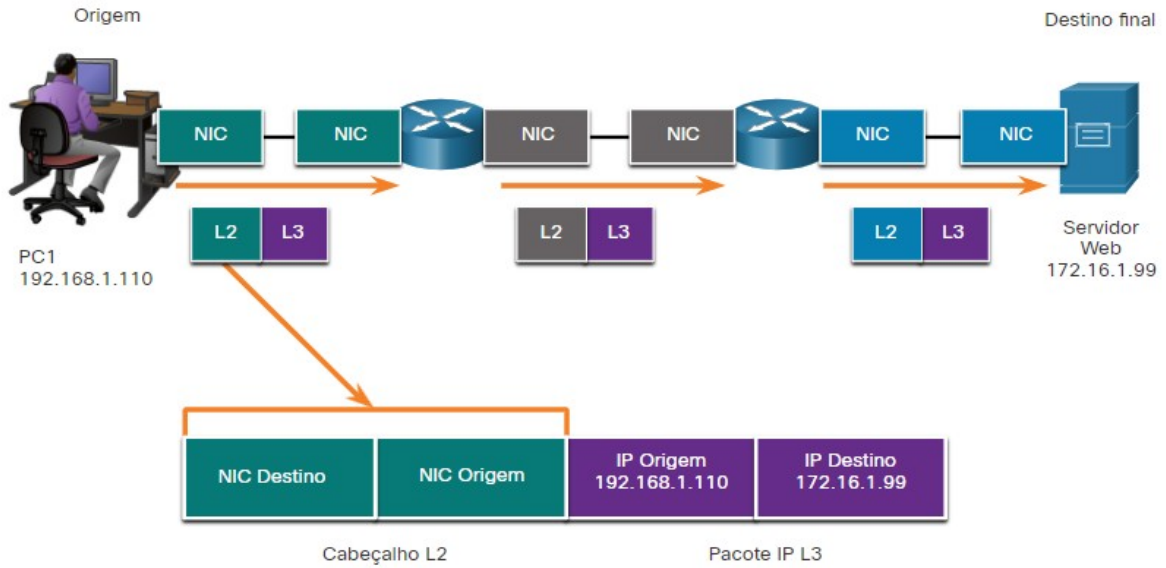
Fonte: Cisco

Endereços de enlace de dados



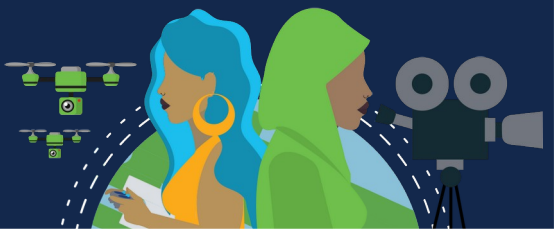
O endereçamento MAC para o segundo salto é:

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



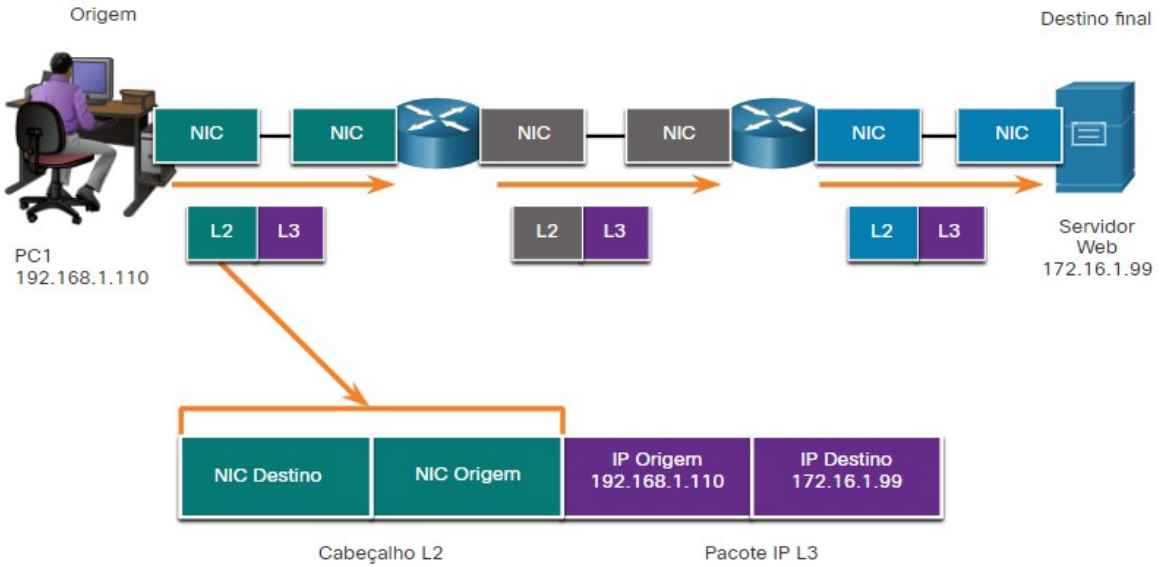
Fonte: Cisco

Endereços de enlace de dados



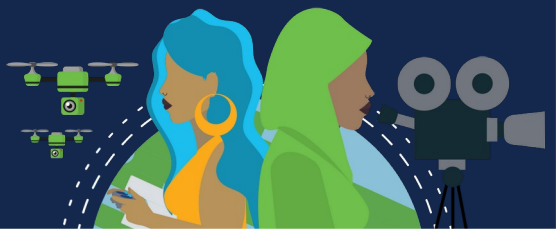
O endereçamento MAC para o último segmento é:

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

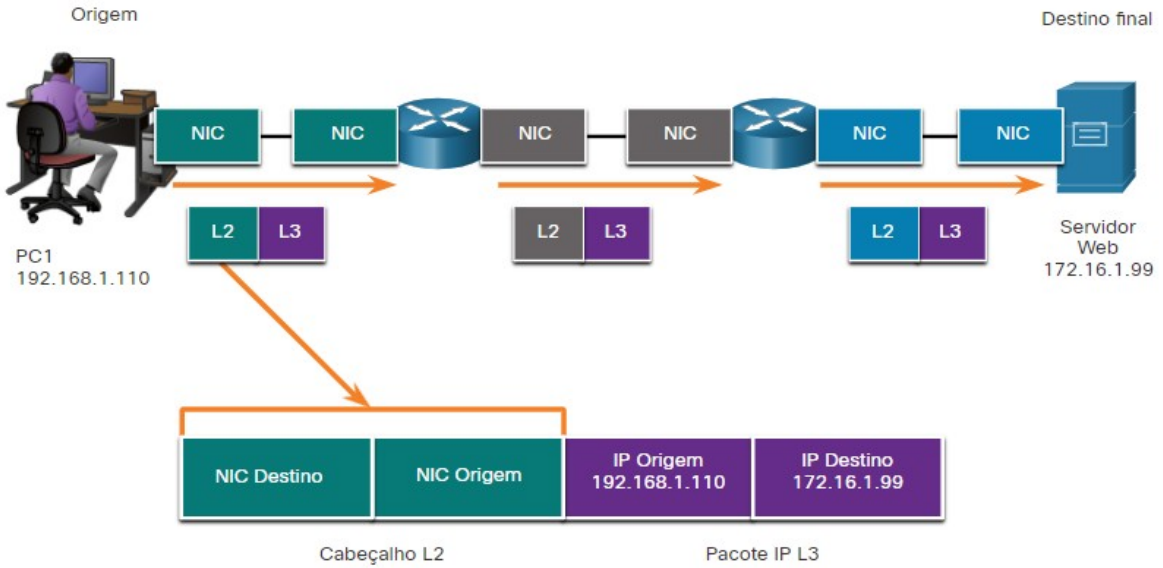


Fonte: Cisco

Endereços de enlace de dados (Cont.)



- 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.



Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

CCNAv7 – ITN – Camada Física

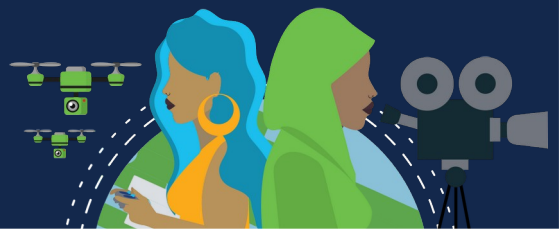
Módulo 4

Embaixadores do Programa 2020, 2021 & 2022:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

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.

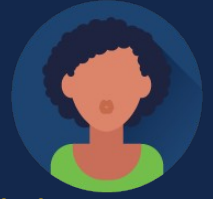
Sem a camada física, você não teria uma rede. Há três maneiras de se conectar à camada física.

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

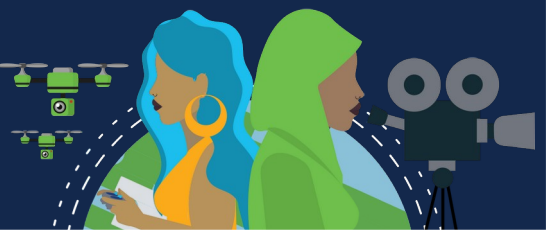
Esse tipo de configuração é uma rede conectada.

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.

Fonte: Cisco



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.

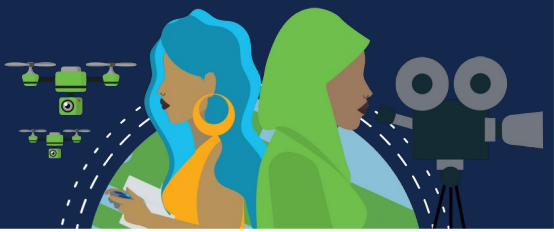
Uma impressora de rede, por exemplo, pode só ter uma NIC Ethernet e, portanto, deve ser conectada à rede com um cabo Ethernet.

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.

Fonte: Cisco

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.

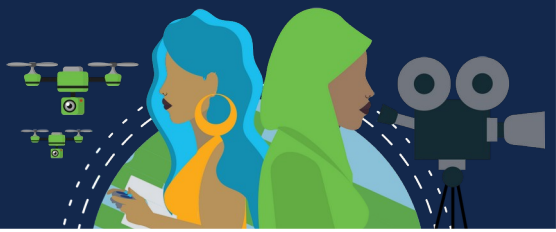
Processo de encapsulamento.

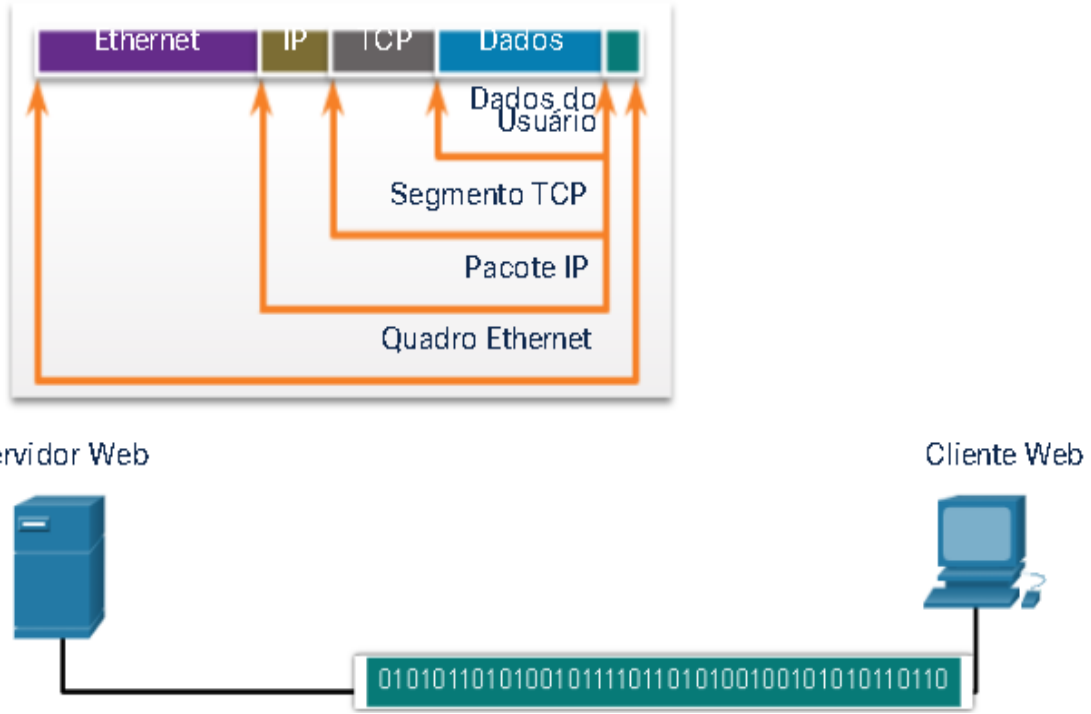
A camada física codifica os quadros e cria os sinais de onda elétrica, óptica ou de rádio que representam os bits em cada quadro. Esses sinais são então enviados pela mídia, um de cada vez. A última parte deste processo mostra os bits que estão sendo enviados através do meio físico.

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.

Fonte: Cisco

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.

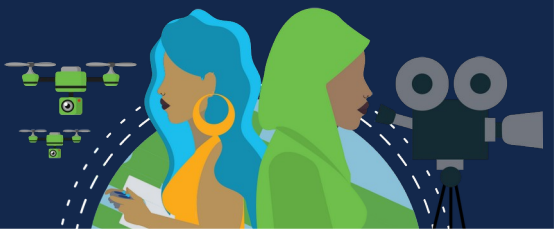
Esses sinais são então enviados pela mídia, um de cada vez.
A última parte deste processo mostra os bits que estão sendo enviados através do meio físico.

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.

Fonte: Cisco

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.

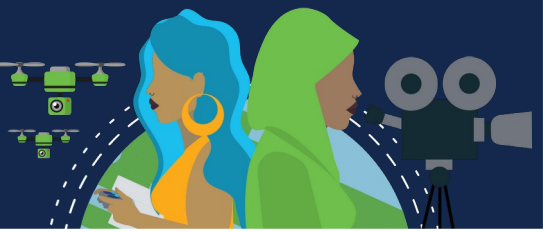
Os serviços e protocolos na suíte TCP/IP são definidos pela Internet Engineering Task Force (IETF).

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.

Fonte: Cisco

Características da camada física



Exemplo de organizações:

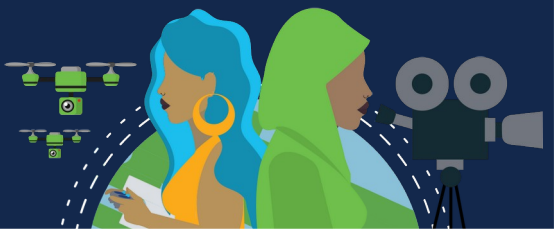
- International Organization for Standardization (ISO).
- Telecommunications Industry Association/Electronic Industries Association (TIA/EIA).
- União Internacional de Telecomunicações (ITU).
- Instituto Nacional de Padronização Americano (ANSI).
- Institute of Electrical and Electronics Engineers (IEEE).

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.

Fonte: Cisco

Características da camada física

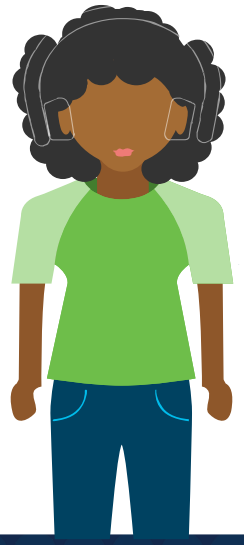


Camadas do modelo OSI

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

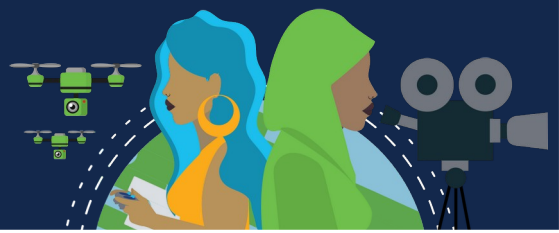
Os padrões da camada física são implementados em hardware e orientados por muitas organizações, inclusive:

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



Fonte: Cisco

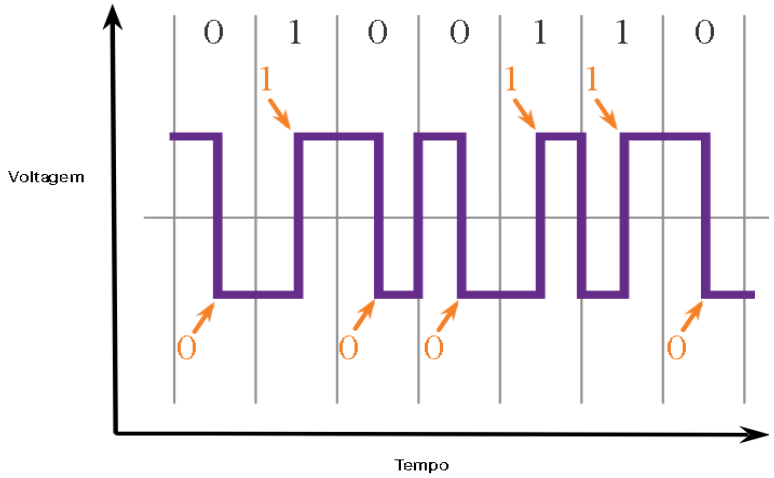
Componentes Físicos



Os padrões da camada física abordam três áreas funcionais:

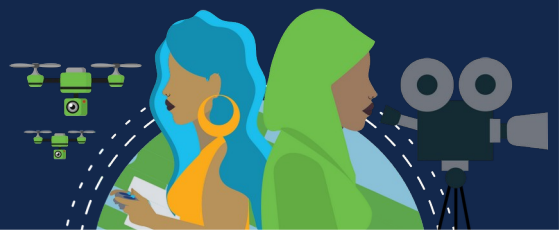
Componentes Físicos:
São os dispositivos de hardware eletrônico, mídia e outros conectores que transmitem os sinais que representam os bits.
Os componentes de hardware, como NICs, interfaces e conectores, materiais de cabo e projetos de cabo são especificados nos padrões associados à camada física.
As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



Fonte: Cisco

Componentes Físicos

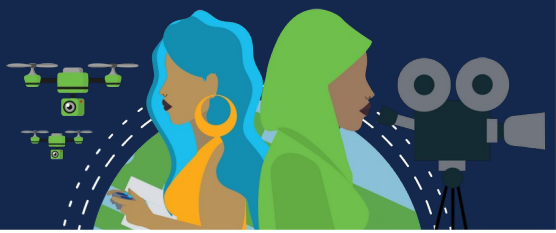


A codificação Manchester representa um bit 0 por uma transição de alta para baixa voltagem, e um bit 1 é representado como uma transição de baixa para alta voltagem.
A transição ocorre no meio de cada período de bit.
Esse tipo de codificação é usado na Ethernet de 10 Mbps. Taxas de dados mais rápidas 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.

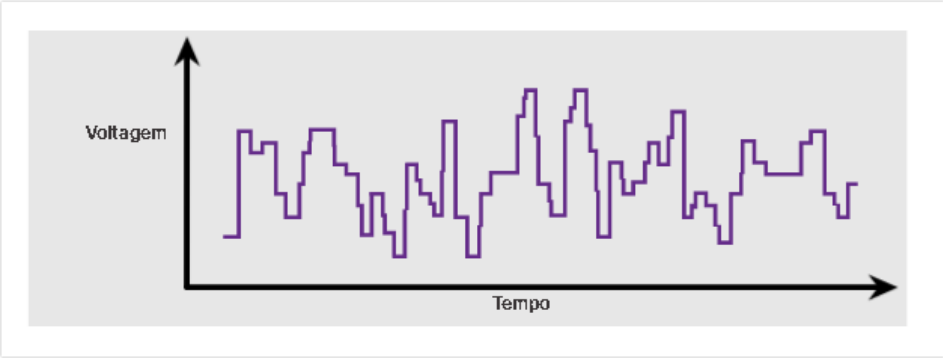
Fonte: Cisco

Componentes Físicos

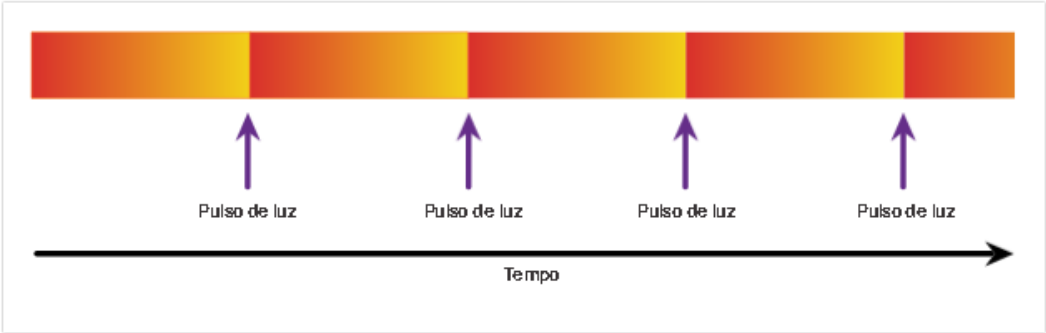


Sinalização para cabo de cobre, cabo de fibra óptica e mídia sem fio.

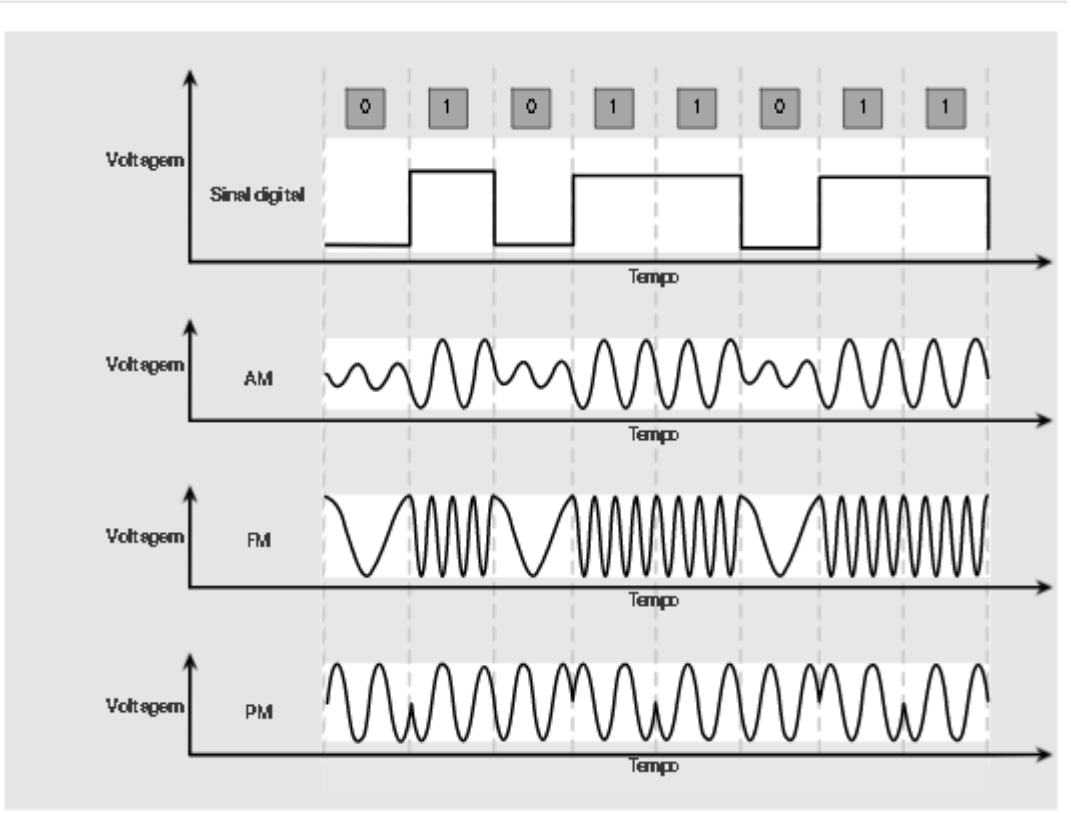
Sinais elétricos em Cabos de Cobre



Pulsos de Luz em Cabos Ópticos

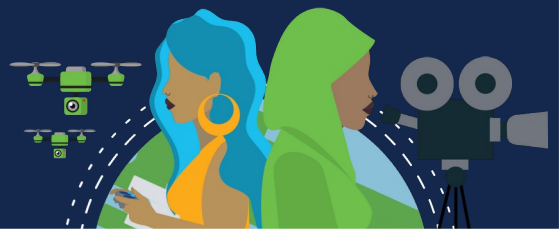


Sinais em microondas sem Fio



Fonte: Cisco

Largura de banda



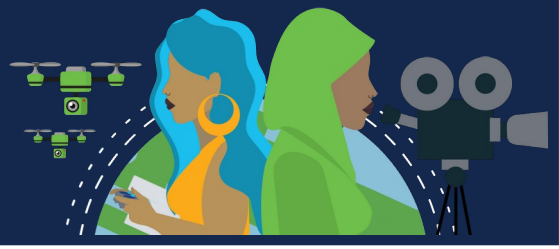
Meios físicos diferentes aceitam a transferência de bits a taxas diferentes.
A transferência de dados é geralmente discutida em termos de largura de banda.
Largura de banda é a capacidade na qual um meio pode transportar dados.
A largura de banda digital mede a quantidade de dados que podem fluir de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

Fonte: Cisco

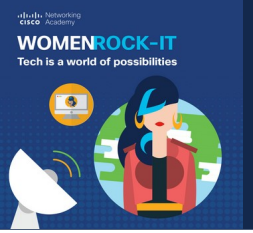
Largura de banda



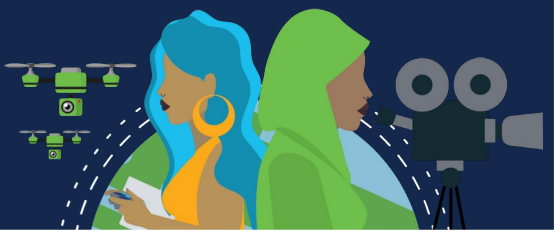
A tabela mostra as unidades de medida comumente usadas para largura de banda.

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

Fonte: Cisco



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.

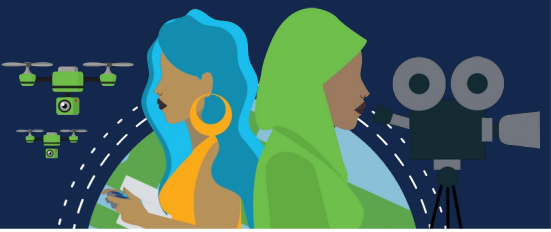
Existem muitos testes de velocidade on-line que podem revelar a taxa de transferência de uma conexão com a Internet.

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.

Fonte: Cisco

Terminologia de largura de banda



- **Dados úteis:**

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

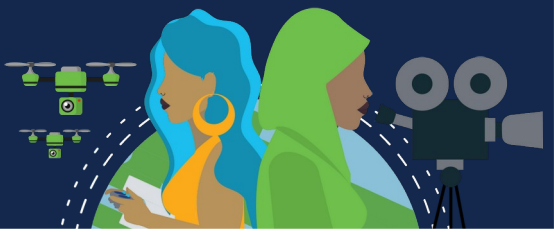
Goodput é a medida de dados usáveis transferidos em um determinado período.

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.

Fonte: Cisco

Cabeamento de Cobre



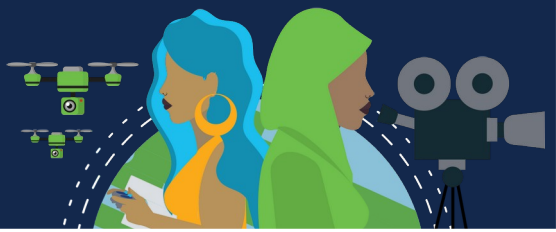
É o tipo mais comum de cabeamento usado nas redes hoje em dia.
Existem três tipos diferentes de cabeamento de cobre que são usados em situações específicas.

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.

Fonte: Cisco

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:**

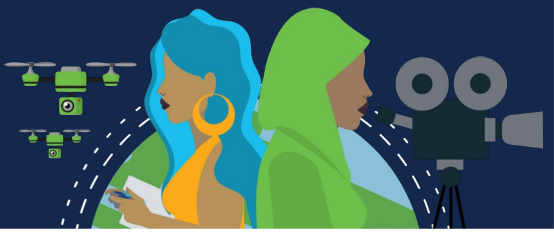
Diafonia é uma perturbação causada pelos campos elétrico ou magnético de um sinal em um fio para o sinal em um fio adjacente.
Nos circuitos de telefone, a diafonia pode fazer com que parte de outra conversa de voz de um circuito adjacente seja ouvida (linha cruzada).
Especificamente, quando uma corrente 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.

Fonte: Cisco

Cisco Life Changer

Changing the way the world WORKS!

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.

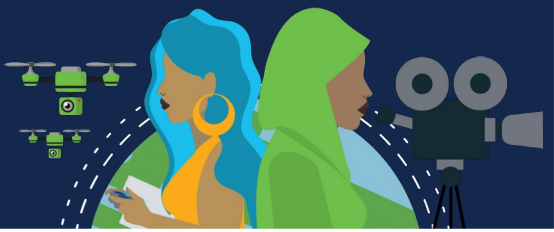
Para contrabalançar os efeitos negativos do crosstalk, alguns tipos de cabos de cobre têm pares de cabos de circuitos opostos juntos, o que efetivamente cancelam o crosstalk.

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.

Fonte: Cisco

Tipos de cabeamento de cobre

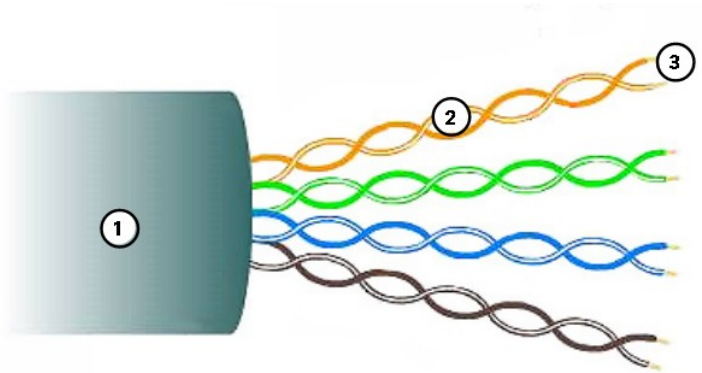


Par trançado não blindado (UTP)

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.

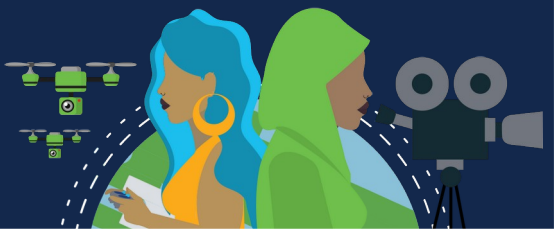
O processo de trançar cabos ajuda na proteção contra interferência de sinais de outros cabos.



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.

Fonte: Cisco

Tipos de cabeamento de cobre



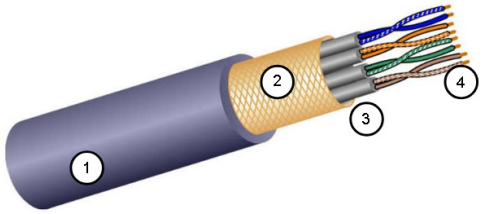
Par trançado blindado (STP)

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.

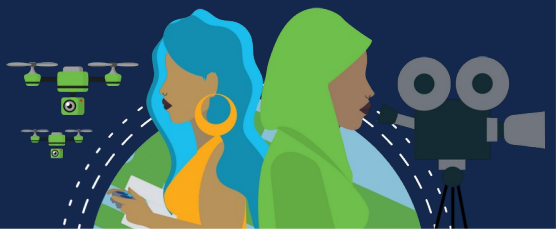
O cabo STP usa quatro pares de cabo, envolvidos em blindagens, que são colocados em uma proteção ou revestimento geral metálico.

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



Fonte: Cisco

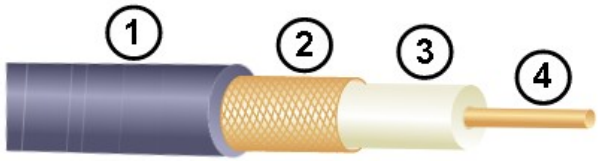
Tipos de cabeamento de cobre



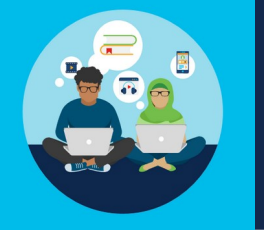
Cabo coaxial

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.

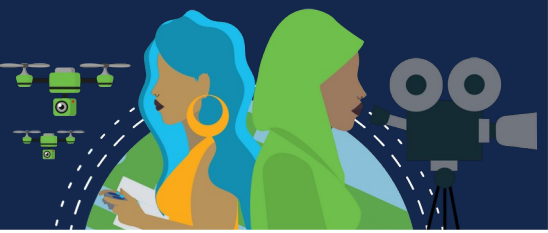
1. Revestimento exterior.
2. Blindagem de cobre trançado.
3. Isolante em plástico.
4. Condutor de cobre.



Fonte: Cisco



Tipos de cabeamento de cobre



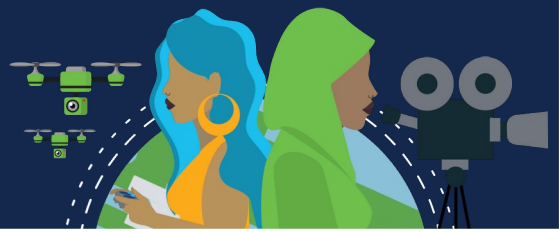
Embora o cabo UTP tenha substituído essencialmente o cabo coaxial nas modernas instalações Ethernet, o design do cabo coaxial é usado nas seguintes situações:

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.

Fonte: Cisco

Cabeamento UTP



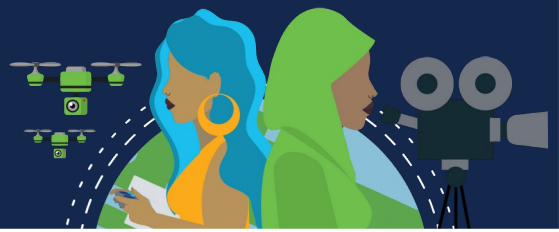
Consiste em 4 pares de fios de cobre com código de cores, torcidos juntos e depois envoltos em uma bainha de plástico flexível.
Não usa blindagem para contrabalançar os efeitos de EMI e RFI.
Limitando efeito negativo da diafonia através de:

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.

Fonte: Cisco

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.

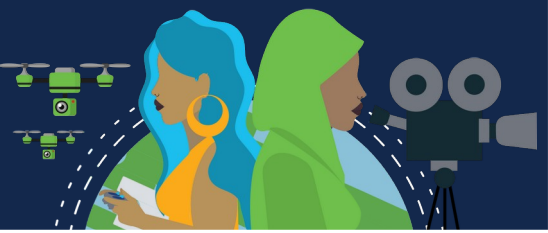
Alguns dos elementos definidos são:

- 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.

Fonte: Cisco

Padrões e conectores de cabeamento UTP

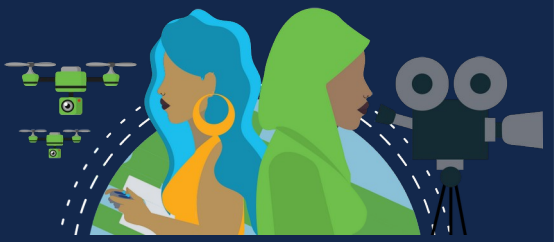


Os cabos em categorias mais altas são desenvolvidos e construídos para suportar taxas de dados mais elevadas.
À medida que novas tecnologias Ethernet de velocidade de gigabit estão sendo desenvolvidas e adotadas, a Categoria 5e é agora o tipo de cabo minimamente aceitável, com a Categoria 6 sendo o tipo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

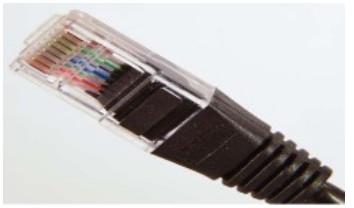
Fonte: Cisco

Padrões e conectores de cabeamento UTP

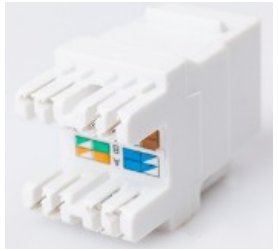


O cabo UTP geralmente é terminado com um conector RJ-45.
O padrão TIA/EIA-568 descreve os códigos de cores de cabos para atribuições dos pinos (pinagem) para cabos Ethernet.

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

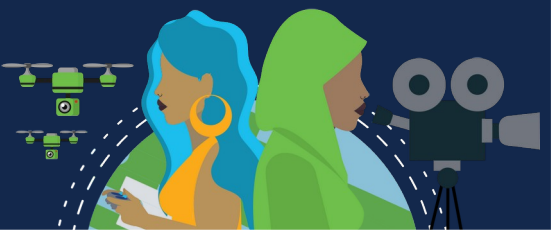


Sockets UTP RJ-45
O soquete é o componente feminino de um dispositivo de rede, parede, tomada de partição de cubículo ou painel de conexões. Quando terminado incorretamente, o cabo é uma fonte potencial de degradação do desempenho da camada física.



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

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:

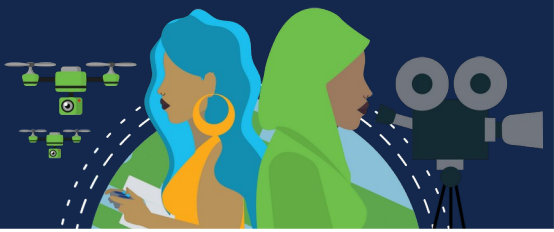
Ethernet direto:
O tipo mais comum de cabo de rede. Geralmente é usado para interconectar um host a um switch e um switch a um roteador.

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.

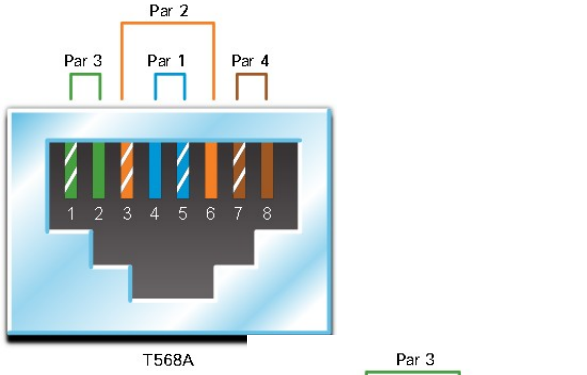
Fonte: Cisco

Cabos UTP diretos e cruzados

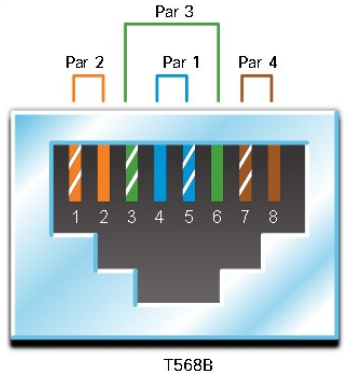


O uso incorreto de um cabo crossover ou direto entre dois dispositivos não danifica os dispositivos, mas a conectividade e comunicação entre os dispositivos não será realizada.
Este é um erro comum e verificar se as conexões do dispositivo estão corretas deve ser a primeira ação de solução de problemas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

Diagramas dos padrões de fiação T568A e T568B.



T568A



T568B

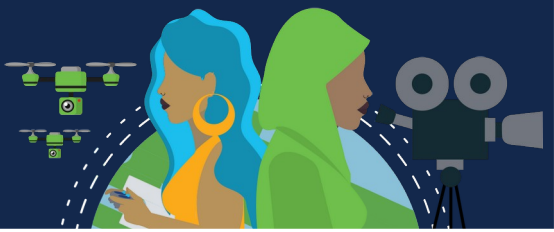
Cada um mostra a pinagem correta para os pares de fios individuais.
Cada par de fios de cor é numerado e consiste em um fio de cor sólida e um fio listrado branco.
O par 1 é azul, o par 2 é laranja, o par 3 é verde e o par 4 é marrom.
Cada padrão alterna entre fios listrados brancos e sólidos.

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.

Fonte: Cisco

Cabos UTP diretos e cruzados

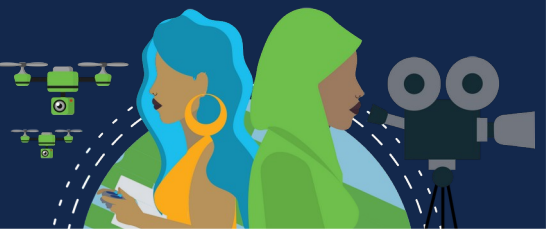


Cable Types and Standards

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

Fonte: Cisco

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.

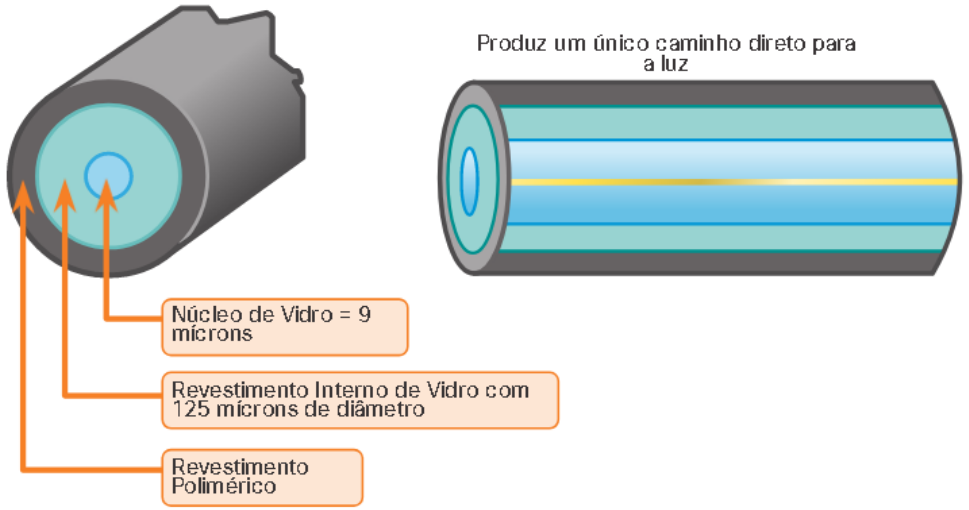
Fonte: Cisco

Tipos de Fibra

- **Fibra monomodo (SMF):**

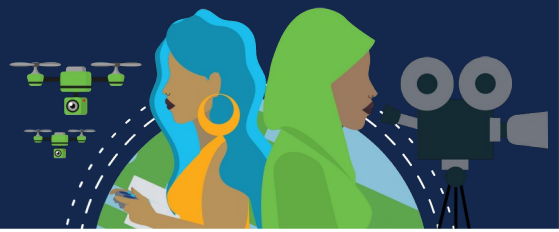
O SMF consiste em um núcleo muito pequeno e usa a tecnologia laser cara para enviar um único raio de luz.

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.



Fonte: Cisco

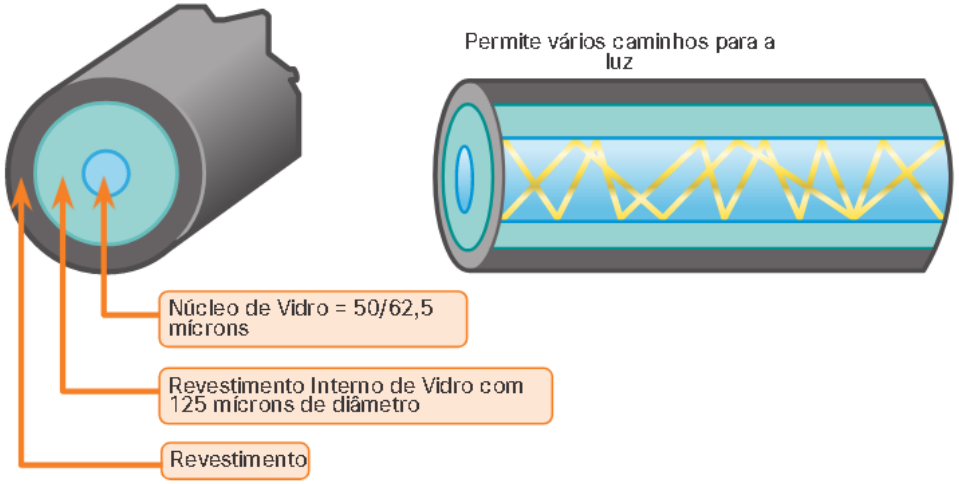
Tipos de Fibra



- **Fibra multimodo (MMF)**

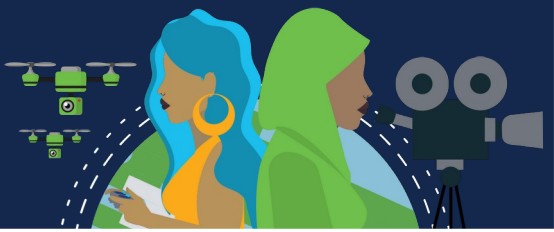
O MMF consiste em um núcleo maior e usa emissores de LED para enviar pulsos de luz. Especificamente, a luz de um LED entra na fibra multimodo em diferentes ângulos, como mostrado na figura. Popular nas LANs porque pode ser acionada por LEDs de baixo custo.
Ela fornece largura de banda até 10 Gb/s por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



Fonte: Cisco

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.

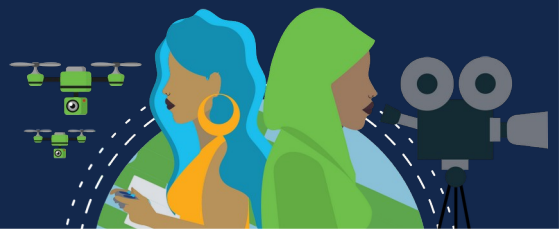
FTTH (Fiber-to-the-Home):
Usado para fornecer serviços de banda larga sempre ativos para residências e pequenas empresas.

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.

Fonte: Cisco

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.

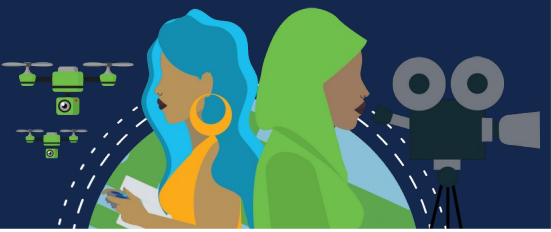
Até recentemente, a luz só podia viajar em uma direção sobre fibra óptica.
Duas fibras foram necessárias para suportar a operação full duplex.
Portanto, os cabos de conexão de fibra óptica agrupam dois cabos de fibra óptica e os terminam com um par de conectores padrão de fibra única. Alguns conectores 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.

Fonte: Cisco

Cisco Life Changer

Changing the way the world WORKS!

Cabos de conexão de fibra



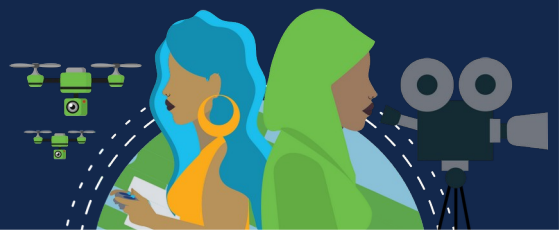
Os cabos de fibra são necessários para interconectar dispositivos da infraestrutura.
O uso das cores diferencia entre cabos monomodo e multimodo.
A cor amarela indica cabos de fibra monomodo e o laranja é para cabos de fibra multimodo.

- **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.

Fonte: Cisco

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.

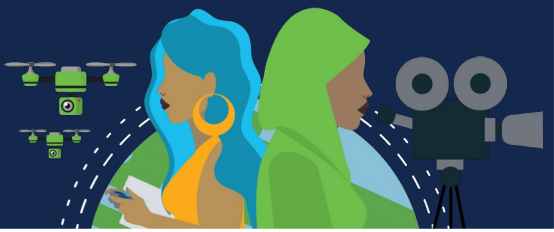
Atualmente, na maioria dos ambientes empresariais, a fibra óptica é usada principalmente como cabeamento de backbone para conexões ponto a ponto de alto tráfego entre instalações de distribuição de dados.
Ele também é usado para a interconexão de edifícios em campus multi-construção.
Como os cabos de 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

Fonte: Cisco

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.

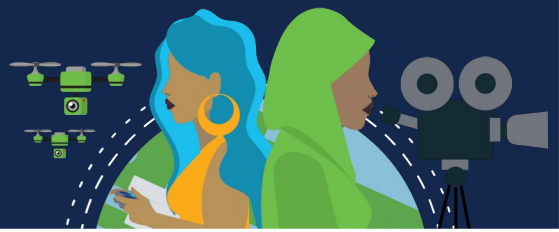
Algumas de suas limitações são:

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.

Fonte: Cisco

Meios sem fio



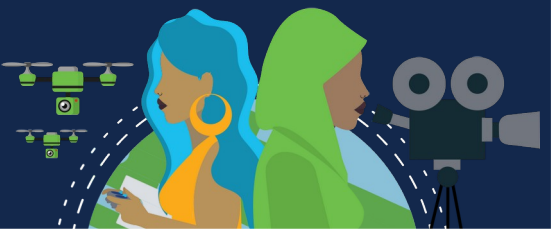
Segurança:
Não requer acesso a uma parte física da mídia.
Portanto, os dispositivos e usuários que não estão autorizados a acessar a rede podem obter acesso à transmissão.
A segurança da rede é o principal componente da administração de uma rede sem fio.

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.

Fonte: Cisco

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:

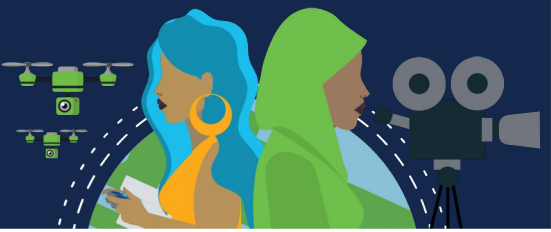
- Codificação de dados para sinal de rádio;
- Frequência e potência de transmissão;
- Requisitos de recepção e decodificação de sinal;
- Projeto e construção de antenas.

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.

Fonte: Cisco

Tipos de Meio Físico Sem Fio



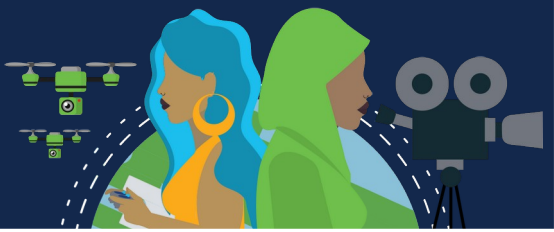
Bluetooth (IEEE 802.15):
Padrão de rede pessoal sem fio (WPAN), conhecido como “Bluetooth”.
Usa um processo de emparelhamento de dispositivo para se comunicar em distâncias de 1 a 100 metros.

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.

Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

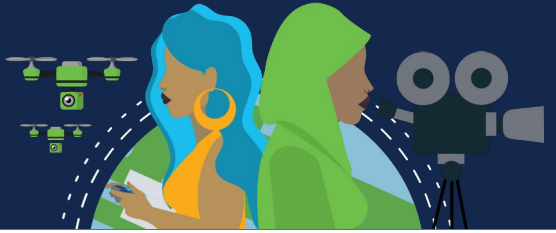
WOMENROCK-IT

CCNAv7 – ITN – Sistemas de Números

Módulo 5

Embaixadores do Programa 2020, 2021 & 2022:

Organizadoras Cisco: Eliana Silva, Veruska Clednev
Professores Coordenadores: Marissol Barros, Moisés Nisenbaum



AGENDA

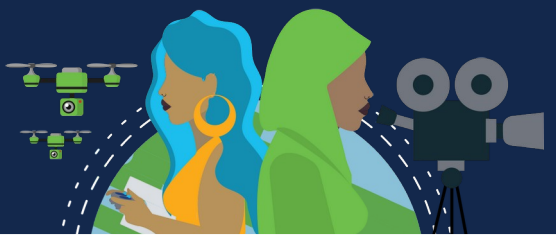
Como converter endereços binários em endereços decimais pontilhados e decimais em binários.

*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.



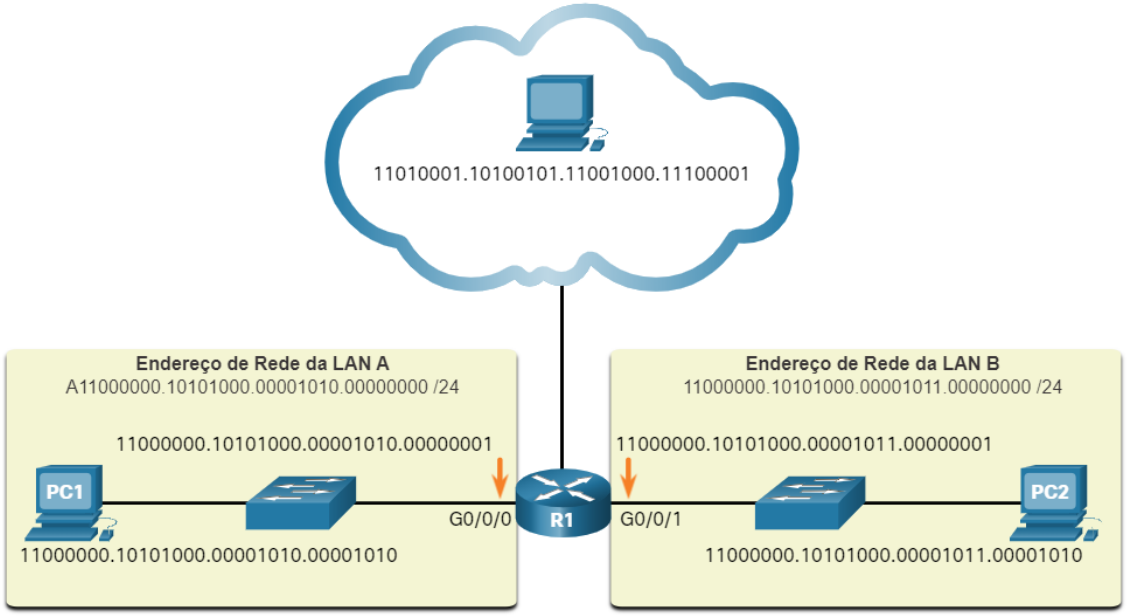
Sistemas de Numeração Binários

Endereços Binários e IPv4

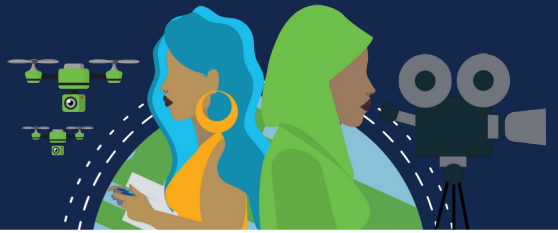
- Os endereços IPV4 são binários, utilizando um sistema matemático compostos pelo algarismos 0 e 1.

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.



Fonte: Cisco



Conversão entre Sistemas

Vídeo - Convertendo entre sistemas de numeração binária e decimal

NOTAÇÃO POSICIONAL BINÁRIA

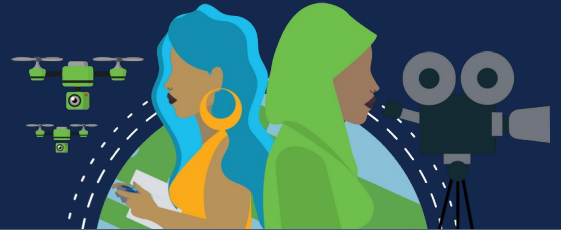
https://contenthub.netacad.com/f5af14ac-f6c8-4d89-8e41-3f191aef5139

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**			

Fonte: Cisco



Conversão entre sistemas

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

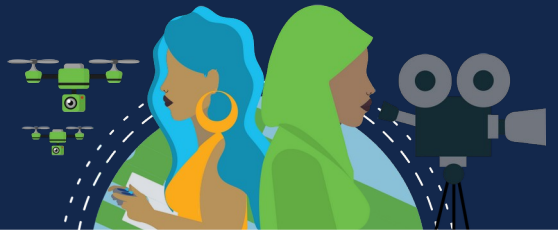
Raiz	2	2	2	2	2	2	2	2
Posição no número	7	6	5	4	3	2	1	0
Cáculo	(2^7)	(2^6)	(2^5)	(2^4)	(2^3)	(2^2)	(2^1)	(2^0)
Valor da posição	128	64	32	16	8	4	2	1

- 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**							

Fonte: Cisco



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**							

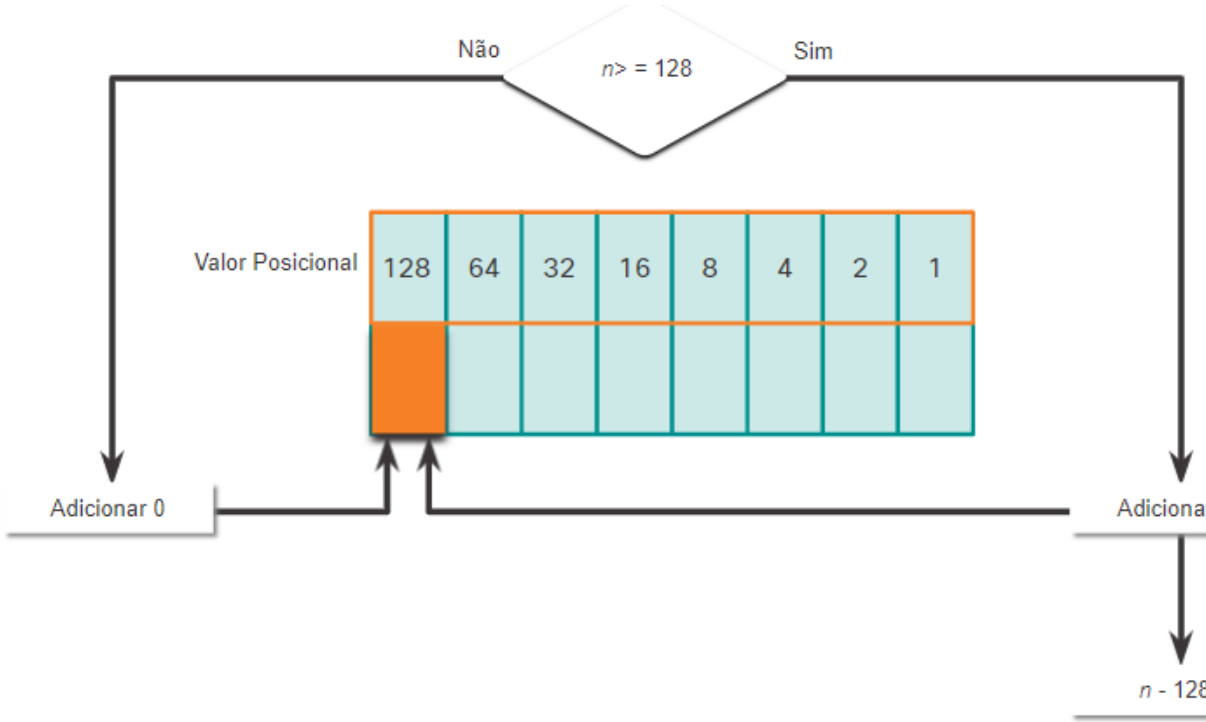
Fig4. Quarto Octeto

Fonte: Cisco

Conversão de decimal para binário

Utilize a tabela de valores posicionais binários

128	64	32	16	8	4	2	1



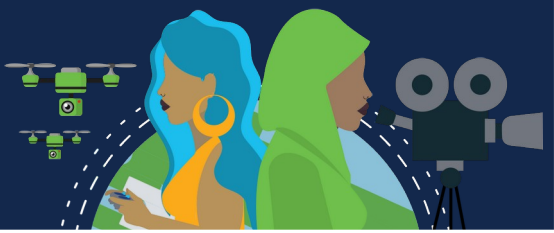
O número decimal do octeto (n) é igual ou superior ao bit mais significativo (**128**)?

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

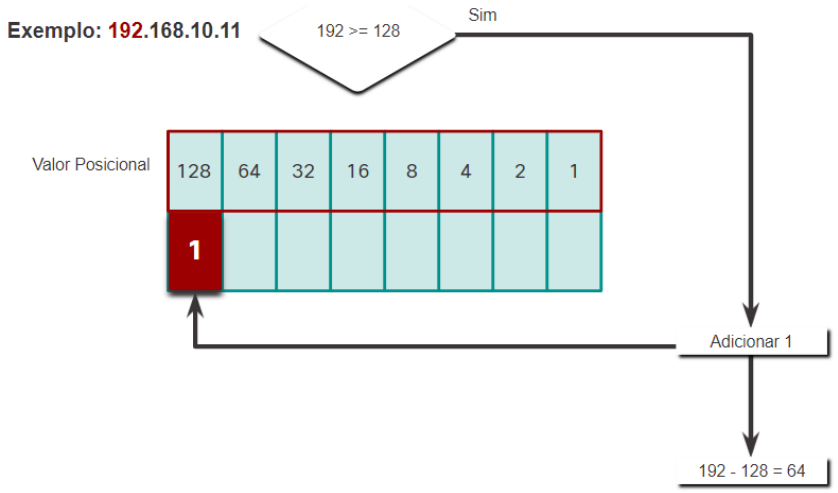
Fonte: Cisco

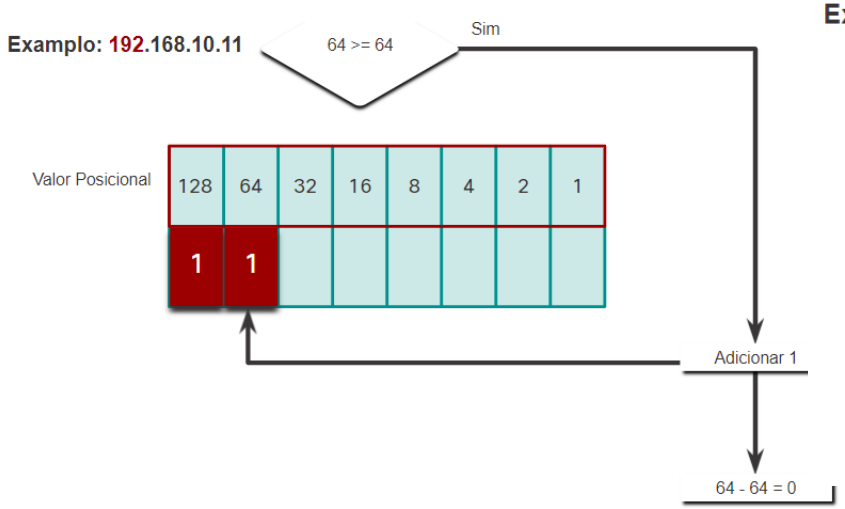
Exemplo de Conversão de Decimal para Binário

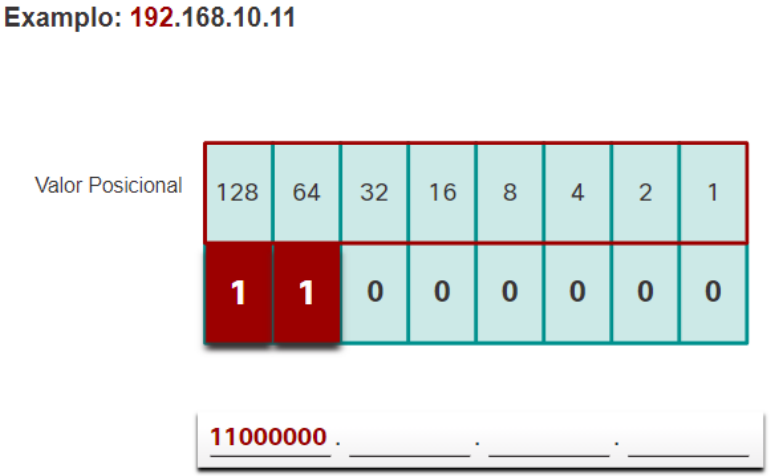
192.168.11.10



Converter primeiro octeto para binário



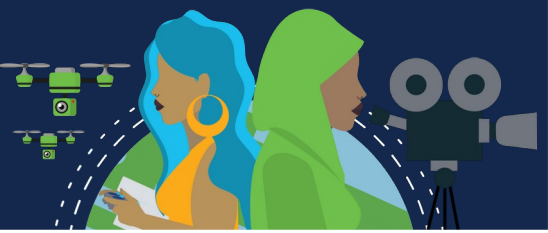




Fonte: Cisco

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

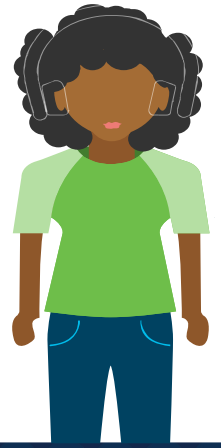
Valor Posicional	128	64	32	16	8	4	2	1
	0	0	0	0	**1**	0	**1**	0

11000000 . 10101000 . **00001010** . _____

Converter quarto octeto para binário

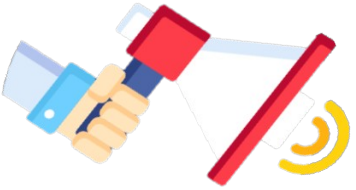
Valor Posicional	128	64	32	16	8	4	2	1
	0	0	0	0	**1**	0	**1**	**1**

11000000 . 10101000 . 00001010 . **00001011**



Fonte: Cisco

Jogo Binário



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

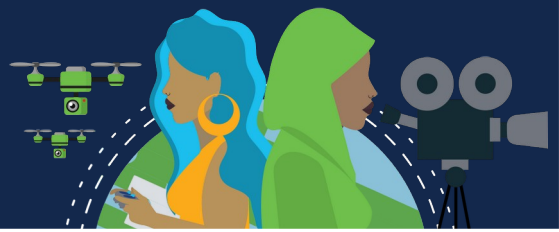
Game Link: https://learningnetwork.cisco.com/docs/DOC-1803

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

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

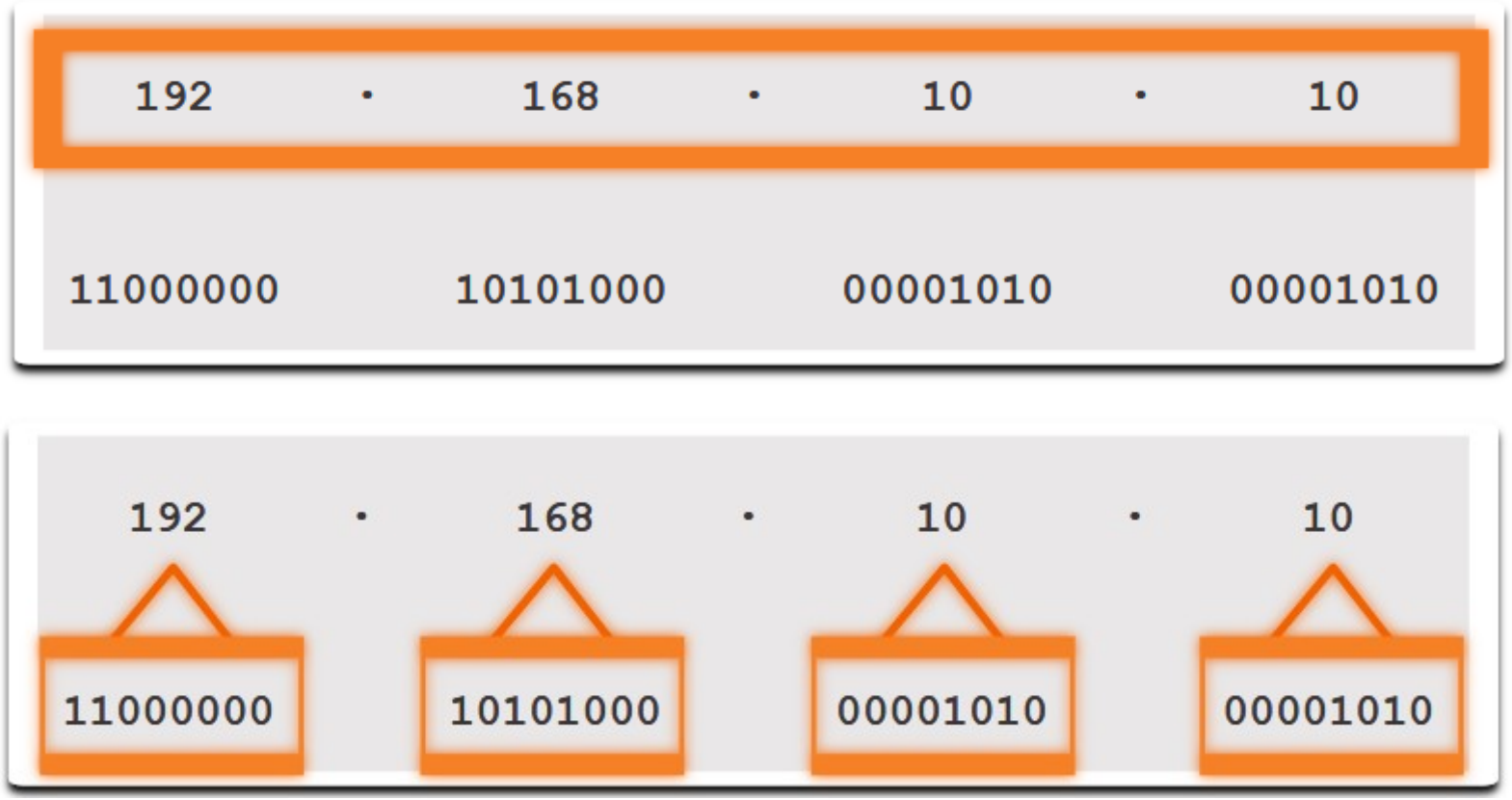
Fonte: Cisco

Endereços IPV4



Roteadores e computadores utilizam binários.

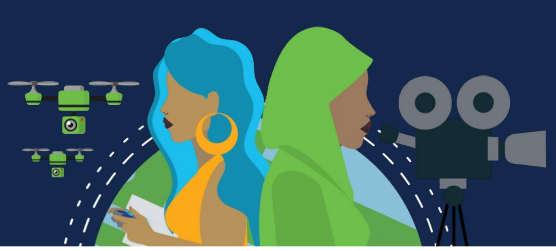
Humanos trabalham em decimal.



IP - Computador

Composto por quatro octetos diferentes

Fonte: Cisco



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.

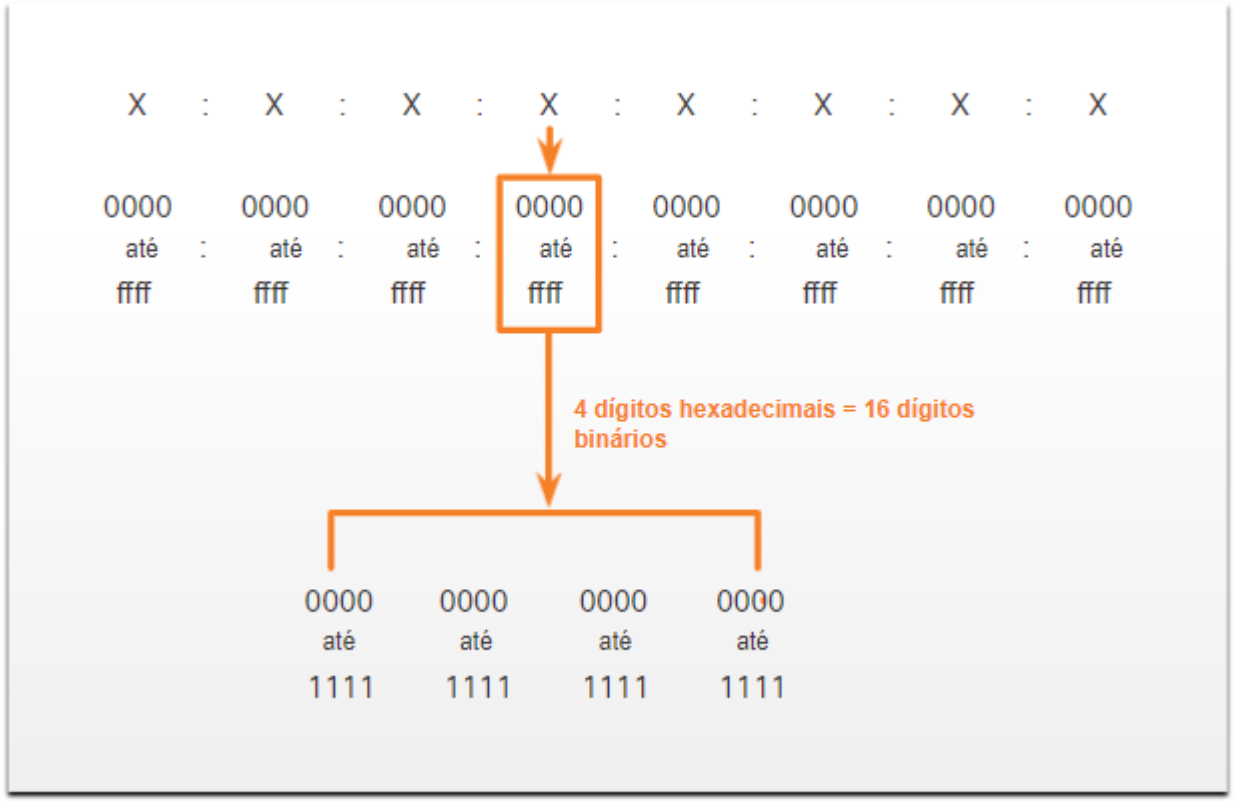
Os endereços IPv6 têm 128 bits de comprimento e a cada 4 bits é representado por um único dígito hexadecimal; para um total de 32 valores hexadecimais.

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.

Fonte: Cisco

Sistema de numeração hexadecimal

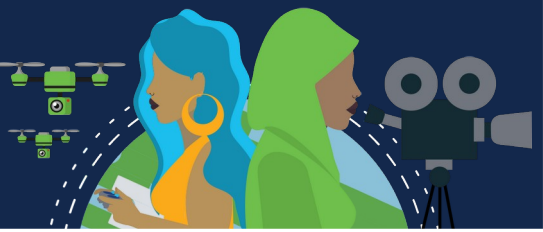
- Cada "x" é um único hextet, 16 bits ou quatro dígitos hexadecimais.



Fonte: Cisco

Sistema de numeração hexadecimal

Endereços hexadecimais e IPv6



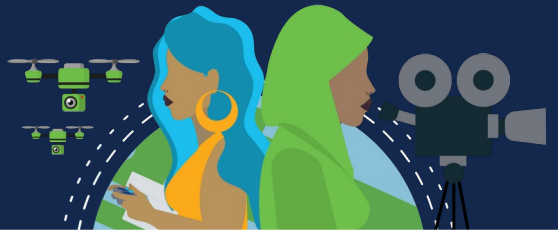
Para Converter números decimais em valores hexadecimais é simples:

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:

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

Fonte: Cisco



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

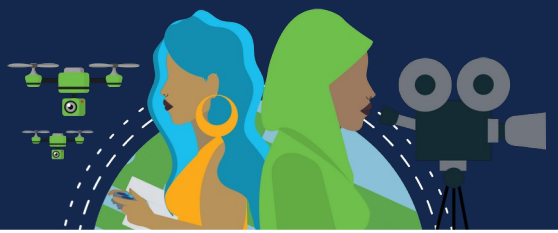
Por exemplo, 168 convertidos em hexadecimal usando o processo de três etapas:

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.

Fonte: Cisco



Conversão hexadecimal em decimal

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

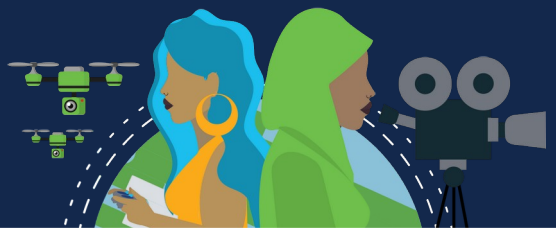
Por exemplo, Hexadecimal **D2** para **decimal**:

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.

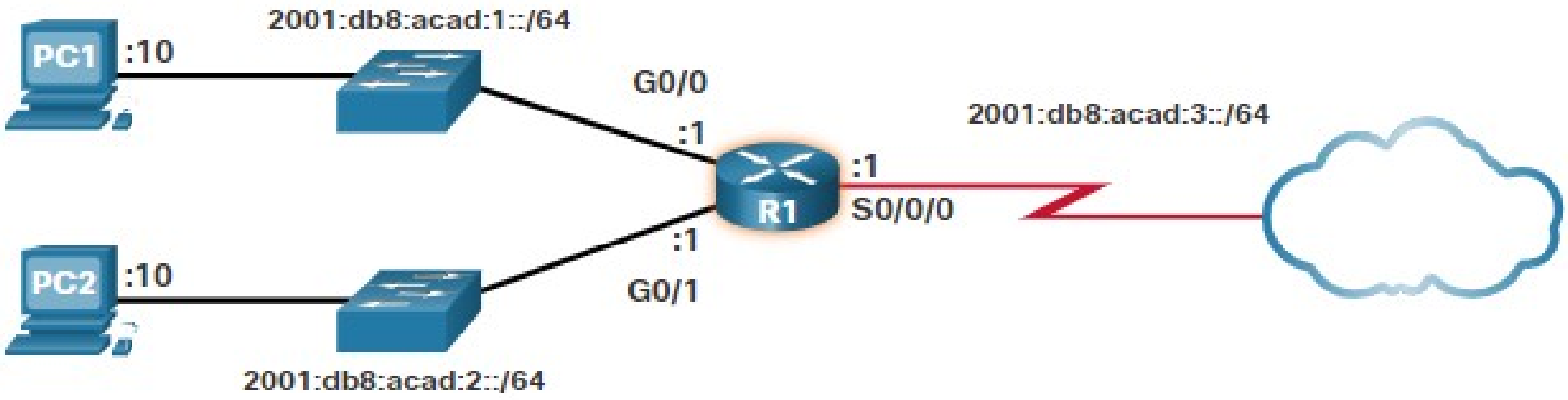
Fonte: Cisco



Exemplo topologia IPV6

Cisco Life Changer

Changing the way the world WORKS!



Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

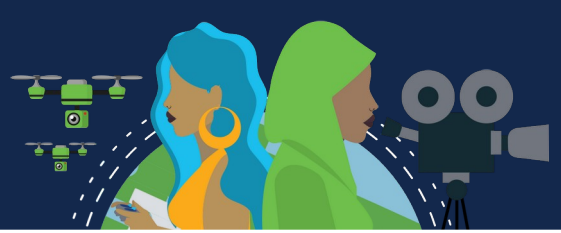
CCNAv7 – ITN – Camada Enlace de Dados

Módulo 6

Embaixadores do Programa 2020, 2021 & 2022:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum



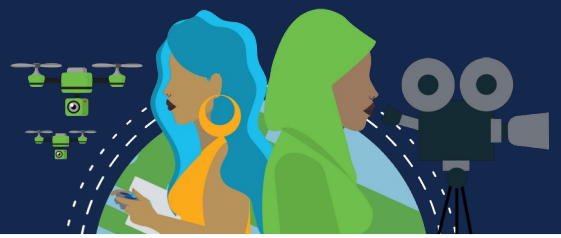
Camada de Enlace

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.

Fonte: Cisco

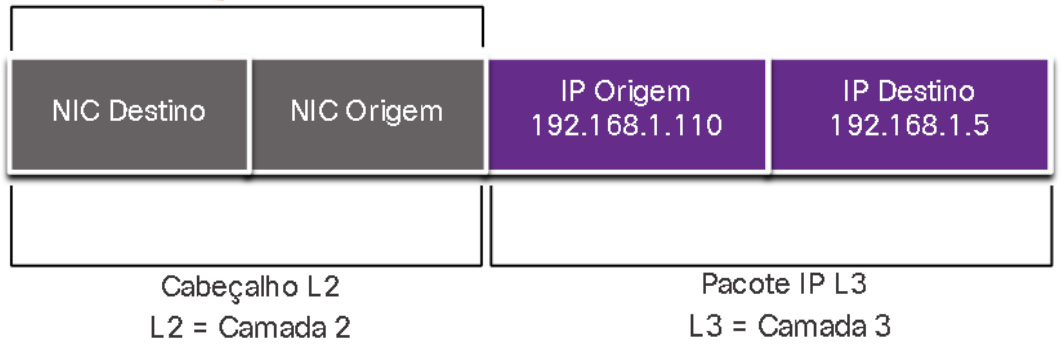


Camada de Enlace

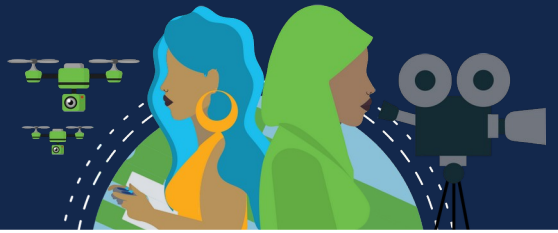
Um nó pode ser um dispositivo final, como um laptop ou telefone celular, ou um dispositivo intermediário, como um switch Ethernet, que pode receber, criar, armazenar ou encaminhar dados ao longo de um caminho de comunicação.

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).



Fonte: Cisco



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:

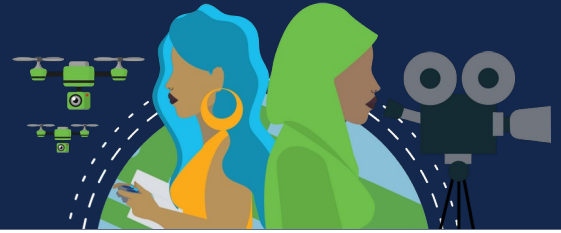
Logical Link Control (LLC) (IEEE 802.2): Essa subcamada comunica entre o software de rede nas camadas superiores e o hardware do dispositivo nas camadas inferiores. Ela pega os dados do protocolo de rede, como um pacote IPv4 ou IPv6, e adiciona informações de controle da camada 2 para ajudar a entregar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

<table>
<tr><td>Camada de Rede</td><td colspan="4">Protocolo de camada de rede</td></tr>
<tr><td rowspan="3">Camada de Enlace de Dados</td><td>Subcamada LLC</td><td colspan="3">Subcamada LLC - IEEE 802.2</td></tr>
<tr><td rowspan="2">Subcamada MAC</td><td>Ethernet
IEEE 802.3</td><td>WLAN
IEEE 802.11</td><td>WPAN
IEEE 802.15</td></tr>
<tr><td>Vários padrões Ethernet para FastEthernet, GigabitEthernet, etc.</td><td>Vários padrões WLAN para diferentes tipos de comunicações sem fio.</td><td>Vários padrões WPAN, para Bluetooth, RFID, etc.</td></tr>
<tr><td colspan="2">Camada Física</td><td colspan="3"></td></tr>
</table>

Fonte: Cisco



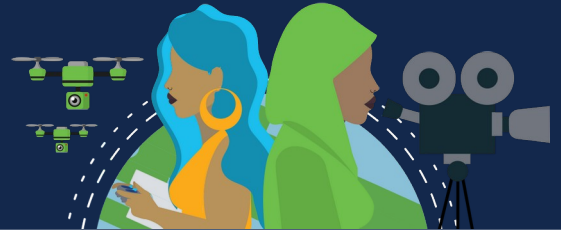
SUBCAMADAS DE ENLACE IEEE 802 LAN/MAN

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.

Fonte: Cisco



Fornecimento de Acesso ao Meio Físico

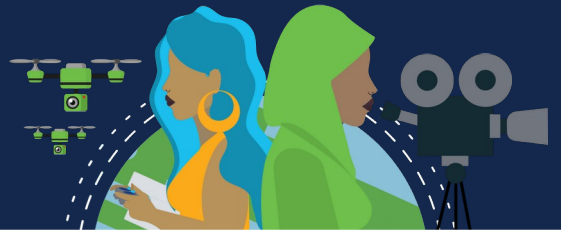
Cada ambiente de rede pode ter diferentes características. Em uma LAN Ethernet geralmente consiste em muitos hosts que disputam o acesso ao meio físico para envio de dados.
A subcamada MAC resolve isso.

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.

Fonte: Cisco



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)

Fonte: Cisco

Topologias Físicas e Lógicas

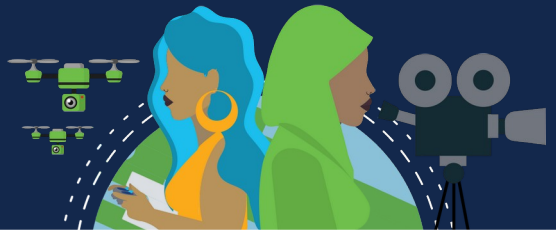
A camada de link de dados prepara os dados da rede para a rede física. Para isso ela deve conhecer a topologia lógica de uma rede para poder determinar o que é necessário para transferir quadros de um dispositivo para outro.

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.

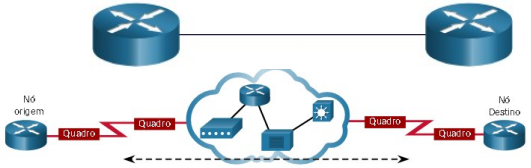
A camada de enlace de dados “vê” a topologia lógica da rede quando controla o acesso de dados ao meio físico. É a topologia lógica que influencia o tipo de enquadramento de rede e o controle de acesso ao meio usado.

Fonte: Cisco

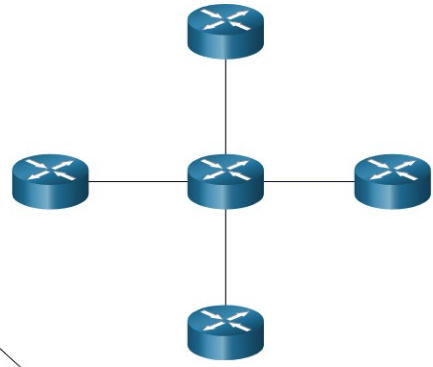


Topologias WAN

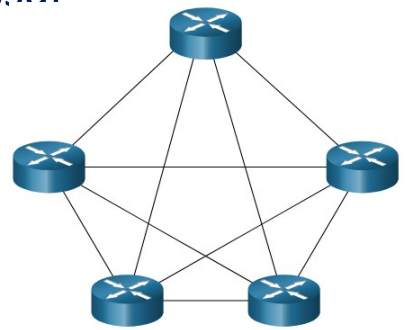
Ponto a Ponto: Mais simples e comum. Consiste em uma ligação permanente entre 2 pontos finais, que não compartilham o meio físico com outros hosts.
Usando um protocolo de comunicação serial como o PPP, um nó não precisa determinar se um quadro de entrada é destinado a ele ou a outro nó. Sendo os protocolos 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.



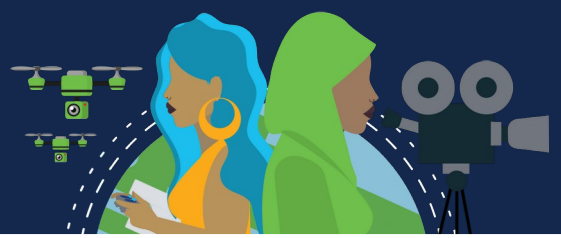
Estrela: Consiste em um site central interconectando sites de filiais através do uso de links ponto a ponto. Os sites de filiais não trocam dados com outras filiais sem passar pelo site central.



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.



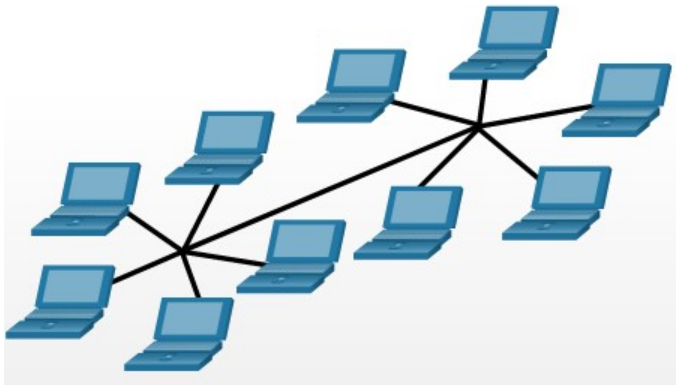
Fonte: Cisco



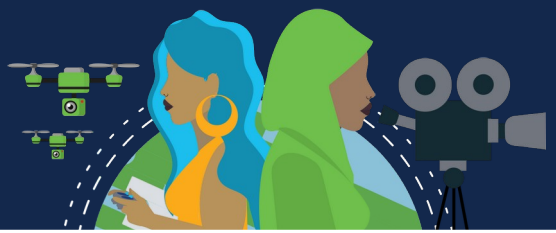
Topologias LAN

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**.



Fonte: Cisco



Comunicação Duplex

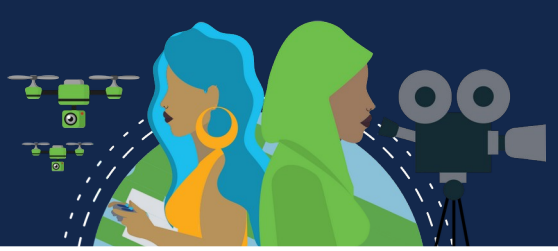
A comunicação duplex é se refere à direção da transmissão de dados entre dois dispositivos.
Existem dois modos comuns de duplex.

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.

Fonte: Cisco



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.

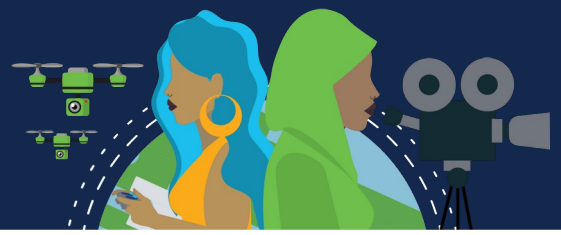
São dois os métodos:

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.

Fonte: Cisco



Métodos de Controle de Acesso

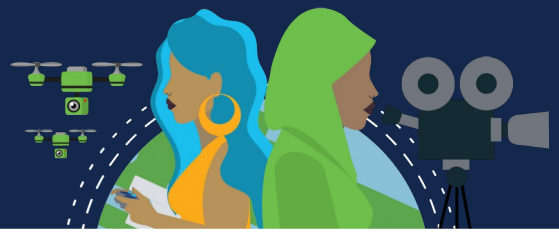
2. Acesso Controlado: Cada nó tem seu próprio tempo para usar o meio. São ineficientes porque um dispositivo deve aguardar sua vez para acessar o meio. Usada em topologia legada, anel de token.

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**.

Fonte: Cisco



Quadro de Enlace de Dados

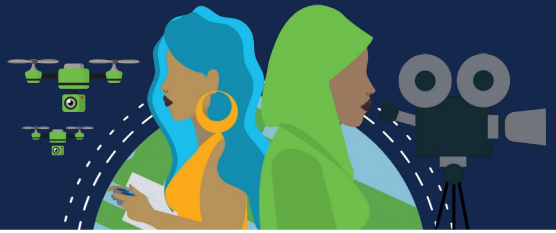
A camada de enlace, prepara os dados encapsulados para o transporte pela mídia local, encapsulando-o com um cabeçalho e um trailer para criar um quadro.
Cada tipo de quadro tem três partes básicas:

- 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.

Fonte: Cisco



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.

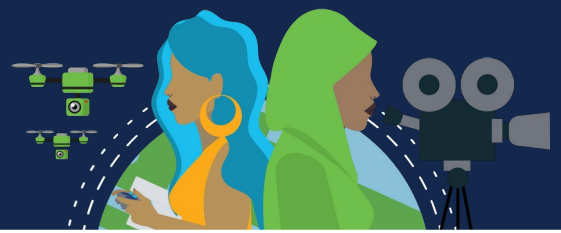
Tipo: Identifica o protocolo da camada 3 no campo de dados.

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.

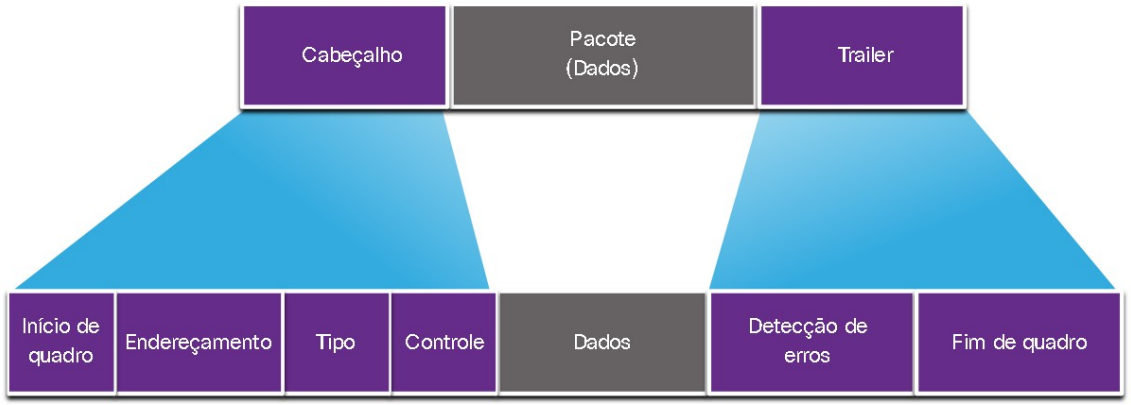
Dados: Contém a carga útil do quadro (ou seja, cabeçalho do pacote, cabeçalho do segmento e os dados).

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

Fonte: Cisco



Campos do Quadro



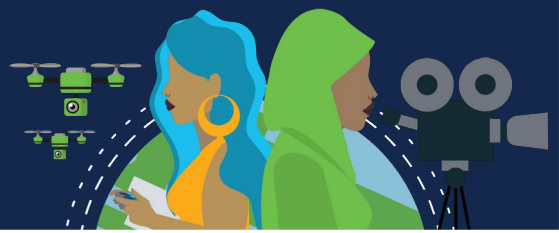
Em um pacote de dados encapsulado por um cabeçalho de link de dados e um trailer de link de dados.
O cabeçalho do link de dados é dividido em 4 campos: início do quadro, endereçamento, tipo e controle.
O trailer do link de dados é dividido em dois campos: Detecção de erro e parada de quadros.

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.

Fonte: Cisco

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.

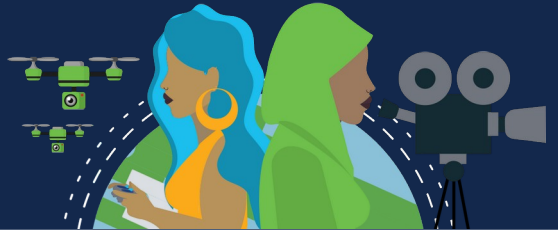
Os endereços físicos não indicam em qual rede o dispositivo está localizado.
Trata se de um endereço exclusivo do dispositivo. Um dispositivo ainda funcionará com o mesmo endereço físico da Camada 2, mesmo que o dispositivo se mova para outra rede ou sub-rede. Portanto, os endereços de Camada 2 são usados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

Fonte: Cisco



Quadros de LAN e WAN

Protocolos Ethernet são usados por LANs com fio. As comunicações sem fio se enquadram nos protocolos WLAN (IEEE 802.11), projetados para redes multiacesso.

As WANs usavam outros tipos de protocolos para vários tipos de topologias ponto a ponto, hub-spoke e malha completa, que agora estão sendo substituídos na WAN por Ethernet.

Como, por exemplo:

Modo de Transferência Assíncrona (ATM);

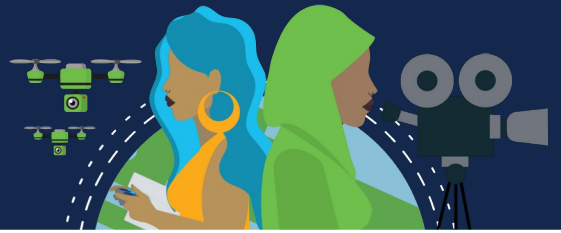
X.25;

Em uma rede TCP/IP, todos os protocolos de Camada 2 do modelo OSI trabalham com o IP na Camada 3 do modelo.
No entanto, o protocolo de Camada 2 usado depende da topologia lógica e do meio físico, também determinado pelo tamanho da rede, escopo geográfico e serviços a serem fornecidos.

Cada protocolo desempenha controle de acesso ao meio para as topologias lógicas da Camada 2 especificadas.

Uma LAN normalmente usa uma tecnologia de alta largura de banda capaz de suportar um grande número de hosts. A área geográfica relativamente pequena de uma LAN (um único edifício ou um campus com vários edifícios) e sua alta densidade de usuários tornam essa tecnologia econômica.

Fonte: Cisco



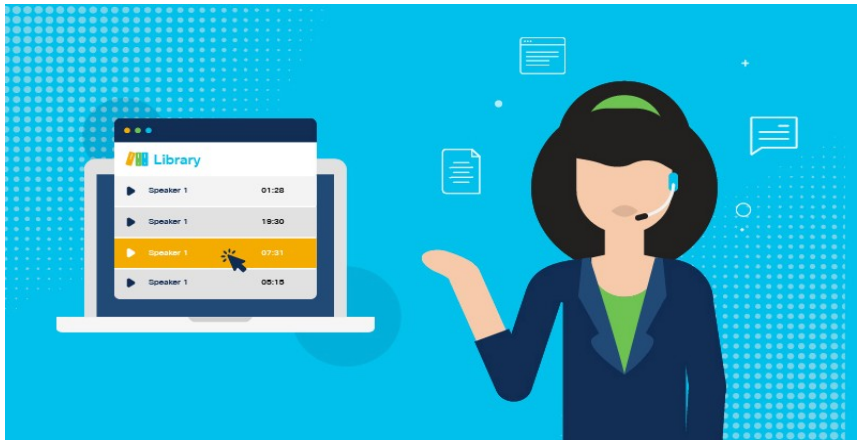
Quadros de LAN e WAN

No entanto, o uso de uma tecnologia de alta largura de banda geralmente não é economicamente viável para WANs que abrangem grandes áreas geográficas (cidades ou várias cidades, por exemplo).
O custo dos links físicos de longa distância e a tecnologia usada para transportar os sinais por essas distâncias geralmente resultam em menor capacidade de largura de banda.

A diferença na largura de banda resulta normalmente no uso de diferentes protocolos para LANs e WANs.

Os protocolos da camada de enlace de dados incluem:

- Ethernet;
- 802.11 sem fio;
- Protocolo ponto a ponto (PPP);
- Controle de Enlace de Dados de Alto Nível (HDLC);
- Frame Relay.



Fonte: Cisco

Obrigade!

Networking Academy

Networking Academy
cisco

WOMEN ROCK-IT

Networking Academy

WOMENROCK-IT

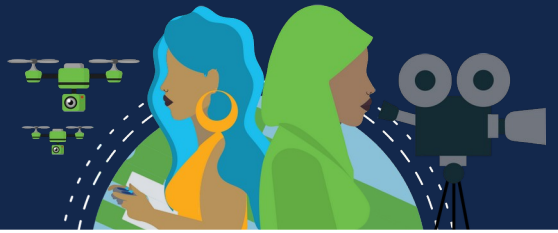
CCNAv7 – ITN – Switching Ethernet

Módulo 7

Embaixadores do Programa 2020, 2021 & 2022:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum



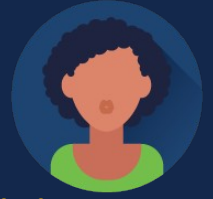
Quadros Ethernet

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:

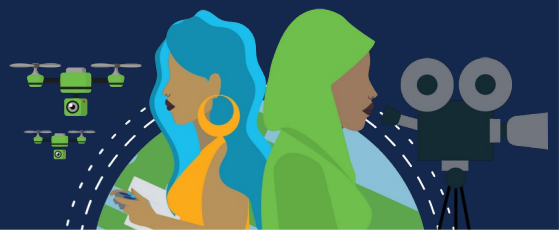
- 10 Mbps
- 100 Mbps
- 1000 Mbps (1 Gbps)
- 10,000 Mbps (10 Gbps)
- 40,000 Mbps (40 Gbps)
- 100,000 Mbps (100 Gbps)

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

Fonte: Cisco



Quadros Ethernet

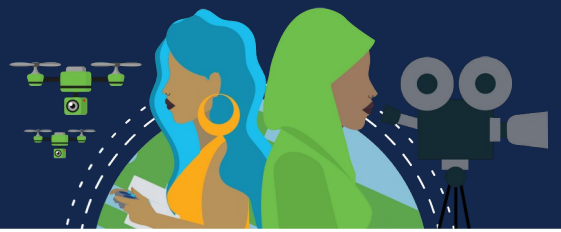


Protocolos IEEE 802 LAN/MAN, incluindo Ethernet, usam as seguintes duas subcamadas separadas da camada de link de dados para operar.
Eles são o controle de link lógico (LLC) e o controle de acesso de mídia (MAC).

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.

Fonte: Cisco



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.

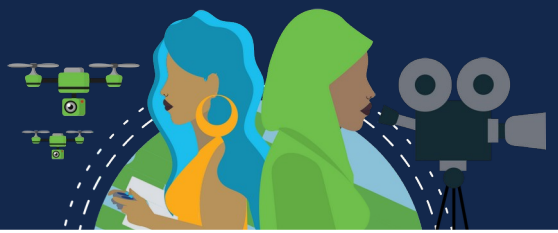
Detecção de erro Ethernet - O quadro Ethernet inclui um trailer de sequência de verificação de quadros (FCS) usado para detecção de erros.

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.

<table>
<tr><td>Camada de Rede</td><td colspan="6">Protocolo de camada de rede</td></tr>
<tr><td rowspan="3">Camada de Enlace de Dados</td><td>Subcamada LLC</td><td colspan="5">Subcamada LLC - IEEE 802.2</td></tr>
<tr><td rowspan="2">Subcamada MAC</td><td colspan="5">Ethernet - IEEE 802.3</td></tr>
<tr><td>IEE 802.3u Fast Ethernet</td><td>IEEE 802.3z Gigabit Ethernet sobre fibra</td><td>IEEE 802.3ab Gigabit Ethernet sobre cobre</td><td>IEEE 802.3ae 10 Gigabit Ethernet sobre fibra</td><td>Etc.</td></tr>
<tr><td colspan="2">Camada Física</td></tr>
</table>

Fonte: Cisco



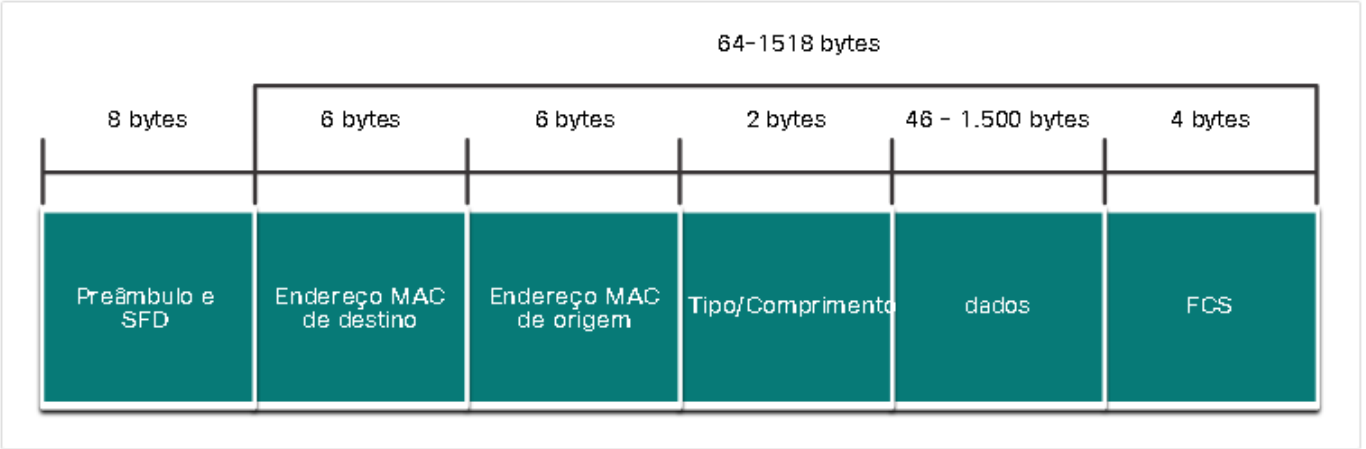
Campos de Quadro Ethernet

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.

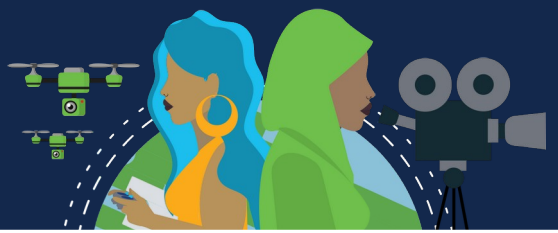
Qualquer quadro com comprimento menor que 64 bytes é considerado um "fragmento de colisão" ou um "quadro desprezível" e é automaticamente descartado pelas estações receptoras.
Quadros com mais de 1.500 bytes de dados são considerados “jumbo” ou “baby giant”.

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



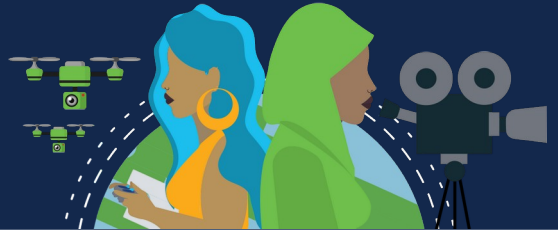
Fonte: Cisco



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.

Fonte: Cisco



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.

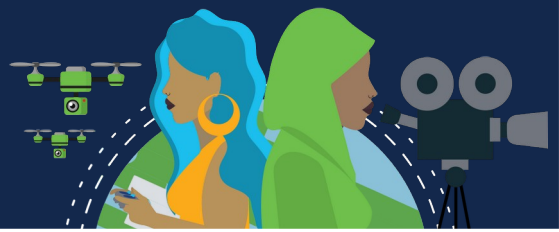
Um endereço MAC Ethernet consiste em um valor binário de 48 bits.
Hexadecimal é usado para identificar um endereço Ethernet porque um único dígito hexadecimal representa quatro bits binários.
Portanto, um endereço MAC Ethernet de 48 bits pode ser expresso usando apenas 12 valores hexadecimais.

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

Fonte: Cisco

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.

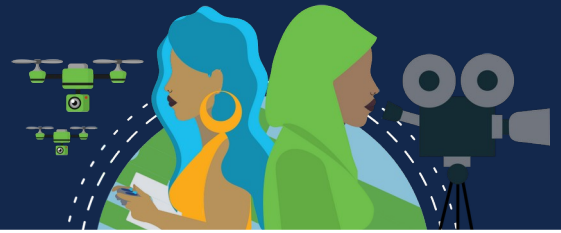
Ao usar hexadecimal, os zeros à esquerda são sempre exibidos para concluir a representação de 8 bits. Por exemplo, na tabela, o valor binário 0000 1010 é mostrado em hexadecimal como 0A.

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).

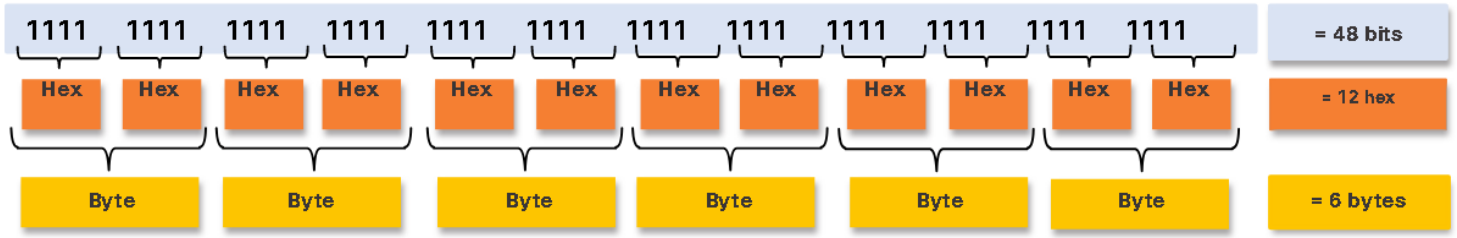
Talvez seja necessário converter entre valores decimal e hexadecimais. Se tais conversões forem necessárias, converta o valor decimal ou hexadecimal em binário e, em seguida, converta o valor binário em decimal ou hexadecimal, conforme apropriado.

Fonte: Cisco



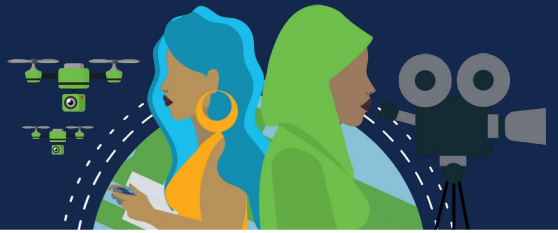
Endereços MAC Ethernet

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).

Fonte: Cisco

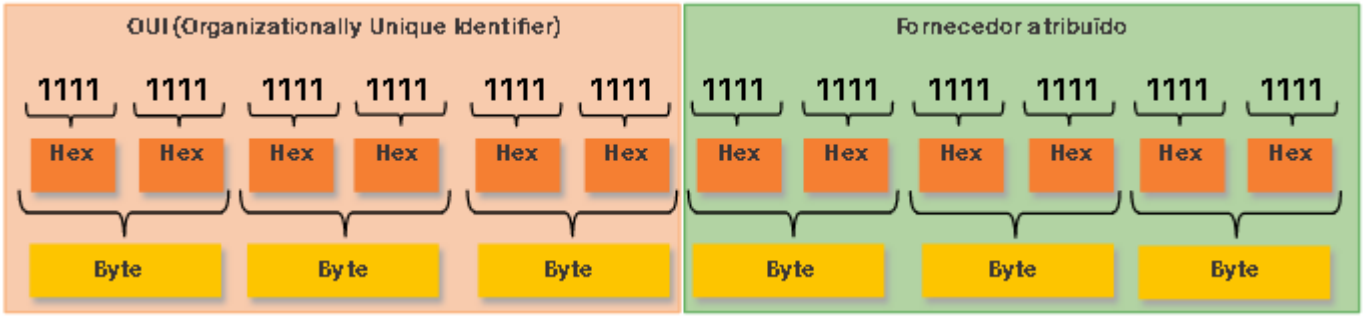


Endereços MAC Ethernet

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

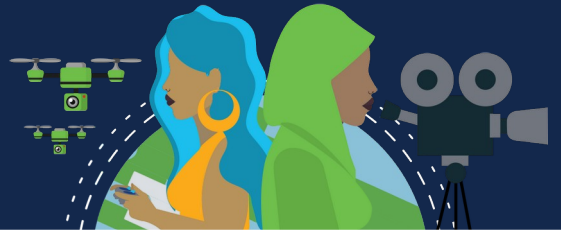
- Usar sua OUI atribuída como os primeiros 6 dígitos hexadecimais.
- Atribuir um valor exclusivo nos últimos 6 dígitos hexadecimais.

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.

Fonte: Cisco



Processamento de Quadros

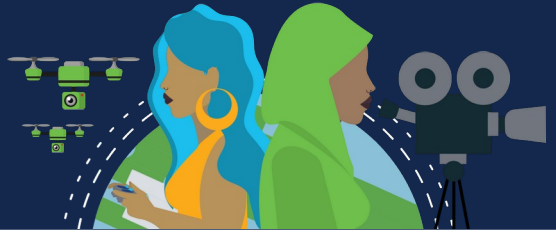
Às vezes, o endereço MAC é referido como endereço gravado de fábrica (BIA, burned-in-address) porque o endereço é codificado na memória somente leitura (ROM) na NIC.
Isso significa que o endereço é codificado no chip da ROM permanentemente.

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.

Fonte: Cisco



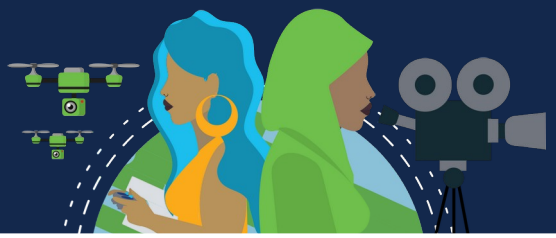
Processamento de Quadros

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.

Fonte: Cisco



Endereço MAC Unicast

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

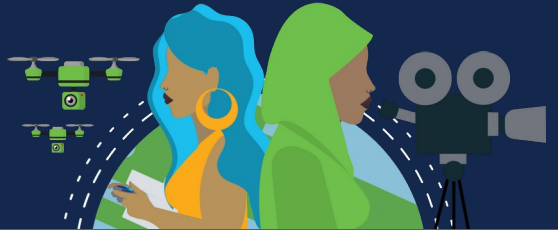
Um endereço MAC de unicast é o endereço exclusivo usado quando um quadro é enviado de um único dispositivo de transmissão para um único dispositivo de destino.

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.

Fonte: Cisco



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:

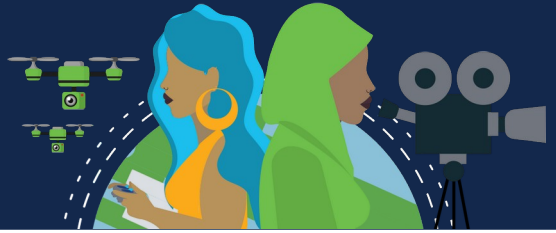
Possui um endereço MAC de destino de FF-FF-FF-FF-FF-FF em hexadecimal (48 números binários (sendo eles no valor de 0 ou 1)).

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.

Fonte: Cisco



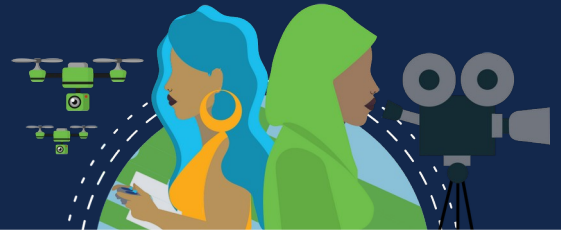
Endereço MAC Multicast

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.

Fonte: Cisco



A Tabela de Endereços MAC

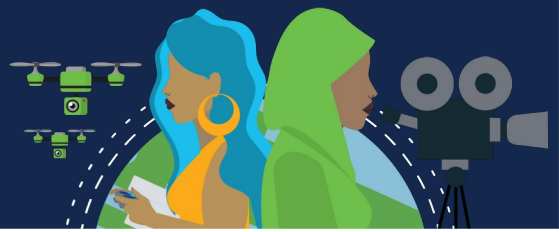
Se um switch apenas encaminhasse cada quadro recebido de todas as portas, sua rede ficaria tão congestionada que provavelmente chegaria a uma parada completa.

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



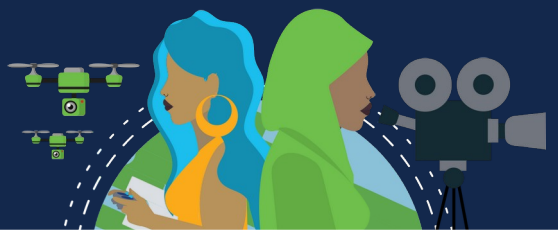
O switch cria a tabela de endereços MAC dinamicamente examinando o endereço MAC de origem dos quadros recebidos em uma porta. O switch encaminha os quadros procurando uma correspondência entre o endereço MAC de destino no quadro e uma entrada na tabela de endereços MAC.
Todo quadro que entra em um switch 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.

Fonte: Cisco

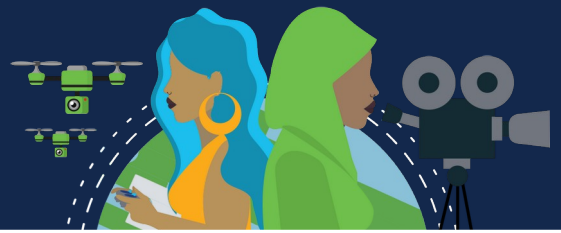


A Tabela de Endereços MAC

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

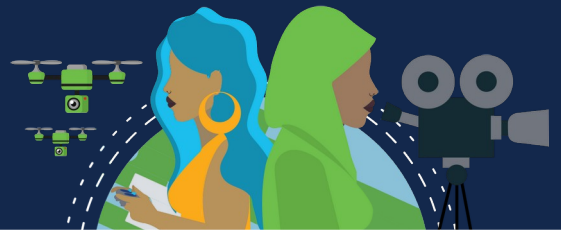
Os switches usam suas tabelas de endereço MAC para determinar qual porta usar para encaminhar quadros. Com os switches Cisco, existem dois métodos de encaminhamento de quadros e há boas razões para usar um em vez do outro, dependendo da situação.

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.

Fonte: Cisco



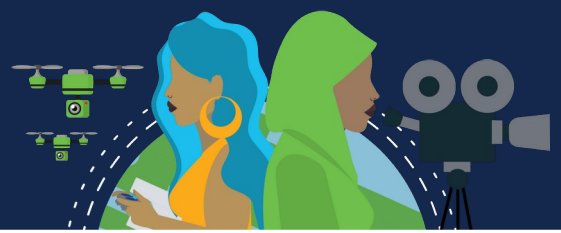
Métodos de encaminhamento e velocidades de switches

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.

Fonte: Cisco



Métodos de encaminhamento e velocidades de switches

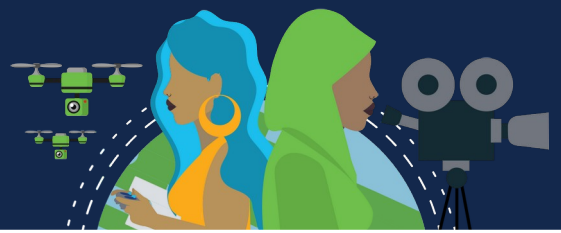
Um switch Ethernet pode usar uma técnica de armazenamento de quadros em buffers antes de enviá-los. O buffer também pode ser usado quando a porta de destino está ocupada devido ao congestionamento. O switch armazena o quadro até que ele possa ser transmitido.

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.

Fonte: Cisco



Métodos de encaminhamento e velocidades de switches

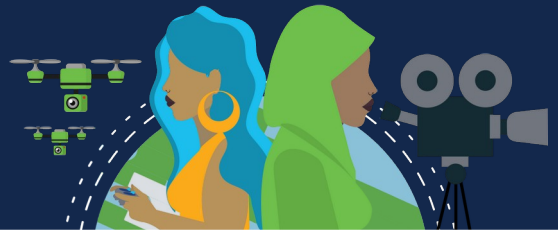
Duas das configurações mais básicas em um switch são as configurações de largura de banda e duplex para cada porta do switch individual.
É fundamental a correspondência dessas configurações na porta do switch e nos dispositivos conectados, como um computador ou outro switch.

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.

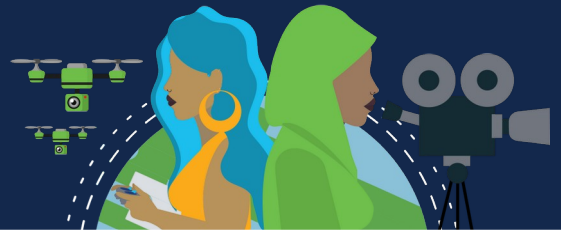


Métodos de encaminhamento e velocidades de switches

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.

Fonte: Cisco

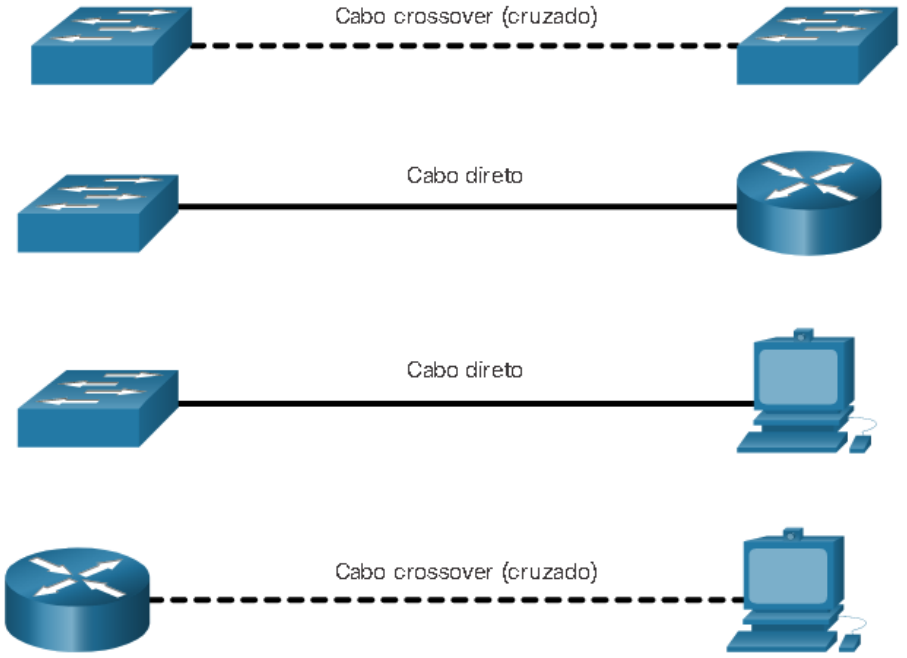


Métodos de encaminhamento e velocidades de switches

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.



Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

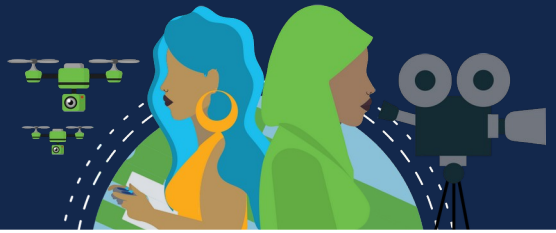
CCNAv7 – ITN – Camada de Rede

Módulo 8

Embaixadores do Programa 2020, 2021 & 2022:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum



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.

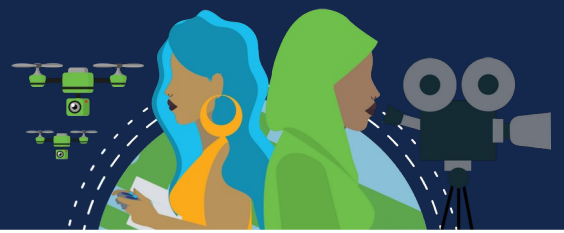
Encapsulamento: A camada de rede encapsula a unidade de dados de protocolo (PDU) da camada de transporte em um pacote, adicionando informações de cabeçalho IP, como os endereços IP dos hosts origem (emissor) e destino (receptor). O processo de encapsulamento é executado pela origem do pacote IP.

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.

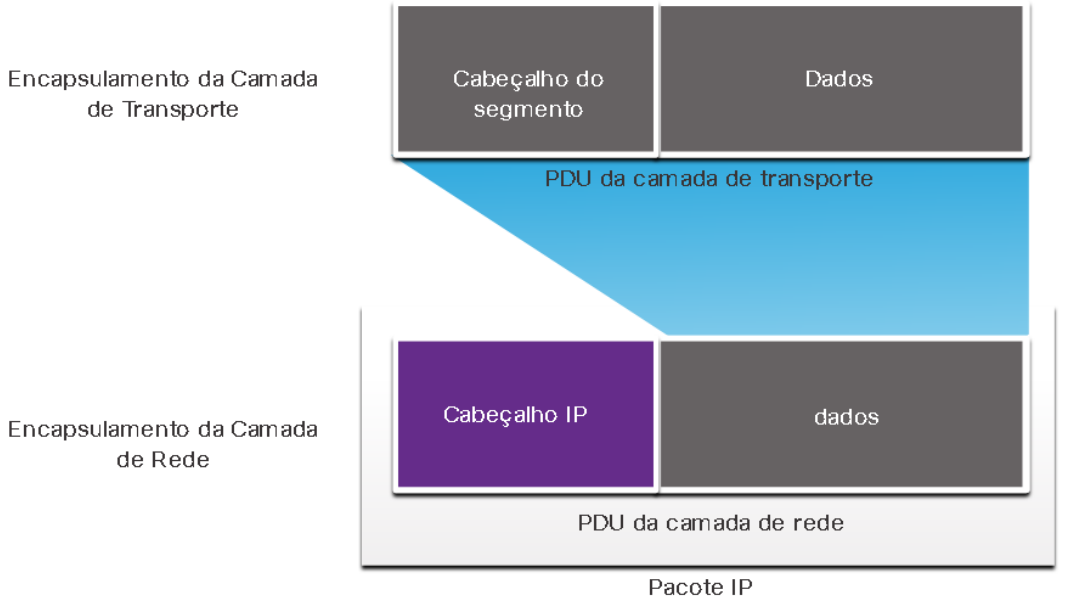
Fonte: Cisco



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.

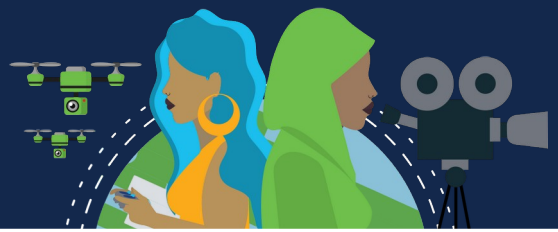
O processo de encapsulamento camada por camada possibilita o desenvolvimento e a expansão dos serviços nas diferentes camadas sem afetar outras camadas. Isso significa que os segmentos da camada de transporte podem ser imediatamente empacotados por IPv4, IPv6 ou qualquer protocolo que venha a ser desenvolvido 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.

Fonte: Cisco



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.

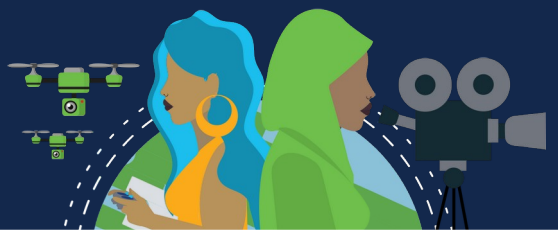
Características básicas da IP:

- **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.

Fonte: Cisco

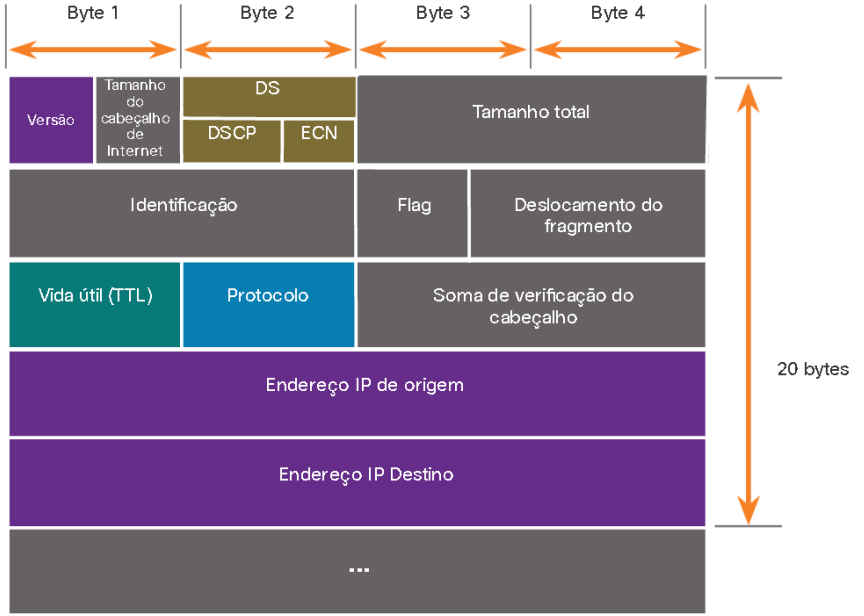


Pacote IPV4

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.

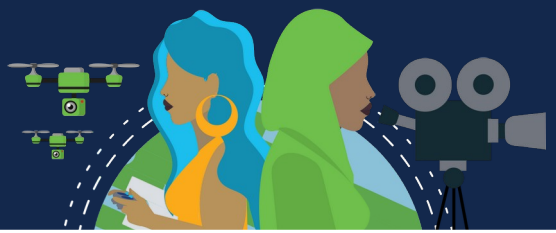
Normalmente, esses endereços não mudam durante a viagem da origem ao destino.



- **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.

Fonte: Cisco



Pacote IPV6

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

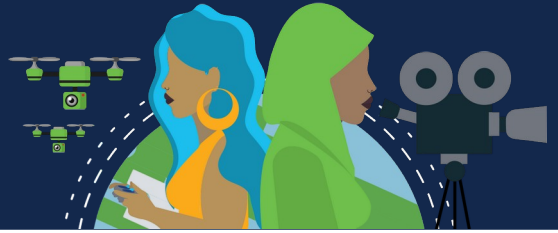
- **Esgotamento do endereço IPv4:** Possui um número limitado de endereços públicos exclusivos disponíveis. Embora haja aproximadamente 4 bilhões de endereços IPv4, o número crescente de novos dispositivos habilitados para IP, conexões sempre ativas e o potencial de crescimento de regiões menos desenvolvidas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

Fonte: Cisco



Pacote IPV6

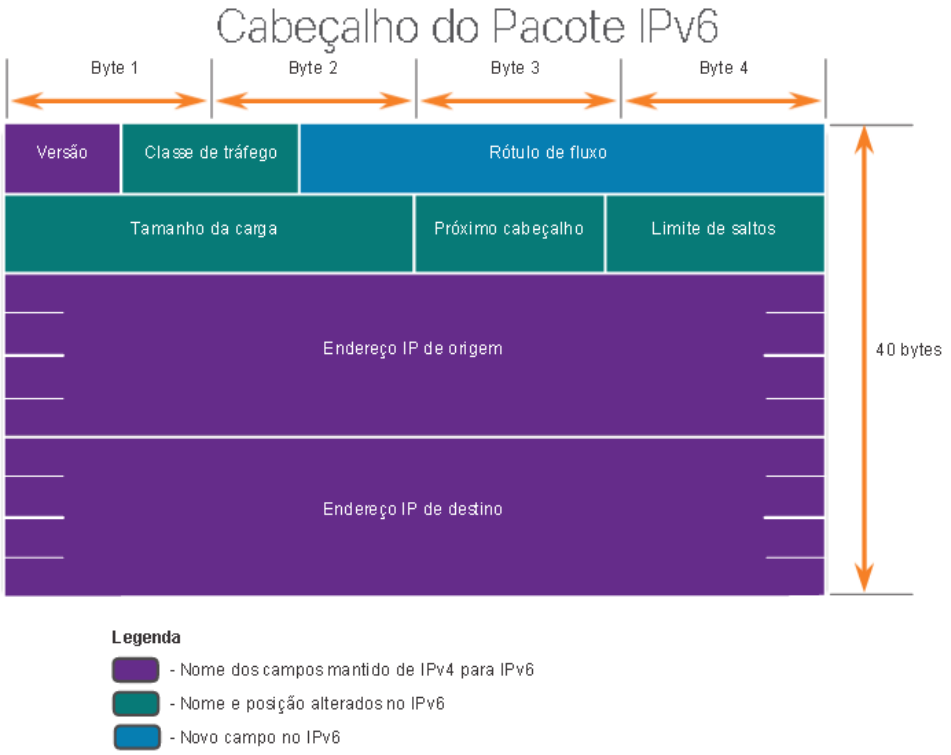
Uma das principais melhorias de design do IPv6 em relação ao IPv4 é o cabeçalho IPv6 simplificado que permite um processamento mais eficiente de cabeçalhos IPv6.

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**.

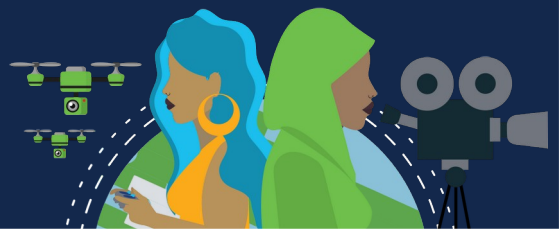
O cabeçalho simplificado do IPv6 consiste em um cabeçalho de comprimento fixo de 40 octetos (em grande parte devido ao comprimento dos endereços IPv6 de origem e de destino).

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**.



Fonte: Cisco

Pacote IPV6



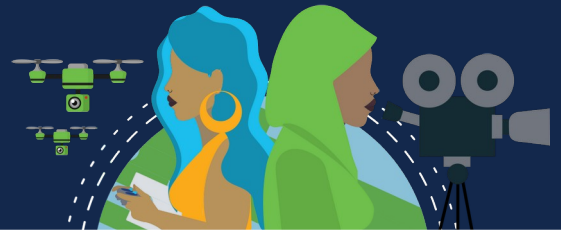
Os campos no cabeçalho do pacote IPv6 incluem o seguinte:

- **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.

Fonte: Cisco



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:

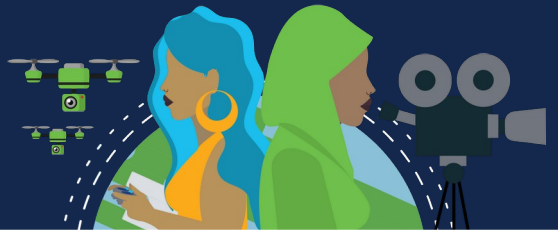
- **Si mesmo:** Um host pode executar ping em si mesmo enviando um pacote para o endereço IPv4 127.0.0.1 ou para o endereço IPv6 ::1, que é referido como a interface de loopback. O ping na interface de loopback testa a pilha de protocolos do TCP/IP no host.
- **Host local:** Host de destino que está 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).

Fonte: Cisco



Introdução ao Roteamento

Cisco Life Changer

Changing the way the world WORKS!

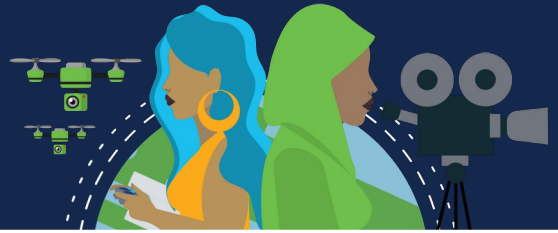
Quando um host envia um pacote para outro host, ele consulta sua tabela de roteamento para determinar para onde enviar o pacote. Se o host de destino estiver em uma rede remota, o pacote será encaminhado para o gateway padrão, que geralmente é o roteador local.
O roteador, desencapsula o cabeçalho Ethernet 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.

Fonte: Cisco



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:

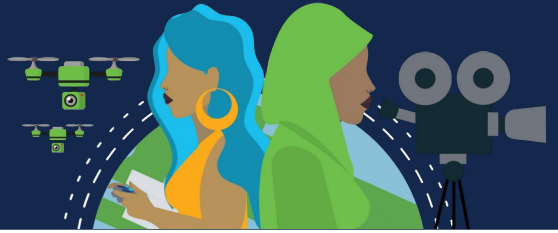
- Uma rota estática deve ser configurada manualmente.
- Precisa ser reconfigurada se houver uma alteração na topologia ou a rota estática não for mais viável.
- Uma rota estática é apropriada para uma rede pequena e quando há poucos ou nenhum vínculo redundante.
- Comumente usada com um protocolo de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

Fonte: Cisco



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#
```

Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

CCNAv7 – ITN – Resolução de endereços

Módulo 9

Embaixadores do Programa 2020, 2021 & 2022:

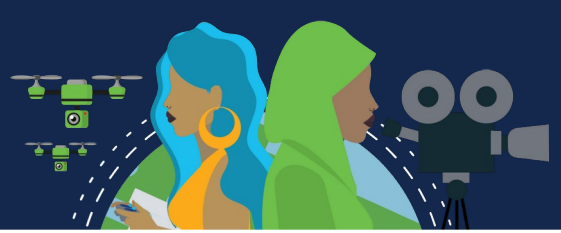
Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

WOMENROCK-IT
Brasil 2021

Networking Academy

Resolução de Endereços



MAC E IP

Destino na Mesma Rede

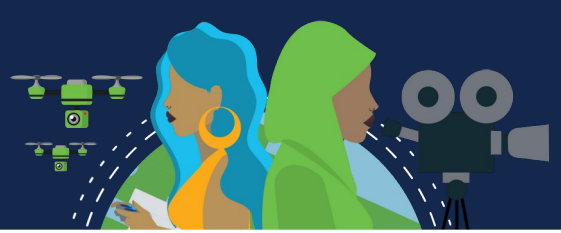
A resolução de endereços é usada quando um host ao enviar uma mensagem sabe apenas o endereço IP do dispositivo e necessita saber o endereço de camada 2, MAC desse mesmo dispositivo.

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.

Fonte: Cisco



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).

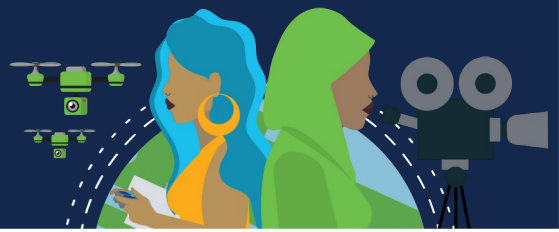
Os roteadores examinam o endereço IPv4 destino para determinar o melhor caminho para encaminhar o pacote IPv4. Quando o roteador recebe o quadro Ethernet, ele desencapsula as informações da Camada 2. Usando o endereço IPv4 de destino, ele determina o dispositivo do próximo salto e, em seguida, encapsula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

Fonte: Cisco

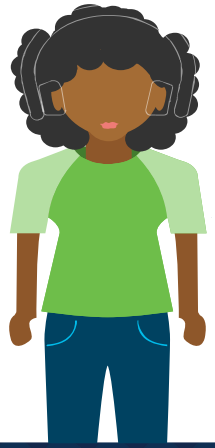
ARP



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.**

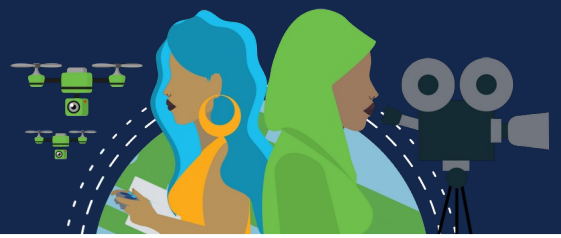
Um dispositivo utiliza o protocolo ARP (Address Resolution Protocol) para determinar o endereço MAC de destino de um dispositivo local quando conhece o endereço IPv4.



O ARP fornece duas funções básicas:

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

Fonte: Cisco



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.

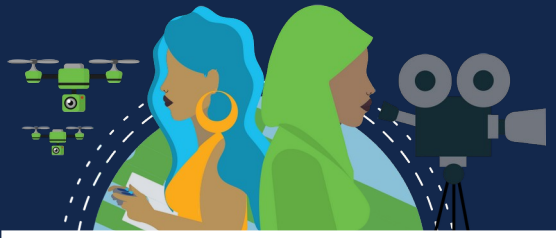
- Se o endereço IPv4 destino do pacote estiver na mesma rede que o endereço IPv4 origem, o dispositivo pesquisará o endereço IPv4 destino na tabela ARP.
- Se o endereço IPv4 destino do pacote estiver em uma rede diferente do endereço IPv4 origem, o dispositivo pesquisará o endereço IPv4 do gateway padrão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

Fonte: Cisco



Solicitação ARP

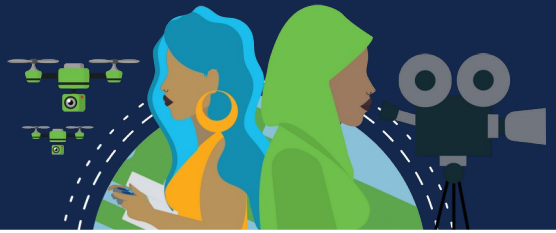
A requisição ARP é encapsulada em um quadro Ethernet, sem cabeçalho IPv4, usando as seguintes informações de cabeçalho:

- **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.

Fonte: Cisco



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.

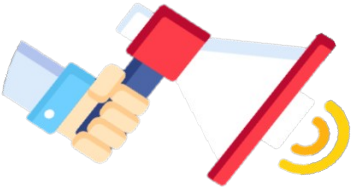
As entradas na tabela ARP têm carimbo de data/hora (timestamp), que são removidas, caso o dispositivo não receba um quadro de um dispositivo específico antes que o carimbo expire.

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**.

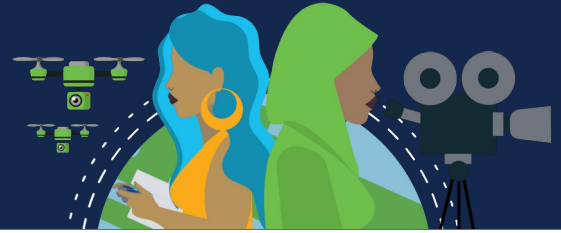
Fonte: Cisco

WireShark



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

Fonte: Cisco



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.

Fonte: Cisco

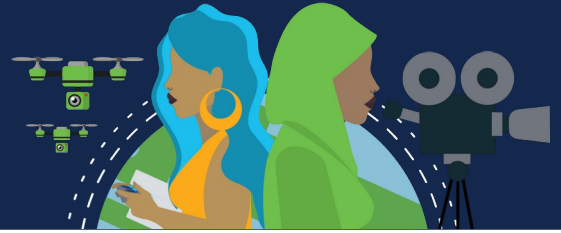


Tabela ARP

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.

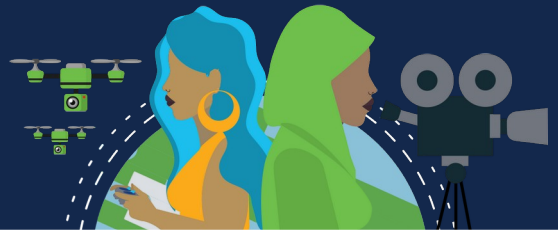
Os comandos também podem ser usados para remover manualmente algumas ou todas as entradas na tabela ARP. Após a remoção de uma entrada, o processo de envio de uma requisição ARP e de recebimento de uma resposta ARP deve ocorrer novamente para inserir o mapa na tabela ARP.

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#
```

Fonte: Cisco

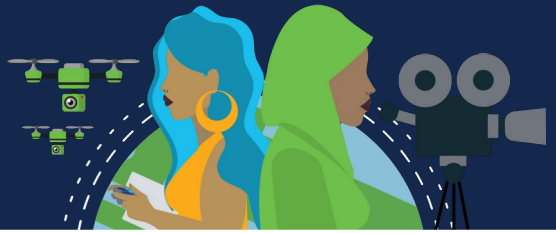


Problemas de ARP

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.

Fonte: Cisco



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.

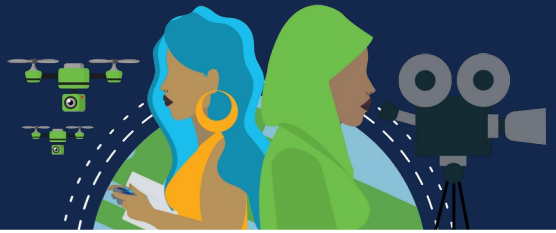
As mensagens de solicitação de vizinho e anúncio de vizinho são usadas para mensagens de dispositivo a dispositivo, como resolução de endereço (semelhante ao ARP para IPv4). Os dispositivos incluem computadores e roteadores.

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.

Fonte: Cisco



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.

Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

CCNAv7 – ITN – Configuração básica do roteador

Módulo 10

Embaixadores do Programa 2020, 2021 & 2022:

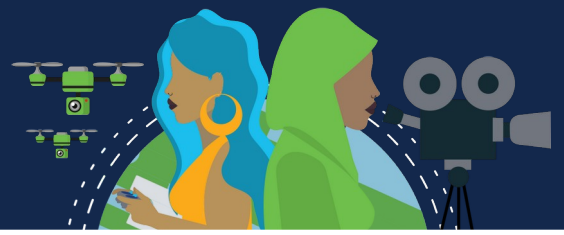
Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

WOMENROCK-IT
Brasil 2021

Networking Academy

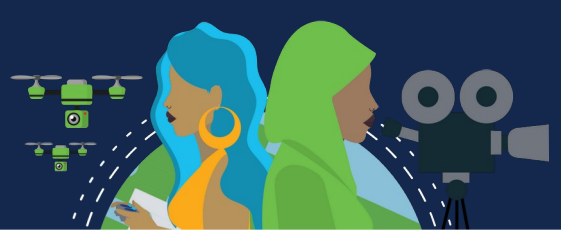
Configuração básica do roteador



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***

Fonte: Cisco



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.

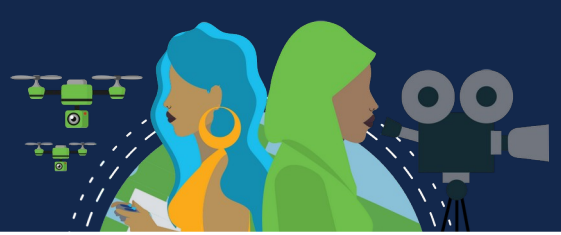
Todo o acesso ao roteador deve ser protegido, o modo EXEC privilegiado, o modo EXEC do usuário, o acesso remoto via telnet e SSH e as senhas de texto simples devem ser criptografadas.

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.

Fonte: Cisco



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
```

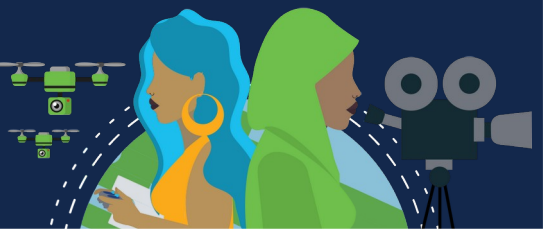
O uso do comando **description** é recomendável por ser útil na solução de problemas, fornecendo informações sobre o tipo de rede conectada. O texto da descrição está limitado a 240 caracteres.

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.

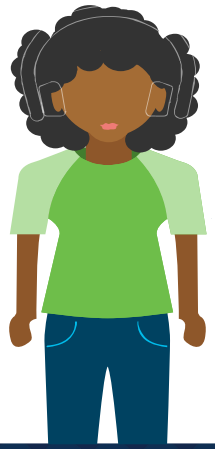
Observação: Em conexões entre roteadores onde não há switch Ethernet, ambas as interfaces de interconexão devem ser configuradas e habilitadas.

Fonte: Cisco

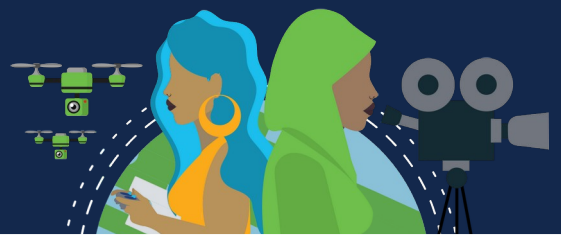
Exemplo de configuração de interfaces



```
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
```



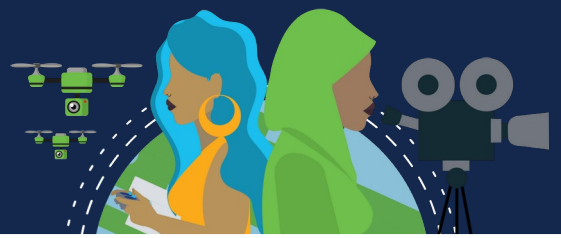
Fonte: Cisco



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.

Fonte: Cisco



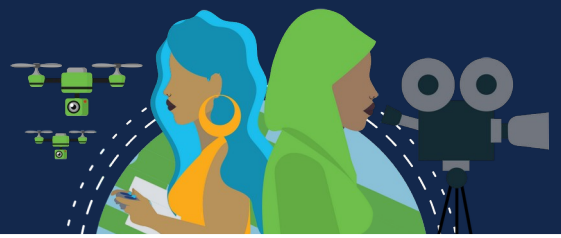
Verificação da Configuração

Black Lives Matter

```
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
```

Fonte: Cisco



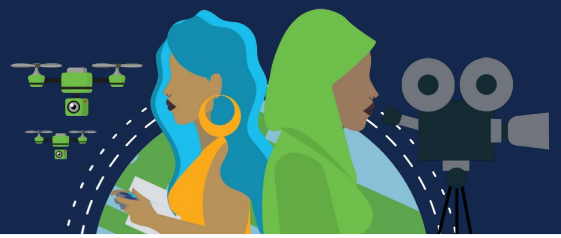
Verificação da Configuração

Black Lives Matter

```
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#
```

Fonte: Cisco



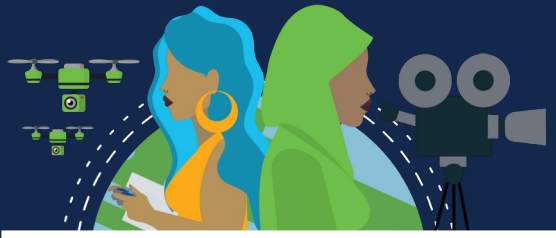
Verificação da Configuração

Black Lives Matter

```
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
```

Fonte: Cisco



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.

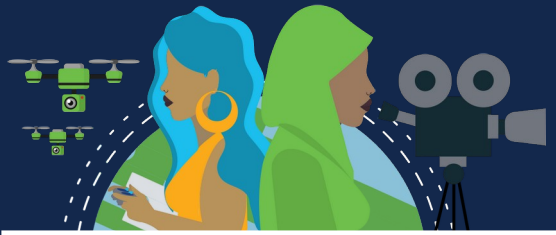
O endereço IP do dispositivo host e o endereço da interface do roteador devem estar na mesma rede.

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.

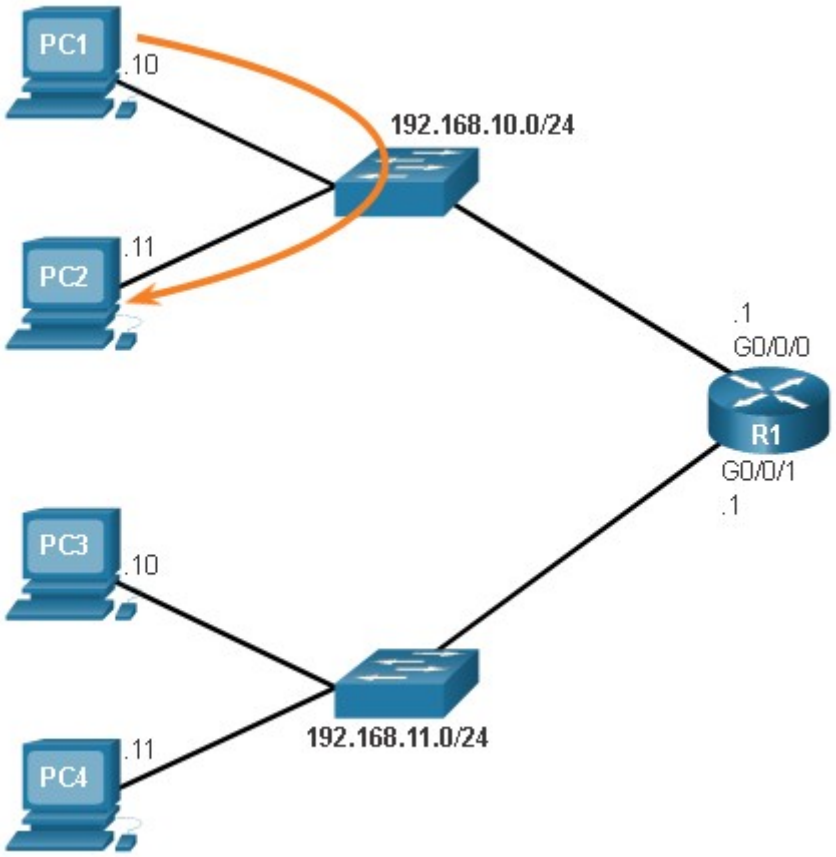
Ao enviar um pacote para um host em outra rede, o pacote é endereçado com o IPv4 do host destino mas encaminhado para a interface do gateway padrão. O roteador aceita o pacote, acessa sua tabela de roteamento e determina qual a interface apropriada para encaminhar o pacote, com base no endereço de destino e encaminha o pacote para fora da interface de saída para alcançar o host de destino.

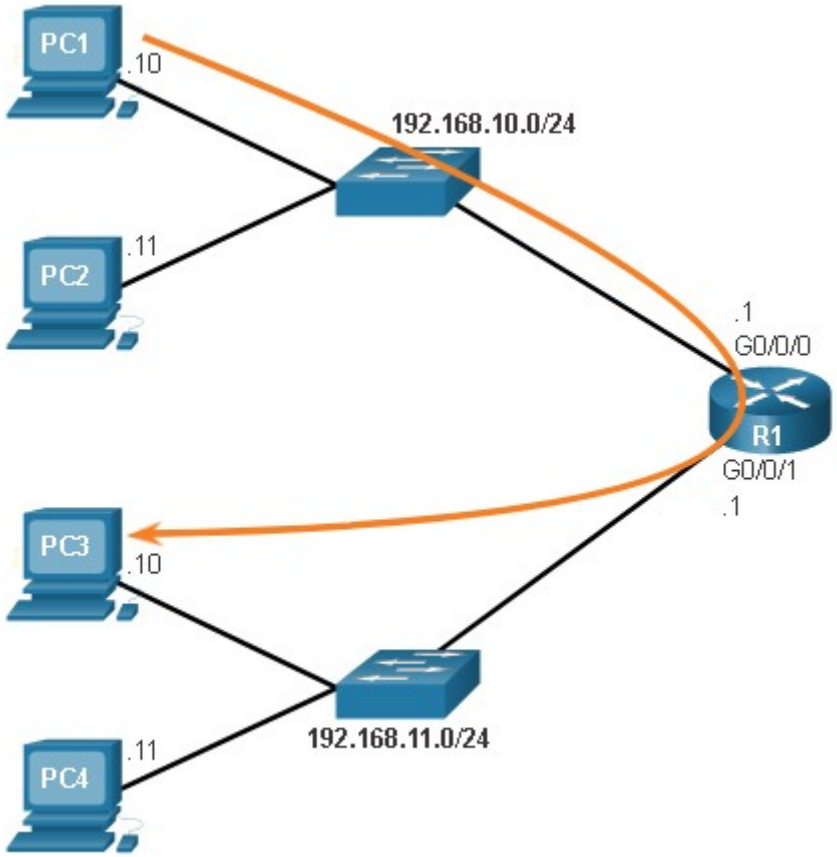
O mesmo processo ocorre numa rede IPv6.

Fonte: Cisco

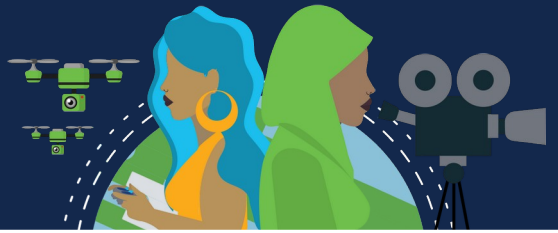


Gateway Padrão em Host





Fonte: Cisco



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.

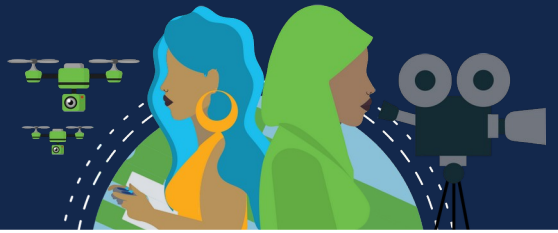
O endereço de gateway padrão geralmente é configurado em todos os dispositivos que se comunicam além da rede local.

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.

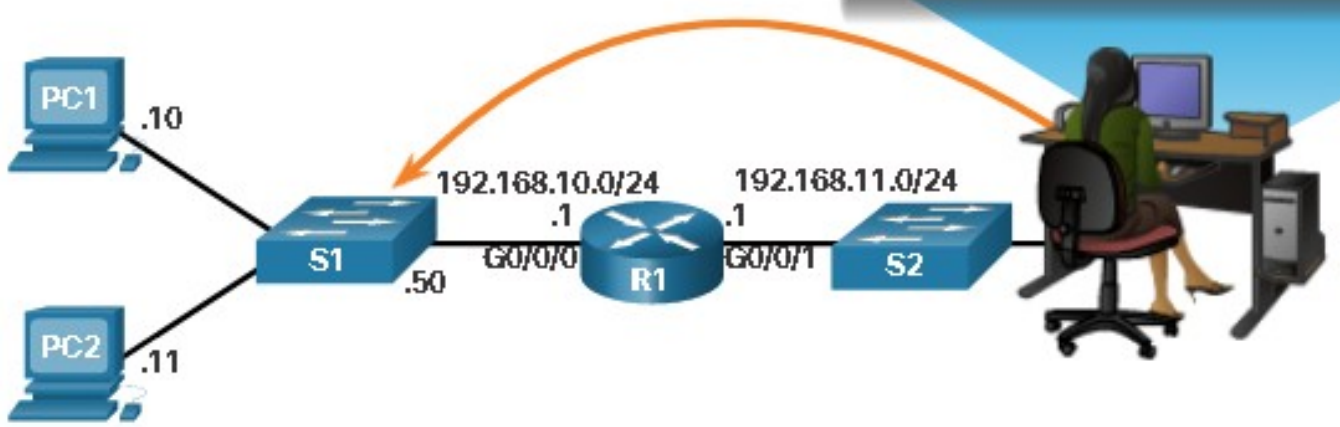
Um switch de grupo de trabalho também pode ser configurado com um endereço IPv6 em um SVI. No entanto, o switch não requer que o endereço IPv6 do gateway padrão seja configurado manualmente. O switch receberá automaticamente seu gateway padrão da mensagem de anúncio do roteador ICMPv6 do roteador.

Fonte: Cisco



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>
```



Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

CCNAv7 – ITN – Endereçamento IPv4

Módulo 11

Embaixadores do Programa 2020, 2021 & 2022:

Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

WOMENROCK-IT
Brasil 2021

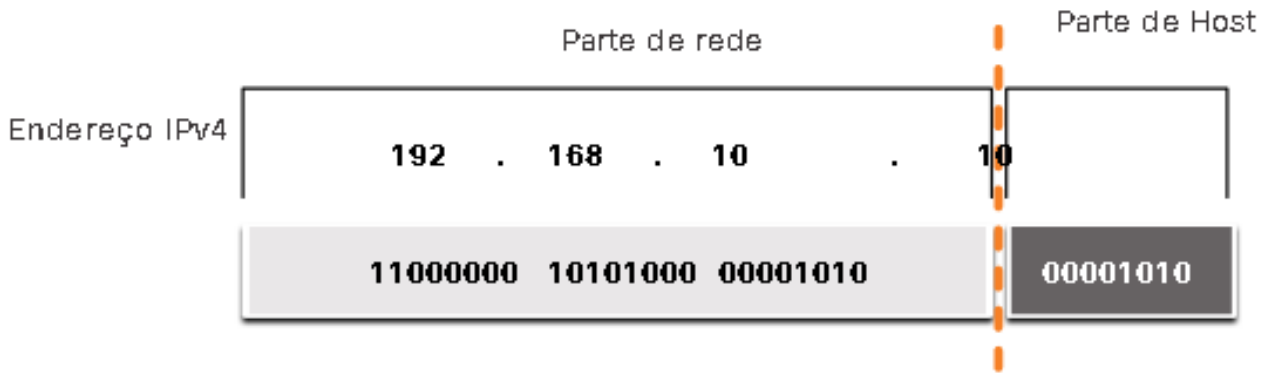
Networking Academy

Endereçamento IPv4

Estrutura do Endereço IPv4

Partes de Rede e de Host

Um endereço IPv4 é um endereço hierárquico de 32 bits, composto por uma parte da rede e uma parte do host. Ao determinar a parte da rede versus a parte do host, você deve observar o fluxo de 32 bits.

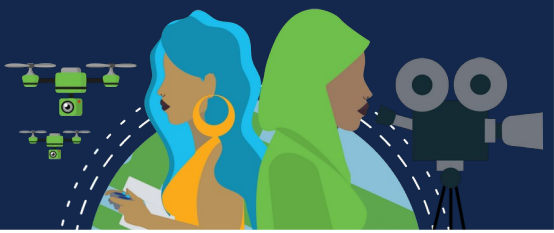


Os bits na **parte de rede** do endereço devem ser iguais em todos os dispositivos que residem na mesma rede. Os bits na **parte de host** do endereço devem ser exclusivos para identificar um host específico dentro de uma rede.

Através da mascara de sub-rede os hosts sabem qual parte dos 32 bits identifica a rede.

Fonte: Cisco

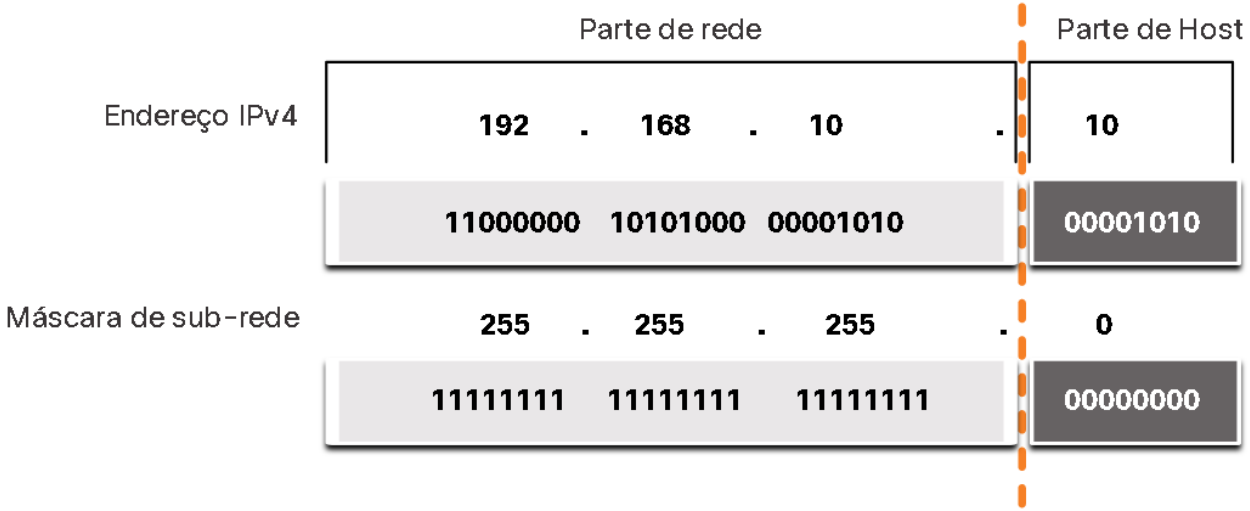
Estrutura do Endereço IPv4

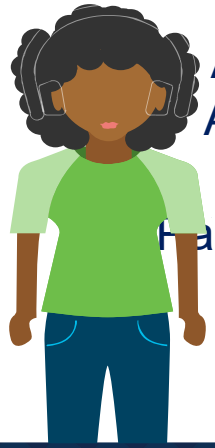


Máscara de Sub-Rede

Ao configurar um host com um endereço IPv4 requer;

Endereço IPv4: Endereço IPv4 exclusivo do host.
Máscara de sub-rede: Usada para identificar a parte da rede / host do endereço IPv4.
Endereço IPv4 de gateway padrão: Necessário para acessar redes remotas.
Endereços IPv4 do servidor DNS: Necessários para converter nomes de domínio em endereços IPv4.



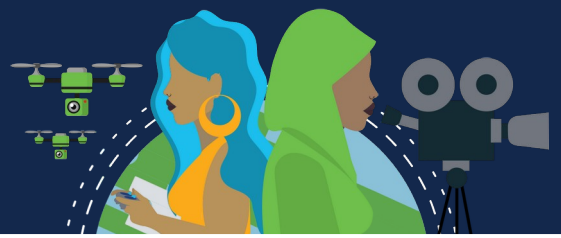


A máscara de sub-rede é usada para diferenciar a parte da rede da parte do host de um endereço IPv4. Ao atribuir o endereço IPv4 a um dispositivo, a máscara é usada para determinar o endereço de rede do dispositivo. O endereço de rede representa todos os dispositivos na mesma rede.

Para identificar as partes da rede e do host de um endereço IPv4, a máscara de sub-rede é comparada com o endereço IPv4 bit por bit, da esquerda para a direita.

O processo real usado para identificar a parte da rede e a parte de host é chamado de AND.

Fonte: Cisco



Estrutura do Endereço IPv4

Comprimento do Prefixo

O comprimento do prefixo é o número de bits definido como 1 na máscara de sub-rede.

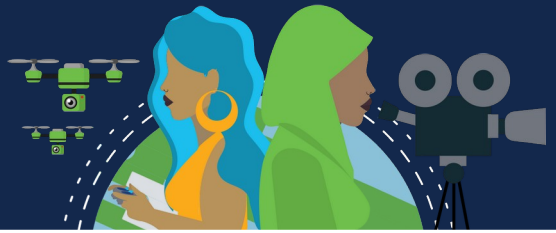
Está escrito em "notação de barra", que é anotada por uma barra (/) seguida pelo número de bits definido como 1.

Um endereço de rede também é referido como prefixo ou prefixo de rede.

Ao representar um endereço IPv4 usando um comprimento de prefixo, o endereço IPv4 é gravado seguido do comprimento do prefixo sem espaços. Exemplo; 192.168.10.10 255.255.255.0 seria gravado como 192.168.10.10/24.

Máscara de Sub-Rede	Endereço de 32 bits	Comprimento do Prefixo
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Fonte: Cisco



Estrutura do Endereço IPv4

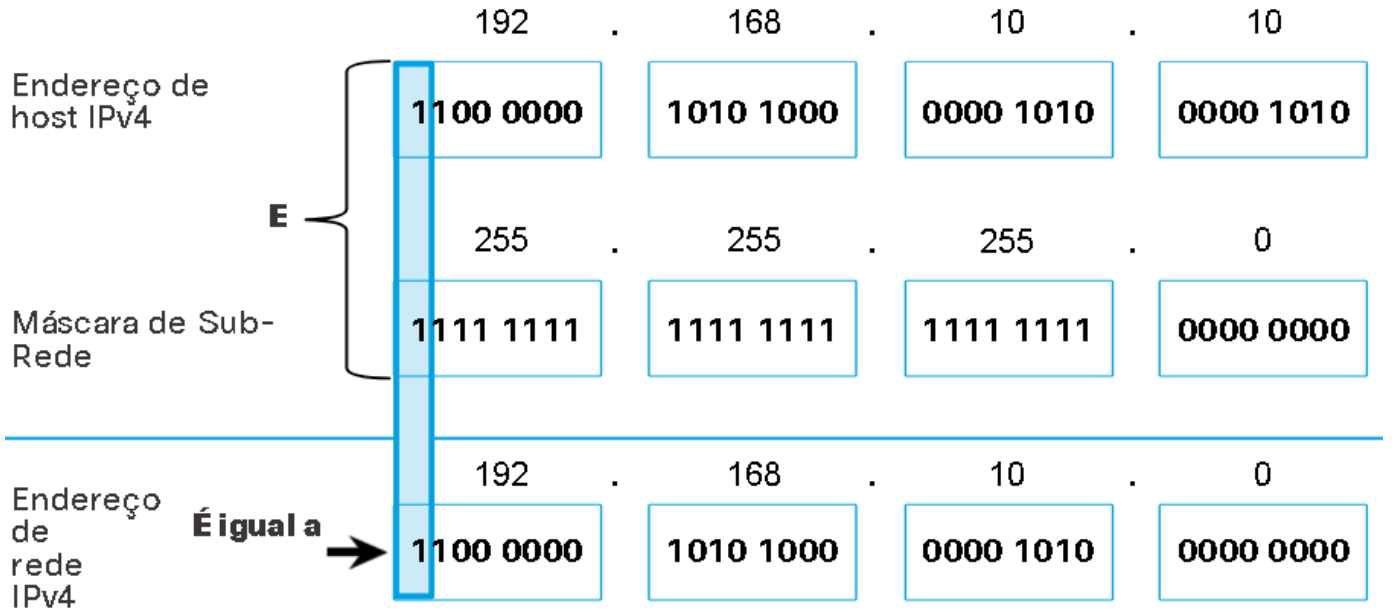
Lógica AND

Um AND lógico é uma das três operações booleanas usadas na lógica booleana ou digital. As outras duas são OR e NOT. A operação AND é usada para determinar o endereço de rede.

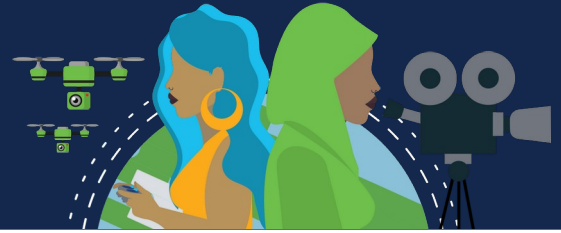
AND lógico é a comparação de dois bits que produz os resultados mostrados abaixo. 1 representa Verdadeiro e 0 representa Falso. Ao usar uma operação AND, ambos os valores de entrada devem ser Verdadeiro (1) para que o resultado seja Verdadeiro (1). Qualquer outra combinação resulta em um 0.

- 1 E 1 = 1
- 0 E 1 = 0
- 1 E 0 = 0
- 0 E 0 = 0

Para identificar o endereço de rede de um host IPv4, é feito um AND lógico, bit a bit, entre o endereço IPv4 e a máscara de sub-rede, o resultado é o endereço de rede.



Fonte: Cisco



Estrutura do Endereço IPv4

Endereços de Broadcast, de Host e de Rede

Dentro de cada rede há três tipos de endereços IP:

- **Endereço de Rede:** Representa uma rede específica. *Por exemplo: 192.168.10.0/24*
- **Endereços de Host:** São endereços que podem ser atribuídos a um dispositivo. A parte do host é representada pelos bits indicados por 0 bits na máscara de sub-rede. Podem ter qualquer combinação de bits, exceto todos os 0 bits, pois este é o endereço de rede, ou todos os 1 bits, pois este é o endereço de broadcast. As demais combinações dentro desse intervalo são os endereços de hosts disponíveis de um endereço de rede.

Todos os dispositivos dentro da mesma rede devem ter a mesma máscara de sub-rede e os mesmos bits de rede. Somente os bits do host serão diferentes e devem ser exclusivos.

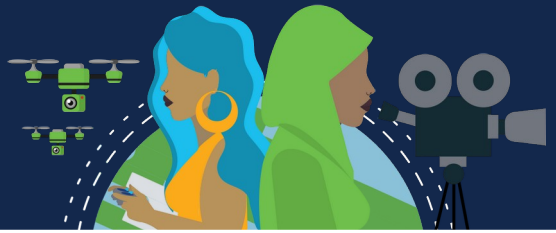
O primeiro endereço de host dentro de uma rede tem todos os 0 bits com o último bit (mais à direita) como um bit. *Exemplo: 192.168.10.1/24*

O último endereço de host dentro de uma rede tem todos os 1 bits com o último bit (mais à direita) como um bit 0. *Exemplo: 192.168.10.254/24*

Qualquer endereço entre e inclusive, 192.168.10.1/24 a 192.168.10.254/24 são endereços de hosts disponíveis no endereço de rede 192.168.10.0/24

- **Endereço de broadcast:** é usado quando é necessário acessar todos os dispositivos na rede IPv4. Tem todos os 1 bits na parte do host, conforme determinado pela máscara de sub-rede. Um endereço de broadcast não pode ser atribuído a um dispositivo. *Exemplo: 192.168.10.255/24*

Fonte: Cisco



Unicast, broadcast e multicast IPv4

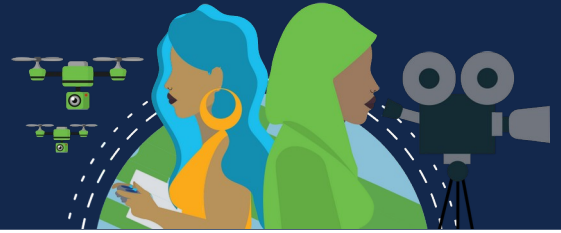
Unicast

Comunicação um-para-um : Envio de uma mensagem de um dispositivo para um único destino em uma rede IPV4.

O pacote unicast tem um endereço de destino que é um endereço unicast pois vai para um único destinatário. O endereço IP de origem sempre será um endereço unicast, independentemente de o endereço de destino ser unicast, broadcast ou multicast.

Os endereços de host unicast IPv4 estão no intervalo de endereços de 1.1.1.1 a 223.255.255.255. Contudo, dentro desse intervalo há muitos endereços que já são reservados para fins especiais, discutidos mais adiante neste módulo.

Fonte: Cisco



Unicast, broadcast e multicast IPv4

Broadcast

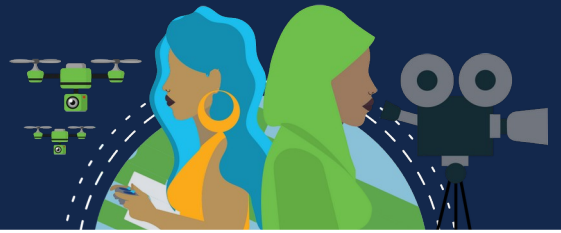
Comunicação um para todos: Envio de uma mensagem de um dispositivo para todos em uma rede IPV4. Não há pacotes de broadcast com IPv6.

Um domínio de broadcast identifica todos os hosts no mesmo segmento de rede.
O pacote de broadcast possui no endereço de destino todos os (1s) na parte do host ou 32 (um) bits.
É recebido e processado por todos os dispositivos no mesmo domínio de broadcast.

Broadcast direcionado é enviado para o endereço de broadcast em um endereço de rede específico.
Exemplo: 172.16.4.255/24.
Broadcast limitado é enviado para 255.255.255.255.

Quando o switch recebe o pacote de broadcast, ele o encaminha para todas as portas, exceto a porta de entrada do pacote.
Por padrão, os roteadores não encaminham broadcasts.
Envio de broadcasts usam recursos na rede e faz com que todos os hosts receptores processem o pacote, podendo prejudicar o desempenho da rede ou dos dispositivos.
Roteadores separam domínios de broadcast, subdividir as redes melhora o desempenho eliminando o excesso de tráfego broadcast.
Devido a preocupações de segurança e abuso prévio de usuários mal-intencionados, broadcasts direcionados são desativados por padrão, começando com o Cisco IOS Release 12.0 com o comando de configuração global *no ip directed-broadcasts*.

Fonte: Cisco



Unicast, broadcast e multicast IPv4

Multicast

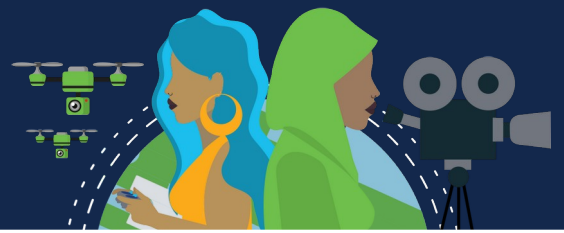
Reduz o tráfego permitindo que um host envie um único pacote para um conjunto de hosts que participem de um grupo multicast.

Um pacote multicast é um pacote com um endereço IP de destino que é um endereço multicast. O IPv4 reservou os endereços 224.0.0.0 a 239.255.255.255 como intervalo de multicast.

Os hosts que participam de um grupo multicast são chamados de clientes multicast e usam serviços solicitados por um programa cliente para se inscrever no grupo multicast.

Cada grupo é representado por um único endereço IPv4 de destino. Quando um host IPv4 se inscreve em um grupo multicast, o host processa pacotes endereçados tanto a esse endereço multicast como a seu endereço unicast alocado exclusivamente.

Protocolos de roteamento, como OSPF, usam multicast. Roteadores habilitados com OSPF se comunicam entre si usando o endereço multicast 224.0.0.5. Somente dispositivos habilitados com OSPF processarão esses. Todos os outros dispositivos descartam esses pacotes.



Tipos de endereços IPv4

Endereços IPv4 Públicos e Privados

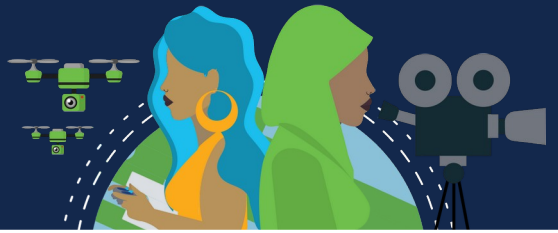
Endereços IPv4 públicos são endereços roteados globalmente entre os roteadores do provedor de serviços de Internet (ISP).

Endereços privados são usados pela maioria das organizações para atribuir endereços IPv4 a hosts internos e não são roteados globalmente.

Foram introduzidos em meados dos anos 90, com a introdução da World Wide Web (WWW), devido ao esgotamento do espaço de endereços IPv4. Os endereços IPv4 privados não são exclusivos e podem ser usados internamente em qualquer rede. São definidos na RFC 1918 e às vezes referidos como espaço de endereço RFC 1918.

Endereço de rede e prefixo	RFC 1918 Intervalo de endereçosprivados
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Fonte: Cisco



Tipos de endereços IPv4

Roteamento para a Internet

A maioria das redes internas, de grandes empresas a redes domésticas, usa endereços IPv4 privados para endereçar todos os dispositivos internos (intranet), incluindo hosts e roteadores. No entanto, os endereços privados não são globalmente roteáveis.

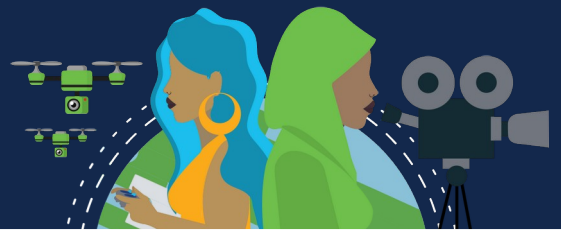
Um pacote com um endereço privado, no endereço de origem, e um endereço IPv4 de destino público (globalmente roteável) como destino devem ser filtrados (descartados) ou traduzidos para um endereço público antes de encaminhar o pacote para um ISP, usando Network Address Translation (NAT).

O NAT é usado para converter entre endereços IPv4 privados e IPv4 públicos. Isso geralmente é feito no roteador que conecta a rede interna à rede ISP. Os endereços IPv4 privados na intranet da organização serão traduzidos para endereços IPv4 públicos antes do encaminhamento para a Internet.

O IETF não considera endereços IPv4 privados ou NAT como medidas de segurança eficazes.

Organizações que têm recursos disponíveis para a Internet, como um servidor Web, também terão dispositivos com endereços IPv4 públicos. Esta parte da rede é conhecida como a DMZ (zona desmilitarizada).

Fonte: Cisco



Tipos de endereços IPv4

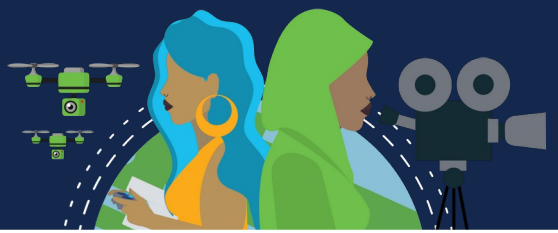
Endereços IPv4 de Uso Especial

Determinados endereços, como o endereço de rede e o endereço de broadcast, não podem ser atribuídos aos hosts. Há endereços especiais que podem ser atribuídos a hosts, mas com restrições quanto ao modo como interagem na rede.

Os endereços de loopback (127.0.0.0 / 8 ou 127.0.0.1 a 127.255.255.254) são mais comumente identificados como apenas 127.0.0.1, esses são endereços especiais usados por um host para direcionar o tráfego para si próprio, usado em um host para testar se a configuração TCP / IP está operacional.

Os endereços locais de link (169.254.0.0 / 16 ou 169.254.0.1 a 169.254.255.254) são mais conhecidos como endereçamento IP privado automático (APIPA) ou endereços auto-atribuídos. Eles são usados por um cliente DHCP do Windows para auto-configurar no caso de não existirem servidores DHCP disponíveis. Endereços de link local podem ser usados em uma conexão ponto a ponto, mas não são comumente usados para esse fim.

Fonte: Cisco



Tipos de endereços IPv4

Endereçamento Classful Legado

Em 1981, os endereços IPv4 eram atribuídos usando o endereço classful, definido na RFC 790, que dividiu os intervalos de unicast em classes da seguinte maneira:

Classe A (0.0.0.0/8 to 127.0.0.0/8) – Para redes grandes. Usou um prefixo fixo /8, com o primeiro octeto indicando o endereço de rede e os três octetos restantes para endereços de host (mais de 16 milhões de endereços de host por rede).

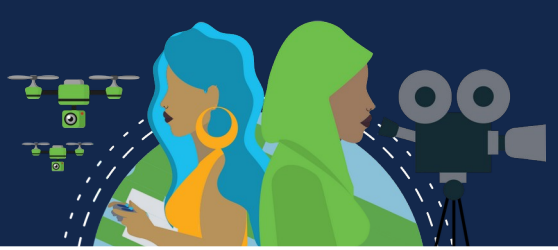
Classe B (128.0.0.0 /16 - 191.255.0.0 /16) – Para de redes de tamanho moderado a grande. Usou um prefixo fixo /16, com os dois primeiros octetos indicando o endereço de rede e os dois octetos restantes para endereços de host (mais de 65.000 endereços de host por rede).

Classe C (192.0.0.0 /24 - 223.255.255.0 /24) - Para redes pequenas. Usou um prefixo fixo / 24, com os três primeiros octetos para indicar a rede e o octeto restante para os endereços de host (apenas 254 endereços de host por rede).

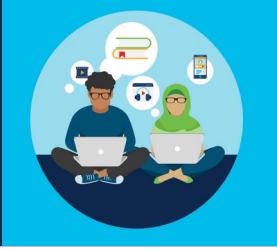
Havia um bloco multicast de Classe D de 224.0.0.0 a 239.0.0.0 e um bloco experimental de Classe E de 240.0.0.0 - 255.0.0.0.

Na época era um meio eficaz para alocar endereços. A classe A representaram 50% das redes IPv4. Isso fez com que a maioria dos endereços IPv4 disponíveis não fossem utilizados. Em meados da década de 1990, com a introdução da World Wide Web, o endereçamento ficou obsoleto limitando o espaço de endereços IPv4 e foi substituída por endereçamento sem classe, que é usado hoje.

Fonte: Cisco



Tipos de endereços IPv4



Atribuição de Endereços IP

Endereços IPv4 públicos são endereços roteados globalmente pela Internet. Endereços IPv4 públicos devem ser exclusivos.

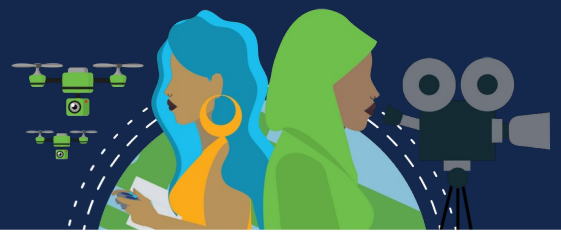
Os endereços IPv4 e IPv6 são gerenciados pela IANA (Internet Assigned Numbers Authority). A IANA gerencia e aloca blocos de endereços IP aos registros regionais de Internet (RIRs). Os cinco RIRs são mostrados na figura.

Os RIRs são responsáveis por alocar endereços IP aos ISPs que fornecem blocos de endereços IPv4 para organizações e ISPs menores. As organizações também podem obter seus endereços diretamente de um RIR (sujeito às políticas desse RIR).

Regional Internet Registries

- **AfriNIC** (Centro de Informação de Redes Africanas) - Região da África
- **APNIC** (Centro de informações de redes da Ásia-Pacífico) - Região Ásia/Pacífico
- **ARIN** (Registro Americano de Números da Internet) - Região da América do Norte
- **LACNIC** (Registro regional de endereços IP da América Latina e do Caribe) - América Latina e algumas ilhas do Caribe
- **RIPE NCC** (Centro de coordenação da rede Réseaux IP Européens) - Europa, Oriente Médio e Ásia Central

Fonte: Cisco



Segmentação de rede

Domínios de broadcast e segmentação

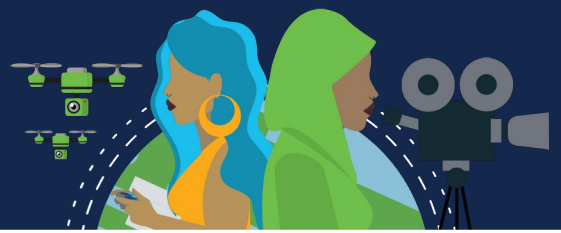
Em uma LAN Ethernet, os dispositivos usam broadcast e o Protocolo de Resolução de Endereços (ARP) para localizar outros dispositivos. O ARP envia mensagens da Camada 2 para um endereço IPv4 conhecido na rede local para descobrir o endereço MAC associado. Os dispositivos em LANs Ethernet também localizam outros dispositivos usando serviços. Um host normalmente adquire sua configuração de endereço IPv4 usando o protocolo DHCP (Dynamic Host Configuration Protocol), enviando mensagens na rede local para localizar um servidor DHCP.

Os switches propagam broadcasts por todas as interfaces, exceto a interface em que foram recebidos.

Roteadores não propagam broadcasts. Quando um roteador recebe um broadcast, ele não o encaminha por outras interfaces.

Portanto, cada interface do roteador se conecta a um domínio de broadcast especifico, segmentando as redes e o trafego broadcast é propagado apenas dentro desse domínio específico.

Fonte: Cisco



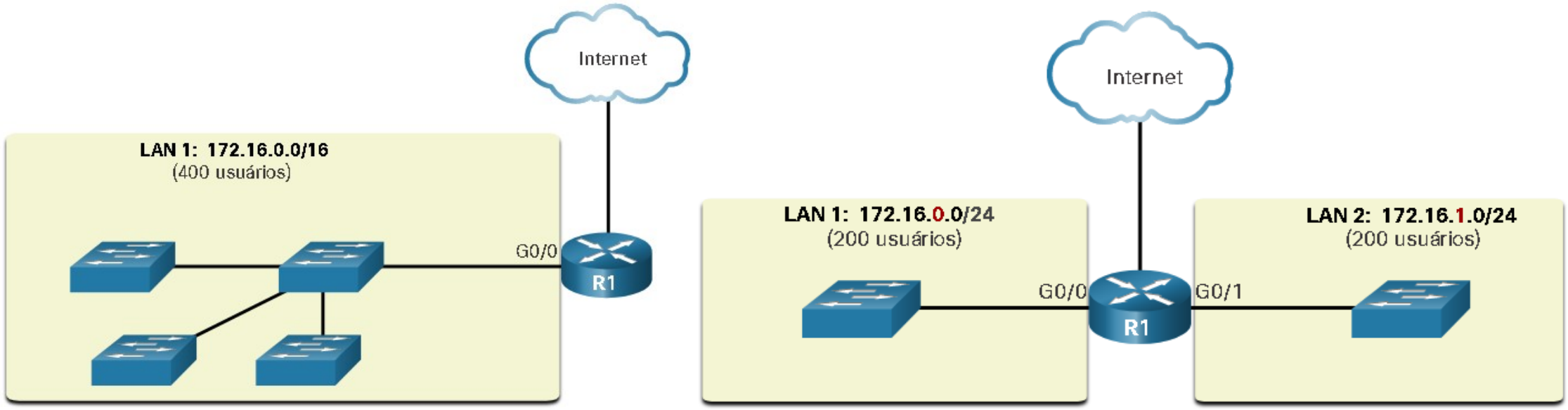
Segmentação de rede

Problemas com Grandes Domínios de Broadcast

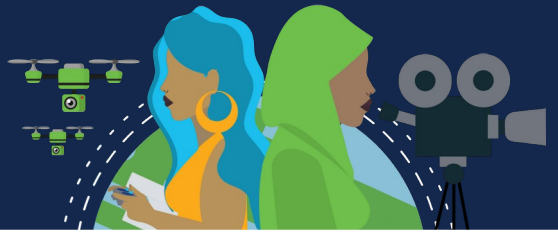
Um grande domínio de broadcast é uma rede que conecta vários hosts. Um problema desse tipo de domínio é que os hosts podem gerar broadcasts em excesso e afetar a rede de forma negativa. Resultando em operações de rede lentas devido à quantidade significativa de tráfego que pode causar e operações de dispositivo lentas porque um dispositivo deve aceitar e processar cada pacote de broadcast.

A solução é reduzir o tamanho da rede para criar domínios de broadcast menores em um processo denominado divisão em sub-redes. A base da divisão em sub-redes usa bits de host para criar sub-redes adicionais.

Observação: A maioria das redes são uma sub-rede de um bloco de endereços maior.



Fonte: Cisco

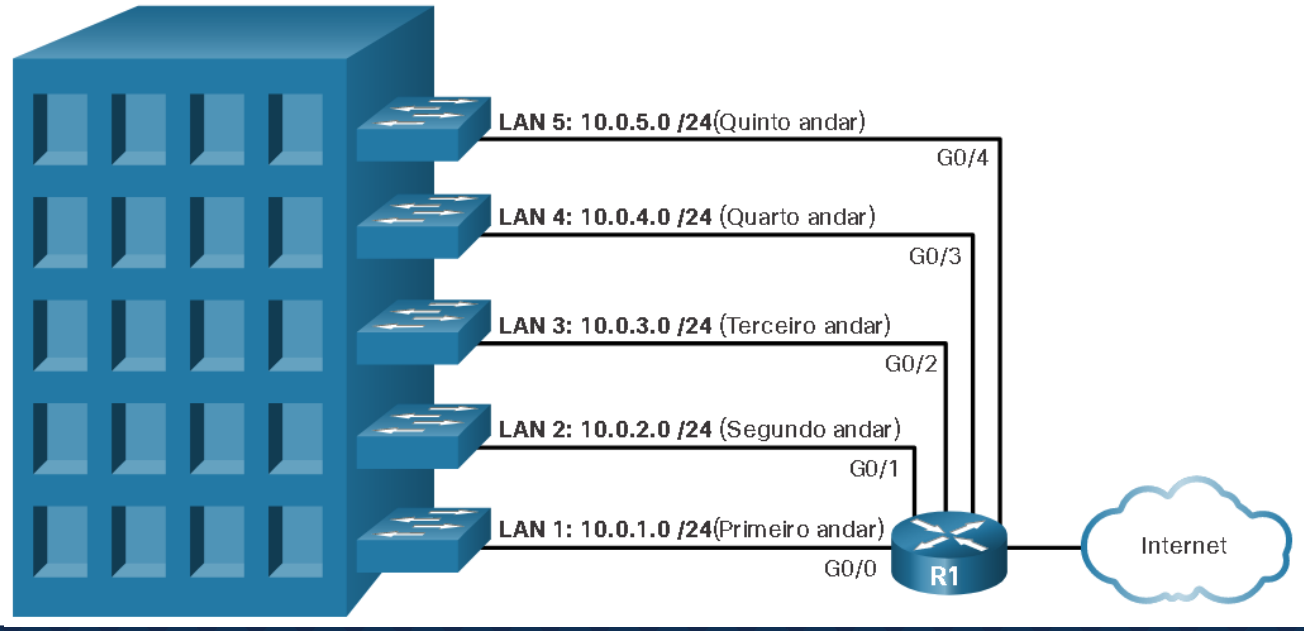


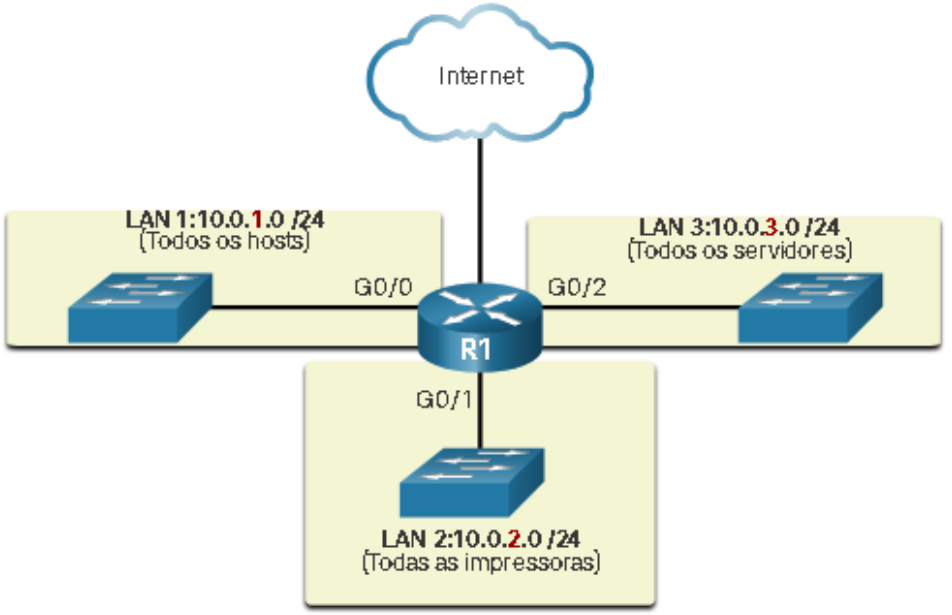
Segmentação de rede

Razões para segmentar redes

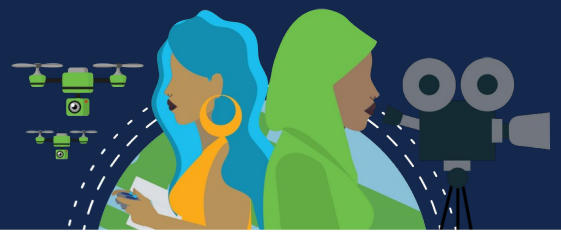
A divisão em sub-redes reduz o tráfego total da rede e melhora seu desempenho. Permite que o administrador implemente políticas de segurança como, por exemplo, quais sub-redes podem ou não se comunicar com quais sub-redes. Reduz o número de dispositivos afetados pelo tráfego anormal de broadcast devido a configurações incorretas, problemas de hardware/software ou atitudes mal-intencionadas.

Há várias maneiras de usar sub-redes para gerenciar dispositivos de rede. Como por exemplo, dividir Sub-Redes por Local, por grupo ou função ou por tipo de dispositivo.





Fonte: Cisco



Sub-rede de uma rede IPv4

Sub-rede em um limite de octeto

As sub-redes IPv4 são criadas com um ou mais bits de host sendo usados como bits de rede. Isso é feito estendendo-se a máscara de sub-rede para pegar emprestado alguns dos bits da parte de host do endereço e criar bits de rede adicionais. Quanto mais bits de host forem emprestados, mais sub-redes poderão ser definidas. Quanto mais bits forem emprestados para aumentar o número de sub-redes haverá menos número de hosts por sub-rede.

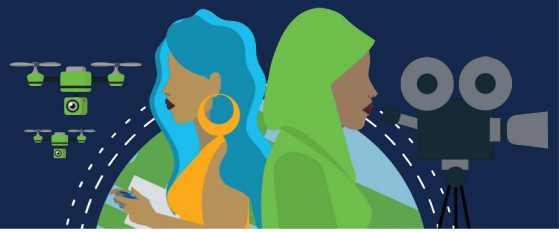
É mais fácil dividir redes em sub-redes nos limites dos octetos: /8, /16 e /24. A tabela identifica esses comprimentos de prefixo.

Comprimento do Prefixo	Máscara de sub-rede	Máscara de sub-rede em binário (n = rede, h = host)	# de hosts
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16.777.214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65.534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

Endereço da Sub-Rede (256 possíveis sub-redes)	Intervalo de host (65,534 possíveis hosts por sub-rede)	Broadcast
10.0.0.0/16	10.0.0.1 - 10.0.255.254	10.0.255.255
10.1.0.0/16	10.1.0.1 - 10.1.255.254	10.1.255.255
10.2.0.0/16	10.2.0.1 - 10.2.255.254	10.2.255.255
10.3.0.0/16	10.3.0.1 - 10.3.255.254	10.3.255.255
10.4.0.0/16	10.4.0.1 - 10.4.255.254	10.4.255.255
10.5.0.0/16	10.5.0.1 - 10.5.255.254	10.5.255.255
10.6.0.0/16	10.6.0.1 - 10.6.255.254	10.6.255.255
10.7.0.0/16	10.7.0.1 - 10.7.255.254	10.7.255.255
...	...	...
10.255.0.0/16	10.255.0.1 - 10.255.255.254	10.255.255.255

Fonte: Cisco

Sub-rede de uma rede IPv4



Sub-rede dentro de um limite de octeto

As sub-redes podem pedir emprestado bits de qualquer posição dos bits de host para criar outras máscaras. Um endereço de rede /24 costuma ser dividido em sub-redes menores, usando prefixos mais longos ao pedir bits emprestados do quarto octeto, dando mais flexibilidade na hora de atribuir endereços de rede a um número menor de dispositivos finais.

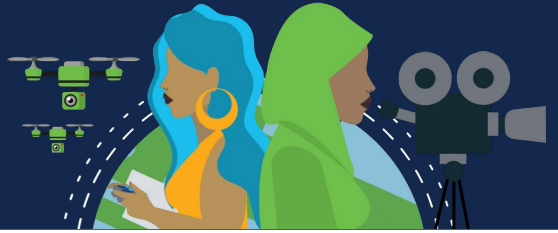
Para cada bit emprestado no quarto octeto, o número de sub-redes disponíveis é dobrado, enquanto reduz o número de endereços de host por sub-rede:

Prefixo	Máscara	Máscara em binário (1 = rede, 0 = host)	# de sub-redes	# de hosts	
/25	255.255.255.128	11111111.11111111.11111111.**1**0000000	**2**	126	O empréstimo 1 bit do quarto octeto cria 2 sub-redes que suportam 126 hosts cada.
/26	255.255.255.192	11111111.11111111.11111111.**11**000000	**4**	62	O empréstimo de 2 bits cria 4 sub-redes que suportam 62 hosts cada.
/27	255.255.255.224	11111111.11111111.11111111.**111**00000	**8**	30	O empréstimo de 3 bits cria 8 sub-redes que suportam 30 hosts cada.
/28	255.255.255.240	11111111.11111111.11111111.**1111**0000	**16**	14	O empréstimo de 4 bits cria 16 sub-redes que suportam 14 hosts cada.
/29	255.255.255.248	11111111.11111111.11111111.**11111**000	**32**	6	O empréstimo de 5 bits cria 32 sub-redes que suportam 6 hosts cada.
/30	255.255.255.252	11111111.11111111.11111111.**111111**00	**64**	2	O empréstimo de 6 bits cria 64 sub-redes que suportam 2 hosts cada.

Cisco Life Changer

Changing the way the world WORKS!

Fonte: Cisco



Sub-rede um /16 e um prefixo /8

Criar sub-redes com um prefixo de barra 16

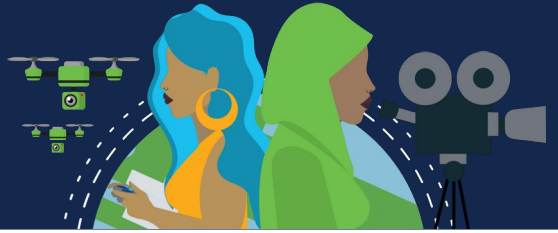
Algumas sub-redes são mais fáceis do que outras sub-redes. Este tópico explica como criar sub-redes que tenham o mesmo número de hosts.

Em uma situação que exige um número maior de sub-redes, é necessária uma rede IPv4 com mais bits de host disponíveis para empréstimo. Por exemplo, o endereço de rede 172.16.0.0 tem uma máscara padrão 255.255.0.0 ou /16. Esse endereço tem 16 bits na parte de rede e 16 bits na parte de host. Esses 16 bits da parte de host estão disponíveis para serem emprestados na criação de sub-redes. A tabela destaca todos os cenários possíveis para a sub-rede de um prefixo /16.

Embora você não precise memorizar esta tabela, você ainda precisa de uma boa compreensão de como cada valor na tabela é gerado. Não se deixe intimidar pelo tamanho da tabela. O motivo é grande: possui 8 bits adicionais que podem ser emprestados e, portanto, o número de sub-redes e hosts é simplesmente maior.

Prefixo	Máscara	Máscara em binário (1 = rede, 0 = host)	# de sub-redes	# de hosts
/17	255.255.128.0	11111111.11111111.**1**0000000.00000000	**2**	32766
/18	255.255.192.0	11111111.11111111.**11**000000.00000000	**4**	16382
/19	255.255.224.0	11111111.11111111.**111**00000.00000000	**8**	8190
/20	255.255.240.0	11111111.11111111.**1111**0000.00000000	**16**	4094
/21	255.255.248.0	11111111.11111111.**11111**000.00000000	**32**	2046
/22	255.255.252.0	11111111.11111111.**111111**00.00000000	**64**	1022
/23	255.255.254.0	11111111.11111111.**1111111**0.00000000	**128**	510
/24	255.255.255.0	11111111.11111111.**11111111**.00000000	**256**	254
/25	255.255.255.128	11111111.11111111.**11111111.1**0000000	**512**	126
/26	255.255.255.192	11111111.11111111.**11111111.11**000000	**1024**	62
/27	255.255.255.224	11111111.11111111.**11111111.111**00000	**2048**	30
/28	255.255.255.240	11111111.11111111.**11111111.1111**0000	**4096**	14
/29	255.255.255.248	11111111.11111111.**11111111.11111**000	**8192**	6
/30	255.255.255.252	11111111.11111111.**11111111.111111**00	**16384**	2

Fonte: Cisco



Sub-rede um /16 e um prefixo /8

Crie 100 sub-redes com um prefixo barra 16

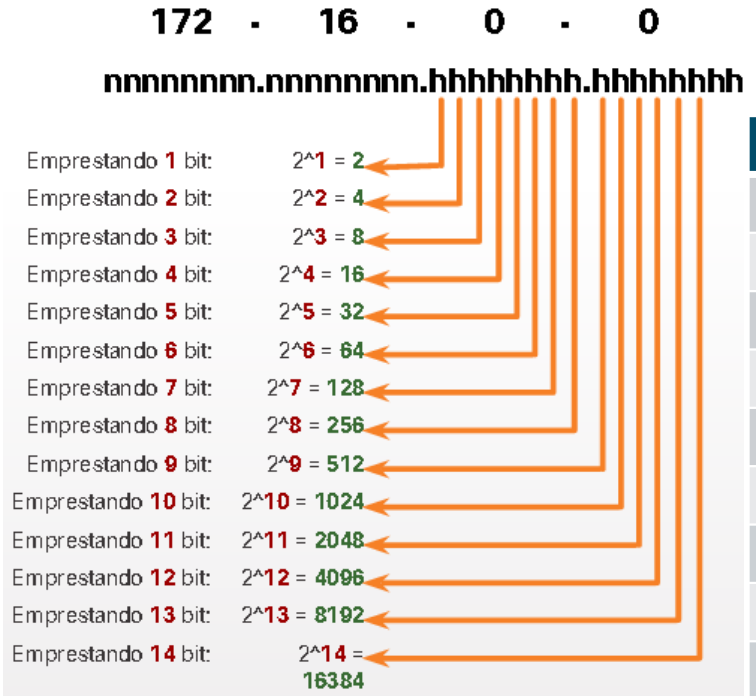
Considere a rede 172.16.0.0/16.

Comece pegando emprestado os bits do terceiro octeto, indo da esquerda para a direita, um bit por vez, até atingir o número de bits necessário para criar 100 sub-redes.

7 bits precisam ser emprestados para um total de 128 sub-redes, resultando em redes /23.

Altere a mascara para refletir os valores emprestados; 255.255.254.0 ou um prefixo /23.

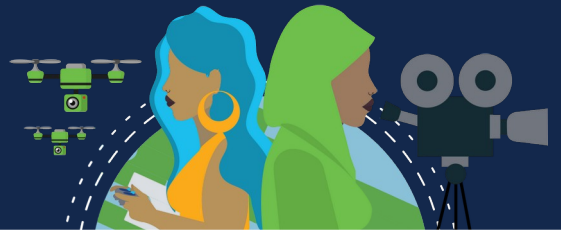
1 bit de host no terceiro octeto mais 8 bits de host restantes no quarto octeto, totalizam 9 bits que não foram emprestados, disponibilizando 512 endereços de host. O primeiro endereço é reservado para o endereço de rede e o último endereço é reservado para o endereço de broadcast, ficando 510 endereços de host disponíveis para cada sub-rede /23.



Sub-Redes 172.16.0.0/23 Resultantes		
172.16.0000000	0.00000000	172.16.0.0/23
172.16.0000001	0.00000000	172.16.2.0/23
172.16.0000010	0.00000000	172.16.4.0/23
172.16.0000011	0.00000000	172.16.6.0/23
172.16.0000100	0.00000000	172.16.8.0/23
172.16.0000101	0.00000000	172.16.10.0/23
172.16.0000111	0.00000000	172.16.14.0/23
…		
172.16.1111111	0.00000000	172.16.254.0/23

Intervalo de Endereços de Host para a Sub-Rede 172.16.0.0/23			
Endereço de Rede	172.16.0000000	0.00000000	172.16.0.0/23
Primeiro Endereço de Host Válido	172.16.0000000	0.00000001	172.16.0.1/23
Último Endereço de Host Válido	172.16.0000000	1.11111110	172.16.1.254/23
Endereço de Broadcast	172.16.0000000	1.11111111	172.16.1.255/23

Fonte: Cisco



Sub-redes para atender requisitos

Sub-redes Privadas X Endereçamento Público

A rede de uma organização pode usar endereços IPv4 públicos e privados e isto afeta a forma como segregar a rede.

Intranet - Esta é a parte interna da rede de uma empresa, acessível apenas dentro da organização. Os dispositivos na intranet usam endereços IPv4 privados.

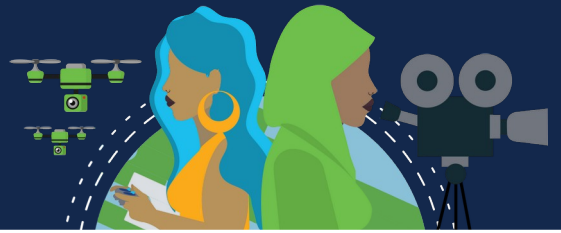
DMZ - Faz parte da rede da empresa que contém recursos disponíveis para a internet, como um servidor web. Os dispositivos na DMZ usam endereços IPv4 públicos.

Tanto a intranet quanto a DMZ têm seus próprios requisitos e desafios de sub-rede.

A intranet usa espaço de endereçamento IPv4 privado. Isso permite que uma organização use qualquer um dos endereços de rede IPv4 privados, incluindo o prefixo 10.0.0.0/8 com 24 bits de host e mais de 16 milhões de hosts.

Os dispositivos na DMZ exigem endereços IPv4 públicos. O esgotamento do espaço de endereços IPv4 público tornou-se um problema a partir de meados da década de 1990. Desde 2011, a IANA e quatro de cinco RIRs estão sem espaço de endereços IPv4. Embora as organizações estejam fazendo a transição para o IPv6, o espaço de endereço IPv4 restante permanece severamente limitado. Isso significa que uma organização deve maximizar seu próprio número limitado de endereços IPv4 públicos. Isso requer que o administrador de rede subnet seu espaço de endereço público em sub-redes com diferentes máscaras de sub-rede, a fim de minimizar o número de endereços de host não utilizados por sub-rede. Isso é conhecido como Variable Subnet Length Masking (VLSM).

Fonte: Cisco



Sub-redes para atender requisitos

Minimizar endereços IPv4 de host não utilizados e maximizar sub-redes

Para minimizar o número de endereços IPv4 de host não utilizados e maximizar o número de sub-redes disponíveis, há duas considerações ao planejar sub-redes: o número de endereços de host necessários para cada rede e o número de sub-redes individuais necessárias.

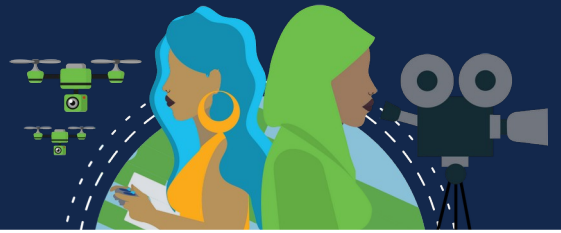
A tabela exibe os detalhes específicos para a sub-rede de uma rede /24. Note que há um relacionamento inverso entre o número de sub-redes e o número de hosts. Quanto mais bits forem emprestados para criar sub-redes, menos bits do host permanecerão disponíveis. Se forem necessários mais endereços de host, mais bits de host serão exigidos, resultando em menos sub-redes.

O número de endereços de host exigidos na maior sub-rede determina quantos bits devem ser deixados na parte de host. Lembre-se de que dois dos endereços não podem ser usados, portanto o número utilizável de endereços pode ser calculado como 2n-2.

Os administradores de rede precisam preparar um esquema de endereçamento da rede que acomode o máximo possível de hosts para cada rede e o número de sub-redes. O esquema de endereçamento deve permitir o crescimento do número de endereços de host por sub-rede e do número total de sub-redes.

Prefixo	Máscara	Máscara em binário (1 = rede, 0 = host)	# de sub-redes	# de hosts
/25	255.255.255.128	11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	11111111.11111111.11111111.**111111**00	**64**	2

Fonte: Cisco



Sub-redes para atender requisitos

Exemplo: sub-rede IPv4 eficiente

Uma sede corporativa recebeu um endereço de rede público 172.16.0.0/22 (10 bits de host) pelo seu ISP, isso fornecerá 1.022 endereços de host (2^{10}-2).

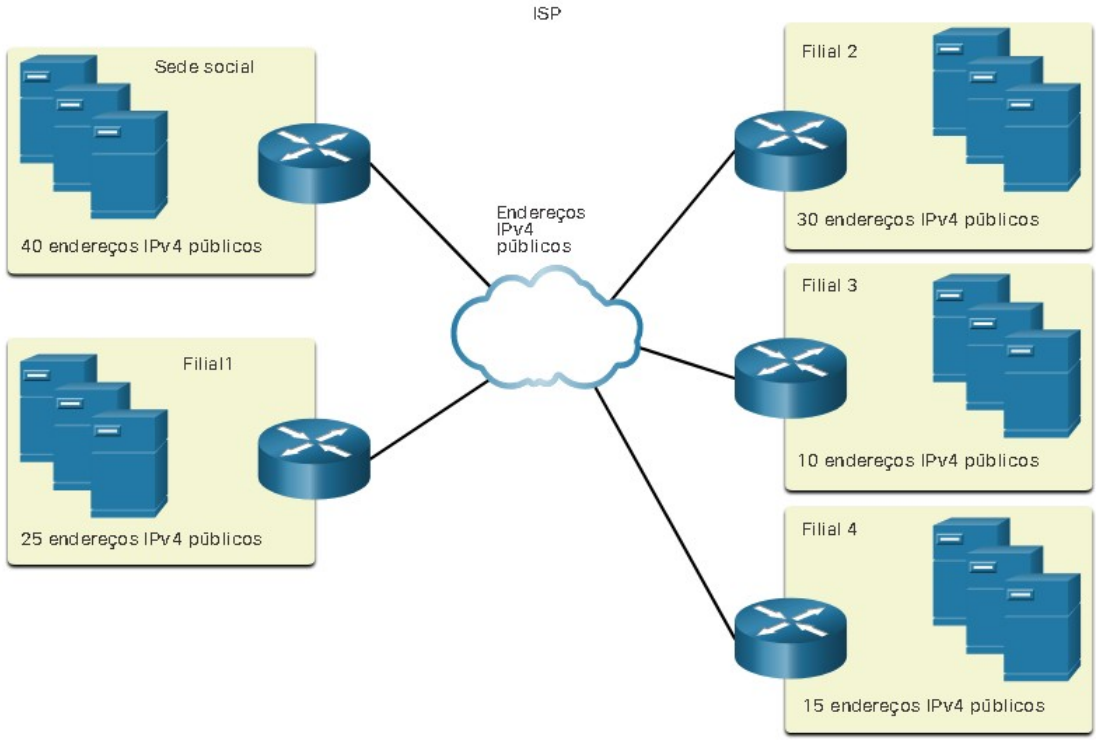
É preciso fazer o melhor uso do espaço de endereços recebido.

A sede possui a DMZ e quatro filiais, que precisam de seu próprio espaço público de endereços IPv4.

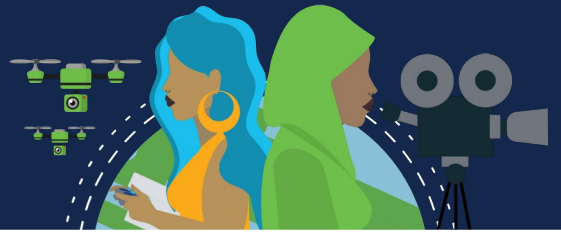
Sendo precisos 10 sub-redes do range público 172.16.0.0/22.

A maior sub-rede requer 40 endereços.

O endereço de rede 172.16.0.0/22 possui 10 bits de host.



Fonte: Cisco

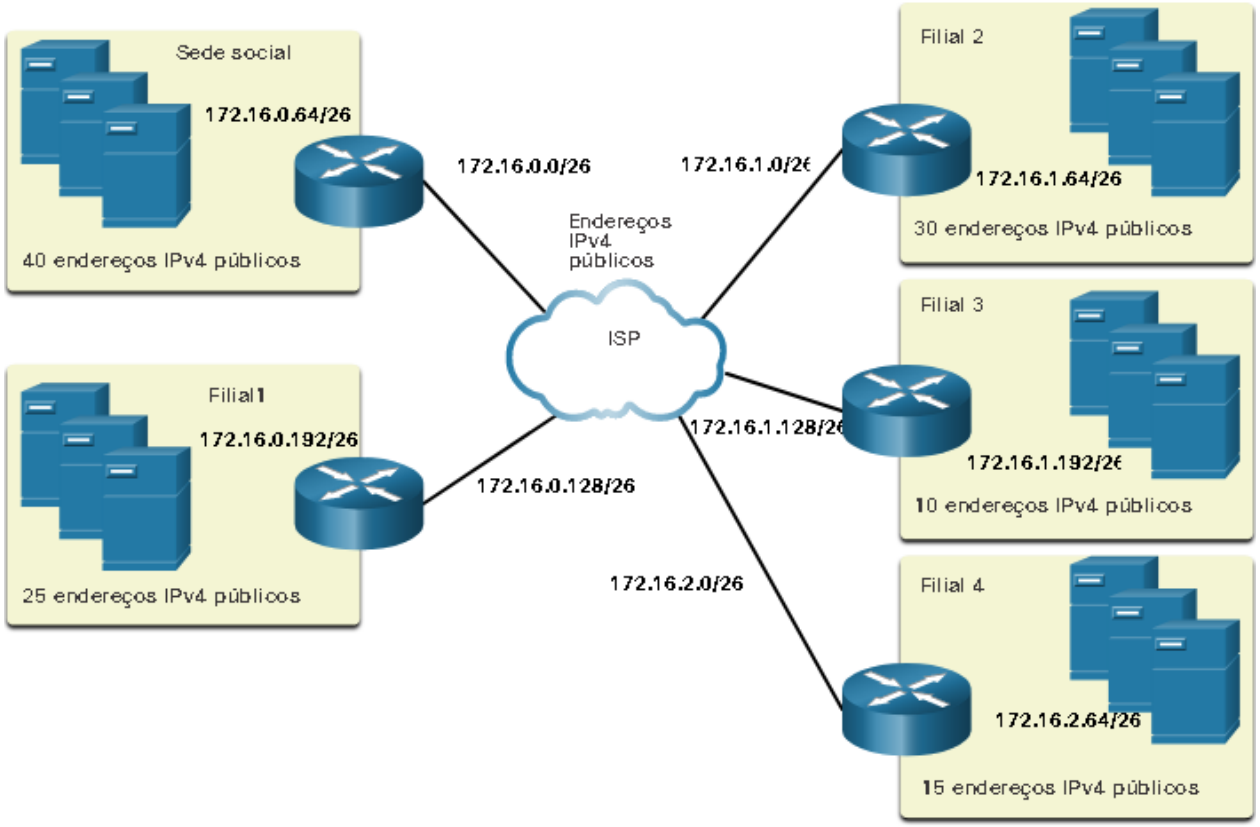


Sub-redes para atender requisitos

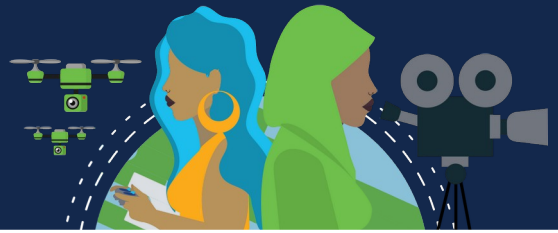
Como a maior sub-rede precisa de 40 hosts, são necessários pelo menos 6 bits de host para fornecer endereçamento para 40 hosts. Isso é determinado usando a fórmula: $2^6 - 2 = 62$ hosts.
O uso da fórmula para determinar sub-redes resulta em 16 sub-redes: $2^4 = 16$.
Como a internetwork requer 10 sub-redes, isso atenderá ao requisito e permitirá um crescimento adicional.
Portanto, os 4 primeiros bits do host podem ser usados para alocar sub-redes. Isto significa que dois bits do 3º octeto e dois bits do 4º octeto serão emprestados. Quando 4 bits são emprestados da rede 172.16.0.0/22, o novo tamanho do prefixo é /26 com uma máscara de sub-rede 255.255.255.192.

	Parte de rede	Parte de Host		Decimal com Pontos
	10101100.00010000.000000	00.00	000000	172.16.0.0/22
0	10101100.00010000.000000	00.00	000000	172.16.0.0/26
1	10101100.00010000.000000	00.01	000000	172.16.0.64/26
2	10101100.00010000.000000	00.10	000000	172.16.0.128/26
3	10101100.00010000.000000	00.11	000000	172.16.0.192/26
4	10101100.00010000.000000	01.00	000000	172.16.1.0/26
5	10101100.00010000.000000	01.01	000000	172.16.1.64/26
6	10101100.00010000.000000	01.10	000000	172.16.1.128/26
	Redes 7 – 13 não mostradas			
14	10101100.00010000.000000	11.10	000000	172.16.3.128/26
15	10101100.00010000.000000	11.11	000000	172.16.3.192/26

4 bits emprestados da parte do host para criar sub-redes



Fonte: Cisco



VLSM

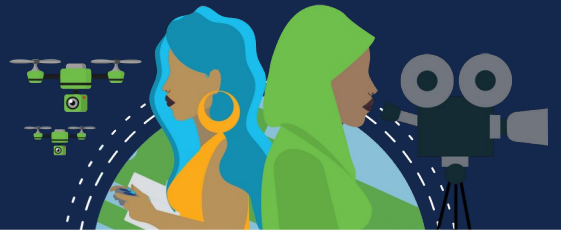
Os endereços públicos e privados afetam a maneira como você faria a sub-rede da rede. Há também outros problemas que afetam os esquemas de sub-rede. Um esquema de sub-rede padrão /16 cria sub-redes que cada uma tem o mesmo número de hosts. Nem todas as sub-redes criadas precisarão de tantos hosts, deixando muitos endereços IPv4 não utilizados. Talvez você precise de uma sub-rede que contenha muitos mais hosts. É por isso que a máscara de sub-rede de comprimento variável (VLSM) foi desenvolvida.

Devido ao esgotamento de endereços IPv4 públicos, tirar o máximo proveito dos endereços é a preocupação principal. O endereço IPv6 permite um maior planejamento e alocação de endereços muito mais fáceis do que o IPv4. Usando a divisão em sub-redes tradicional, o mesmo número de endereços é alocado para cada sub-rede. Se todas as sub-redes tiverem os mesmos requisitos para o número de hosts ou se não houver problema em conservar o espaço de endereços IPv4, esses blocos de endereços de tamanho fixo seriam eficientes. Mas normalmente esse não é o caso, resultando em um desperdício significativo de endereços não usados, além de limitar o crescimento futuro da rede. Esse uso ineficiente de endereços é característico da divisão em sub-redes tradicional.

A máscara de sub-rede de comprimento variável (VLSM) foi desenvolvida para evitar o desperdício de endereços, permitindo-nos subdividirmos uma sub-rede (subnetar).

Cada sub-rede em uma divisão tradicional usa a mesma máscara de sub-rede. O VLSM permite que um espaço de rede seja dividido em partes desiguais. A máscara de sub-rede vai variar de acordo com o número de bits emprestados para uma determinada sub-rede, ou seja, a parte “variável” da VLSM.

Fonte: Cisco

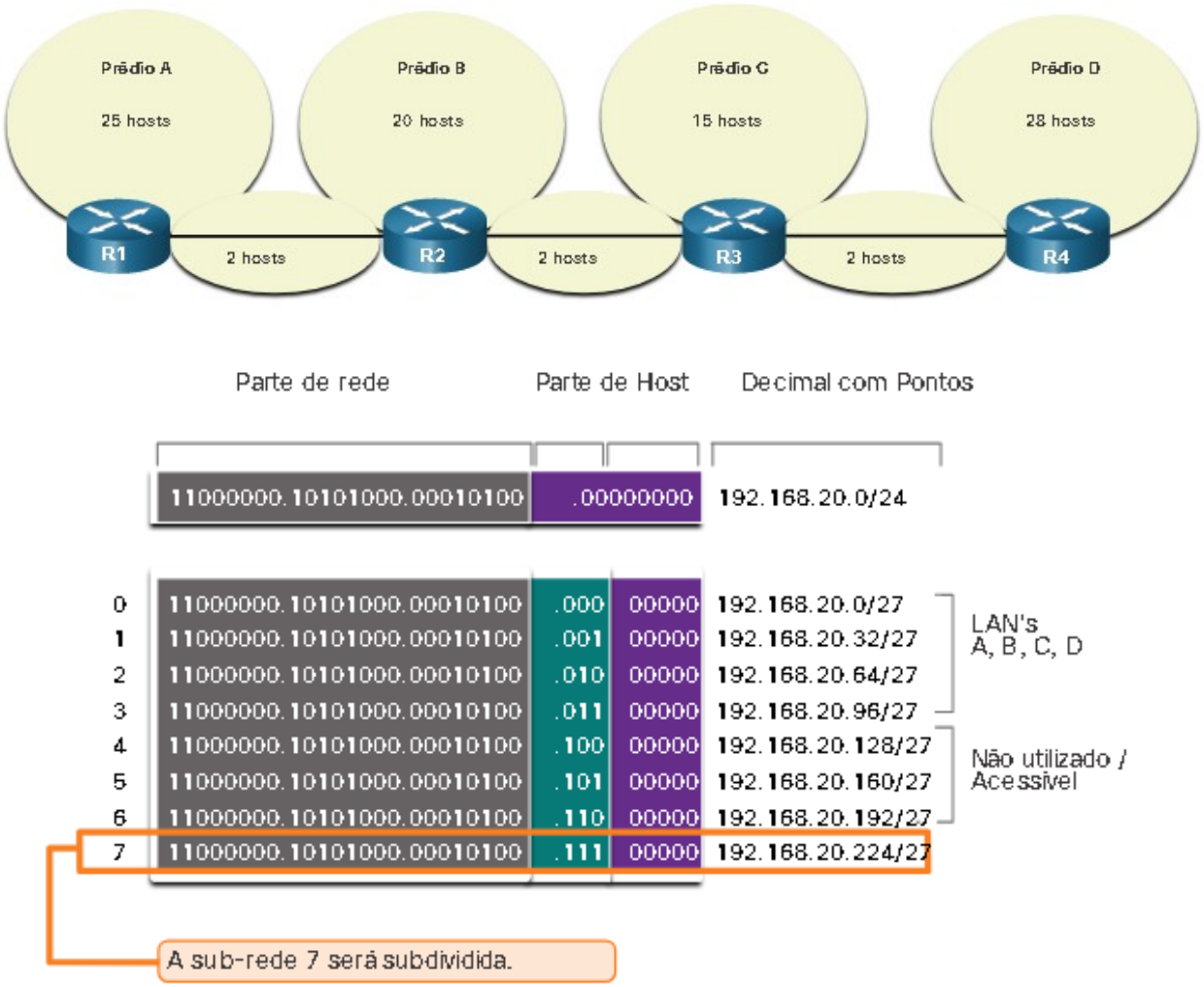


VLSM

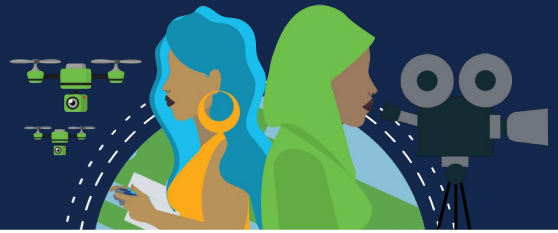
Usaremos a rede 192.168.20.0/24 e a dividiremos em sete sub-redes, uma para cada uma das quatro LANs e uma para cada uma das três conexões entre os roteadores.

A rede 192.168.20.0/24 foi dividida em oito sub-redes de tamanho igual com 30 endereços de host utilizáveis por sub-rede. Quatro sub-redes são usadas para as LANs e três sub-redes para as conexões entre os roteadores.

No entanto, as conexões entre os roteadores exigem apenas dois endereços de host por sub-rede (um endereço de host para cada interface de roteador). Para evitar desperdiçar 28 endereços por sub-rede, o VLSM é usado para criar sub-redes menores para as conexões entre roteadores,dividindo novamente uma das sub-redes. Neste exemplo, a última sub-rede, 192.168.20.224/27, será subdividida usando a máscara de sub-rede 255.255.255.252 ou /30.



Fonte: Cisco



VLSM

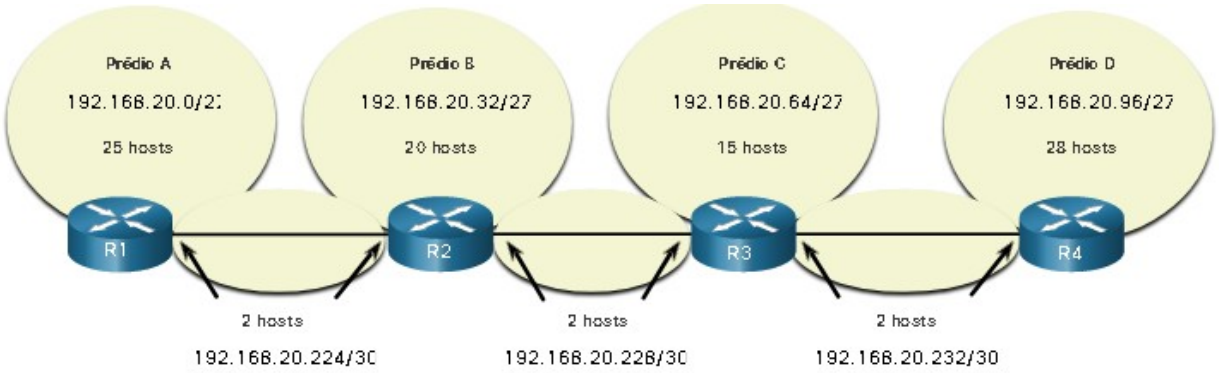
A fórmula 2n \ -2 (onde n é igual ao número de bits de host restantes) pode ser usada. Para fornecer dois endereços utilizáveis, dois bits de host devem ser deixados na parte do host.

Como existem cinco bits de host no espaço de endereço 192.168.20.224/27 da sub-rede, mais três bits podem ser emprestados, deixando dois bits na parte do host. Os cálculos neste ponto são exatamente os mesmos que aqueles usados para a divisão em sub-redes tradicional.

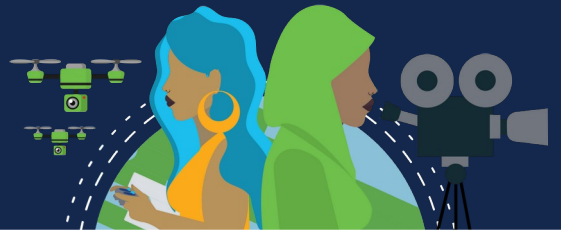
Esse esquema de sub-rede do VLSM reduz o número de endereços por sub-rede para um tamanho apropriado para as redes que exigem menos sub-redes. A sub-rede 7, para links entre roteadores, permite que as sub-redes 4, 5 e 6 estejam disponíveis para redes futuras, além de cinco sub-redes adicionais disponíveis para conexões entre roteadores.

Observação: Ao usar o VLSM, comece sempre satisfazendo os requisitos de host da maior sub-rede. Continue a divisão em sub-redes até atender ao requisitos de host da menor sub-rede.

	Parte de rede	Parte de Host		Decimal com Pontos	
7	11000000.10101000.00010100	.111	00000	192.168.20.224/27	
	Mais 3 bits emprestados da sub-rede?				
7:0	11000000.10101000.00010100	.111000	00	192.168.20.224/30	
7:1	11000000.10101000.00010100	.111001	00	192.168.20.228/30	WANs
7:2	11000000.10101000.00010100	.111010	00	192.168.20.232/30	
7:3	11000000.10101000.00010100	.111011	00	192.168.20.236/30	
7:4	11000000.10101000.00010100	.111100	00	192.168.20.240/30	
7:5	11000000.10101000.00010100	.111101	00	192.168.20.244/30	Não Usado/Disponível
7:6	11000000.10101000.00010100	.111110	00	192.168.20.248/30	
7:7	11000000.10101000.00010100	.111111	00	192.168.20.252/30	
	Subdivisão de uma sub-rede				



Fonte: Cisco



VLSM

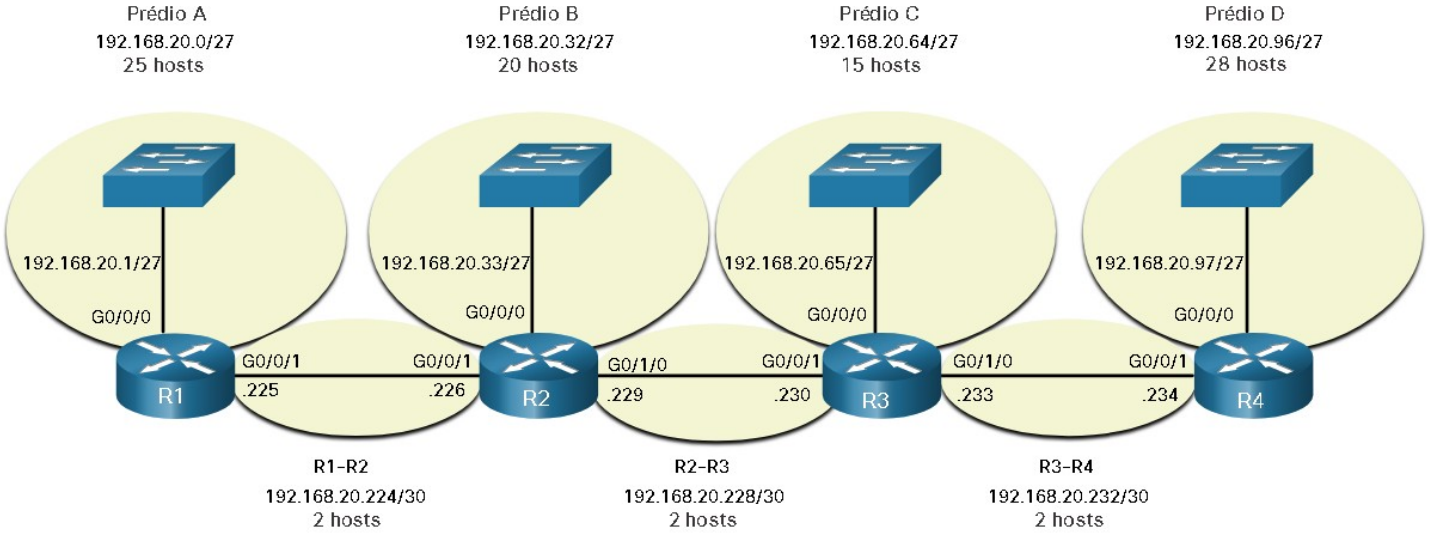
Atribuição de endereço de topologia VLSM

Usando as sub-redes VLSM, as redes LAN e entre roteadores podem ser tratadas sem desperdício desnecessário.

A figura mostra as atribuições de endereço de rede e os endereços IPv4 atribuídos a cada interface de roteador.

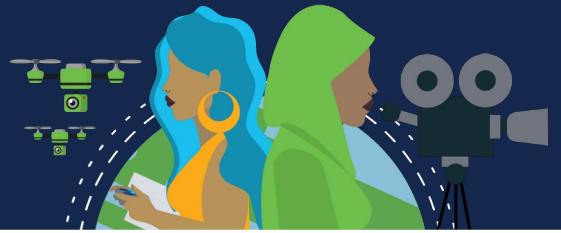
Com o uso de um esquema de endereçamento comum, o primeiro endereço IPv4 de host para cada sub-rede é atribuído à interface LAN do roteador. Os hosts em cada sub-rede terão um endereço IPv4 de host no intervalo de endereços de host para aquela sub-rede e uma máscara apropriada. Os hosts usarão como endereço de gateway padrão o endereço da interface LAN do roteador conectada àquela rede.

A tabela mostra os endereços de rede e o intervalo de endereços de host para cada rede. O endereço de gateway padrão é exibido para as quatro LANs.



	Endereço de rede	Intervalo de endereços de host	Endereço de gateway padrão
Prédio A	192.168.20.0/27	192.168.20.1/27 a 192.168.20.30/27	192.168.20.1/27
Prédio B	192.168.20.32/27	192.168.20.33/27 a 192.168.20.62/27	192.168.20.33/27
Prédio C	192.168.20.64/27	192.168.20.65/27 a 192.168.20.94/27	192.168.20.65/27
Prédio D	192.168.20.96/27	192.168.20.97/27 a 192.168.20.126/27	192.168.20.97/27
R1-R2	192.168.20.224/30	192.168.20.225/30 a 192.168.20.226/30	
R2-R3	192.168.20.228/30	192.168.20.229/30 a 192.168.20.230/30	
R3-R4	192.168.20.232/30	192.168.20.233/30 a 192.168.20.234/30	

Fonte: Cisco



Projeto estruturado

Planejamento de endereços de rede IPv4

Antes de iniciar a subdivisão, você deve desenvolver um esquema de endereçamento IPv4 para toda a rede. Identificar quantas sub-redes serão necessárias, quantos hosts cada sub-rede requer, quais dispositivos fazem parte da sub-rede, onde usar endereços privados e públicos e muitos outros fatores determinantes. Um bom esquema de endereçamento permite o crescimento futuro e é sinal de um bom administrador de rede.

O planejamento exige que você examine as necessidades de uso da rede de uma organização e como as sub-redes serão estruturadas. O plano de endereçamento inclui determinar onde a conservação do endereço é necessária (geralmente dentro da DMZ) e onde há mais flexibilidade (geralmente dentro da intranet).

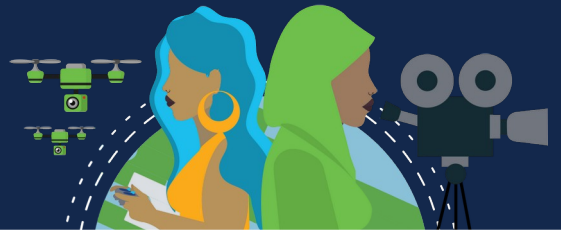
Geralmente é necessário endereço IPv4 público dentro da DMZ. E, provavelmente incluirá o uso do VLSM. Dentro da intranet, a conservação de endereços não é um problema graças ao endereçamento IPv4 privado, incluindo 10.0.0.0/8, com mais de 16 milhões de endereços IPv4 de host. Nas organizações onde o espaço de endereços IPv4 privado não é suficiente para acomodar suas necessidades internas estão fazendo a transição para o IPv6.

Para intranets que usam endereços IPv4 privados e DMZs que usam endereços IPv4 públicos, o planejamento e a atribuição de endereços são importantes.

O plano de endereço também precisa incluir como os endereços de host serão atribuídos, quais hosts exigirão endereços IPv4 estáticos e quais hosts podem usar o DHCP para obter suas informações de endereçamento. Isso também ajudará a evitar a duplicação de endereços, permitindo ao mesmo tempo o monitoramento e o gerenciamento de endereços por motivos de desempenho e segurança.

Conhecer os requisitos de endereço IPv4 determinará o intervalo, ou intervalos, de endereços de host que você implementa e ajudará a garantir que haja endereços suficientes para cobrir suas necessidades de rede.

Fonte: Cisco



Projeto estruturado

Atribuição de endereço de dispositivo

Diferentes tipos de dispositivos que exigem endereços:

Usuário final: Normalmente alocam endereços IPv4 dinamicamente usando o DHCP (Dynamic Host Configuration Protocol). Ele reduz a carga sobre a equipe de suporte de rede e praticamente elimina erros de entrada. Os endereços só são alugados por um período de tempo e podem ser reutilizados quando a concessão expira. É um recurso importante para redes que suportam usuários transitórios e dispositivos sem fio. Alterar o esquema de sub-rede significa que o servidor DHCP precisa ser reconfigurado e os clientes devem renovar seus endereços IPv4. Os clientes IPv6 podem obter informações de endereço usando DHCPv6 ou SLAAC.

Servidores e periféricos: Devem ter um endereço IP estático com numeração consistente.

Servidores acessíveis a partir da Internet: Devem ter um endereço IPv4 público, frequentemente acessado usando NAT. Em algumas organizações, os servidores internos devem ser disponibilizados aos usuários remotos. Na maioria dos casos, esses servidores recebem endereços privados internamente e o usuário é obrigado a criar uma conexão VPN (rede virtual privada) para acessar o servidor. Isso tem o mesmo efeito que se o usuário estiver acessando o servidor de um host dentro da intranet.

Dispositivos intermediários: Recebem endereços para gerenciamento, monitoramento e segurança de rede. Precisam ter endereços previsíveis e atribuídos estaticamente.

Gateway: Os roteadores e os dispositivos de firewall têm um endereço IP atribuído a cada interface que serve como gateway para os hosts nessa rede. Usam o endereço mais baixo ou mais alto da rede.

Ao desenvolver um esquema de endereçamento é recomendável ter um padrão definido de como os endereços são alocados para cada tipo de dispositivo. Isso beneficia os administradores ao adicionar e remover dispositivos, filtrando o tráfego com base em IP e simplificando a documentação.

Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

CCNAv7 – ITN – Endereçamento IPv6

Módulo 12

Embaixadores do Programa 2020, 2021 & 2022:

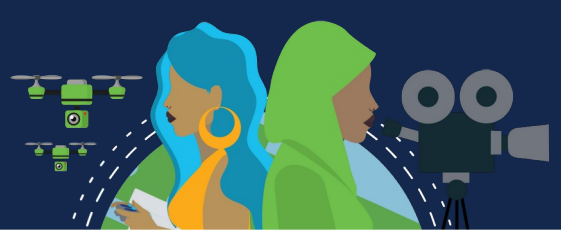
Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

WOMENROCK-IT
Brasil 2021

Networking Academy

Endereçamento IPv6



Problemas do IPv4

Necessidade de IPv6

A redução do espaço de endereços IPv4 tem sido o principal fator para migrar para o IPv6. Projetado para ser o sucessor do IPv4, o IPv6 tem um maior espaço de endereços de 128 bits, fornecendo 340 undecilhões de endereços (340 seguido por 36 zeros). Quando a IETF começou o desenvolvimento de um sucessor para o IPv4, aproveitou para corrigir as limitações do IPv4 e incluir aprimoramentos. Um exemplo é o ICMPv6 (Internet Control Message Protocol versão 6), que inclui a resolução de endereços e a configuração automática de endereços, não encontradas no ICMPv4.

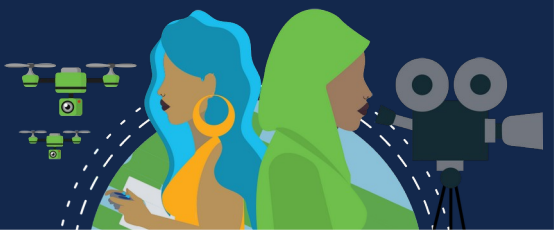
O IPv4 tem um máximo teórico de 4,3 bilhões de endereços. Combinados ao NAT, os endereços privados foram imprescindíveis para retardar a redução de endereços IPv4. No entanto, o NAT é problemático para muitos aplicativos, cria latência e possui limitações que impedem as comunicações ponto a ponto.

Com o número cada de vez maior de dispositivos móveis, os provedores móveis têm liderado o caminho com a transição para o IPv6. A maioria dos principais ISPs e provedores de conteúdo, como YouTube, Facebook e NetFlix, também fizeram a transição. Empresas como Microsoft, Facebook e LinkedIn estão fazendo transição para IPv6 somente internamente. Em 2018, a ISP Comcast de banda larga relatou uma implantação de mais de 65% e a British Sky Broadcasting mais de 86%.

A Internet em evolução está se tornando uma **Internet das Coisas (IoT).** Os dispositivos equipados com sensor e prontos para a Internet incluirão tudo, desde automóveis e dispositivos biomédicos, até eletrodomésticos e ecossistemas naturais. Com uma população crescente na Internet, endereços IPv4 limitados, problemas com NAT e **IoT**, chegou o momento de iniciar a transição para o IPv6.

Fonte: Cisco

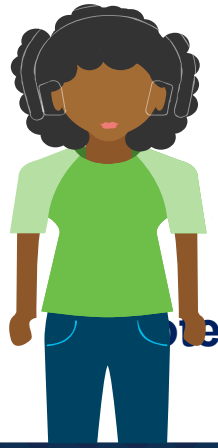
Problemas do IPv4



Coexistência do IPv4 com o IPv6

Não há uma data exata para migrar para o IPv6. Tanto o IPv4 como o IPv6 coexistirão no futuro próximo e a transição levará vários anos. A IETF criou vários protocolos e ferramentas para ajudar os administradores de rede a migrarem as redes para IPv6. As técnicas de migração podem ser divididas em três categorias:

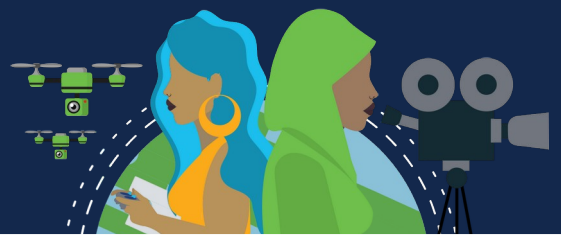
- A **pilha dupla** permite que IPv4 e IPv6 coexistam no mesmo segmento de rede. Os dispositivos de pilha dupla executam os protocolos IPv4 e IPv6 simultaneamente. Conhecido como IPv6 nativo, isso significa que a rede do cliente tem uma conexão IPv6 com seu ISP e é capaz de acessar o conteúdo encontrado na internet através de IPv6.
- **Tunelamento** é um método de transporte de pacote IPv6 através de uma rede IPv4. O pacote IPv6 é encapsulado dentro de um pacote IPv4, de forma semelhante a outros tipos de dados.



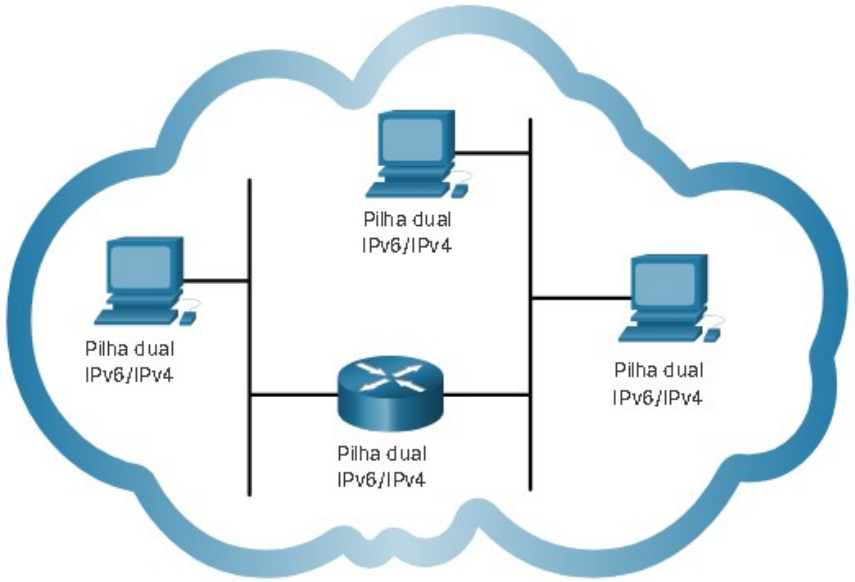
- A **NAT64** (Network Address Translation 64) permite que os dispositivos habilitados para IPv6 se comuniquem com os dispositivos habilitados para IPv4 usando uma técnica de conversão semelhante à NAT IPv4. Um pacote IPv6 é traduzido para um pacote IPv4 e um pacote IPv4 é traduzido para um pacote IPv6.

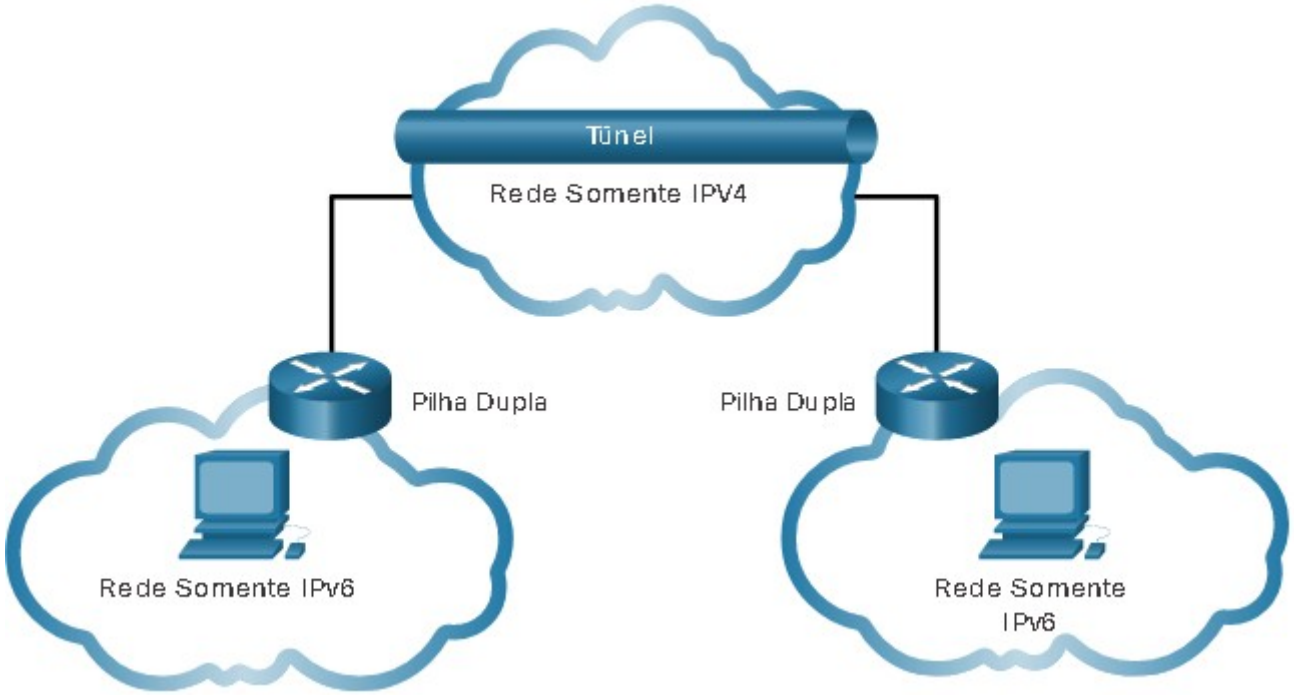
Nota: O tunelamento e NAT64 são para transição para o IPv6 nativo e só devem ser usados quando necessário. O objetivo deve ser as comunicações IPv6 nativas da origem até o destino.

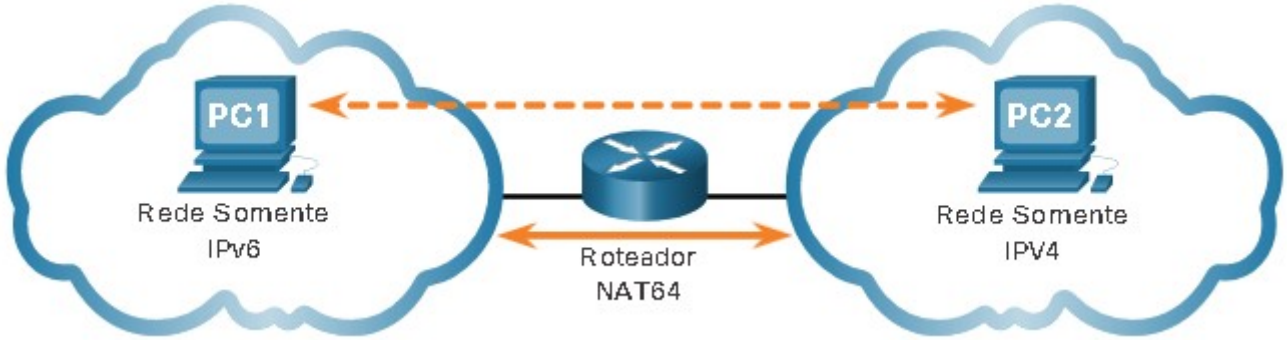
Fonte: Cisco



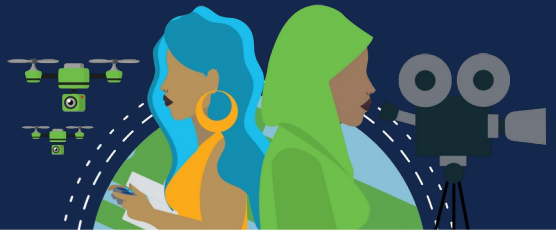
Problemas do IPv4







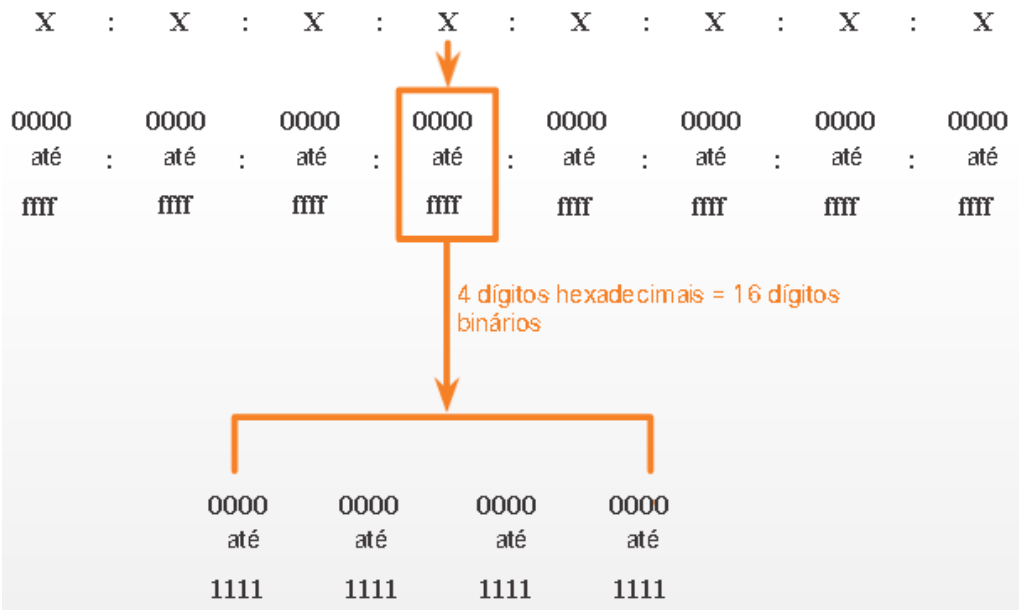
Fonte: Cisco



Representação do Endereço IPv6

Formatos de Endereço IPv6

O primeiro passo para aprender sobre IPv6 em redes é entender a forma como um endereço IPv6 é escrito e formatado.
Os endereços IPv6 têm 128 bits e são escritos como uma sequência de valores hexadecimais. Cada 4 bits são representados por um único dígito hexadecimal, totalizando 32 valores hexadecimais. Os endereços IPv6 não diferenciam maiúsculas e minúsculas.



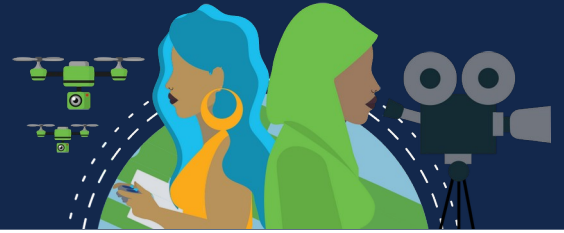
Formato preferido

O formato preferencial para escrever um endereço IPv6 é x: x: x: x: x: x: x: x, com cada “x” consistindo de quatro valores hexadecimais. O termo octeto refere-se aos oito bits de um endereço IPv4. No IPv6, um hexteto é o termo não oficial usado para se referir a um segmento de 16 bits ou quatro valores hexadecimais. Cada “x” equivale a um único hexteto, 16 bits ou quatro dígitos hexadecimais.

Formato preferencial significa que o endereço IPv6 é gravado usando todos os 32 dígitos hexadecimais. Isso não significa necessariamente que é o método ideal para representar o endereço IPv6. Existem duas regras que ajudam a reduzir o número de dígitos necessários para representar um endereço IPv6.

```
2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000: 0000
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef
fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001
```

Fonte: Cisco



Representação do Endereço IPv6

Regra 1 – Omitir zeros à esquerda

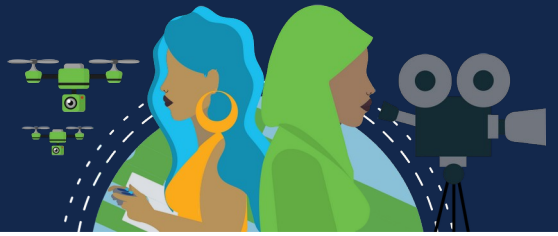
A primeira regra para ajudar a reduzir a notação de endereços IPv6 é omitir os 0s (zeros) à esquerda de qualquer seção de 16 bits ou hexteto. Aqui estão quatro exemplos de maneiras de omitir zeros à esquerda:

- 01AB pode ser representado como 1AB
- 09f0 pode ser representado como 9f0
- 0a00 pode ser representado como a00
- 00ab pode ser representado como ab

Essa regra se aplica somente aos 0s à esquerda, e NÃO aos 0s à direita. Caso contrário, o endereço ficaria ambíguo. Por exemplo, o hexteto “abc” poderia ser “0abc” ou “abc0”, mas essas duas representações não se referem ao mesmo valor.

Preferencial	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Nenhum 0 à esquerda	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200
Preferencial	2001 : 0db8 : 0000 : 00a3 : ab00 : 0ab0 : 00ab : 1234
Nenhum 0 à esquerda	2001 : db8 : 0 : a3 : ab00 : ab0 : ab : 1234
Preferencial	2001 : 0db8 : 000a : 0001 : c012 : 90ff : fe90 : 0001
Nenhum 0 à esquerda	2001 : db8 : a : 1 : c012 : 90ff : fe90 : 1

Fonte: Cisco



Representação do Endereço IPv6

Regra 2 – Dois pontos duplos

A segunda regra para ajudar a reduzir a notação de endereços IPv6 é o uso de dois-pontos duplo (::) para substituir uma única sequência contígua de um ou mais segmentos de 16 bits (hextetos) compostos exclusivamente por 0s.

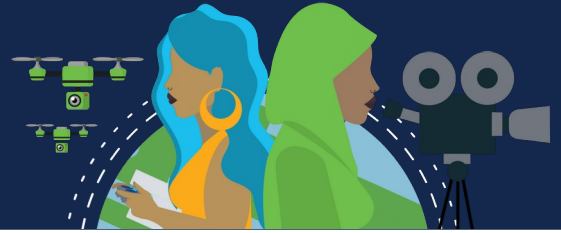
Exemplo: 2001:db8:cafe:1:0:0:0:1 poderia ser representado como 2001:db8:cafe:1::1.
O dois-pontos duplos (::) é usado no lugar dos três hextets all-0 (0:0:0).

Os dois-pontos (::) só podem ser usados uma vez em um endereço; caso contrário, haveria mais de um endereço resultante possível. Quando associada à técnica de omissão dos 0s à esquerda, a notação de endereço IPv6 pode ser bastante reduzida. É o chamado **formato compactado**.

Se um endereço tiver mais de uma cadeia contígua de todos os hextets 0, a prática recomendada é usar dois pontos duplos (::) na cadeia mais longa. Se as strings forem iguais, a primeira string deve usar dois pontos duplos (::).

Preferêncial	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Compressados/espaços	2001 : db8 : 0 : 1111 : : 200
Compactado	2001:db8:0:1111::200
Preferêncial	2001 : 0db8 : 0000 : 0000 : ab00 : 0000 : 0000 : 0000
Compressados/espaços	2001 : db8 : 0 : 0 : ab00 ::
Compactado	2001:db8:0:0:ab00::
Preferêncial	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000
Compressados/espaços	::
Compactado	::
Preferêncial	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
Compressados/espaços	:: 1
Compactado	::1

Fonte: Cisco



Tipos de Endereço IPv6

Tal como acontece com o IPv4, existem três grandes categorias de endereços IPv6:

Unicast: Identifica exclusivamente uma interface em um dispositivo habilitado para IPv6.

Multicast: Usado para enviar um único pacote IPv6 para vários destinos.

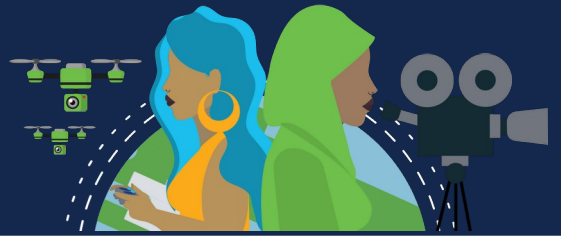
Anycast: Qualquer endereço IPv6 unicast que possa ser atribuído a vários dispositivos. Um pacote enviado a um endereço de anycast é roteado para o dispositivo mais próximo que tenha esse endereço.

Os endereços anycast estão fora do escopo deste curso.

Ao contrário do IPv4, o IPv6 não possui um endereço de broadcast.

No entanto, há um endereço multicast para todos os nós IPv6 que fornece basicamente o mesmo resultado.

Fonte: Cisco

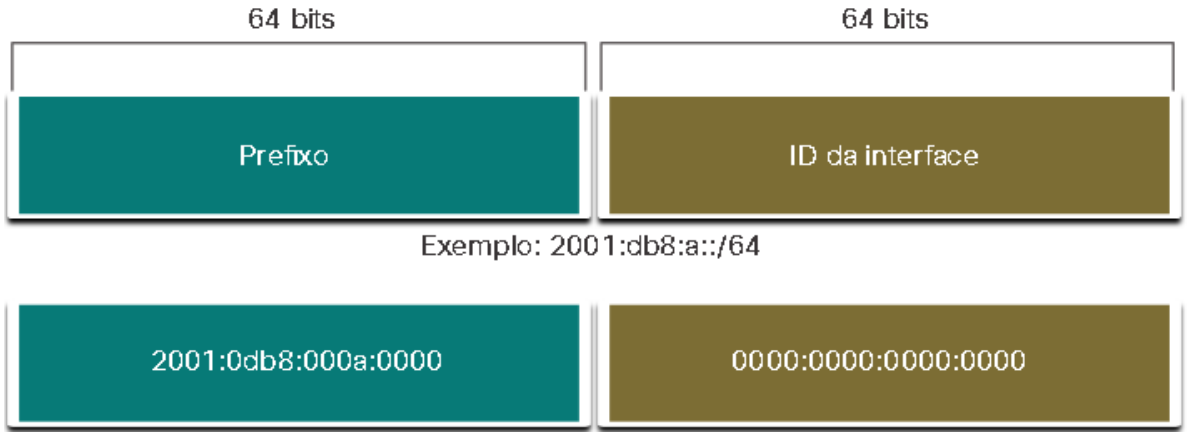


Tipos de Endereço IPv6

Comprimento do Prefixo IPv6

O comprimento do prefixo identifica a parte de rede no endereço IPv6, representado na notação de barra.

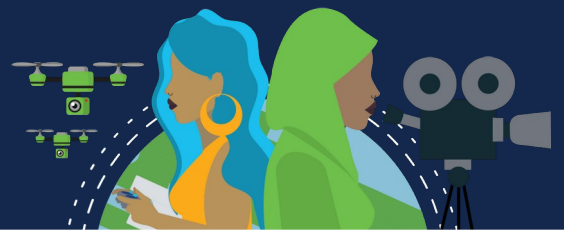
Pode variar de 0 a 128 bits. O comprimento recomendado para LANs e a maioria dos outros tipos de redes é /64.



Isso significa que o prefixo ou a parte de rede do endereço é de 64 bits, restando outros 64 bits para a ID da interface (parte de host) do endereço.

É altamente recomendável usar um ID de interface de 64 bits para a maioria das redes. Isso ocorre porque a configuração automática de endereço sem estado (SLAAC) usa 64 bits para o ID de interface. Também facilita a criação e o gerenciamento de sub-redes.

Fonte: Cisco

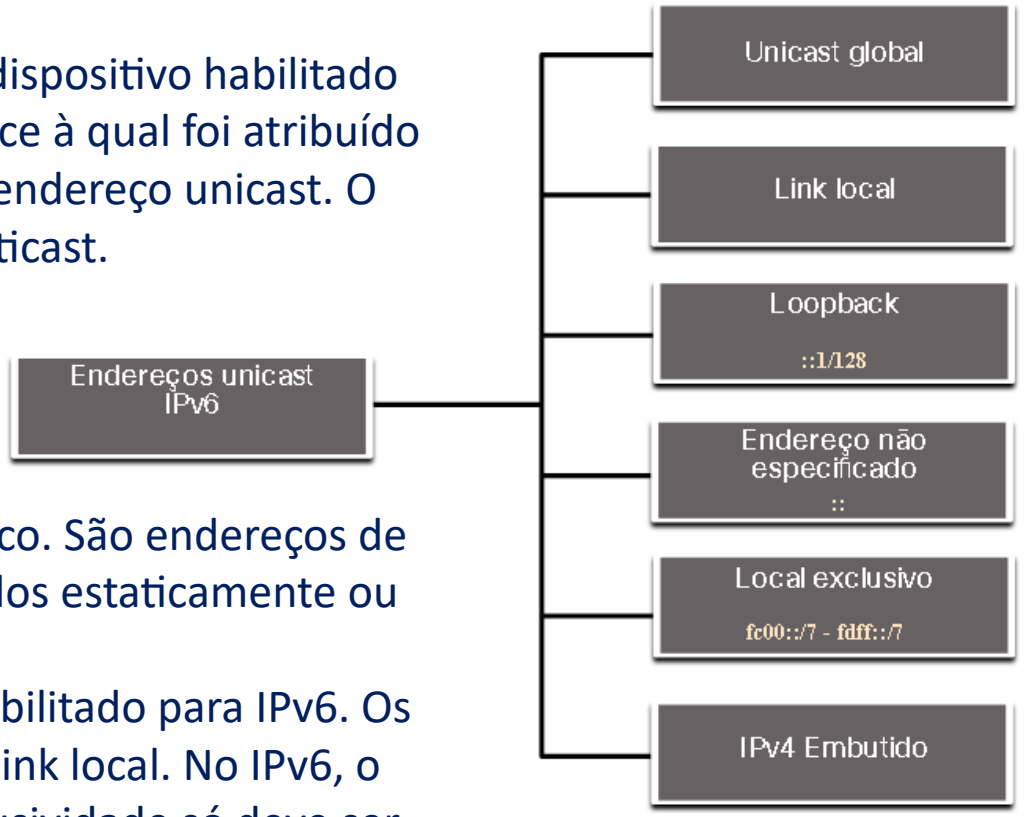


Tipos de Endereço IPv6

Outros Tipos de Endereços IPv6 Unicast

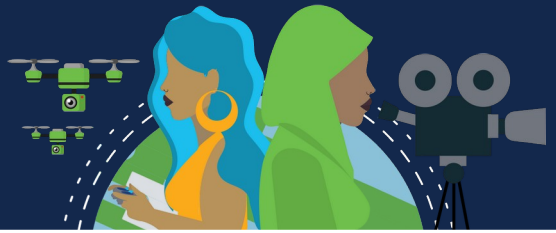
Um endereço IPv6 unicast identifica exclusivamente uma interface em um dispositivo habilitado para IPv6. Um pacote enviado a um endereço unicast é recebido pela interface à qual foi atribuído esse endereço. Semelhante ao IPv4, o endereço IPv6 origem deve ser um endereço unicast. O endereço IPv6 destino pode ser um endereço unicast ou multicast.

Ao contrário dos dispositivos IPv4 que têm apenas um único endereço, os endereços IPv6 normalmente têm dois endereços unicast:



- **Endereço Unicast Global (GUA):** é semelhante a um endereço IPv4 público. São endereços de Internet roteáveis e globalmente exclusivos. GUAs podem ser configurados estaticamente ou dinamicamente distribuídos
- **Endereço LLA (Link-Local Address):** É necessário para cada dispositivo habilitado para IPv6. Os LLAs são usados para se comunicar com outros dispositivos no mesmo link local. No IPv6, o termo link se refere a uma sub-rede. Limitados a um único link. Sua exclusividade só deve ser confirmada nesse link, porque eles não são roteáveis além do link. Em outras palavras, os roteadores não encaminham pacotes com um endereço de link local origem ou destino.

Fonte: Cisco



Tipos de Endereço IPv6

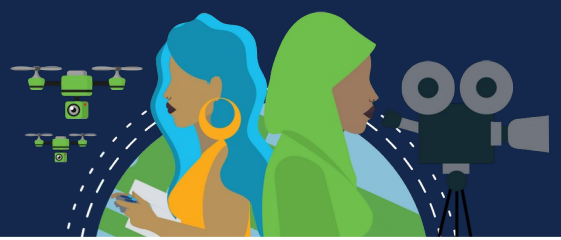
Uma observação sobre o endereço local exclusivo

Endereços locais exclusivos (intervalo **fc00::/7** a **fdff::/7**) ainda não são comumente implementados. Portanto, este módulo abrange apenas a configuração GUA e LLA. No entanto, endereços locais exclusivos podem eventualmente ser usados para endereçar dispositivos que não devem ser acessíveis de fora, como servidores internos e impressoras.

Os endereços IPv6 unique local têm alguma semelhança com endereços privados do RFC 1918 para o IPv4, mas há diferenças significativas:

- São utilizados para endereçamento local dentro de um site ou entre um número limitado de sites.
- Podem ser usados em dispositivos que nunca terão acesso por outra rede.
- Não são globalmente roteados ou traduzidos para um endereço IPv6 global.

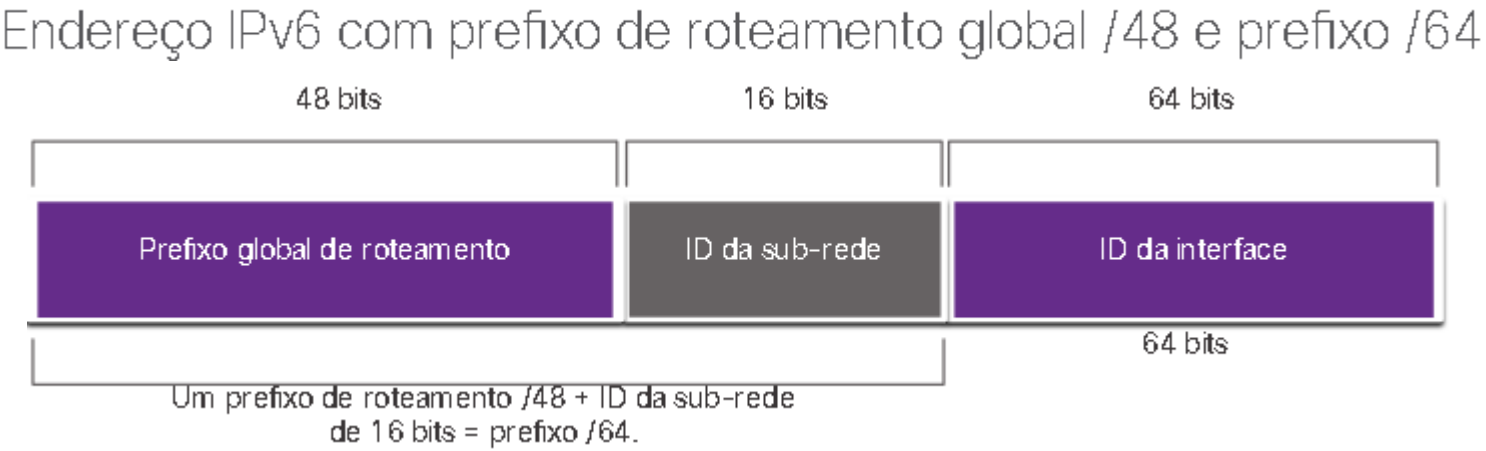
Observação: Muitos locais usam a natureza privada de endereços da RFC 1918 para proteger sua rede contra possíveis riscos à segurança ou ocultá-la. No entanto, essa nunca foi a finalidade dessas tecnologias. A IETF sempre recomendou que os sites tomassem as devidas precauções de segurança em seu roteador de Internet.



Tipos de Endereço IPv6

GUA IPv6

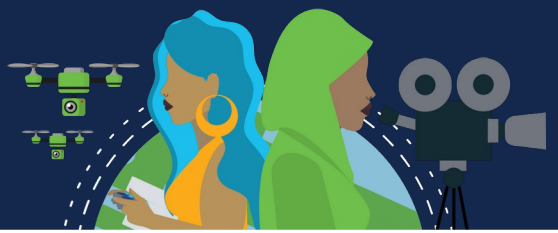
Endereço globalmente exclusivo e roteável na Internet IPv6, equivalentes aos endereços públicos do IPv4. O Internet Committee for Assigned Names and Numbers (ICANN), operador da Internet Assigned Numbers Authority (IANA), aloca blocos de endereço IPv6 para os cinco RIRs. No momento, somente endereços unicast globais com os primeiros três bits de 001 ou 2000::/3 estão sendo atribuídos



A GUA tem três partes:

- Prefixo global de roteamento
- ID da Sub-Rede
- ID da Interface

Fonte: Cisco



Tipos de Endereço IPv6

Estrutura IPv6 GUA

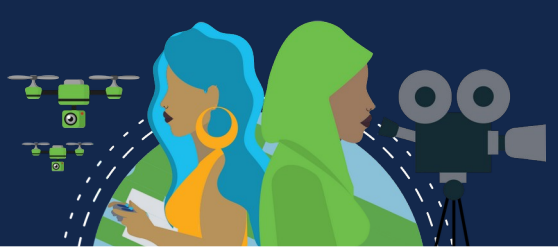
Prefixo de roteamento global: É a parte de rede do endereço atribuído pelo ISP. Prefixos /48 são os mais comuns atribuídos. Determina o tamanho da ID da sub-rede.

Exemplo: 2001:db8:acad::/ 48 indica que os primeiros 48 bits ou 3 hextets (2001:db8:acad), são como o ISP conhece essa rede. Dois-pontos duplos (::) indicam que o restante do endereço contém apenas 0s.

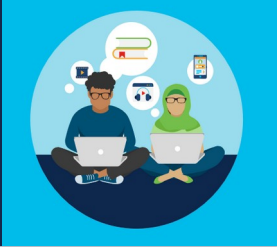
ID de sub-rede: Área entre o Prefixo de roteamento global e o ID da interface. Identifica as sub-redes locais. Quanto maior o ID da sub-rede, mais sub-redes disponíveis.
Um prefixo de roteamento global /32 e um ID de sub-rede de 32 bits terá 4,3 bilhões de sub-redes, cada uma com 18 quintilhões de hosts por sub-rede. Em um prefixo /64, os quatro primeiros hexteto são para a parte da rede, com o quarto hexteto indicando o ID da sub-rede. Os quatro hextetos restantes são para o ID da interface.

ID da interface: Equivale a parte de host. É recomendado o uso de sub-redes /64, que permitem 18 quintilhões de hosts por sub-rede.
Uma sub-rede /64 deixa 64 bits para o ID da interface. O que permite que dispositivos habilitados para SLAAC criem seu próprio ID de interface de 64 bits e torna o plano de endereçamento IPv6 simples e eficaz.
No IPv6 os endereços de host apenas com 1s podem ser atribuídos a um host pois endereços de broadcast não são usados no IPv6. Endereços apenas de 0s também são usados, mas são reservados como endereço anycast de roteadores de sub-redes e só deve ser atribuído a roteadores.

Fonte: Cisco



Tipos de Endereço IPv6



IPv6 LLA

Link local address: permite que um host se comunique com outros habilitados para IPv6 no mesmo link e somente nesse link (sub-rede). Os pacotes com endereço de link local origem ou destino não podem ser roteados além do link de onde o pacote foi originado.

O GUA não é um requisito. No entanto, cada interface habilitada para IPv6 deve ter um LLA.

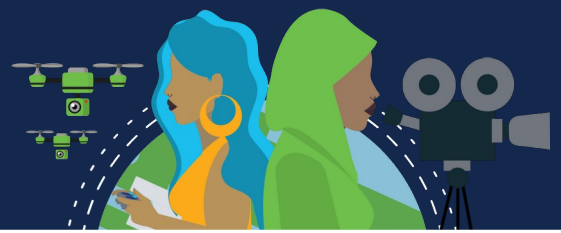
Se não for configurado manualmente em uma interface, o dispositivo criará automaticamente um próprio, sem se comunicar com um servidor DHCP. Os hosts habilitados para LLA IPv6 criarão um endereço IPv6 mesmo que não tenha sido atribuído um endereço IPv6 unicast global ao dispositivo. Isso permite que dispositivos habilitados para IPv6 se comuniquem com outros dispositivos semelhantes na mesma sub-rede, incluindo o gateway padrão.

Estão no intervalo **fe80::/10**. O /10 Indica que os primeiros 10 bits são 1111 1110 10xx xxxx. O primeiro hexteto tem um intervalo de 1111 1110 1000 000000 000000 0000 (fe80) a 1111 1110 1011 111111 111111 1111 (febf).

Normalmente, é o LLA do roteador, e não a GUA, que é usado como endereço do gateway padrão.

Há duas maneiras pelas quais um dispositivo pode obter um LLA: **Estaticamente**, configurado manualmente ou **Dinamicamente**, onde o dispositivo cria seu próprio ID de interface usando valores gerados aleatoriamente ou usando o método de Identificador Único Extended (EUI), que usa o endereço MAC do cliente juntamente com bits adicionais.

Fonte: Cisco

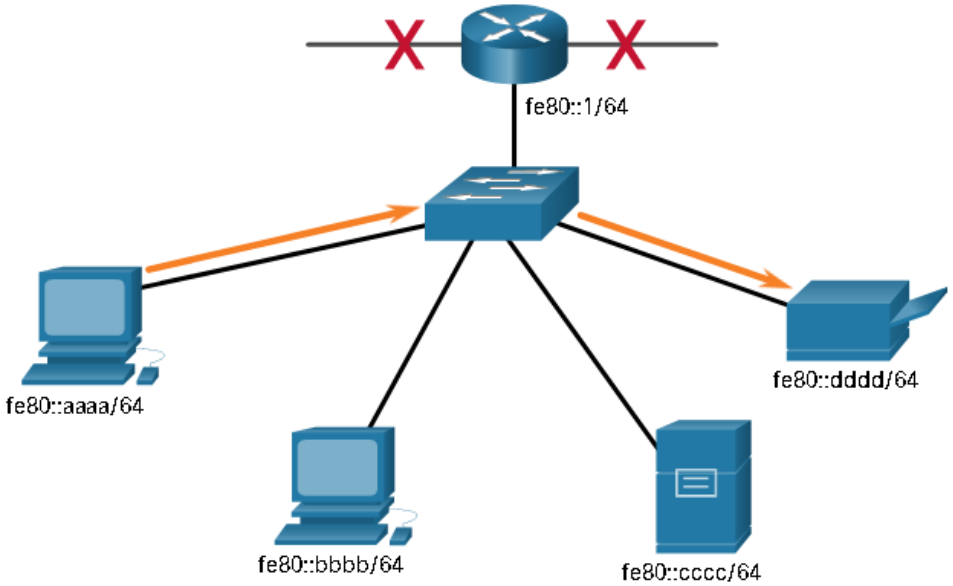


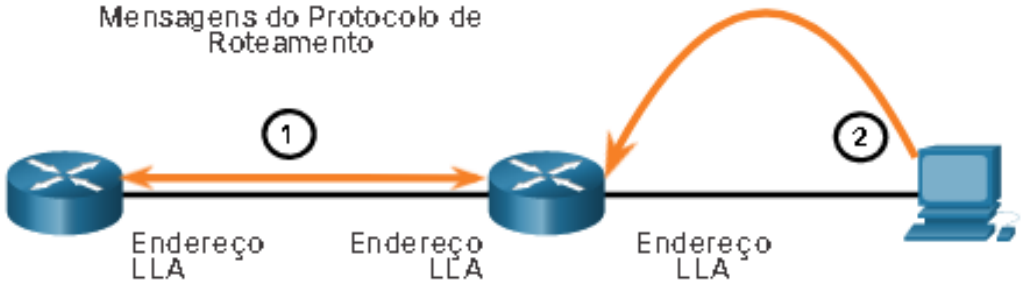
Tipos de Endereço IPv6

Comunicações IPv6 de Link Local

Pacote IPv6

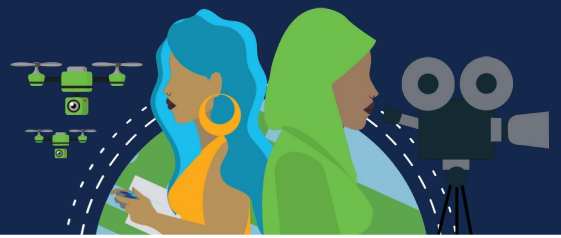
Endereço IPv6 origem	Endereço IPv6 Destino
fe80::aaaa	fe80::dddd





1. Os roteadores usam o LLA de roteadores vizinhos para enviar atualizações de roteamento.
2. Os hosts usam o LLA de um roteador local como gateway padrão.

Fonte: Cisco



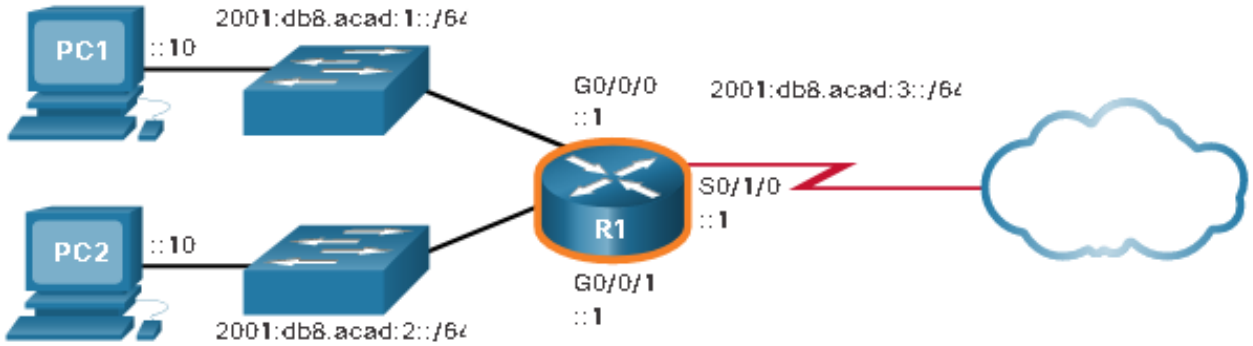
Configuração Estática do GUA e do LLA

Configuração de GUA estática em um roteador

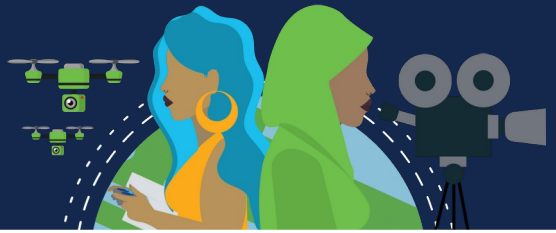
GUAs IPv6 são iguais aos endereços IPv4 públicos. O endereço IPv6 unicast global (GUA) é globalmente exclusivo e roteável na Internet IPv6. Um LLA IPv6 permite que dois dispositivos habilitados para IPv6 se comuniquem uns com os outros no mesmo link (sub-rede).

A maioria dos comandos de configuração e verificação do IPv6 no Cisco IOS são semelhantes aos seus equivalentes no IPv4. Em muitos casos, a única diferença é o uso de ipv6 no lugar ip de dentro dos comandos.

```
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface GigabitEthernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```



Fonte: Cisco



Configuração Estática do GUA e do LLA

Configuração de GUA estática em um Host Windows

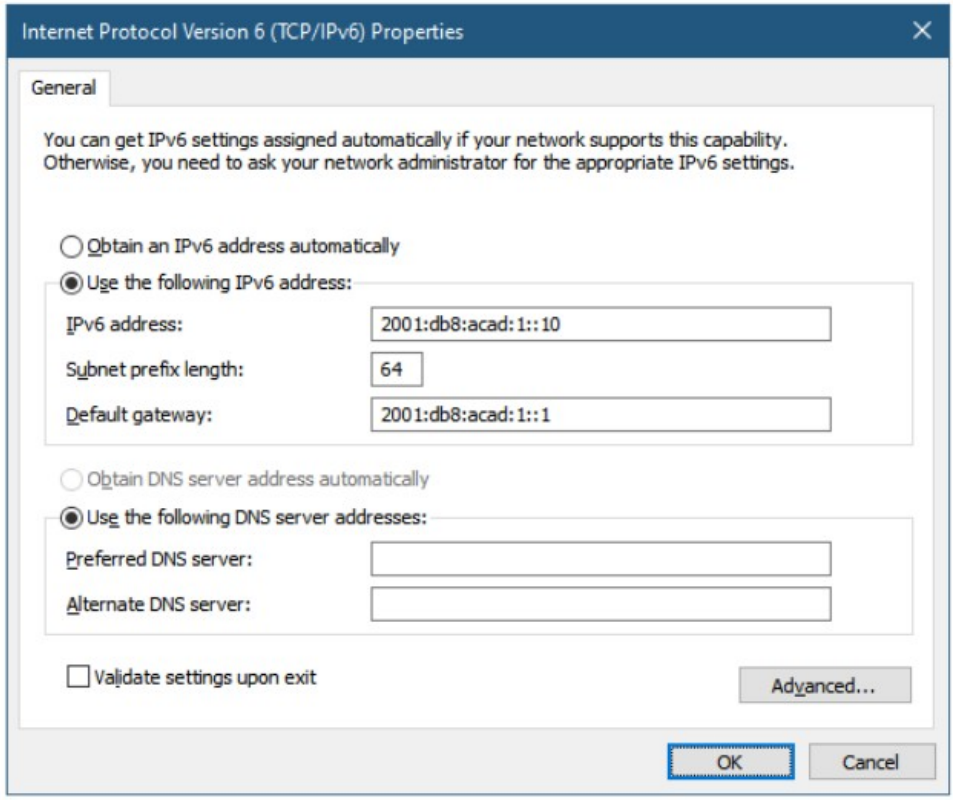
Configurar manualmente o endereço IPv6 em um host é semelhante a configurar um endereço IPv4. O endereço de gateway padrão configurado para PC1 é 2001:db8:acad: 1::1. Essa é a GUA da interface R1 GigabitEthernet na mesma rede. Como alternativa, o endereço de gateway padrão pode ser configurado para corresponder ao endereço LLA da interface Gigabit Ethernet. O uso do LLA do roteador como endereço de gateway padrão é considerado prática recomendada. Qualquer uma das configurações funcionará.

Assim como ocorre no IPv4, a configuração de endereços estáticos em clientes não é escalavel para ambientes maiores. Sendo usada a atribuição dinâmica de endereços IPv6.

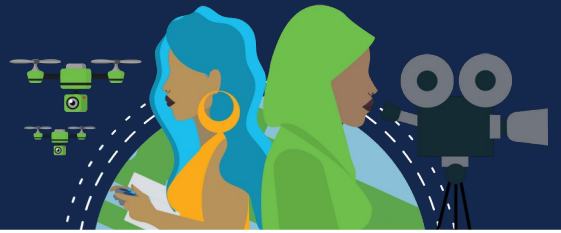
Há duas maneiras de um dispositivo obter um endereço IPv6 unicast global automaticamente:

- Configuração automática de endereço stateless (SLAAC)
- Com estado DHCPv6

Quando o DHCPv6 ou o SLAAC são usados, o LLA do roteador será especificado automaticamente como o endereço de gateway padrão.



Fonte: Cisco



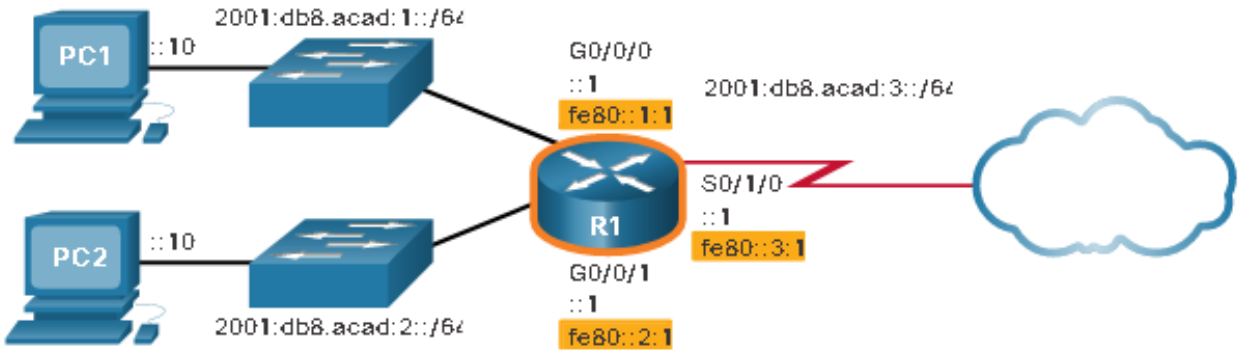
Configuração Estática do GUA e do LLA

Configuração estática de um endereço Unicast local de link (LLA)

A configuração manual do LLA permite criar um endereço reconhecível e fácil de lembrar. Geralmente, só é necessário criar endereços de link local reconhecíveis nos roteadores. Isso é benéfico porque os LLAs do roteador são usados como endereços de gateway padrão e no roteamento de mensagens de anúncio.

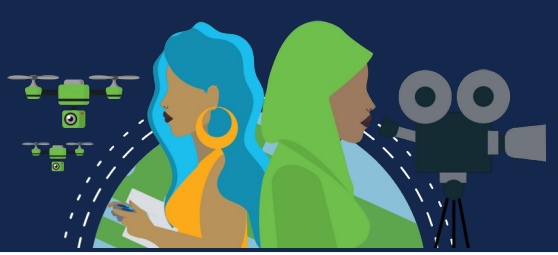
Quando um endereço começa dentro do intervalo de fe80 a febf, o parâmetro **link-local** deve seguir o endereço.

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address fe80::1:1 link-local
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 address fe80::2:1 link-local
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address fe80::3:1 link-local
R1(config-if)# exit
```



Observação: O mesmo LLA pode ser configurado em cada link, desde que seja exclusivo nesse link. Isso é possível porque as interfaces de link local só precisam ser exclusivas nesse link. No entanto, a prática comum é criar um LLA diferente em cada interface do roteador para facilitar a identificação do roteador e da interface específica.

Fonte: Cisco

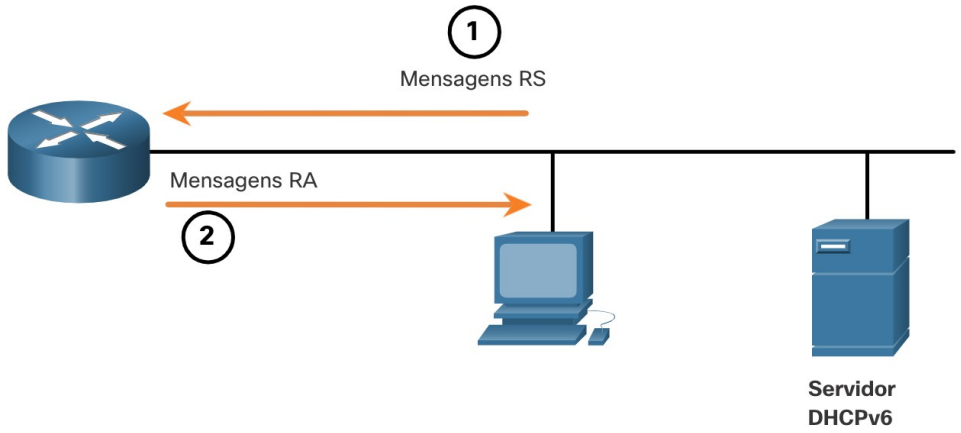


Endereçamento dinâmico para GUAs IPv6

Mensagens RS e RA

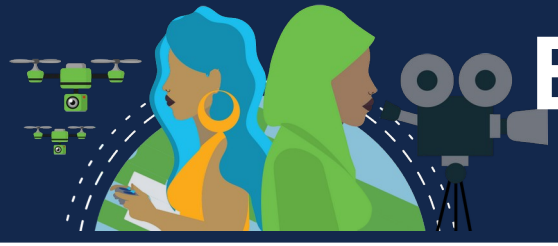
Nesse topico mostramos a diferença entre os três métodos que um anúncio de roteador pode usar, bem como o processo EUI-64 para criar um ID de interface difere de um processo gerado aleatoriamente.

Para o GUA, um dispositivo obtem dinamicamente através de mensagens ICMPv6 (Internet Control Message Protocol versão 6). Os roteadores IPv6 enviam mensagens ICMPv6 de RA a cada 200 segundos para todos os dispositivos em IPv6 na rede. Uma mensagem de RA envia resposta a um host que envia mensagem ICMPv6 de RS (Solicitação de Roteador).



1. As mensagens RS são enviadas a todos os roteadores IPv6 por hosts solicitando informações de endereçamento.
2. Mensagens RA são enviadas para todos os nós IPv6. Se o Método 1 (somente SLAAC) for usado, o RA incluirá informações de prefixo de rede, prefixo e gateway padrão.

Fonte: Cisco



Endereçamento dinâmico para GUAs IPv6

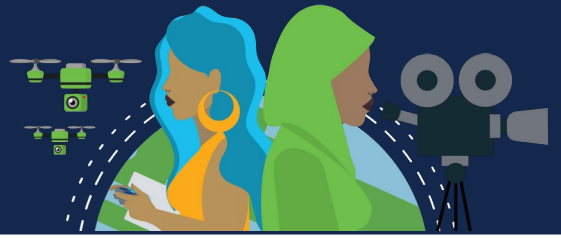
A mensagem ICMPv6 de RA inclui:

Prefixo de rede e comprimento do prefixo – Informa ao dispositivo a que rede ele pertence.
Endereço do gateway padrão – É um endereço LLA IPv6, o endereço IPv6 origem da mensagem de RA.
Endereços DNS e nome de domínio – Endereços de servidores DNS e um nome de domínio.

Existem três métodos para mensagens RA:

Method 1: SLAAC - “Eu tenho tudo o que você precisa, incluindo o prefixo, comprimento do prefixo e endereço de gateway padrão.”
Method 2: SLAAC com um servidor DHCPv6 sem estado - "Aqui estão as minhas informações, mas você precisa obter outras informações, como endereços DNS, de um servidor DHCPv6 sem estado".
Method 3: DHCPv6 com estado (sem SLAAC) - “Posso dar-te o seu endereço de gateway padrão. Você precisa pedir a um servidor DHCPv6 com estado para todas as suas outras informações.”

Fonte: Cisco

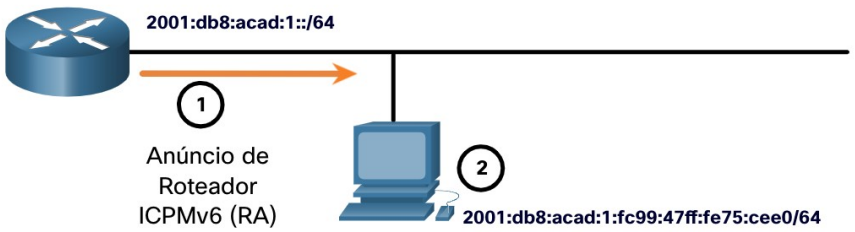


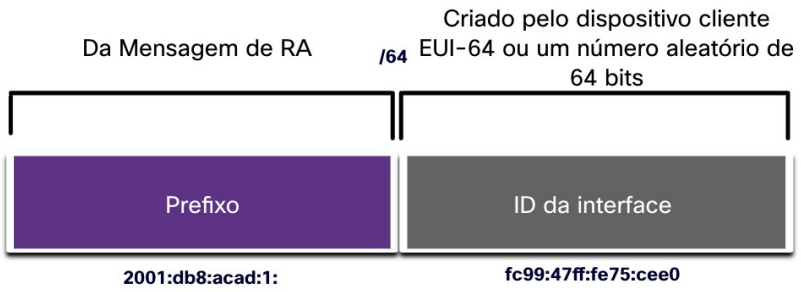
Endereçamento dinâmico para GUAs IPv6

Método 1: SLAAC

SLAAC é um método que permite que um dispositivo crie seu próprio GUA sem os serviços do DHCPv6.
Por padrão, a mensagem de RA o dispositivo usa a informaçao para crir o endereço IPv6 unicast global e para todas as demais informações.
DHCPv6 não são obrigatórios.
SLAAC é stateless, sem servidor central (por exemplo, um servidor DHCPv6 stateful) alocando endereços unicast globais e mantendo uma lista de dispositivos e seus endereços.

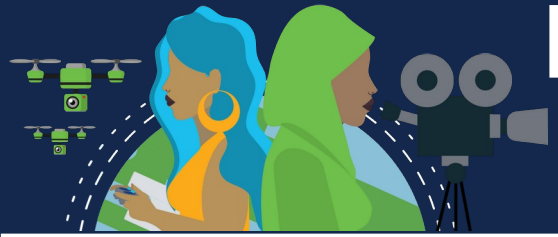
As duas partes do endereço são:
Prefixo - Isso é anunciado na mensagem RA.
ID da Interface - Isso usa o processo EUI-64 ou gera um número aleatório de 64 bits, dependendo do sistema operacional do dispositivo.





1. O roteador envia uma mensagem RA com o prefixo do link local.
2. O PC usa SLAAC para obter um prefixo da mensagem RA e cria seu próprio ID de interface.

Fonte: Cisco



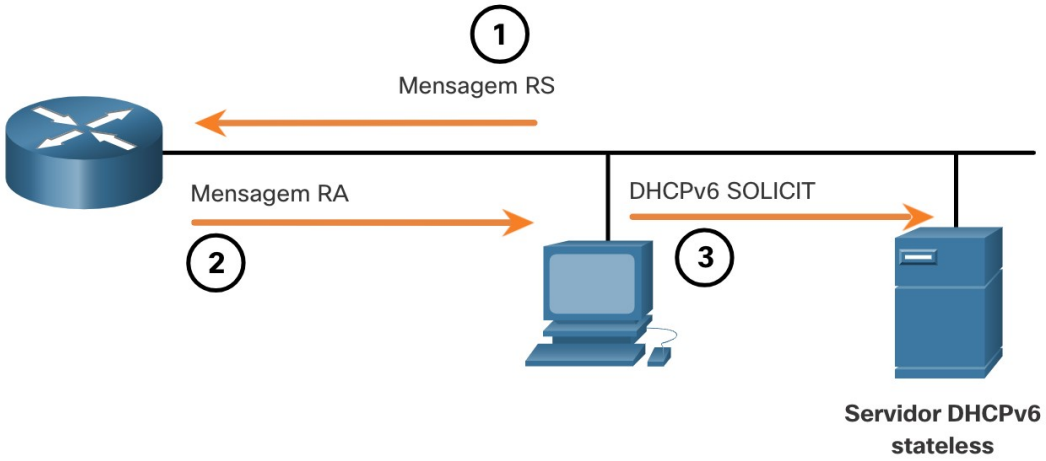
Endereçamento dinâmico para GUAs IPv6

Opção 2 de RA: SLAAC e DHCPv6 stateless

Uma interface de roteador pode ser configurada para enviar um anúncio de roteador usando SLAAC e DHCPv6 sem estado.
Os dispositivos utilizam:

- SLAAC para criar seu próprio IPv6 GUA;
- O LLA do roteador, que é o endereço IPv6 de origem RA, como o endereço de gateway padrão;
- Um servidor DHCPv6 stateless para obter outras informações como o endereço de um servidor DNS e um nome de domínio.

Observação: Um servidor DHCPv6 stateless distribui endereços do servidor DNS e nomes de domínio. Não atribui GUAs.



1. O PC envia um RS para todos os roteadores IPv6, “Preciso de informações de endereçamento”.
2. O roteador envia uma mensagem RA para todos os nós IPv6 com o método 2 (SLAAC e DHCPv6) especificado. Aqui estão as informações de Prefixo, Comprimento do prefixo e Gateway padrão. Mas você precisará obter informações de DNS de um servidor DHCPv6.”
3. O PC envia uma mensagem de solicitação DHCPv6 para todos os servidores DHCPv6. “Usei o SLAAC para criar meu endereço IPv6 e obter meu endereço de gateway padrão, mas preciso de outras informações de um servidor DHCPv6 sem estado. “

Fonte: Cisco

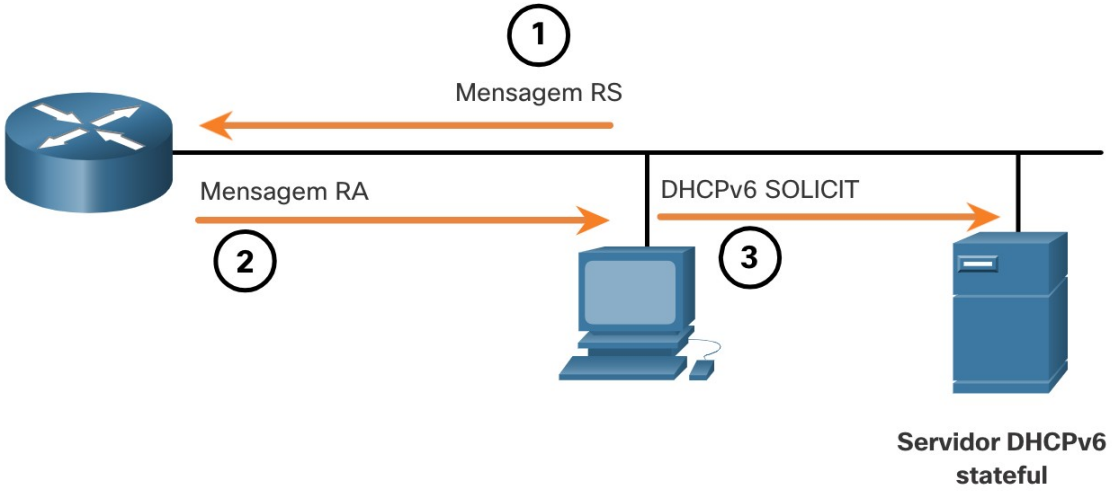
Endereçamento dinâmico para GUAs IPv6

Método 3: DHCPv6 com estado

Uma interface de roteador pode ser configurada para enviar um RA usando apenas DHCPv6 com estado.

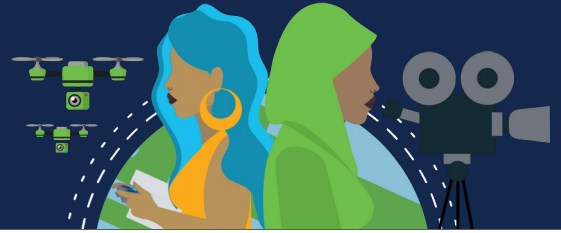
Esse método, a mensagem RA sugere que os dispositivos utilizam:

- O LLA do roteador, que é o endereço IPv6 de origem RA, como o endereço de gateway padrão
- Um servidor DHCPv6 stateful para obter o endereço unicast global, o endereço do servidor DNS, o nome do domínio e todas as demais informações.



1. O PC envia um RS para todos os roteadores IPv6, “Preciso de informações de endereçamento”.
2. O roteador envia uma mensagem RA para todos os nós IPv6 com o Método 3 (DHCPv6 Stateful) especificado, “Eu sou seu gateway padrão, mas você precisa pedir a um servidor DHCPv6 com estado para seu endereço IPv6 e outras informações de endereçamento. “
3. O PC envia uma mensagem de solicitação DHCPv6 para todos os servidores DHCPv6, "Recebi meu endereço de gateway padrão da mensagem RA, mas preciso de um endereço IPv6 e todas as outras informações de endereçamento de um servidor DHCPv6 com estado. “

Fonte: Cisco

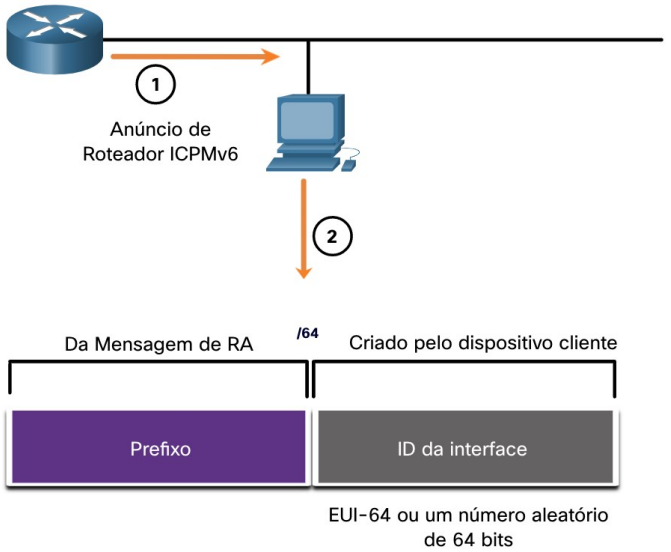


Endereçamento dinâmico para GUAs IPv6

Processo EUI-64 ou Gerado Aleatoriamente

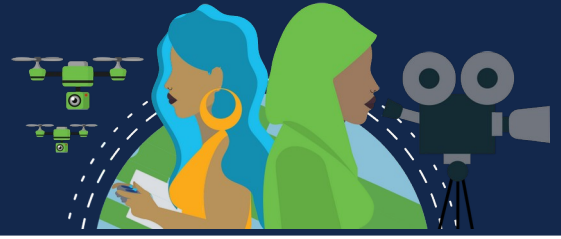
Quando a mensagem de RA é SLAAC ou SLAAC com DHCPv6 stateless, o cliente deve gerar sua própria ID da interface. O cliente conhece a parte de prefixo do endereço da mensagem de RA, mas deve criar sua própria ID da interface. A ID da interface pode ser criada por meio do processo EUI-64 ou de um número de 64 bits gerado aleatoriamente, como mostrado na Figura 1.

Criando dinamicamente um ID de interface



1. O roteador envia a mensagem do RA
2. O PC usa o prefixo na mensagem RA e usa EUI-64 ou um número de 64 bits aleatório para gerar um ID de interface.

Fonte: Cisco



Endereçamento dinâmico para GUAs IPv6

Processo EUI-64

A IEEE definiu o identificador exclusivo estendido (EUI) ou processo EUI-64 modificado. O processo usa o endereço MAC Ethernet de 48 bits de um cliente e insere outros 16 bits no meio do endereço MAC de 48 bits para criar uma ID da interface de 64 bits.

O endereço MAC é composto de duas partes:

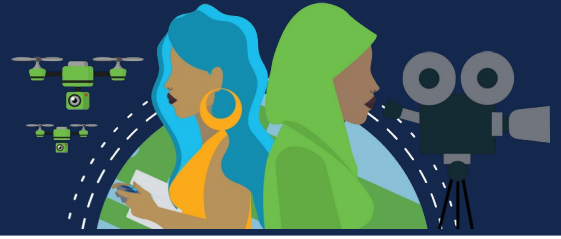
- **Identificador Organizacional Exclusivo (OUI):** Código de 24 bits do fornecedor (6 dígitos hexadecimais) atribuído pela IEEE.
- **Identificador de dispositivo:** Valor exclusivo de 24 bits (6 dígitos hexadecimais) com um OUI em comum.

Uma ID da interface EUI-64 é composta por três partes:

- OUI de 24 bits do endereço MAC do cliente, mas o sétimo bit (o bit universal/local (U/L)) é invertido. Isso significa que, se o sétimo bit for 0, ele se tornará 1, e vice-versa.
- O valor de 16 bits fffe (em hexadecimal) inserido.
- Identificador de dispositivo de 24 bits do endereço MAC do cliente.

O processo EUI-64 está ilustrado na Figura 2, usando o endereço MAC Gigabit Ethernet de R1 fc99:4775:cee0.

Fonte: Cisco



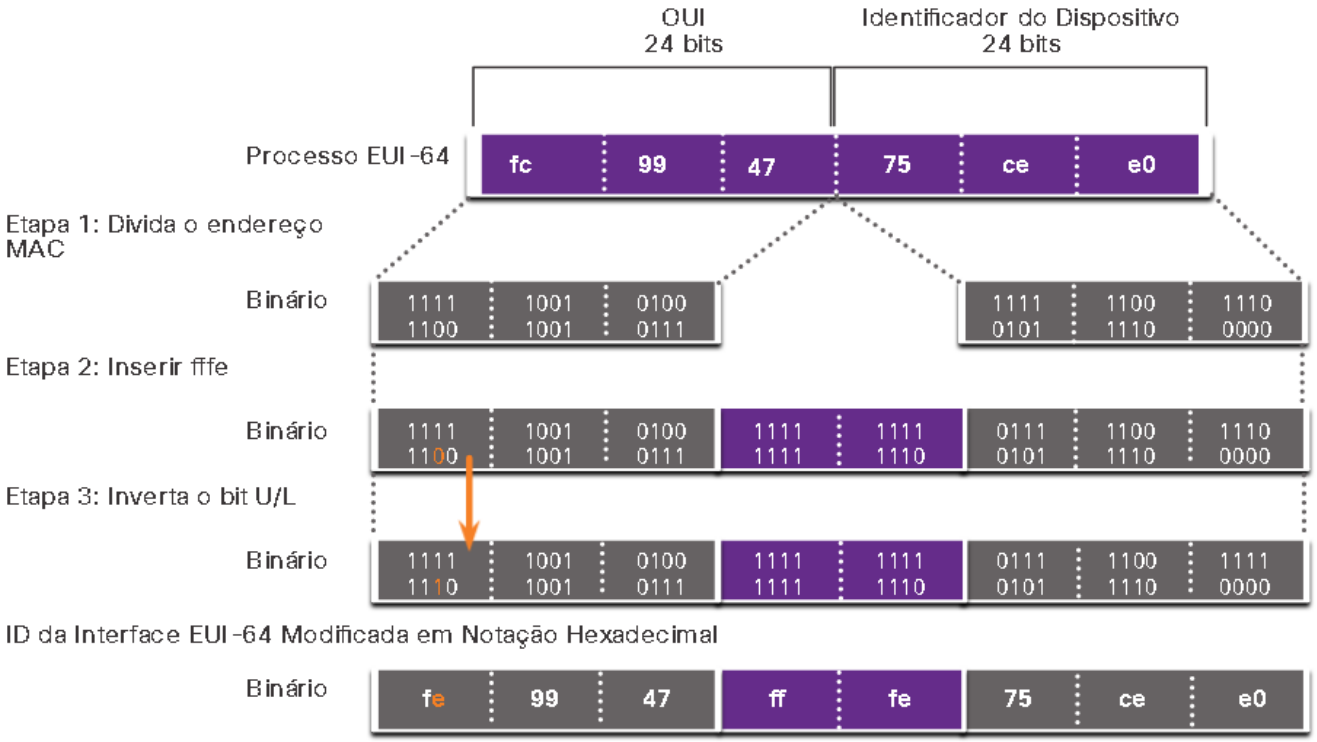
Endereçamento dinâmico para GUAs IPv6

Etapa1: Divida o endereço MAC entre a OUI e o identificador do dispositivo.
Etapa2: Insira o valor hexadecimal fffe, que em binário é: 1111 1111 1111 1110.
Etapa3: Converta os 2 primeiros valores hexadecimais da OUI em binários e inverta o bit U / L (bit 7). Neste exemplo, o 0 do bit 7 é alterado para 1.

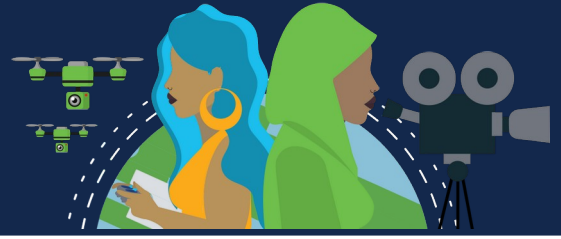
O resultado é um ID de interface gerado pela EUI-64 de fe99: 47ff: fe75: cee0.

Observação: O uso do bit U / L e as razões para reverter seu valor são discutidos na RFC 5342.

A saída de exemplo para o comando ipconfig mostra o GUA IPv6 sendo criado dinamicamente usando o SLAAC e o processo EUI-64. Uma maneira fácil de identificar que um endere



Fonte: Cisco



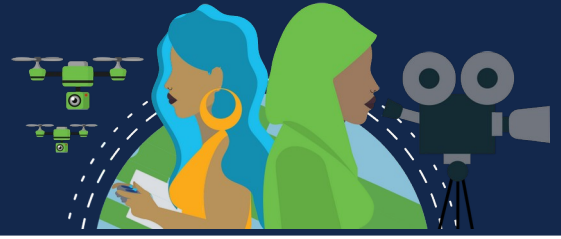
Endereçamento dinâmico para GUAs IPv6

A saída de exemplo para o comando ipconfig mostra o GUA IPv6 sendo criado dinamicamente usando o SLAAC e o processo EUI-64. Uma maneira fácil de identificar que um endereço provavelmente foi criado usando o EUI-64fffe é o localizado no meio do ID da interface.

A vantagem do EUI-64 é o endereço MAC Ethernet que pode ser usado para determinar a ID da interface. Ele também permite que os administradores de rede rastreiem facilmente um endereço IPv6 para um dispositivo final usando o endereço MAC exclusivo. No entanto, isso causou preocupações de privacidade entre muitos usuários que se preocupavam que seus pacotes pudessem ser rastreados para o computador físico real. Devido a essas preocupações, poderá ser utilizada uma ID da interface gerada de forma aleatória.

```
C:\ipconfig
Windows IP Configuration
Adaptador Ethernet Conexão de Área Local:
   Específico de Conexão Sufixo DNS. :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc 99:47ff:fe75:cee0
   Link-local IPv6 Address . . . . .: fe80: :fc 99:47 ff:fe75:cee0
   Gateway Padrão . . . . . . . . . .: fe80: :1
C:\>
```

Fonte: Cisco



IDs da Interface Geradas Aleatoriamente

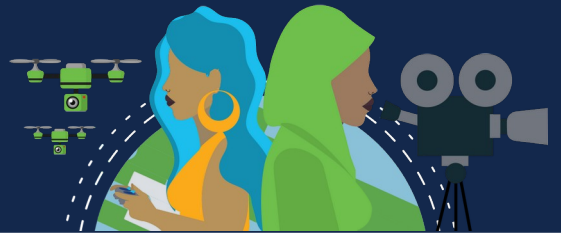
Dependendo do sistema operacional, um dispositivo pode usar uma ID da interface gerada de forma aleatória em vez de usar o endereço MAC e o processo EUI-64. Por exemplo, do Windows Vista em diante, o Windows usa uma ID da interface gerada de forma aleatória em vez de uma criada com o EUI-64. O Windows XP e os sistemas operacionais Windows anteriores usavam o EUI-64.

Depois que a ID da interface for estabelecida, seja pelo processo de EUI-64 ou por geração aleatória, ela poderá ser combinada a um prefixo IPv6 da mensagem de RA para criar um endereço unicast global, como mostra a Figura.

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
   Default Gateway . . . . . . . . . : fe80::1
C:\>
```

Observação: para garantir a exclusividade de qualquer endereço IPv6 unicast, o cliente pode usar um processo conhecido como detecção de endereço duplicado (DAD). Isso equivale a uma solicitação ARP para seu próprio endereço. Se não houver resposta, significa que o endereço é exclusivo.

Fonte: Cisco

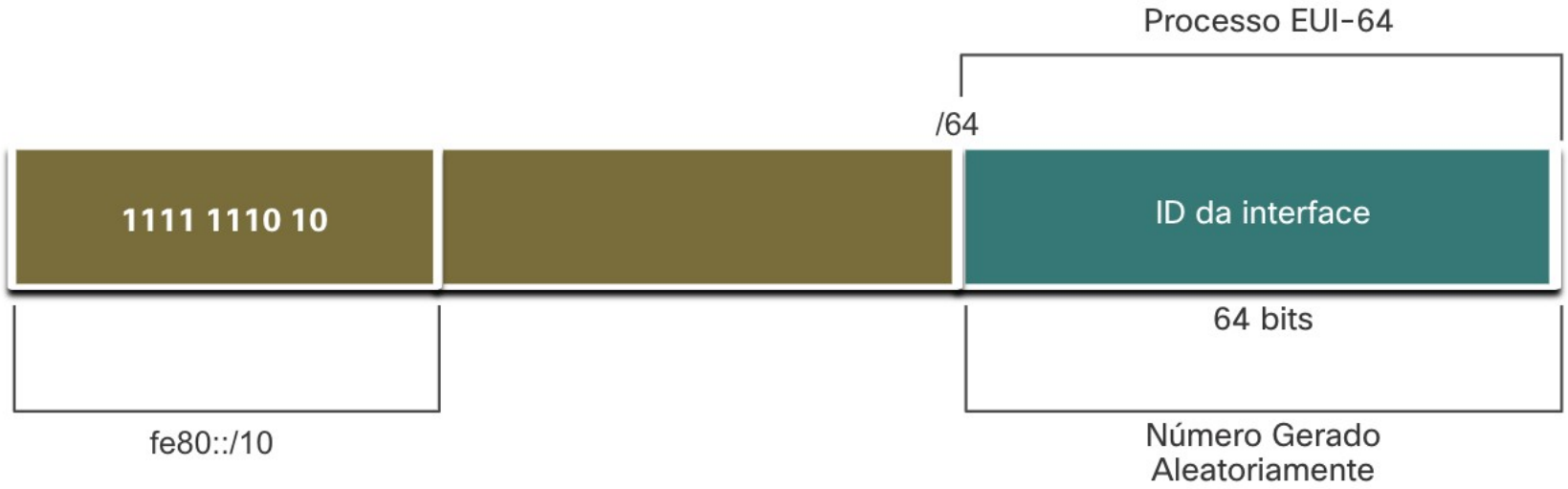


Endereçamento Dinâmico para LLAs IPv6

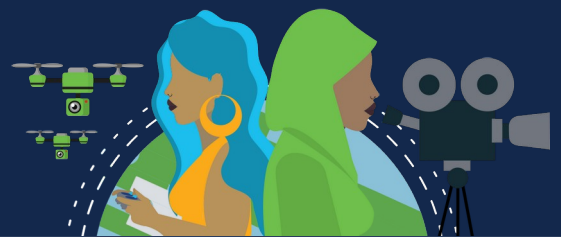
LLAs dinâmicos

Todos os dispositivos IPv6 devem ter um IPv6 LLA. Assim como IPv6 GUAs, pode ser criado LLAs dinamicamente. Independentemente de como criar LLAS (e seus GUAs), verifique toda a configuração de endereço IPv6.

A Figura mostra que o endereço de link local é criado dinamicamente



Fonte: Cisco



Endereçamento Dinâmico para LLAs IPv6

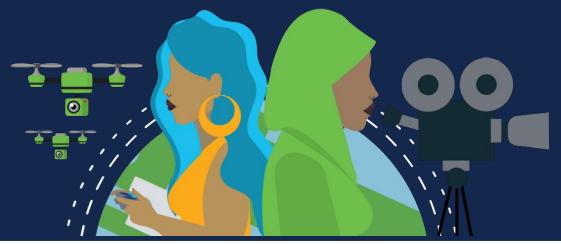
LLAs dinâmicos no Windows

Sistemas operacionais, como o Windows, normalmente usarão o mesmo método para um GUA criado pelo SLAAC e um LLA atribuído dinamicamente. Veja as áreas destacadas nos exemplos a seguir que foram mostrados anteriormente.

ID da interface gerada com EUI-64

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
Link-local IPv6 Address . . . . . : fe80::fc99:47ff:fe75:cee0
Default Gateway . . . . . . . . . : fe80::1
C:\>
```

Fonte: Cisco



Endereçamento Dinâmico para LLAs IPv6

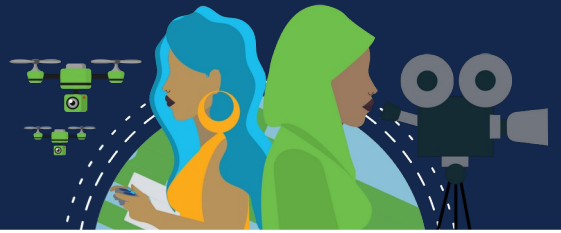
LLAs dinâmicos em Cisco Routers

Os roteadores Cisco criam automaticamente um endereço IPv6 de link local sempre que um endereço unicast global é atribuído à interface. Por padrão, os roteadores Cisco IOS usam o EUI-64 para gerar a ID em interfaces IPv6. Em interfaces seriais, o roteador usará MAC de uma interface Ethernet. O endereço de link local deve ser. No entanto, uma desvantagem é sua ID longa de interface, um desafio identificar e lembrar os endereços atribuídos. A Figura 3 mostra o endereço MAC da interface Gigabit Ethernet 0/0 de R1. Esse endereço criado dinamicamente o LLA na mesma interface Serial 0/1/0.

Para tornar mais fácil, é comum configurar estaticamente endereços IPv6 de link local nos roteadores.

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4221-2x1GE, address is 7079.b392.3640 (bia 7079.b392.3640)
(Output omitted)
R1# show ipv6 interface brief
GigabitEthernet0/0/0    [up/up]
    FE80::7279:B3FF:FE92:3640
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1    [up/up]
    FE80::7279:B3FF:FE92:3641
    2001:DB8:ACAD:2::1
Serial0/1/0             [up/up]
    FE80::7279:B3FF:FE92:3640
    2001:DB8:ACAD:3::1
Serial0/1/1             [down/down]
    unassigned
R1#
```

Fonte: Cisco



Verificar a Configuração de Endereço IPv6

show ipv6 interface brief exibe o endereço MAC das interfaces. Observe que cada interface tem dois endereços IPv6. O segundo endereço para cada interface é o GUA que foi configurado. O primeiro endereço, que começa com FE80, é o endereço de link local unicast da interface. Como as interfaces seriais não têm endereços MAC Ethernet, o Cisco IOS usa o endereço MAC da primeira interface Ethernet disponível.

show ipv6 route verifica a tabela de roteamento IPv6. Exibe somente redes IPv6, não redes IPv4. O L indica uma rota local, o endereço IPv6 específico atribuído à interface. Isto não é um LLA. LLAs não são incluídos na tabela de roteamento pois não são endereços roteáveis.

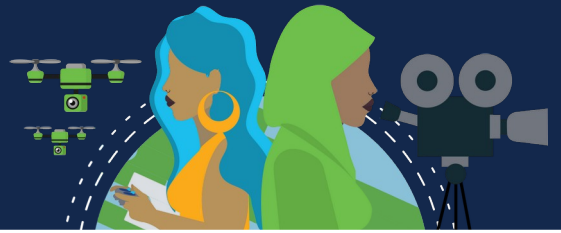
ping para IPv6 é idêntico ao comando usado em IPv4.

```
R1# ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/
```

```
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
    FE80:: 1:1
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1 [up/up]
    FE80:: 1:2
    2001:DB8:ACAD:2::1
Serial0/1/0 [up/up]
    FE80:: 1:3
    2001:DB8:ACAD:3: :1
Serial0/1/1 [down/down]
    unassigned
```

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

C 2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C 2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C 2001:DB8:ACAD:3: :/64 [0/0]
     via Serial0/1/0, directly connected
L 2001:DB8:ACAD:3: :1/128 [0/0]
     via Serial0/1/0, receive
L FF00::/8 [0/0]
     via Null0, receive
```

Fonte: Cisco



Endereços IPv6 Multicast

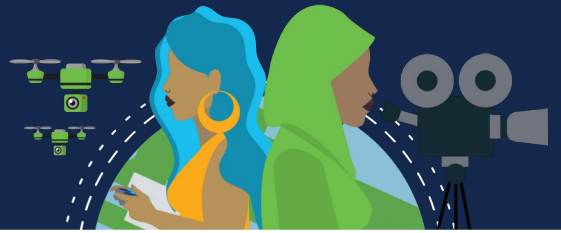
Endereços IPv6 Multicast Atribuídos

O IPv6 multicast é semelhante ao IPv4 multicast. Endereço multicast é usado para enviar um único pacote a um ou mais destinos (grupo multicast). Os endereços multicast IPv6 têm o prefixo ff00::/8.

Observação: Os endereços multicast podem ser apenas endereços de destino e não endereços de origem.

Há dois tipos de endereços IPv6 multicast:

- Endereços multicast conhecidos
- Endereços multicast do nó solicitados



Endereços IPv6 Multicast

Endereços comuns de multicast IPv6.

Endereços comuns de multicast IPv6 são atribuídos. Os endereços multicast atribuídos são endereços multicast reservados para grupos predefinidos de dispositivos. Um endereço multicast atribuído é um único endereço usado para acessar um grupo de dispositivos que executam um serviço ou um protocolo comum. Os endereços multicast atribuídos são usados no contexto com protocolos específicos, como o DHCPv6.

Estes são dois grupos multicast atribuídos ao IPv6 comuns:

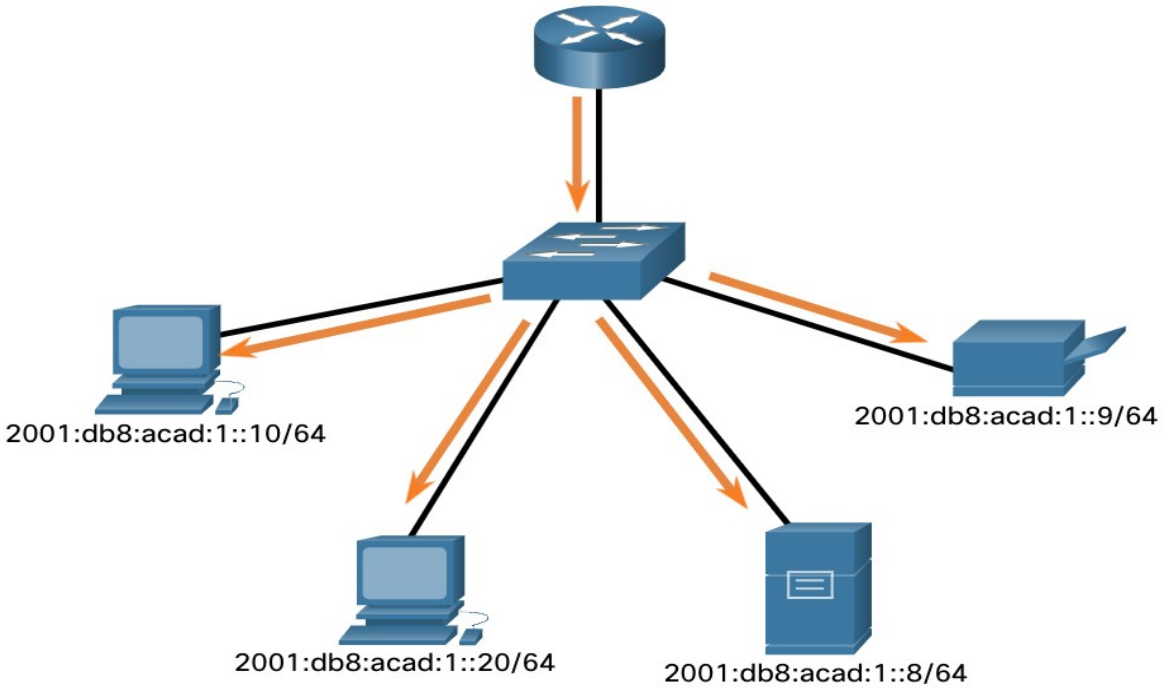
ff02::1 Grupo multicast de todos os nós -Este é um grupo multicast ao qual todos os dispositivos habilitados para IPv6 se juntam. Um pacote é recebido e processado pelo IPv6 no link ou rede. Semelhante ao broadcast no IPv4. A figura mostra a comunicação utilizando multicast all-nodes. Um roteador IPv6 envia mensagens RA ICMPv6 ao grupo multicast de todos os nós.

ff02::2 Grupo multicast de todos os roteadores – Este é um grupo multicastpara todos os roteadores IPv6. O Roteador se torna membro quando é habilitado comum roteador IPv6 com **ipv6 unicast-routing** comando de configuração global. O Pacote é processador para todos os roteadores do IPv6 no link ou rede.

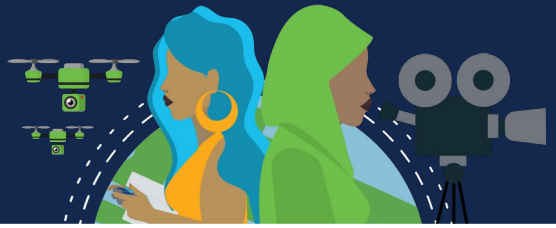
Fonte: Cisco

Endereços IPv6 Multicast

Endereço IPv6 origem	Endereço IPv6 destino
fe80::1	ff02::1

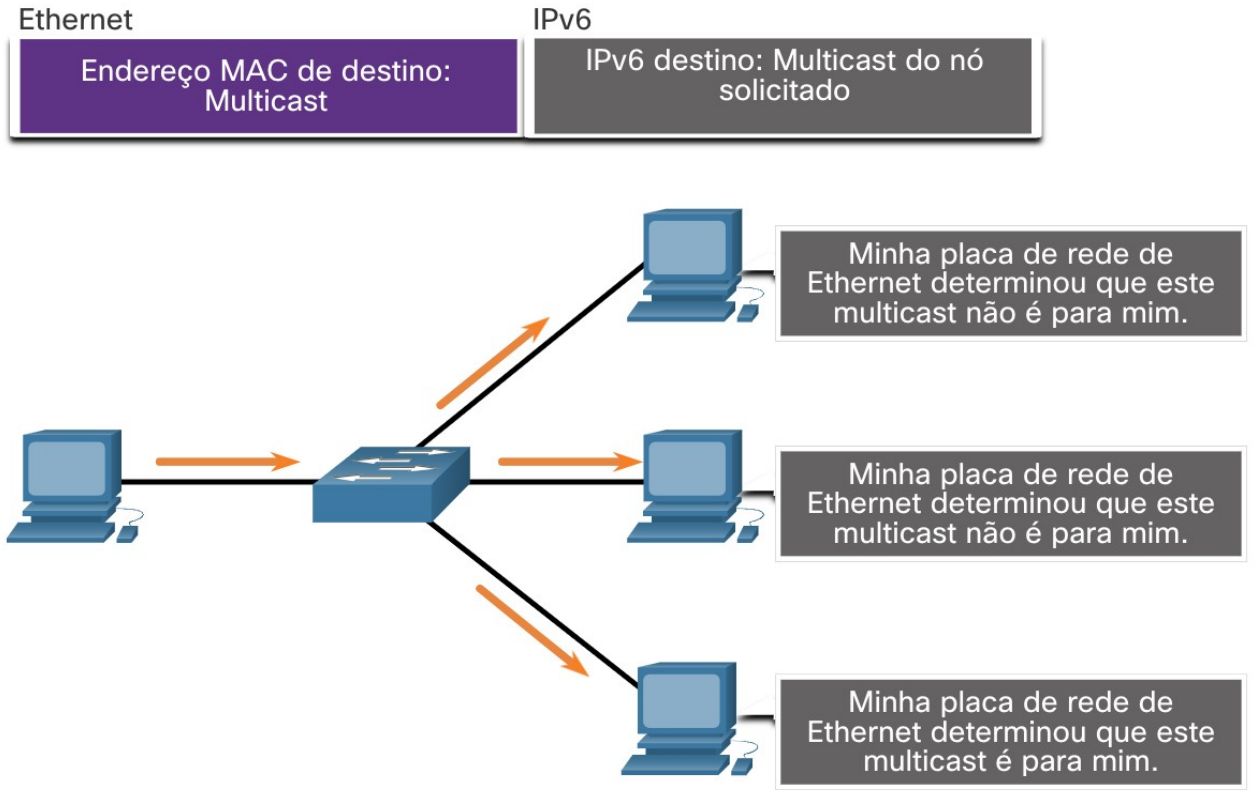


Fonte: Cisco

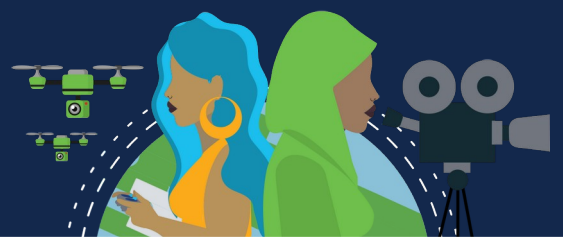


Endereços IPv6 Multicast

Um endereço multicast do nó solicitado". é semelhante ao endereço multicast all-nodes. A vantagem do endereço multicast do nó solicitado". é que ele é mapeado para um endereço multicast Ethernet especial. Isso permite que a placa de rede Ethernet filtre o quadro, examinando o endereço MAC de destino sem enviá-lo ao processo IPv6 para ver se o dispositivo é o alvo pretendido do pacote IPv6.



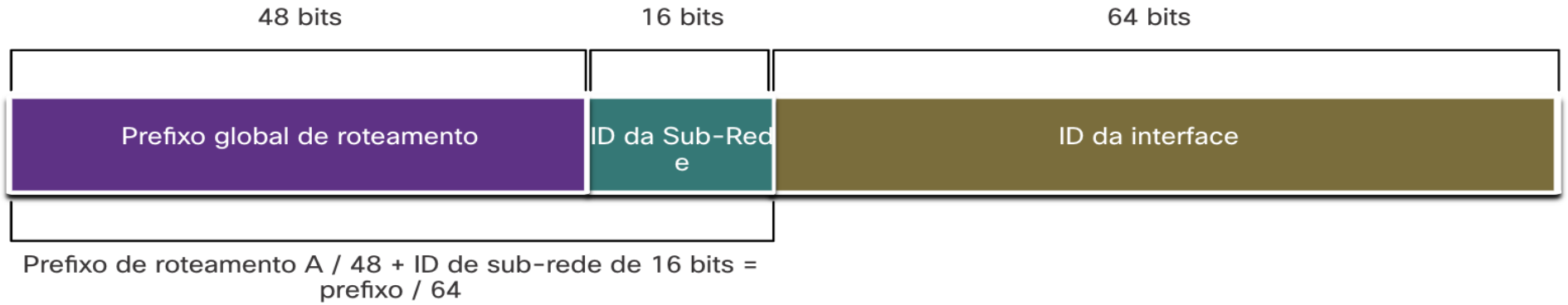
Fonte: Cisco



Sub-rede de uma rede IPv6

Com o IPv4, pedimos bits emprestados da parte do host para criar sub-redes, isso porque a subnet foi pensada depois no IPv4. O IPv6 foi projetado com sub-rede separado no GUA IPv6 usado para criar sub-redes.

GUA com um ID de sub-rede de 16 bits



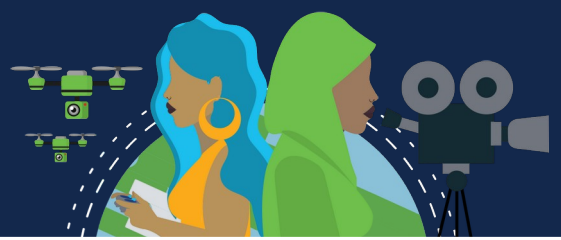
O benefício do 128 bits é suportar mais sub-redes e hosts por sub-rede, para cada rede. Conservação de endereços não é um problema. Por exemplo, se o prefixo de roteamento global for /48, e usando um 64 bits típico para o ID de interface, isso criará um ID de sub-rede de 16 bits:

- **ID de sub-rede de 16 bits** - Cria até 65.536 sub-redes.
- **ID da interface de 64 bits** - Suporta até 18 quintilhões de endereços IPv6 de host por sub-rede (ou seja, 18.000.000.000.000.000.000).

Observação: A sub-rede no ID da interface de 64 bits é possível mas raramente é necessária.

A divisão de IPv6 em sub-redes mais fácil que IPv4, pois não existe conversão em binário. Para determinar sub-rede, basta contar em ordem crescente em hexadecimal.

Fonte: Cisco

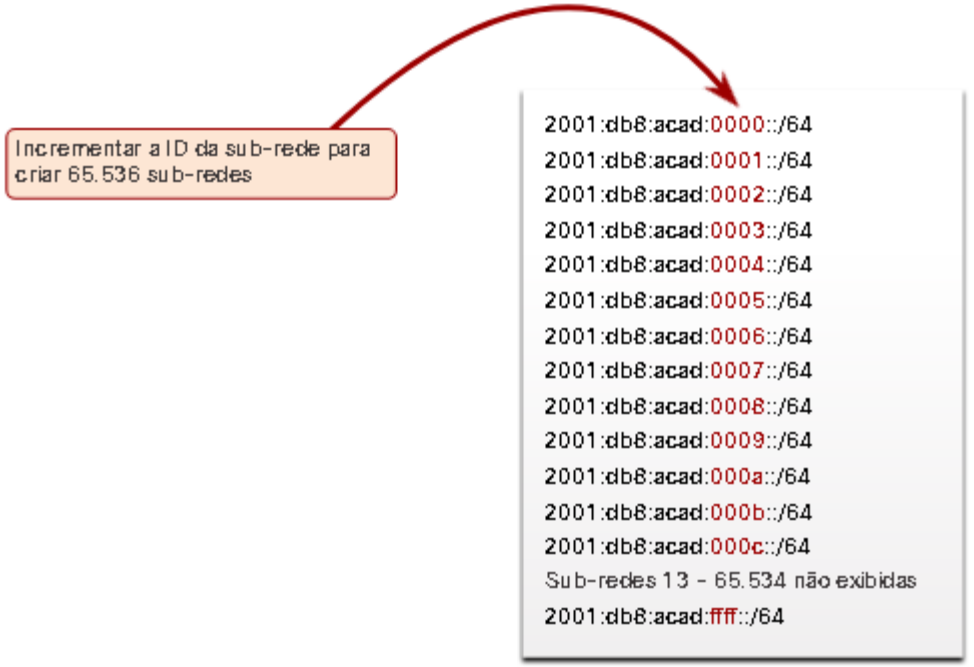


Sub-rede de uma rede IPv6

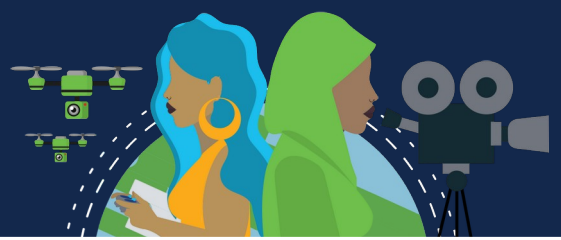
Exemplo de sub-rede IPv6

Por exemplo, o prefixo de roteamento global 2001: db8: acad :: / 48 com um ID de sub-rede de 16 bits. Criando até 64 sub-redes, o prefixo global de roteamento é o mesmo para todas as sub-redes. Somente o hexteto da ID da sub-rede é incrementado em hexadecimal para cada sub-rede.

Sub-rede usando um ID de sub-rede de 16 bits



Fonte: Cisco

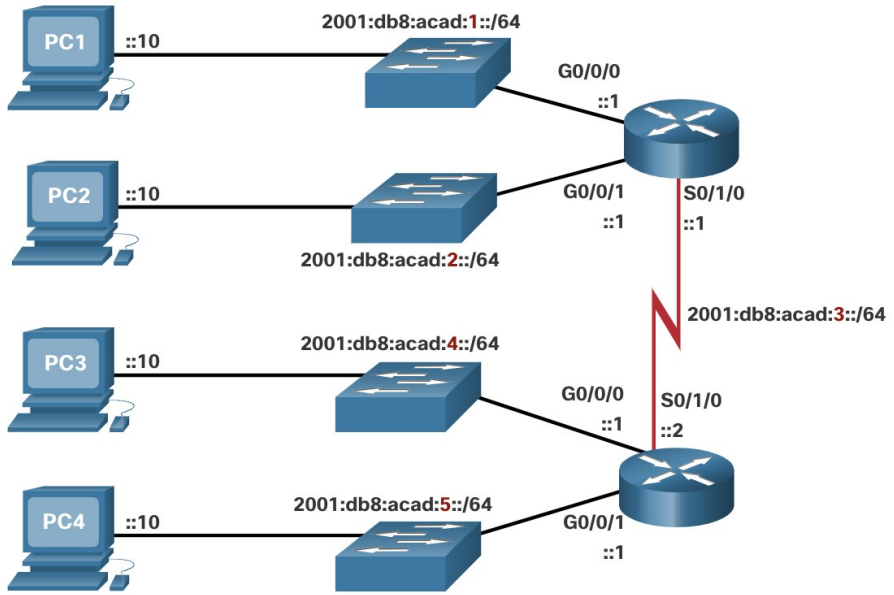


Sub-rede de uma rede IPv6

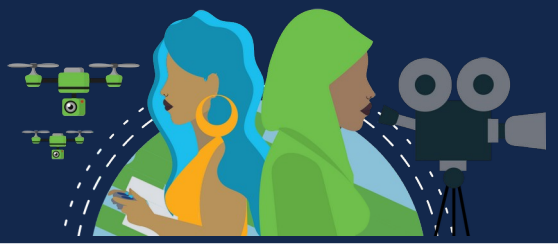
Alocação de Sub-Redes IPv6

Com mais de 65.536 sub-redes para escolher, o administrador de redes deve projetar um esquema lógico para as redes.

Conforme figura, a topologia requer cinco sub-redes, uma para cada LAN e também para o link serial entre R1 e R2. O IPv6 a sub-rede de link serial terá o mesmo comprimento de prefixo que as LANs.

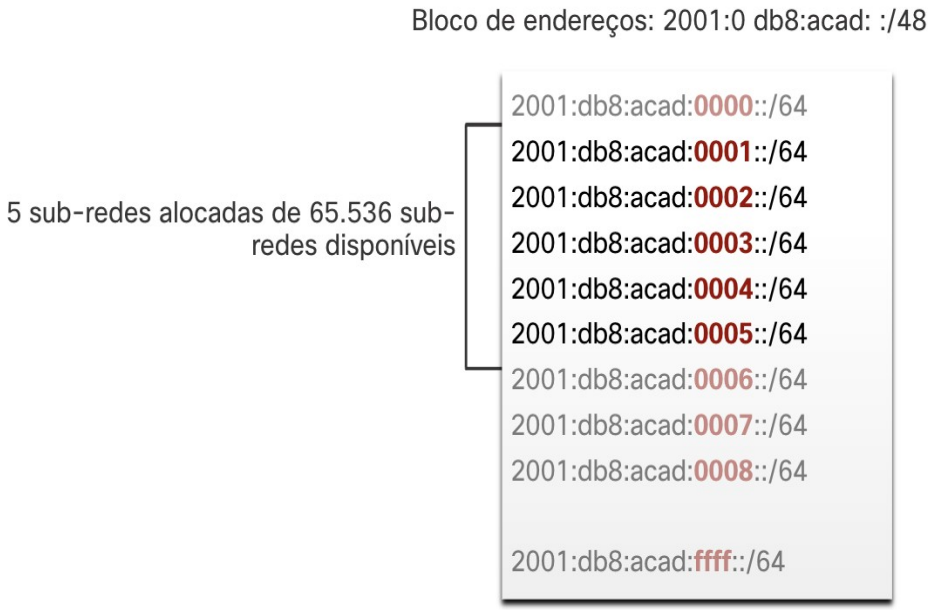


Fonte: Cisco

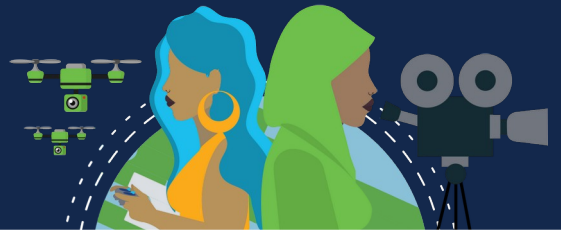


Sub-rede de uma rede IPv6

Conforme mostrado na figura a seguir, as cinco sub-redes IPv6 foram alocadas, com o campo de ID de sub-rede 0001 a 0005 usado neste exemplo. Cada sub-rede /64 fornecerá mais endereços que o necessário.



Fonte: Cisco



Sub-rede de uma rede IPv6

Roteador configurado com sub-redes IPv6

Semelhante à configuração do IPv4, o exemplo mostra que cada uma das interfaces do roteador foi configurada para estar em uma sub-rede IPv6 diferente.

Configuração de Endereço IPv6 no Roteador R1

```
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface GigabitEthernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```

Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

CCNAv7 – ITN – ICMP

Módulo 13

Embaixadores do Programa 2020, 2021 & 2022:

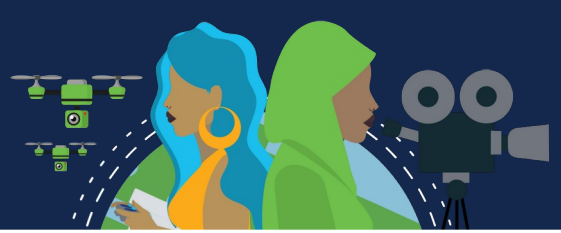
Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

WOMENROCK-IT
Brasil 2021

Networking Academy

ICMP



Mensagens ICMP

Mensagens ICMPv4 e ICMPv6

Embora o IP seja apenas um protocolo de melhor esforço, o pacote TCP/IP fornece mensagens de erro e mensagens informativas ao se comunicar com outro dispositivo IP. Essas mensagens são enviadas com os serviços do ICMP (Internet Control Message Protocol).

O objetivo dessas mensagens é dar feedback sobre questões relativas ao processamento de pacotes IP sob certas condições, e não tornar o IP confiável. As mensagens ICMP não são necessárias e muitas vezes não são permitidas por questões de segurança.

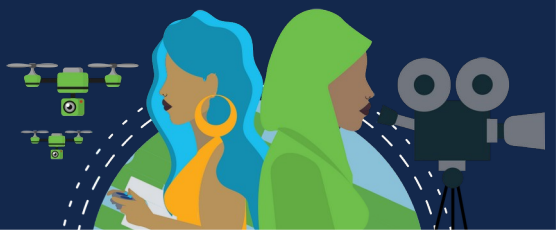
O ICMP está disponível tanto para IPv4 como para IPv6.

Os tipos de mensagens ICMP e os motivos pelos quais são enviadas são extensos. As mensagens ICMP comuns ao ICMPv4 e ICMPv6 incluem:

- **Acessibilidade do host.**
- **Destino ou serviço inalcançável.**
- **Tempo excedido.**

Fonte: Cisco

Mensagens ICMP



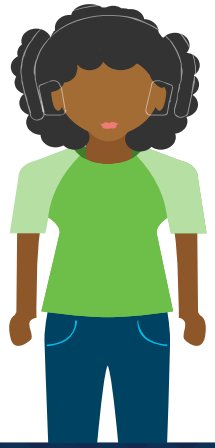
Acessibilidade do host

Uma mensagem de eco ICMP é usada para testar a capacidade de acesso de um host em uma rede IP. O host local envia uma mensagem *ICMP Echo Request* para um host. Se o host estiver disponível, ele enviará uma mensagem *Echo Reply*. Esse uso das mensagens de eco do ICMP é a base do comando **ping**.

Destino ou Serviço Inalcançável

Quando um host ou um gateway não pode entregar um pacote, ele envia uma mensagem ICMP de *destino inalcançável* para notificar à origem que o destino ou o serviço está inalcançável, contendo um código que indica por que não foi possível entregar o pacote. Os códigos usados para ICMPv4 são:

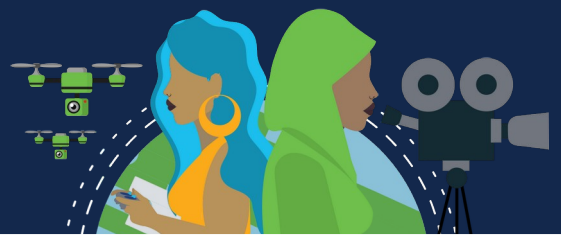
0 = rede inalcançável
1 = host inalcançável
2 = protocolo inalcançável
3 = porta inalcançável



Os códigos para o ICMPv6 são os seguintes:

0 = Nenhuma rota para o destino
1 = A comunicação com o destino é administrativamente proibida (por exemplo, firewall)
2 = Além do escopo do endereço de origem
3 = Endereço inacessível
4 = porta inalcançável

Fonte: Cisco



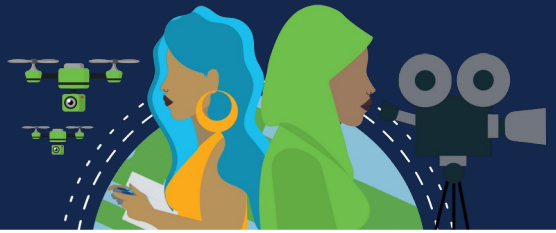
Mensagens ICMP

Tempo Excedido

A mensagem ICMPv4 de tempo excedido é usada por um roteador para indicar que um pacote não pode ser encaminhado porque o campo Vida Útil (TTL) do pacote foi reduzido a 0. Se um roteador recebe um pacote e o campo TTL do pacote IPv4 diminui para zero, ele descarta o pacote e envia uma mensagem de tempo excedido para o host de origem.

O ICMPv6 também enviará uma mensagem de tempo excedido se o roteador não conseguir encaminhar um pacote IPv6 porque o pacote expirou. Em vez do campo TTL do IPv4, o ICMPv6 usa o campo Limite de salto do IPv6 para determinar se o pacote expirou.

Observação: Mensagens de tempo excedido são usadas pelo comando **traceroute**.



Mensagens ICMP

Mensagens ICMPv6

As mensagens encontradas no ICMPv6 são semelhantes às mensagens implementadas pelo ICMPv4. No entanto, o ICMPv6 tem funcionalidade aprimorada e novos recursos. As mensagens ICMPv6 são encapsuladas no IPv6.
O ICMPv6 inclui quatro novos protocolos como parte do protocolo ND ou NDP (Neighbor Discovery Protocol):
As mensagens entre um roteador e um host IPv6, incluindo alocação de endereços dinâmicos, são as seguintes:

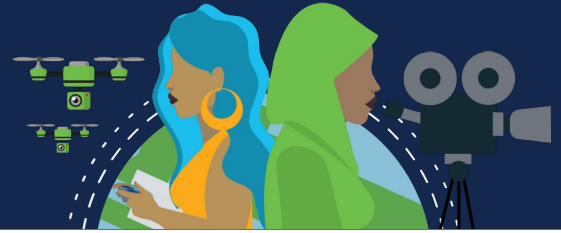
- *Mensagem de Solicitação de Roteador (RS)*
- *Mensagem de Anúncio de Roteador (RA)*

As mensagens entre dispositivos IPv6, incluindo detecção de endereço duplicado e resolução de endereço são as seguintes:

- *Mensagem de solicitação de vizinhos (NS)*
- *Mensagem de anúncio de vizinhos (NA)*

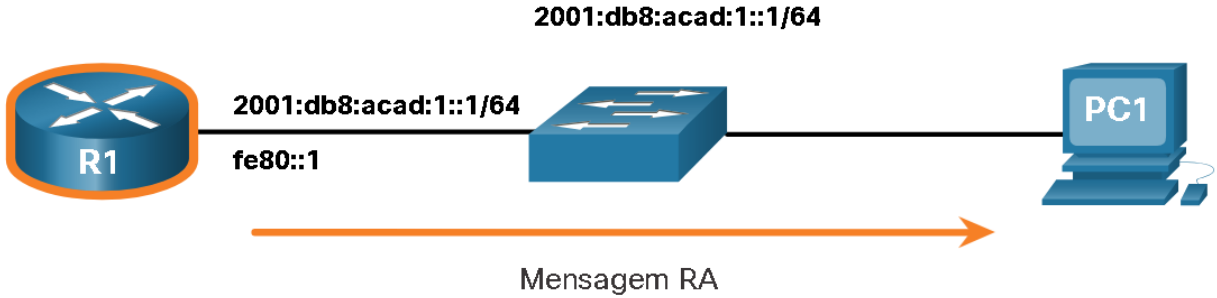
Observação: O ICMPv6 ND também inclui a mensagem de redirecionamento, que possui uma função semelhante à mensagem de redirecionamento usada no ICMPv4.

Fonte: Cisco



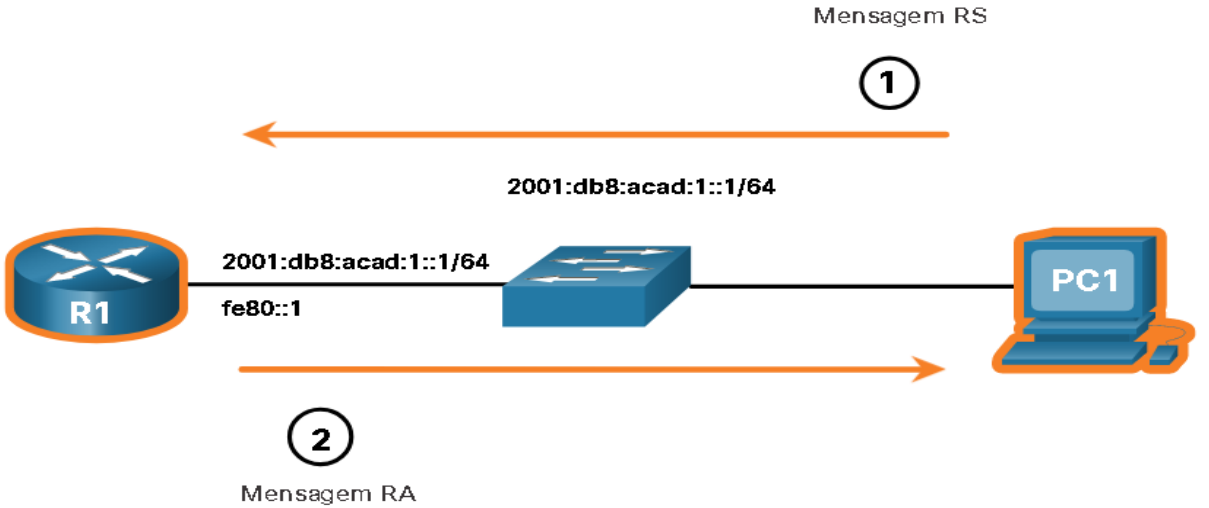
Mensagens ICMP

Mensagem RA: são enviadas por roteadores habilitados para IPv6 a cada 200 segundos para fornecer informações de endereçamento para hosts habilitados para IPv6. A mensagem RA pode incluir informações de endereçamento para o host, como prefixo, comprimento do prefixo, endereço DNS e nome de domínio. Um host que usa a Configuração Automática de Endereço sem Estado (SLAAC) definirá seu gateway padrão para o endereço local do link do roteador que enviou o RA.



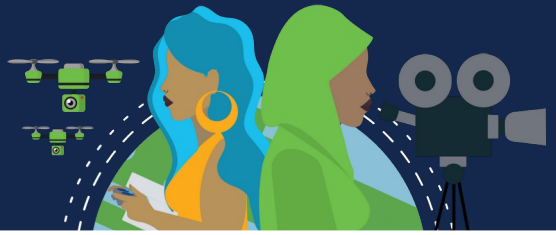
R1 envia uma mensagem RA, “Oi todos os dispositivos habilitados para IPv6. Eu sou R1 e você pode usar SLAAC para criar um endereço unicast global IPv6. O prefixo é 2001:db8:acad:1::/64. A propósito, use meu endereço de link local fe80::1 como seu gateway padrão. “

Mensagem RS: Um roteador habilitado para IPv6 também enviará uma mensagem RA em resposta a uma mensagem RS. Na figura, PC1 envia uma mensagem RS para determinar como receber suas informações de endereço IPv6 dinamicamente.



1. PC1 envia uma mensagem RS: “Oi, acabei de inicializá-lo. Existe um roteador IPv6 na rede? Preciso saber como obter minhas informações de endereço IPv6 dinamicamente.”
2. R1 responde com uma mensagem RA. “Oi todos os dispositivos habilitados para IPv6. Eu sou R1 e você pode usar SLAAC para criar um endereço unicast global IPv6. O prefixo é 2001:db8:acad:1::/64. A propósito, use meu endereço de link local fe80::1 como seu gateway padrão. “

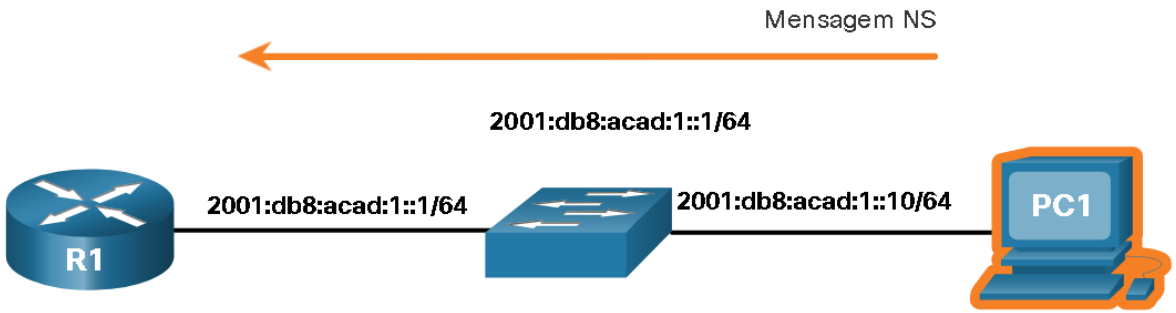
Fonte: Cisco



Mensagens ICMP

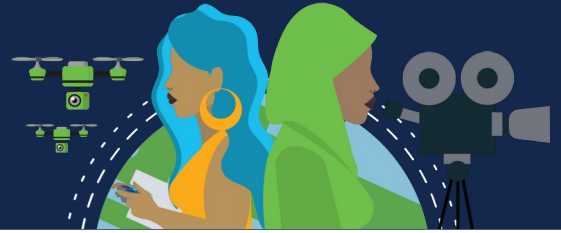
Mensagem NS: Quando um dispositivo recebe um endereço IP unicast global ou unicast local de link, um dispositivo pode receber DAD (detecção de endereço duplicado) para garantir que o endereço IPv6 seja exclusivo. Para verificar a exclusividade de um endereço, o dispositivo enviará uma mensagem NS com seu próprio endereço IPv6 como o endereço IPv6 de destino. Se outro dispositivo na rede tiver esse endereço, ele responderá com uma mensagem de NA, que notificará o dispositivo emissor de que o endereço está em uso. Se uma mensagem não for retornada dentro de um certo período de tempo, o endereço unicast será exclusivo e aceitável para uso.

Observação: O DAD não é necessário, mas o RFC 4861 recomenda que o DAD seja executado em endereços unicast.



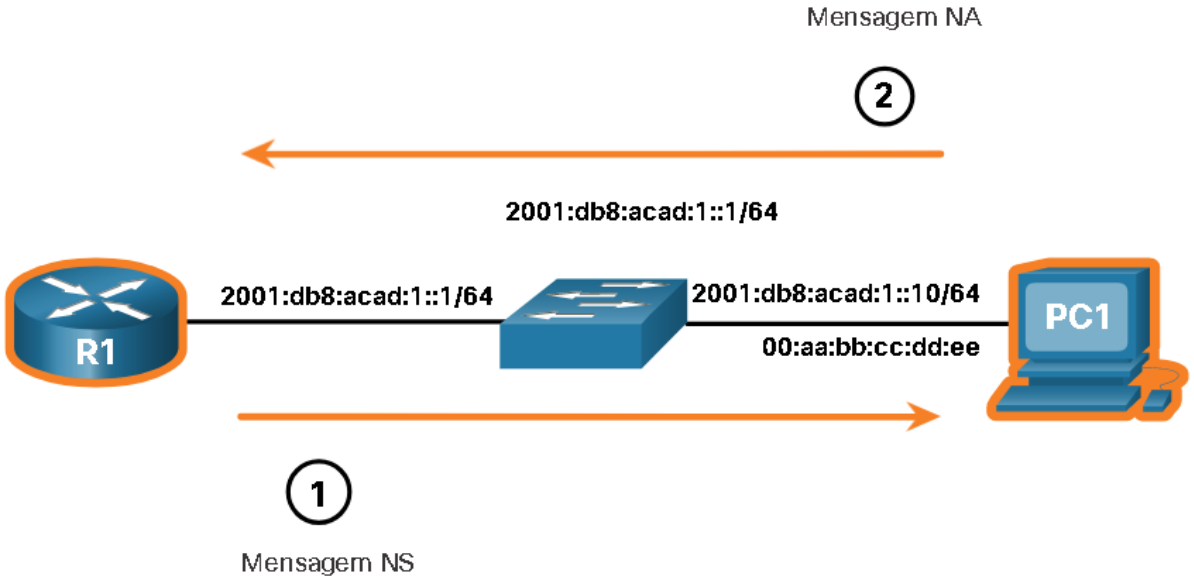
PC1 envia uma mensagem NS para verificar a singularidade de um endereço, “Quem tiver o endereço IPv6 2001:db8:acad:1::10, Envie-me seu endereço MAC? “

Fonte: Cisco



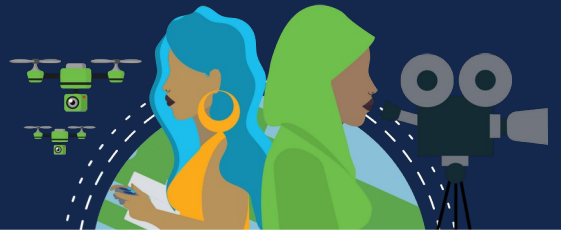
Mensagens ICMP

Mensagem NA: É usada quando um dispositivo na LAN sabe o endereço IPv6 unicast de um destino, mas não seu endereço MAC Ethernet. Para determinar o endereço MAC destino, o dispositivo enviará uma mensagem de NS para o endereço do nó solicitado. A mensagem incluirá o endereço IPv6 (destino) conhecido. O dispositivo que tem o endereço IPv6 alvo responderá com uma mensagem de NA contendo seu endereço MAC Ethernet.



1. R1 envia uma mensagem NS de resolução de endereço. “Quem tiver o endereço IPv6 2001:db8:acad:1::10, Poderia enviar-me o seu endereço MAC?
2. O PC1 responde com uma mensagem NA. “Eu sou 2001:db8:acad:1::10 e meu endereço MAC é 00:aa:bb:cc:dd:ee. “

Fonte: Cisco



Testes de Ping e Traceroute

Ping - Testar conectividade

O Ping é um utilitário de teste IPv4 e IPv6 que usa a solicitação de eco ICMP e as mensagens de resposta de eco para testar a conectividade entre hosts.

Para testar a conectividade com outro host em uma rede, uma solicitação de eco é enviada ao endereço do host usando o comando ping. Se o host no endereço especificado receber a requisição de eco, ele enviará uma resposta de eco. À medida que cada resposta de eco é recebida, ping fornece feedback sobre o tempo entre o envio da solicitação e o recebimento da resposta. Esta pode ser uma medida do desempenho da rede.

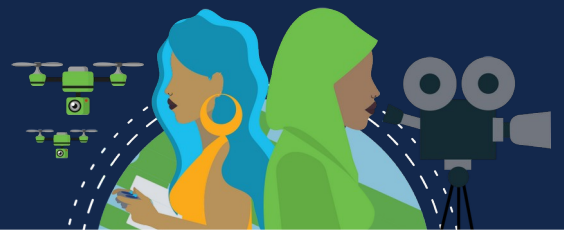
O ping tem um valor de tempo limite para a resposta. Se a resposta não é recebida dentro do tempo de espera, o ping mostra uma mensagem informando que a resposta não foi recebida. Isso pode indicar que há um problema, mas também pode indicar que os recursos de segurança que bloqueiam as mensagens de ping foram ativados na rede. É comum o primeiro ping para o tempo limite se a resolução de endereço (ARP ou ND) precisar ser executada antes de enviar a Solicitação de eco ICMP.

Depois que todas as solicitações são enviadas, o ping fornece um resumo que inclui a taxa de sucesso e o tempo médio de ida e volta para o destino.

O tipo de testes de conectividade realizados com ping incluem o seguinte:

- ping na loopback local
- ping no gateway padrão
- ping no host remoto

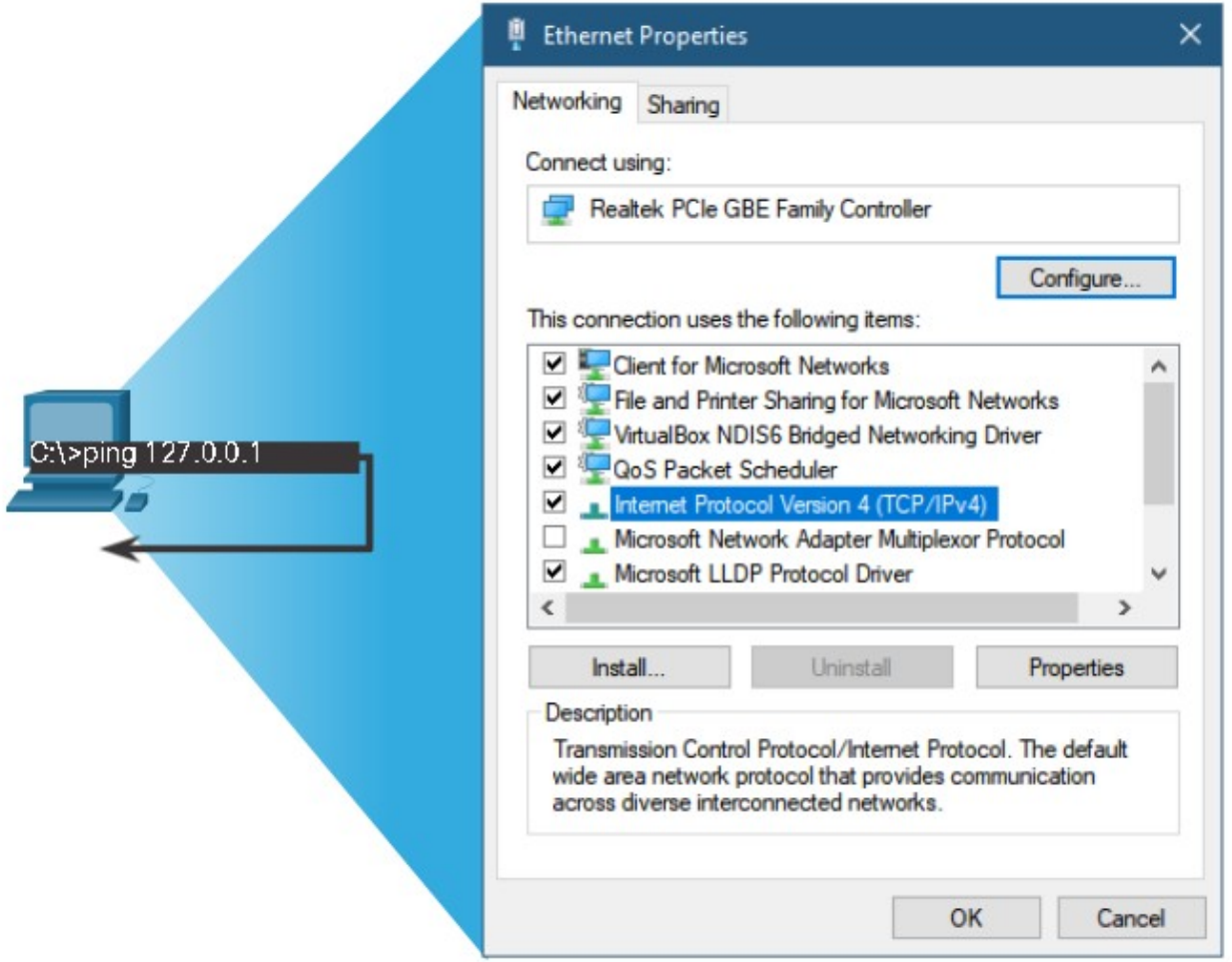
Fonte: Cisco



Testes de Ping e Traceroute

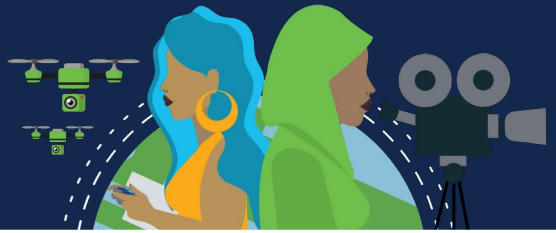
Ping na loopback

O ping pode ser usado para testar a configuração interna do IPv4 ou IPv6 no host local.
Para executar este teste, ping o endereço de loopback local 127.0.0.1 para IPv4 (:: 1 para IPv6).
Uma resposta vinda de 127.0.0.1 para IPv4 (ou ::1 para IPv6) indica que o IP está instalado corretamente no host.
Essa resposta vem da camada de rede. No entanto, ela não significa que os endereços, as máscaras ou os gateways estão configurados adequadamente, Nem indica o status da camada inferior da pilha de rede. Ela simplesmente testa o IP até a camada de rede do IP.
Uma mensagem de erro indica que o TCP/IP não está operacional no host.



O ping no host local confirma que o TCP/IP está instalado e funcionando no host local.
O ping 127.0.0.1 faz com que o dispositivo envie um ping para si mesmo.

Fonte: Cisco



Testes de Ping e Traceroute

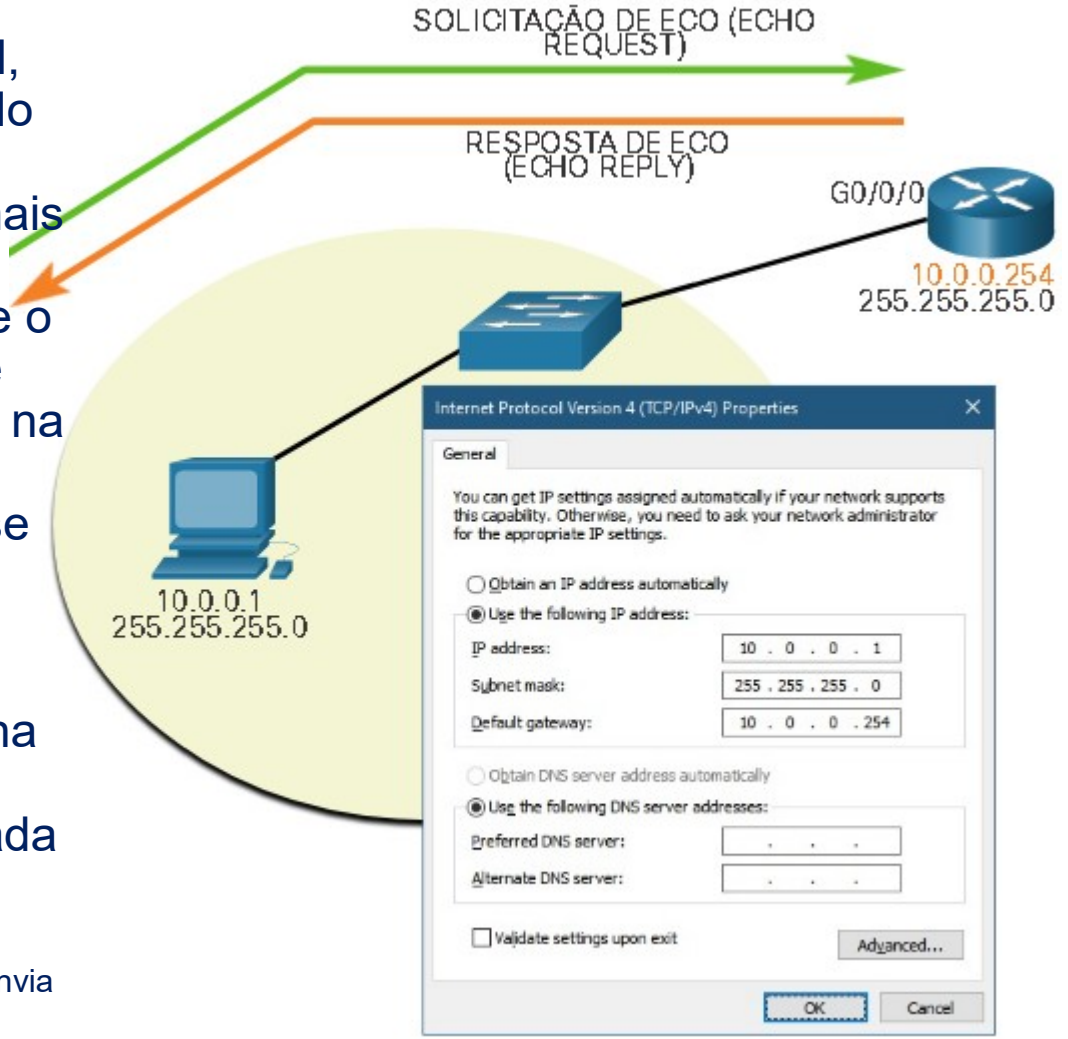
Executar ping no gateway padrão

Para testar a capacidade de um host de se comunicar na rede local, geralmente é feito um ping para o endereço IP do gateway padrão do host. Um ping com êxito no gateway padrão indica que o host e a interface do roteador servindo como gateway padrão estão operacionais na rede local.

O endereço de gateway padrão é usado com mais frequência porque o roteador normalmente está sempre operacional. Se o endereço de gateway padrão não responder, o teste pode ser feito para outro host na rede local que se sabe estar operacional.

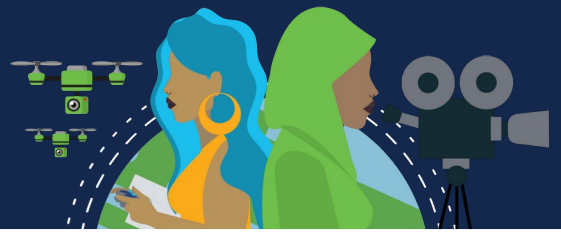
Se o gateway padrão ou outro host responder, o host local poderá se comunicar com êxito pela rede local. Se o gateway padrão não responder, mas outro host, isso pode indicar um problema com a interface do roteador servindo como gateway padrão.

Uma possibilidade é que o endereço de gateway padrão errado tenha sido configurado no host. Outra possibilidade é que a interface do roteador esteja plenamente operacional, mas tenha segurança aplicada a ela que a impeça de processar ou responder a solicitações ping.



O host envia um ping ao gateway padrão, enviando uma solicitação de eco ICMP. O gateway padrão envia uma resposta de eco confirmando a conectividade.

Fonte: Cisco



Testes de Ping e Traceroute

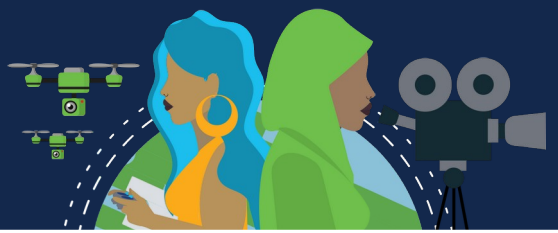
Efetuar ping em um host remoto

O ping também pode ser usado para testar a capacidade de um host local de se comunicar por uma rede interconectada. O host local pode fazer ping em um host IPv4 operacional de uma rede remota. O roteador usa sua tabela de roteamento IP para encaminhar os pacotes.

Se esse ping tiver êxito, a operação de uma grande parte da rede interconectada poderá ser verificada. Um êxito ping na rede confirma a comunicação na rede local, a operação do roteador que serve como gateway padrão e a operação de todos os outros roteadores que possam estar no caminho entre a rede local e a rede do host remoto.

Além disso, a funcionalidade do host remoto pode ser verificada. Se o host remoto não conseguir se comunicar para fora de sua rede local, ele não responderá.

Observação: Muitos administradores de rede limitam ou proíbem a entrada de mensagens ICMP na rede corporativa; por isso a falta de uma resposta pode ser consequência de restrições de segurança.



Testes de Ping e Traceroute

Traceroute - Teste o caminho

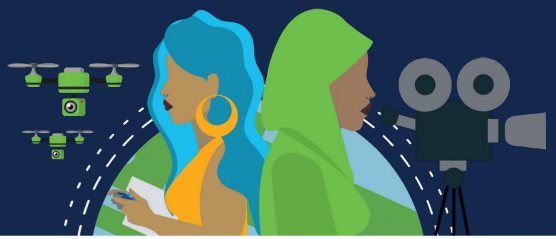
O ping testa a conectividade entre dois hosts, mas não fornece informações sobre detalhes de dispositivos entre os hosts. Traceroute (tracert) gera uma lista de saltos que foram alcançados com sucesso ao longo do caminho. Essa lista pode dar informações importantes para a verificação e a solução de erros. Se os dados atingirem o destino, o rastreamento listará a interface de cada roteador no caminho entre os hosts. Caso ocorra falha nos dados em algum salto ao longo do caminho, o endereço do último roteador que respondeu ao rastreamento poderá fornecer uma indicação de onde está o problema ou das restrições de segurança que foram encontradas.

Tempo de Ida e Volta (RTT): O traceroute fornece tempo de ida e volta para cada salto ao longo do caminho. RRT é o tempo que um pacote leva para alcançar o host remoto e retornar a resposta do host. Um asterisco (*) é usado para indicar um pacote perdido ou não respondido.

Essas informações são uteis para localizar um roteador problemático no caminho ou podem indicar que o roteador está configurado para não responder. Se forem exibidos tempos de resposta elevados ou perdas de dados para um determinado salto, significa que os recursos do roteador ou suas conexões podem estar sobrecarregados.

Limite de salto IPv4 TTL e IPv6: O Traceroute usa o campo TTL no IPv4 e o campo Limite de saltos no IPv6 nos cabeçalhos da camada 3, junto com a mensagem ICMP Time Exceeded.

Fonte: Cisco



Testes de Ping e Traceroute

A primeira sequência de mensagens enviadas pelo traceroute terá um campo TTL de valor 1. Isso faz com que o TTL coloque um tempo limite no pacote IPv4 que ocorrerá no primeiro roteador. Este roteador responde com uma mensagem ICMPv4 com tempo excedido. Agora o Traceroute tem o endereço do primeiro salto.

O Traceroute aumenta progressivamente o campo TTL (2, 3, 4...) para cada sequência de mensagens. Isso fornece ao rastreamento o endereço de cada salto à medida que os pacotes expiram mais adiante no caminho. O campo TTL continua a ser aumentado até alcançar o destino ou até atingir um valor máximo pré-determinado.

Depois que o destino final é alcançado, o host responde com uma mensagem de *Porta inacessível do ICMP* ou uma mensagem *de resposta de eco do ICMP*, em vez da mensagem *Tempo excedido do ICMP*.

Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

CCNAv7 – ITN – Camada de Transporte

Módulo 14

Embaixadores do Programa 2020, 2021 & 2022:

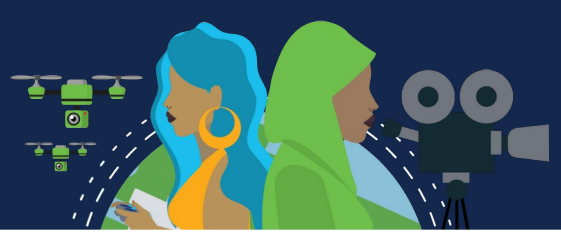
Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

WOMENROCK-IT
Brasil 2021

Networking Academy

Camada de Transporte



Transporte de Dados

Propósito da Camada de Transporte

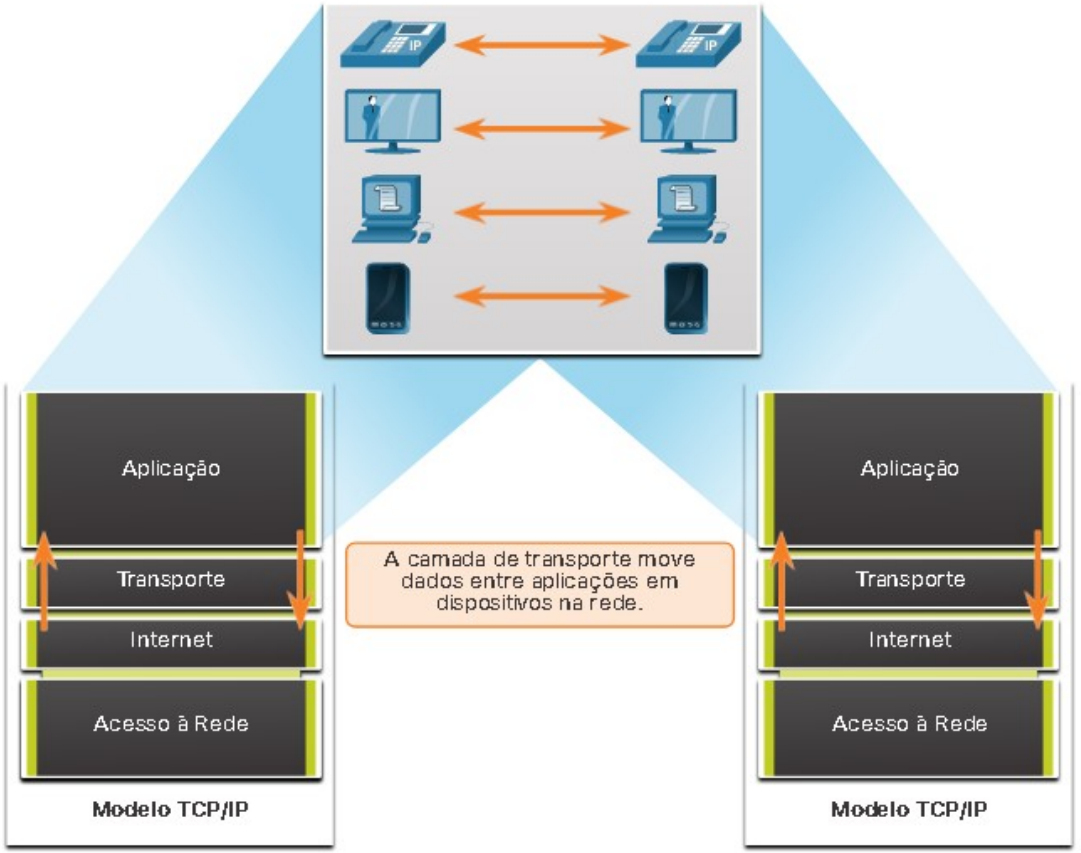
Os programas da camada de aplicação geram dados que devem ser trocados entre os hosts de origem e de destino. A camada de transporte é responsável pela comunicação lógica entre aplicativos executados em hosts diferentes. Isso pode incluir serviços como o estabelecimento de uma sessão temporária entre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

A camada de transporte é o link entre a camada de aplicação e as camadas inferiores que são responsáveis pela transmissão pela rede.

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

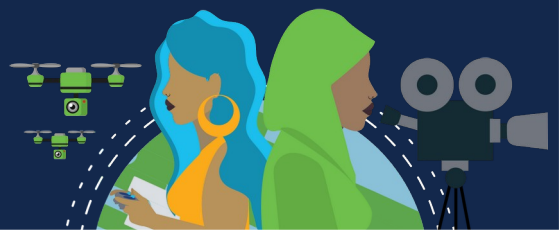
A camada de transporte inclui dois protocolos:

- **Protocolo TCP (Transmission Control Protocol)**
- **Protocolo UDP (User Datagram Protocol)**



Fonte: Cisco

Transporte de Dados



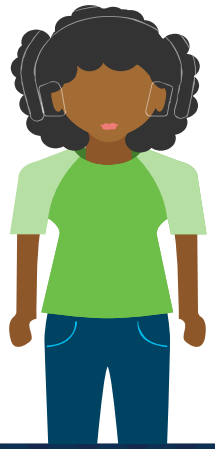
Responsabilidades da Camada de Transporte

- **Rastreamento de Conversações Individuais:** Cada conjunto de dados que flui entre um aplicativo de origem e um aplicativo de destino é conhecido como conversa e é rastreado separadamente. É responsabilidade da camada de transporte manter e monitorar essas várias conversações.

Um host pode ter vários aplicativos que estão se comunicando pela rede simultaneamente.

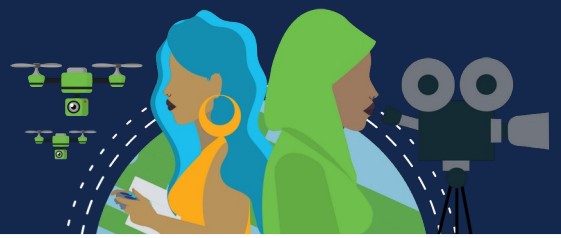
A maioria das redes tem uma limitação da quantidade de dados que pode ser incluída em um único pacote. Portanto, os dados devem ser divididos em partes gerenciáveis.

- **Segmentação de Dados e Remontagem de Segmentos:** É responsável por dividir os dados do aplicativo em blocos de tamanho adequado. Dependendo do protocolo de camada de transporte usado, os blocos de camada de transporte são chamados de segmentos ou datagramas.



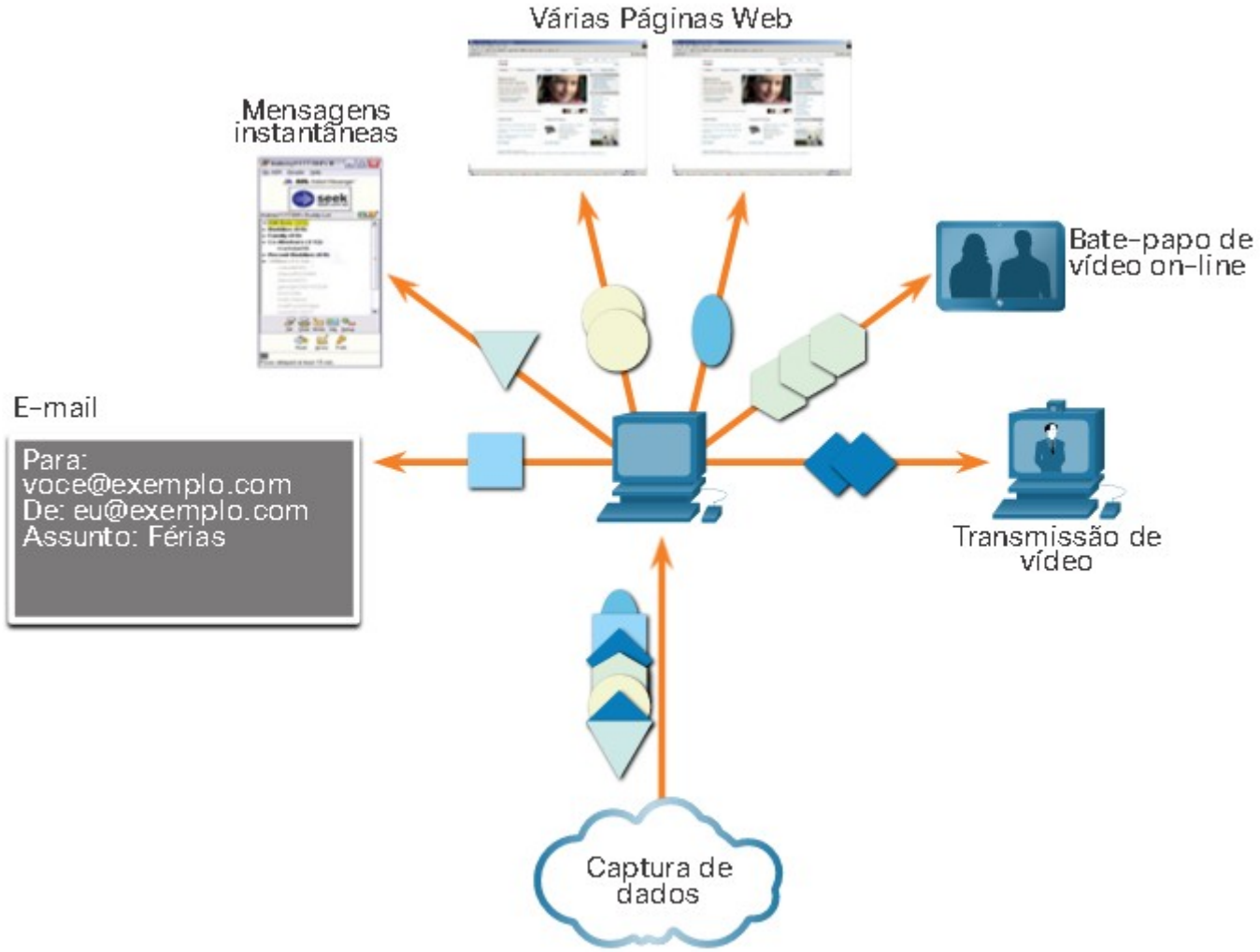
- **Adicionar Informações de Cabeçalho:** Adiciona informações de cabeçalho contendo dados binários organizados em vários campos a cada bloco de dados. Esses valores permitem que os vários protocolos da camada realizem diferentes funções no gerenciamento da comunicação de dados. As informações de cabeçalho são usadas pelo host de recebimento para remontar os blocos de dados em um fluxo de dados completo para o programa de camada de aplicativo de recebimento. A camada garante que, mesmo com vários aplicativos em execução em um dispositivo, todos os aplicativos recebam os dados corretos.

Fonte: Cisco



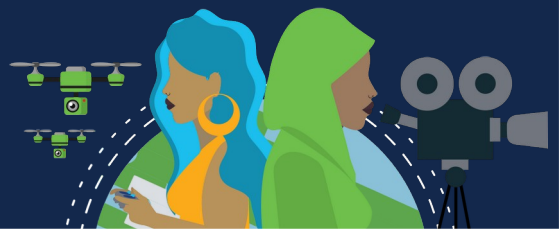
Transporte de Dados

Black Lives Matter



Fonte: Cisco

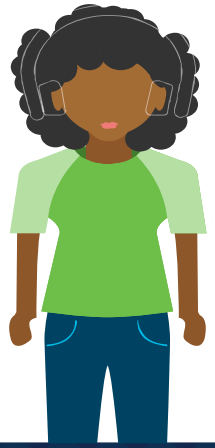
Transporte de Dados



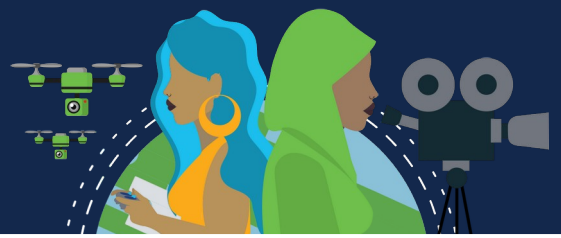
Responsabilidades da Camada de Transporte

- **Identificação das Aplicações:** Para passar fluxos de dados para os aplicativos adequados, a camada de transporte identifica o aplicativo de destino usando um identificador chamado número da porta. Cada processo de software que precisa acessar a rede recebe um número de porta exclusivo para esse host.

- **Multiplexação das Conversas:** O envio de alguns tipos de dados (por exemplo, um vídeo de streaming) através de uma rede, como um fluxo de comunicação completo, pode consumir toda a largura de banda disponível. Isso impediria que outras conversas de comunicação ocorressem ao mesmo tempo. Isso também dificultaria a recuperação de erro e retransmissão dos dados danificados. A camada de transporte usa segmentação e multiplexação para permitir que diferentes conversas de comunicação sejam intercaladas na mesma rede. A verificação de erros pode ser realizada nos dados do segmento, para determinar se o segmento foi alterado durante a transmissão.

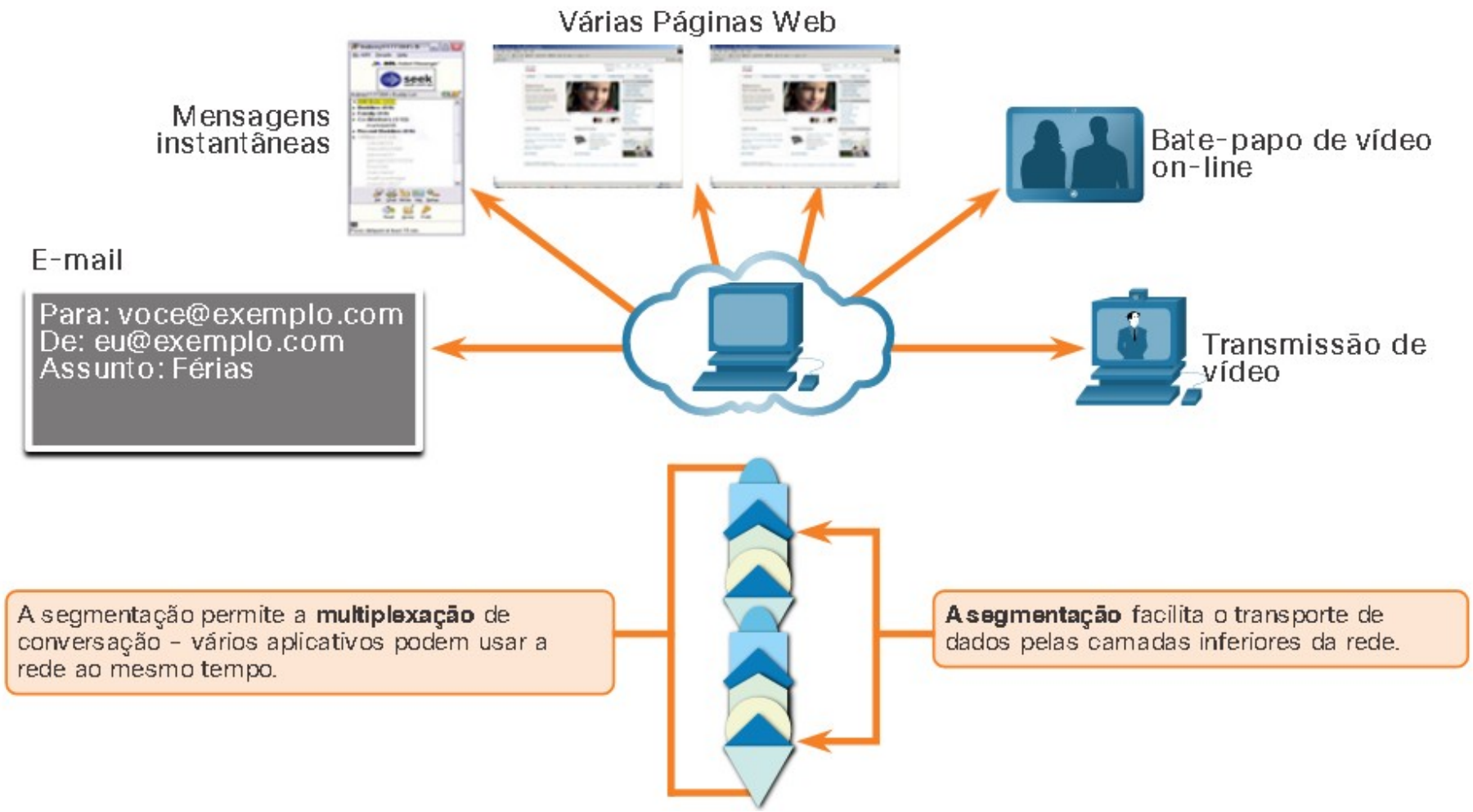


Fonte: Cisco

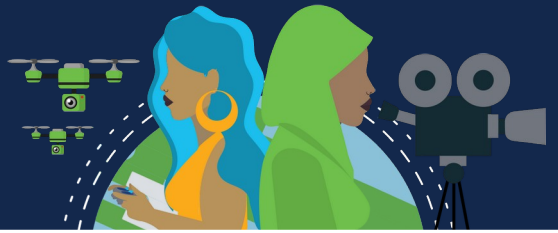


Transporte de Dados

Black Lives Matter



Fonte: Cisco



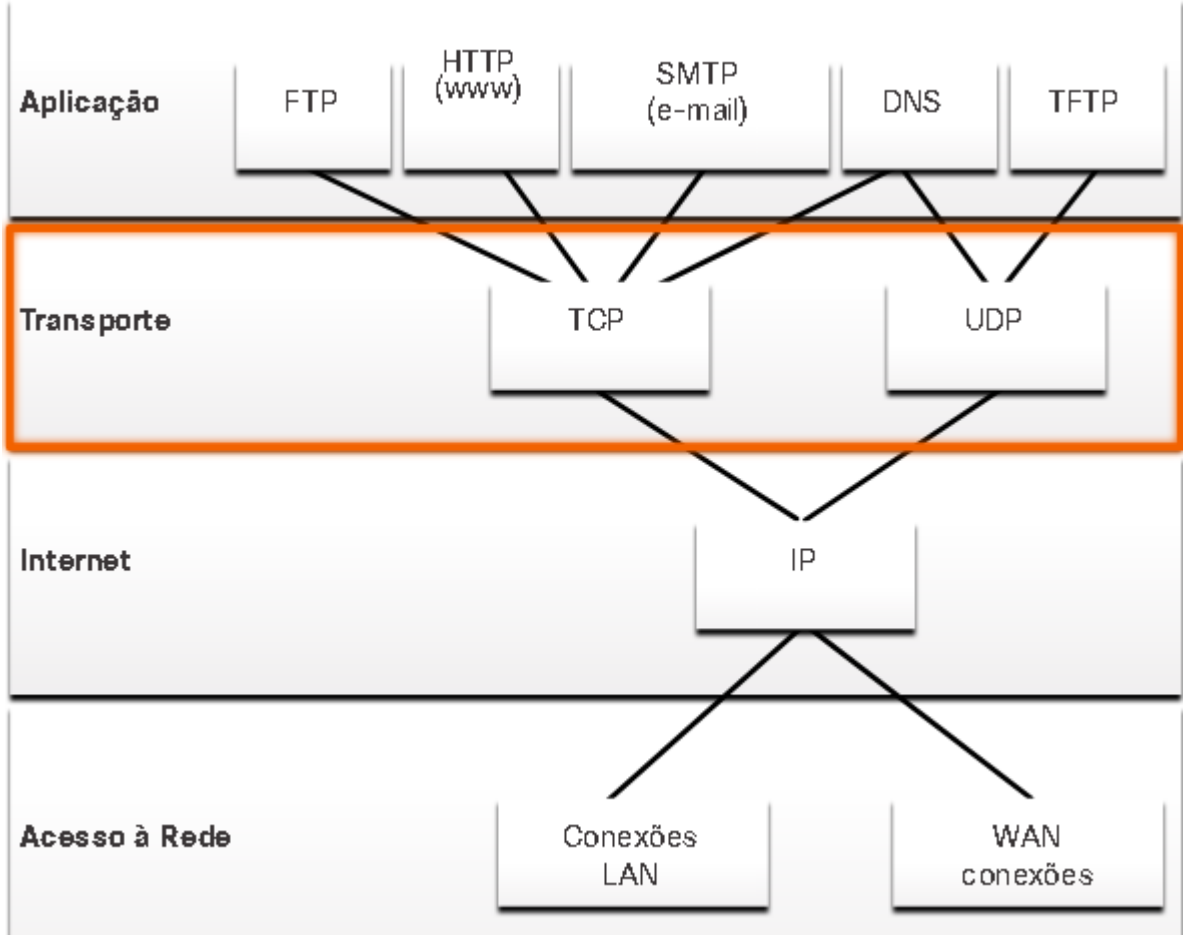
Transporte de Dados

Protocolos da Camada de Transporte

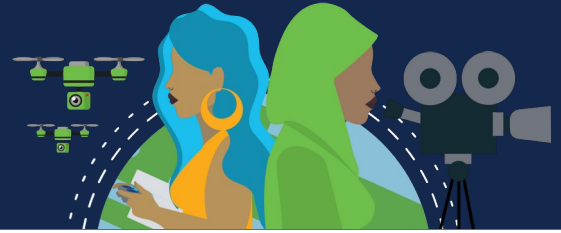
O IP está preocupado apenas com a estrutura, endereçamento e roteamento de pacotes. O IP não especifica como a entrega ou o transporte de pacotes ocorrem.

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

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



Fonte: Cisco



Transporte de Dados

Protocolo TCP (Transmission Control Protocol)

O TCP é considerado um protocolo de camada de transporte confiável, completo, que garante que todos os dados cheguem ao destino. Ele inclui campos que garantem a entrega dos dados do aplicativo, exigindo processamento adicional pelos hosts de envio e recebimento. O TCP divide os dados em segmentos.

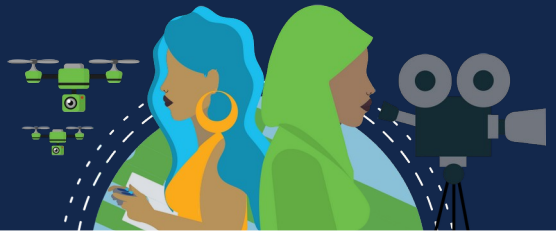
É análogo ao enviar pacotes que são rastreados da origem ao destino. Se um pedido pelo correio estiver dividido em vários pacotes, um cliente poderá verificar on-line a sequência de recebimento do pedido.

O TCP fornece confiabilidade e controle de fluxo operações básicas:

- Número e rastreamento de segmentos de dados transmitidos para um host a partir de um aplicativo específico;
- Confirmar dados recebidos;
- Retransmitir todos os dados não confirmados após um determinado período de tempo;
- Dados de sequência que podem chegar em ordem errada;
- Enviar dados a uma taxa eficiente que seja aceitável pelo receptor.

Para manter o estado de uma conversa e rastrear as informações, o TCP deve primeiro estabelecer uma conexão entre o remetente e o receptor. É por isso que o TCP é conhecido como um protocolo orientado a conexão.

Fonte: Cisco



Transporte de Dados

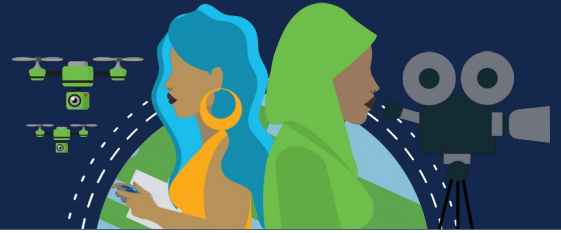
Protocolo UDP (User Datagram Protocol)

É um protocolo mais simples do que o TCP. Não fornece confiabilidade e controle de fluxo, o que significa que requer menos campos de cabeçalho. Não precisa gerenciar confiabilidade e controle de fluxo, isso significa que datagramas UDP podem ser processados mais rápido do que segmentos TCP.
O UDP fornece as funções básicas para fornecer datagramas entre os aplicativos apropriados, com muito pouca sobrecarga e verificação de dados.

O UDP divide os dados em datagramas que também são chamados de segmentos. É um protocolo sem conexão. Não requer uma conexão estabelecida. Não controla informações enviadas ou recebidas entre o cliente e o servidor, sendo também conhecido como um protocolo sem estado.

Protocolo de entrega de melhor esforço porque não há confirmação de que os dados são recebidos no destino. Não há processo de camada de transporte que informe ao remetente se a entrega foi bem-sucedida.

Fonte: Cisco



Transporte de Dados

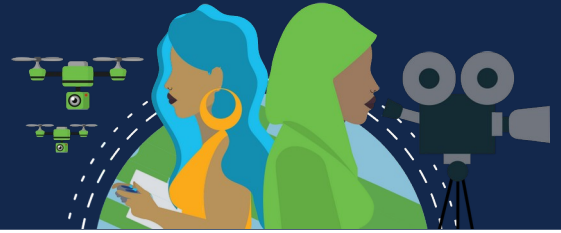
O protocolo de Camada de Transporte Certo para a Aplicação Certa

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

O UDP também é usado por aplicativos de solicitação e resposta onde os dados são mínimos, e a retransmissão pode ser feita rapidamente. O serviço de nome de domínio (DNS) usa UDP para esse tipo de transação. O cliente solicita endereços IPv4 e IPv6 para um nome de domínio conhecido de um servidor DNS. Se o cliente não receber uma resposta em um período predeterminado de tempo, ele simplesmente envia a solicitação novamente.

Se um ou dois segmentos de uma transmissão de vídeo ao vivo não conseguir chegar, isso criará apenas uma interrupção momentânea na transmissão, pode parecer como uma distorção na imagem ou no som e pode não ser notado pelo usuário. Se o dispositivo de destino considerasse os dados perdidos, a transmissão poderia atrasar, enquanto aguardasse as retransmissões, causando, portanto, grandes perdas de áudio e vídeo. Nesse caso, é melhor fornecer a melhor experiência de mídia com os segmentos recebidos e descartar a confiabilidade.

Fonte: Cisco



Transporte de Dados

O protocolo de Camada de Transporte Certo para a Aplicação Certa

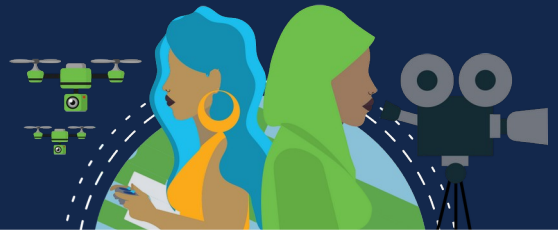
Para outras aplicações, é importante que todos os dados cheguem e que possam ser processados em sua sequência adequada. Para esses tipos de aplicativos, o TCP é usado como o protocolo de transporte. Aplicações como bancos de dados, navegadores e clientes de e-mail exigem que todos os dados enviados cheguem ao destino em seu estado original. Quaisquer dados ausentes podem corromper uma comunicação, tornando-a incompleta ou ilegível.

Os desenvolvedores de aplicações devem escolher que tipo de protocolo de transporte é apropriado com base nas necessidades de suas aplicações. O vídeo pode ser enviado através de TCP ou UDP. Os aplicativos que transmitem áudio e vídeo armazenados normalmente usam TCP. O aplicativo usa TCP para executar buffer, sondagem de largura de banda e controle de congestionamento, a fim de controlar melhor a experiência do usuário.

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

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

Fonte: Cisco



Transporte de Dados

UDP

VoIP
(telefonia IP)

DNS
(resolução de nomes de domínio)

Propriedades necessárias para escolha do protocolo:

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

TCP

SMTP/IMAP
(E-mail)

HTTP/HTTPS
(World Wide Web

Propriedades necessárias para escolha do protocolo:

- Confiável
- Confirma a chegada dos dados
- Reenvia dados perdidos
- Entrega os dados em sequência

Fonte: Cisco

Visão geral do TCP

Recursos TCP

Além de suportar as funções básicas de segmentação e remontagem de dados, o TCP também fornece os seguintes serviços:

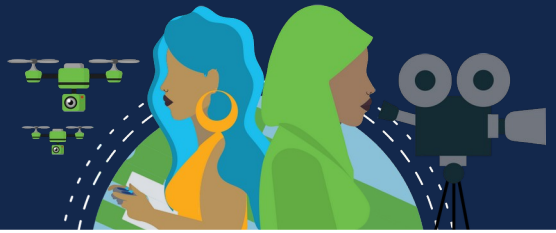
Estabelece uma sessão: O TCP é um protocolo orientado à conexão que negocia e estabelece uma conexão (ou sessão) permanente entre os dispositivos de origem e de destino antes de encaminhar qualquer tráfego. Com o estabelecimento da sessão, os dispositivos negociam o volume de tráfego esperado que pode ser encaminhado em determinado momento e os dados de comunicação entre os dois podem ser gerenciados atentamente.

Garante a entrega confiável: Por várias razões, é possível que um segmento seja corrompido ou perdido. O TCP garante que cada segmento enviado pela fonte chegue ao destino.

Fornece entrega no mesmo pedido: Como as redes podem fornecer várias rotas que podem ter taxas de transmissão diferentes, os dados podem chegar na ordem errada. Ao numerar e sequenciar os segmentos, o TCP garante que os segmentos sejam remontados na ordem correta.

Suporta controle de fluxo: Quando os recursos de rede em um host estão sobrecarregados, o TCP requisita que a aplicação emissora reduza a taxa de fluxo de dados. Para isso, o TCP regula o volume de dados transmitido pelo dispositivo origem. O controle de fluxo pode impedir a necessidade de retransmissão dos dados quando os recursos do host receptor estão sobrecarregados.

Fonte: Cisco

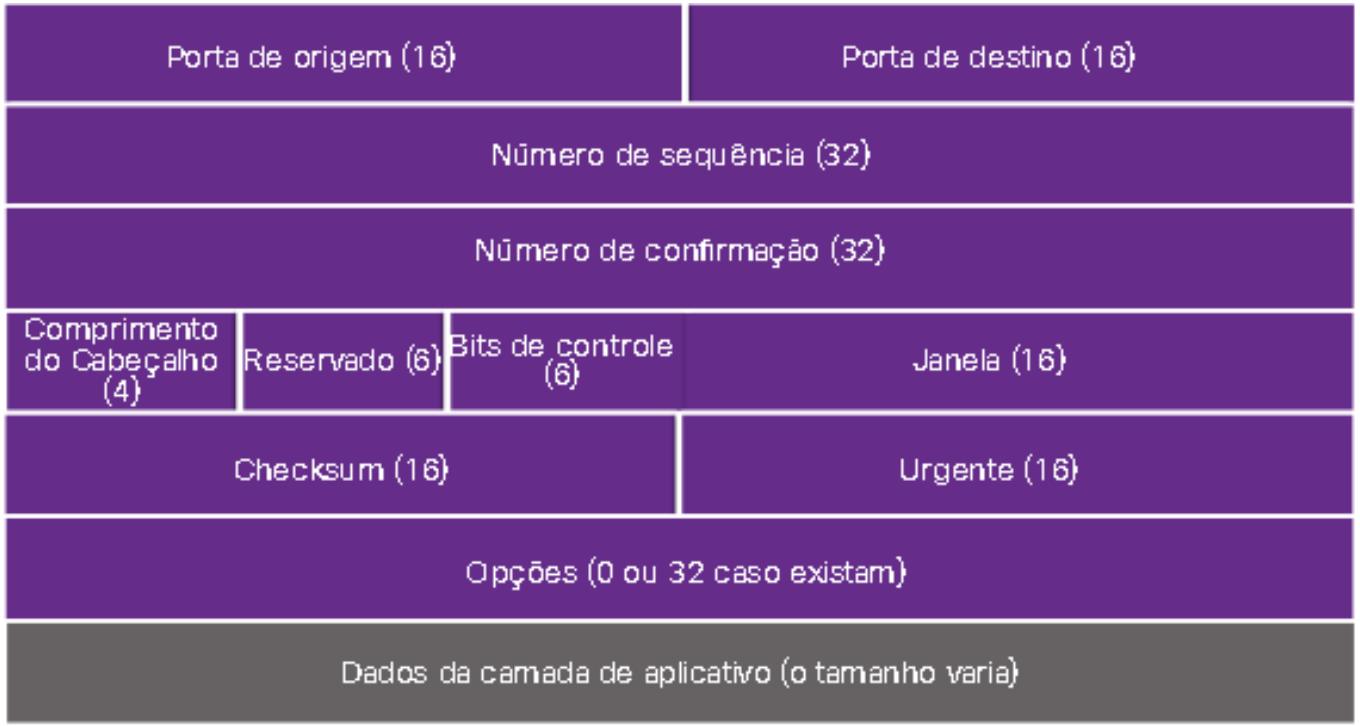


Visão geral do TCP

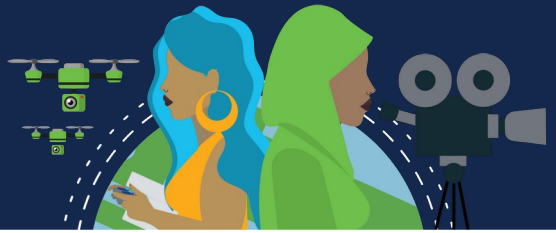
Cabeçalho TCP

TCP é um protocolo stateful, o que significa que ele controla o estado da sessão de comunicação. Para manter o controle do estado de uma sessão, o TCP registra quais informações ele enviou e quais informações foram confirmadas. A sessão com estado começa com o estabelecimento da sessão e termina com o encerramento da sessão.

Um segmento TCP adiciona 20 bytes (ou seja, 160 bits) de sobrecarga ao encapsular os dados da camada de aplicativo.



Fonte: Cisco

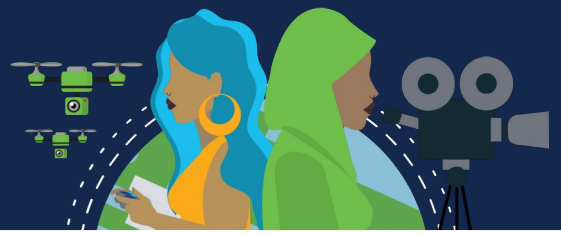


Visão geral do TCP

Campos de cabeçalho TCP

Campo de cabeçalho TCP	Descrição
Porta de origem	Um campo de 16 bits usado para identificar o aplicativo de origem por número de porta.
Porta de destino	Um campo de 16 bits usado para identificar o aplicativo de destino por porta número.
Número sequencial	Um campo de 32 bits usado para fins de remontagem de dados.
Número de Confirmação	Um campo de 32 bits usado para indicar que os dados foram recebidos e o próximo byte esperado da fonte.
Comprimento do cabeçalho	Um campo de 4 bits conhecido como 'offset' de datas' que indica o comprimento do cabeçalho do segmento TCP.
Reservado	Um campo de 6 bits que é reservado para uso futuro.
Bits de controle	Um campo de 6 bits que inclui códigos de bits, ou sinalizadores, que indicam a finalidade e função do segmento TCP.
Tamanho da Janela	Um campo de 16 bits usado para indicar o número de bytes que podem ser aceitos de uma só vez.
Checksum	Um campo de 16 bits usado para verificação de erros do cabeçalho e dos dados do segmento.
Urgente	Um campo de 16 bits usado para indicar se os dados contidos são urgentes.

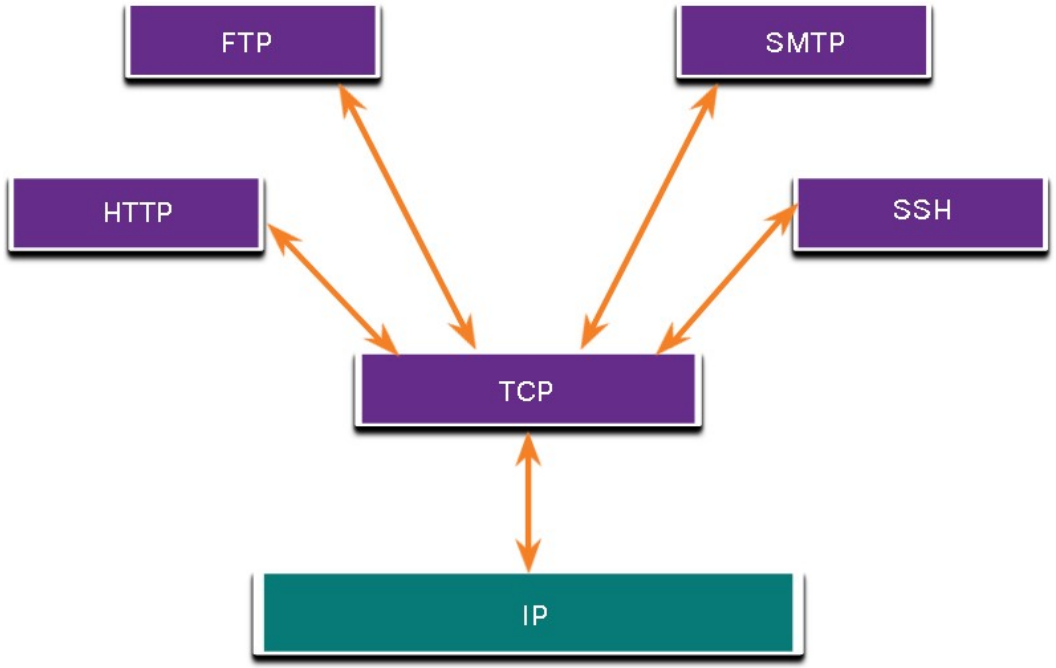
Fonte: Cisco



Visão geral do TCP

Aplicações que usam TCP

O TCP é um bom exemplo de como as diferentes camadas do conjunto de protocolos TCP / IP têm funções específicas. O TCP lida com todas as tarefas associadas à divisão do fluxo de dados em segmentos, fornecendo confiabilidade, controlando o fluxo de dados e reordenando segmentos. O TCP libera a aplicação da obrigação de gerenciar todas essas tarefas. As aplicações podem simplesmente enviar o fluxo de dados à camada de transporte e usar os serviços TCP.



Fonte: Cisco

Visão geral do UDP

Recursos UDP

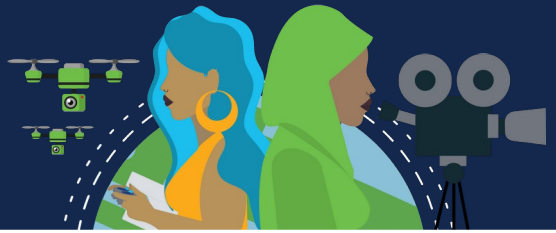
UDP é um protocolo de transporte de melhor esforço. O UDP é um protocolo de transporte leve que oferece a mesma segmentação de dados e remontagem que o TCP, mas sem a confiabilidade e o controle de fluxo do TCP.

É um protocolo simples, normalmente descrito nos termos do que ele não faz em comparação ao TCP.

Os recursos UDP incluem o seguinte:

- Os dados são reagrupados na ordem em que são recebidos.
- Quaisquer segmentos perdidos não são reenviados.
- Não há estabelecimento de sessão.
- O envio não é informado sobre a disponibilidade do recurso.

Fonte: Cisco



Visão geral do UDP

Cabeçalho UDP

UDP é um protocolo sem estado, o que significa que nem o cliente nem o servidor rastreiam o estado da sessão de comunicação. Se a confiabilidade for necessária ao usar o UDP como protocolo de transporte, ela deve ser tratada pela aplicação.

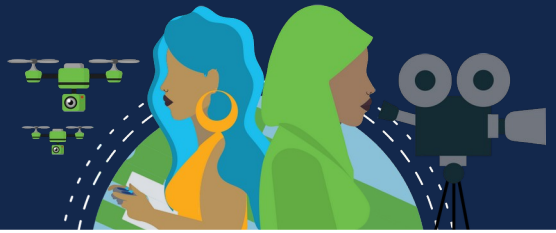
Um dos requisitos mais importantes para transmitir vídeo ao vivo e voz sobre a rede é que os dados continuem fluindo rapidamente. Vídeo ao vivo e aplicações de voz podem tolerar alguma perda de dados com efeito mínimo ou sem visibilidade e são perfeitos para o UDP.

Os blocos de comunicação no UDP são chamados de datagramas ou segmentos. Esses datagramas são enviados como o melhor esforço pelo protocolo da camada de transporte.

O cabeçalho UDP é muito mais simples do que o cabeçalho TCP porque só tem quatro campos e requer 8 bytes (ou seja, 64 bits).

Porta de origem (16)	Porta de Destino (16)
Comprimento (16)	Checksum (16)
Dados da Camada de Aplicação (o tamanho é variado)	

Fonte: Cisco

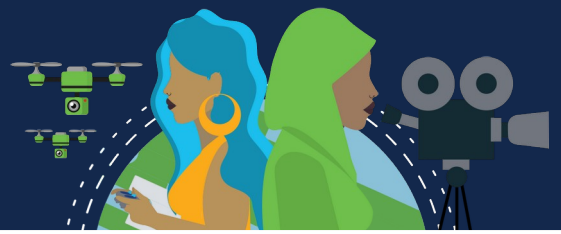


Visão geral do UDP

Campos de cabeçalho UDP

Campo de Cabeçalho UDP	Descrição
Porta de origem	Um campo de 16 bits usado para identificar o aplicativo de origem por número de porta.
Porta de destino	Um campo de 16 bits usado para identificar o aplicativo de destino por porta número.
Tamanho	Um campo de 16 bits que indica o comprimento do cabeçalho do datagrama UDP.
Checksum	Um campo de 16 bits usado para verificação de erros do cabeçalho e dos dados do datagrama.

Fonte: Cisco

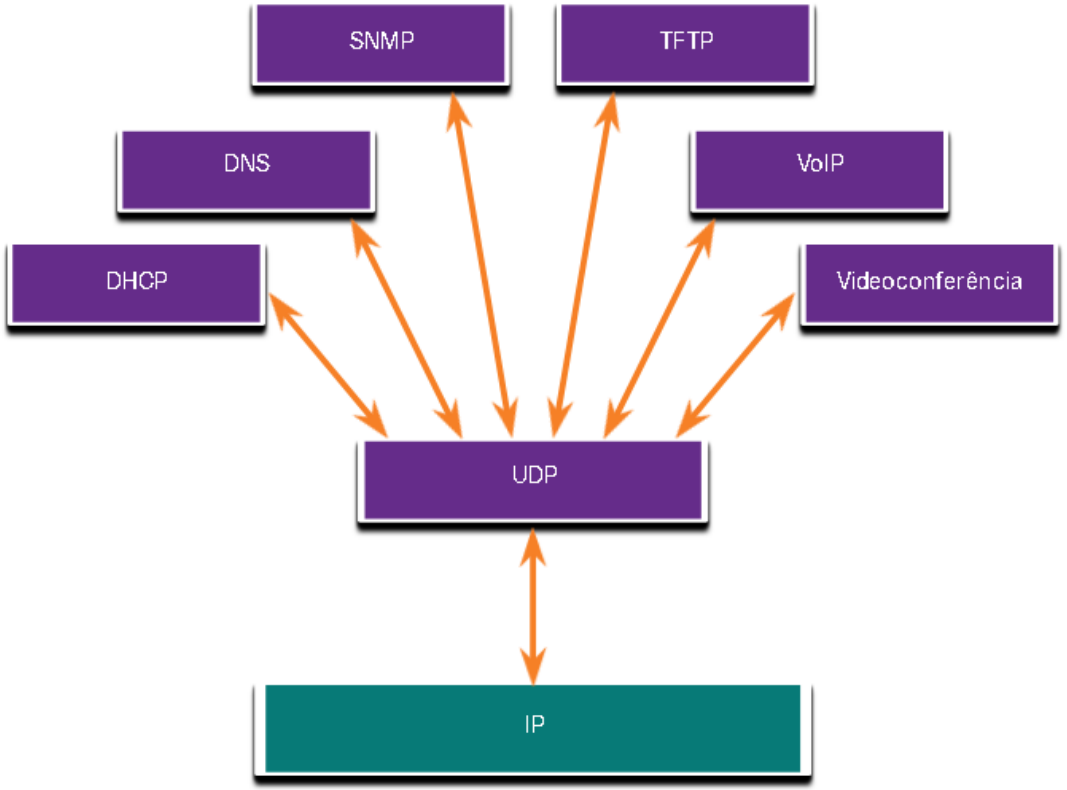


Visão geral do UDP

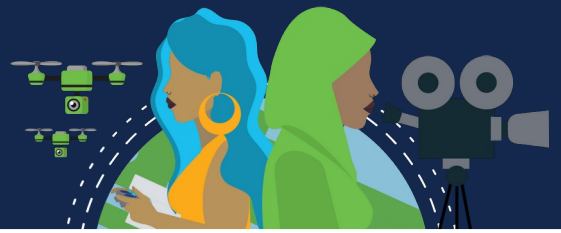
Aplicações que usam UDP

Há três tipos de aplicações que são mais adequadas para o UDP:

- **Aplicativos de vídeo e multimídia ao vivo:** Esses aplicativos podem tolerar a perda de dados, mas requerem pouco ou nenhum atraso. Os exemplos incluem VoIP e transmissão de vídeo ao vivo.
- **Solicitações simples e aplicativos de resposta:** aplicativos com transações simples em que um host envia uma solicitação e pode ou não receber uma resposta. Os exemplos incluem DNS e DHCP.
- **Aplicativos que lidam com a confiabilidade:** Comunicações unidirecionais em que o controle de fluxo, a detecção de erros, as confirmações e a recuperação de erros não são necessários ou podem ser gerenciados pelo aplicativo. Os exemplos incluem SNMP e TFTP.



Fonte: Cisco



Números de porta

Várias comunicações separadas

Independentemente do tipo de dados que estão sendo transportados, tanto o TCP quanto o UDP usam números de porta para gerenciar várias conversas simultâneas. Os campos de cabeçalho TCP e UDP identificam um número de porta do aplicativo de origem e destino.

O número da porta de origem está associado ao aplicativo de origem no host local, enquanto o número da porta de destino está associado ao aplicativo de destino no host remoto.

Por exemplo, suponha que um host está iniciando uma solicitação de página da Web a partir de um servidor Web. Quando o host inicia a solicitação de página da Web, o número da porta de origem é gerado dinamicamente pelo host para identificar exclusivamente a conversa. Cada solicitação gerada por um host usará um número de porta de origem criado dinamicamente diferente. Este processo permite que várias conversações ocorram simultaneamente.

Na solicitação, o número da porta de destino é o que identifica o tipo de serviço que está sendo solicitado do servidor Web de destino. Por exemplo, quando um cliente especifica a porta 80 na porta de destino, o servidor que receber a mensagem sabe que os serviços Web são solicitados.

Um servidor pode oferecer mais de um serviço simultaneamente, como serviços web na porta 80, enquanto oferece o estabelecimento de conexão FTP (File Transfer Protocol) na porta 21.

Números de porta

Pares de Sockets

As portas origem e destino são colocadas no segmento. Os segmentos são encapsulados em um pacote IP. O pacote IP contém o endereço IP de origem e destino. A combinação do endereço IP de origem e o número de porta de origem, ou do endereço IP de destino e o número de porta de destino é conhecida como um socket.

O socket é usado para identificar o servidor e o serviço que está sendo solicitado pelo cliente. Um socket do cliente pode ser assim, com 1099 representando o número da porta de origem: 192.168.1.5:1099

O socket em um servidor da web pode ser 192.168.1.7:80

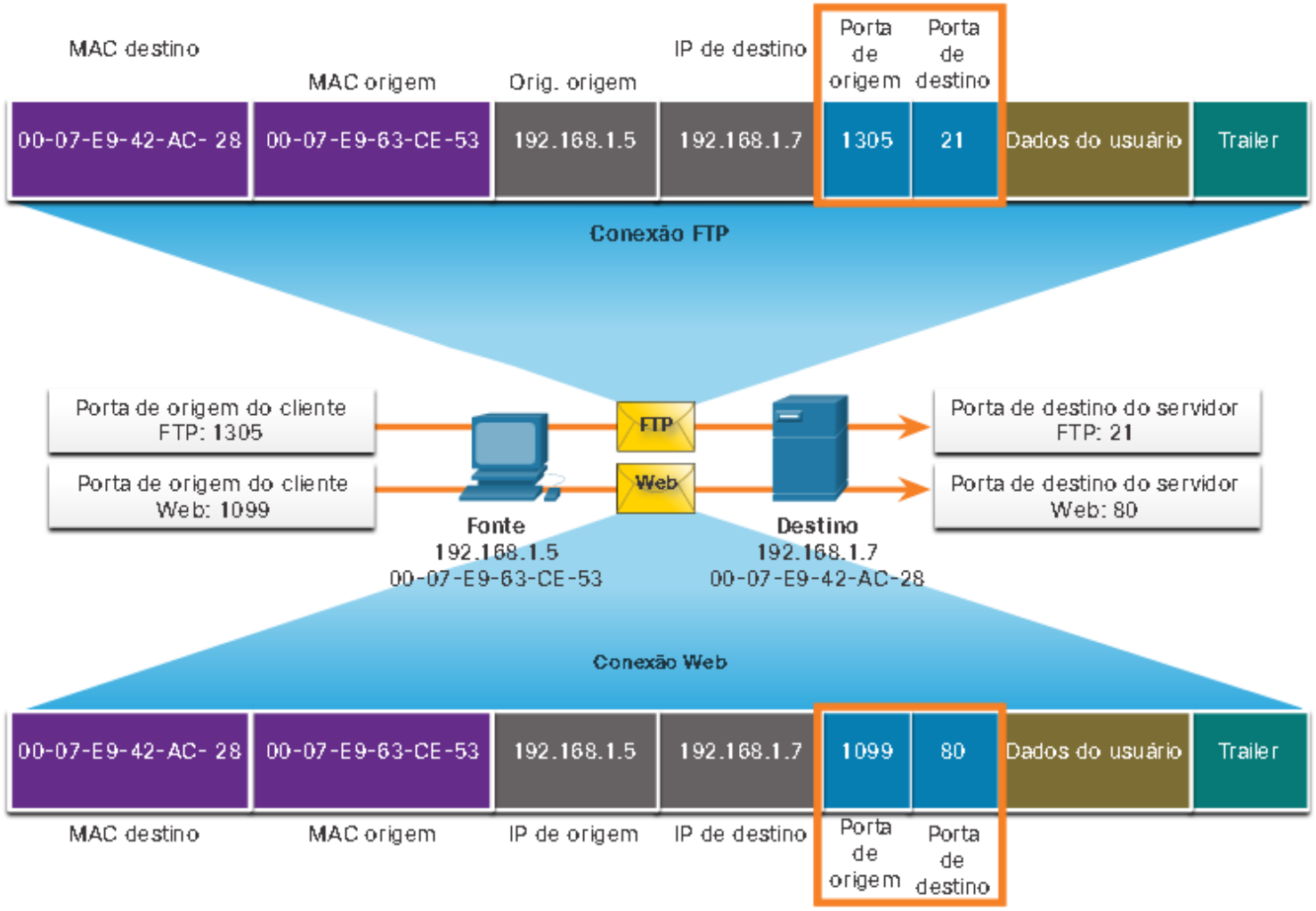
Juntos, esses dois sockets se combinam para formar um par de sockets: 192.168.1.5:1099, 192.168.1.7:80

Os sockets permitem que vários processos em execução em um cliente se diferenciem uns dos outros, e várias conexões com um processo no servidor sejam diferentes umas das outras.

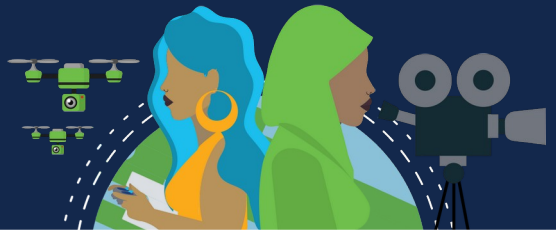
Este número de porta age como um endereço de retorno para a aplicação que faz a solicitação. A camada de transporte rastreia essa porta e a aplicação que iniciou a solicitação, de modo que quando uma resposta é retornada, ela pode ser encaminhada para a aplicação correta.

Fonte: Cisco

Números de porta



Fonte: Cisco



Números de porta

Grupos de Números de Porta

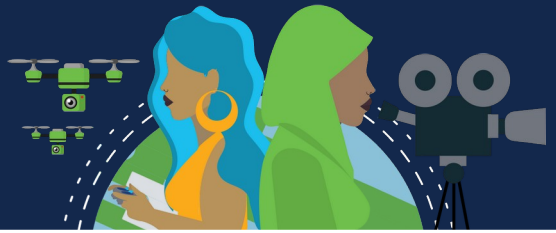
A Internet Assigned Numbers Authority (IANA) é a organização de padrões responsável por atribuir vários padrões de endereçamento, incluindo os números de porta de 16 bits. Os 16 bits usados para identificar os números de porta de origem e destino fornecem um intervalo de portas de 0 a 65535.

A IANA dividiu a gama de números nos três grupos seguintes.

Observação: Alguns sistemas operacionais clientes podem usar números de porta registrados em vez de números de porta dinâmicos para atribuir portas de origem.

Grupo de Portas	Intervalo de números	Descrição
Portas Comuns	**0 a 1.023**	• Estes números de porta são reservados para serviços comuns ou populares e aplicativos como navegadores da web, clientes de e-mail e acesso remoto clientes. • Portas bem conhecidas definidas para aplicativos comuns de servidor permite para identificar facilmente o serviço associado necessário.
Portas registradas	**1.024 a 49.151**	• Esses números de porta são atribuídos pela IANA a uma entidade solicitante para usar com processos ou aplicativos específicos. • Esses processos são principalmente aplicativos individuais que um usuário optou por instalar, em vez de aplicativos comuns que receber um número de porta bem conhecido. • Por exemplo, a Cisco registrou a porta 1812 para seu servidor RADIUS processo de autenticação.
Particular e/ou **portas dinâmicas**	**49.152 a 65.535**	• Essas portas também são conhecidas como portas *efêmeras*. • O sistema operacional do cliente geralmente atribui números de porta dinamicamente quando uma conexão a um serviço é iniciada. • A porta dinâmica é então usada para identificar o aplicativo cliente durante a comunicação.

Fonte: Cisco



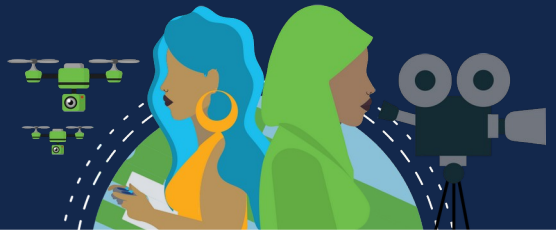
Números de porta

Algumas aplicações podem usar tanto TCP quanto UDP. Por exemplo, o DNS usa o protocolo UDP quando os clientes enviam requisições a um servidor DNS. Contudo, a comunicação entre dois servidores DNS sempre usa TCP.

Número de Portas Comuns

Número da Porta	Protocolo	Aplicação
20	TCP	Protocolo de transferência de arquivos (FTP) – Dados
21	TCP	Protocolo de transferência de arquivos (FTP) – Controle
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Protocolo SMTP
53	UDP, TCP	Protocolo DNS
67	UDP	Protocolo de Configuração Dinâmica de Host (DHCP) – Servidor
68	UDP	Protocolo de configuração dinâmica de host – cliente
69	UDP	Protocolo de Transferência Trivial de Arquivo (TFTP)
80	TCP	Protocolo HTTP
110	TCP	Protocolo POP3 (Post Office Protocol – Protocolo de E-mail)
143	TCP	Protocolo IMAP
161	UDP	Protocolo de Gerenciamento Simples de Rede (SNMP)
443	TCP	HTTPS (Secure Hypertext Transfer Protocol – Protocolo de Transferência de Hipertexto Seguro)

Fonte: Cisco



Números de porta

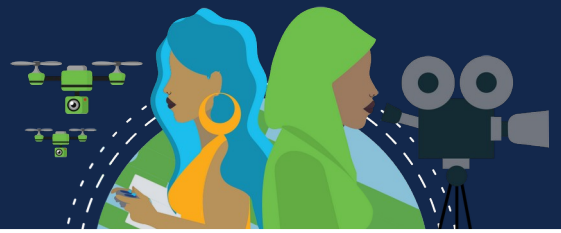
O Comando netstat

Conexões TCP desconhecidas podem ser uma ameaça de segurança maior. Elas podem indicar que algo ou alguém está conectado ao host local. Às vezes é necessário conhecer quais conexões TCP ativas estão abertas e sendo executadas em um host de rede. O **netstat** é um utilitário de rede importante que pode ser usado para verificar essas conexões. Como mostrado abaixo, digite o comando netstat para listar os protocolos em uso, o endereço local e os números de porta, o endereço externo e os números de porta e o estado da conexão.

Por padrão, o comando netstat tentará resolver endereços IP para nomes de domínio e números de porta para aplicativos conhecidos. A opção **-n** exibe endereços IP e números de porta em sua forma numérica.

```
C:\> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.124:3126     192.168.0.2:netbios-ssn    ESTABLISHED
  TCP    192.168.1.124:3158     207.138.126.152:http       ESTABLISHED
  TCP    192.168.1.124:3159     207.138.126.169:http       ESTABLISHED
  TCP    192.168.1.124:3160     207.138.126.169:http       ESTABLISHED
  TCP    192.168.1.124:3161     sc.msn.com:http            ESTABLISHED
  TCP    192.168.1.124:3166     www.cisco.com:http         ESTABLISHED
(output omitted)
```

Fonte: Cisco



Processo de Comunicação TCP

Processos em Servidores TCP

Cada processo de aplicativo em execução em um servidor está configurado para usar um número de porta. O número da porta é atribuído automaticamente ou configurado manualmente.

Um servidor não pode ter dois serviços atribuídos ao mesmo número de porta dentro dos mesmos serviços de camada de transporte.

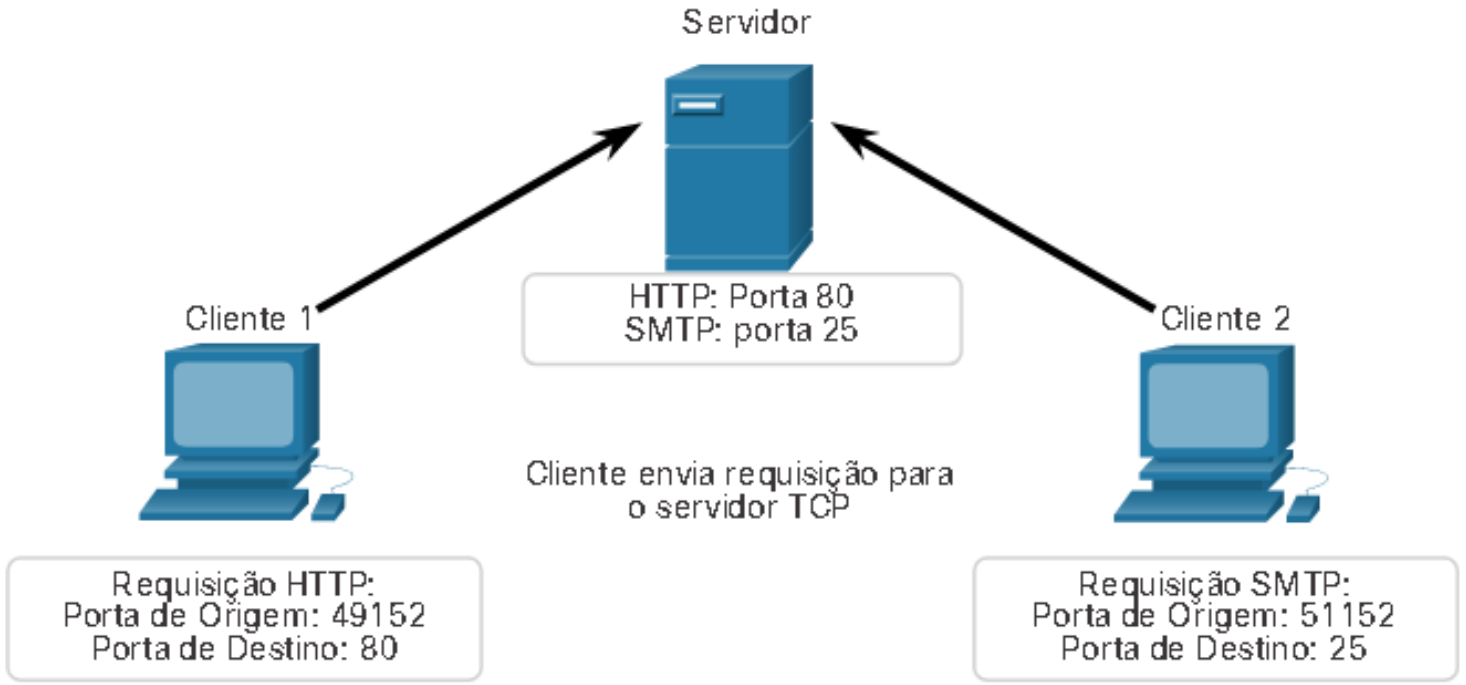
Um aplicativo de servidor ativo atribuído a uma porta específica é considerado aberto, o que significa que a camada de transporte aceita e processa os segmentos endereçados a essa porta. Qualquer solicitação de cliente que chega endereçada ao soquete correto é aceita e os dados são transmitidos à aplicação do servidor. Pode haver muitas portas abertas ao mesmo tempo em um servidor, uma para cada aplicação de servidor ativa.

Processo de Comunicação TCP

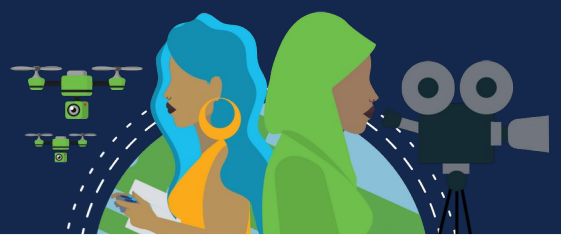
Processos em Servidores TCP

Clientes Enviando Requisições TCP

O Cliente 1 solicita serviços Web e o Cliente 2 está a solicita serviço de correio electrónico do mesmo servidor.



Fonte: Cisco

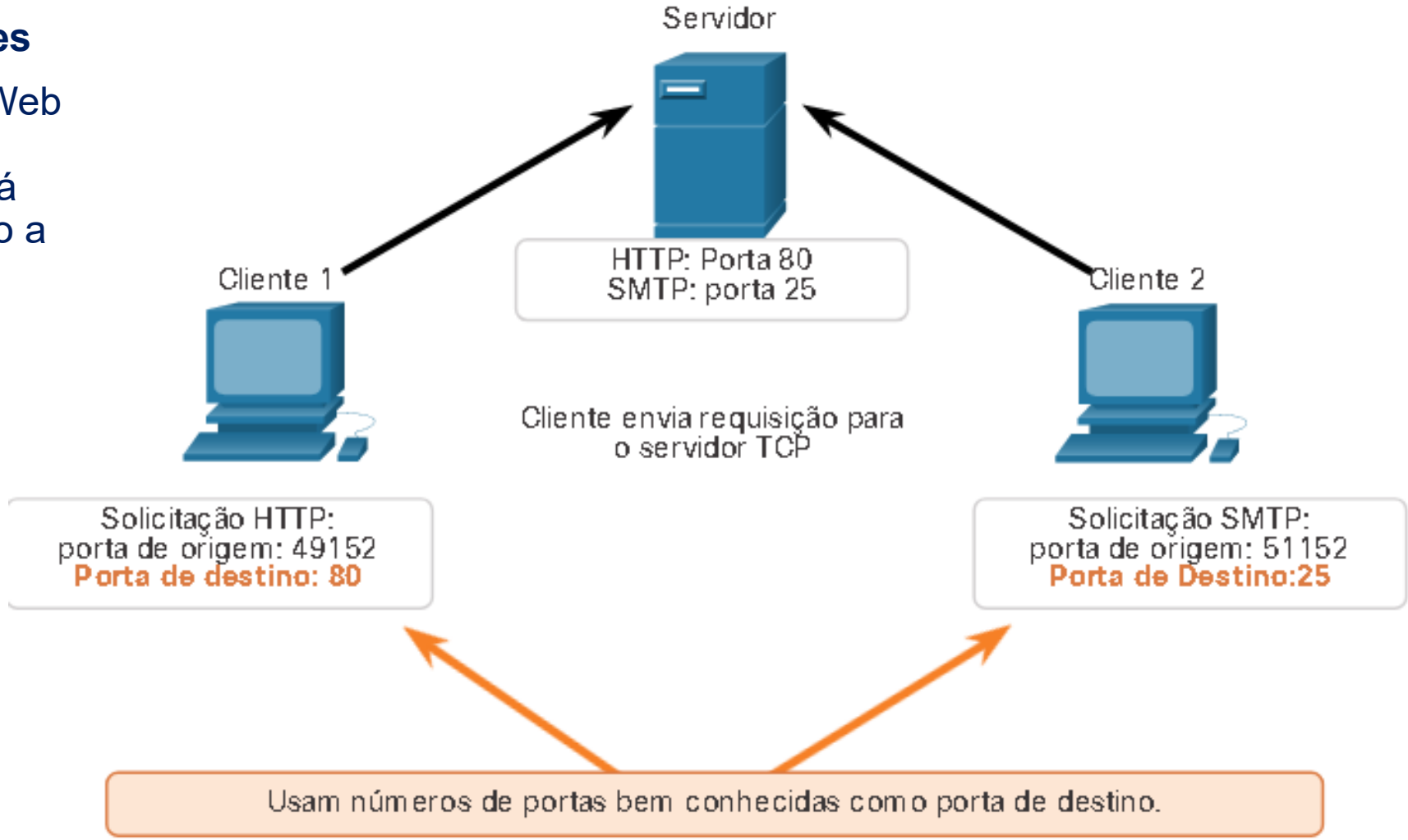


Processo de Comunicação TCP

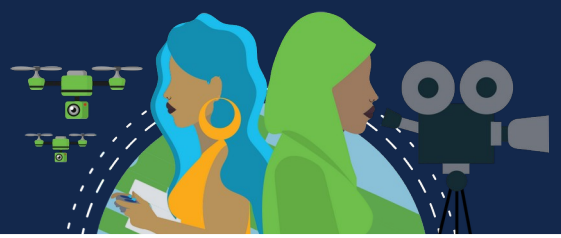
Processos em Servidores TCP

Portas de Destino das Requisições

O cliente 1 está solicitando serviços Web usando a porta 80 de destino bem conhecida (HTTP) e o cliente 2 está solicitando o serviço de email usando a porta 25 (SMTP) bem conhecida..



Fonte: Cisco

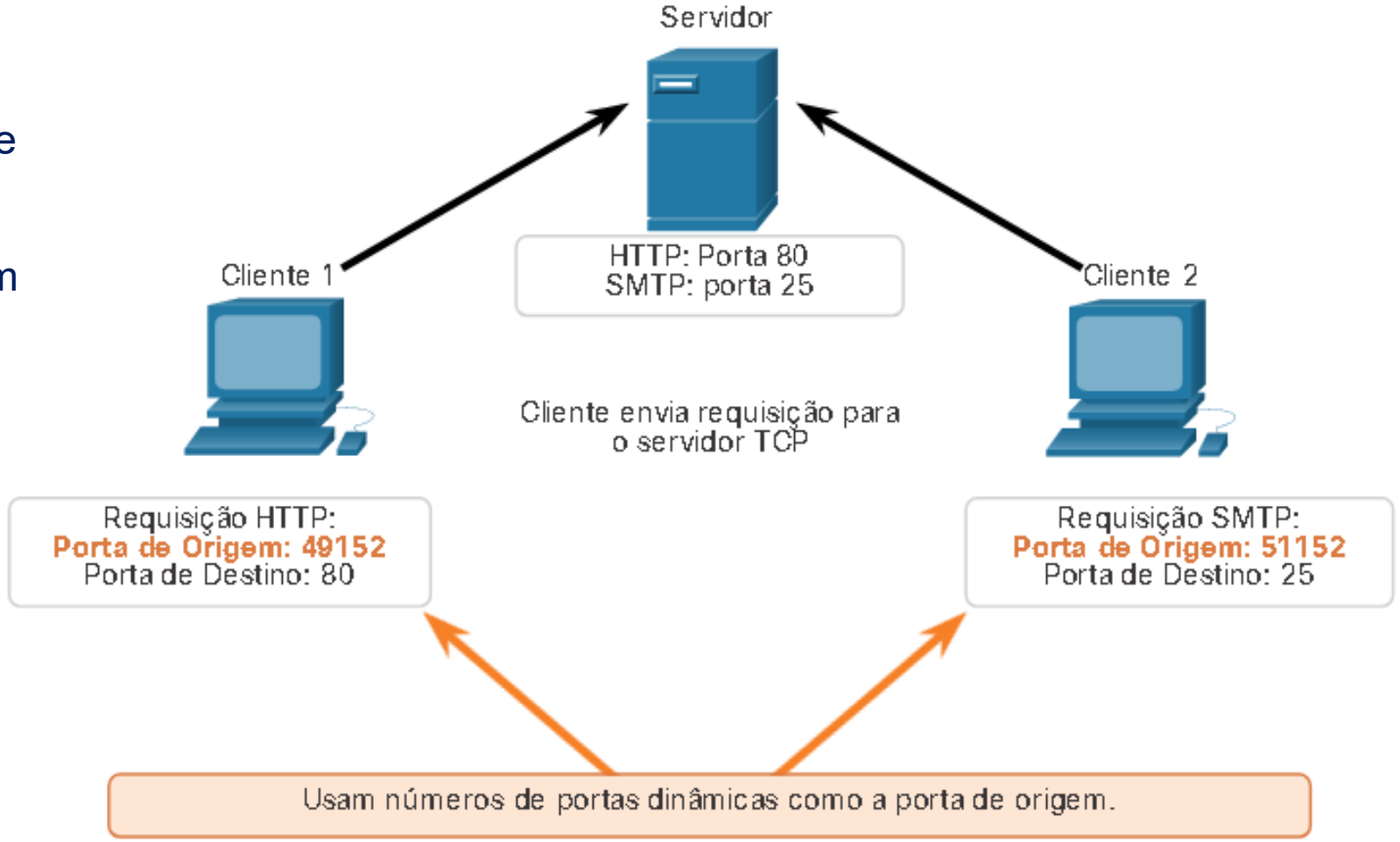


Processo de Comunicação TCP

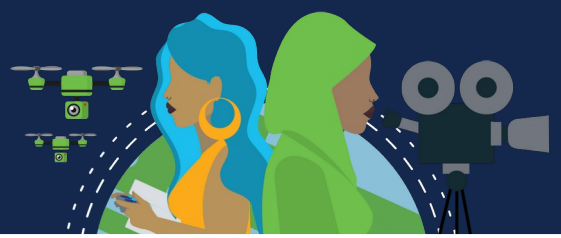
Processos em Servidores TCP

Portas de Origem das Requisições

As solicitações do cliente geram dinamicamente um número de porta de origem. Nesse caso, o cliente 1 está usando a porta de origem 49152 e o cliente 2 está usando a porta de origem 51152.



Fonte: Cisco

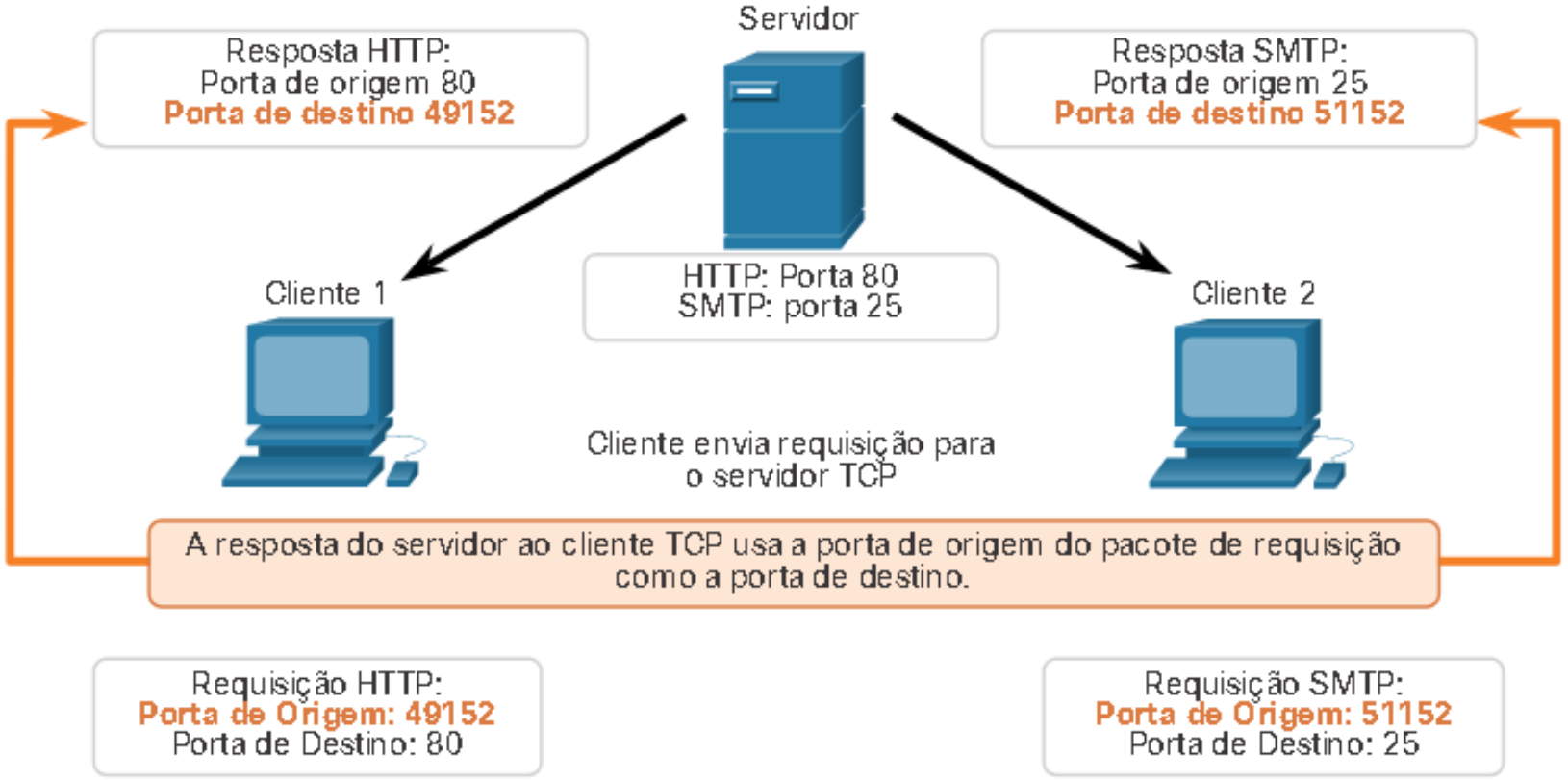


Processo de Comunicação TCP

Processos em Servidores TCP

Portas de Destino das Respostas

Quando o servidor responde às solicitações do cliente, ele reverte as portas de destino e de origem da solicitação inicial. Observe que a resposta do servidor à solicitação da Web agora tem a porta de destino 49152 e a resposta de e-mail agora tem a porta de destino 51152.



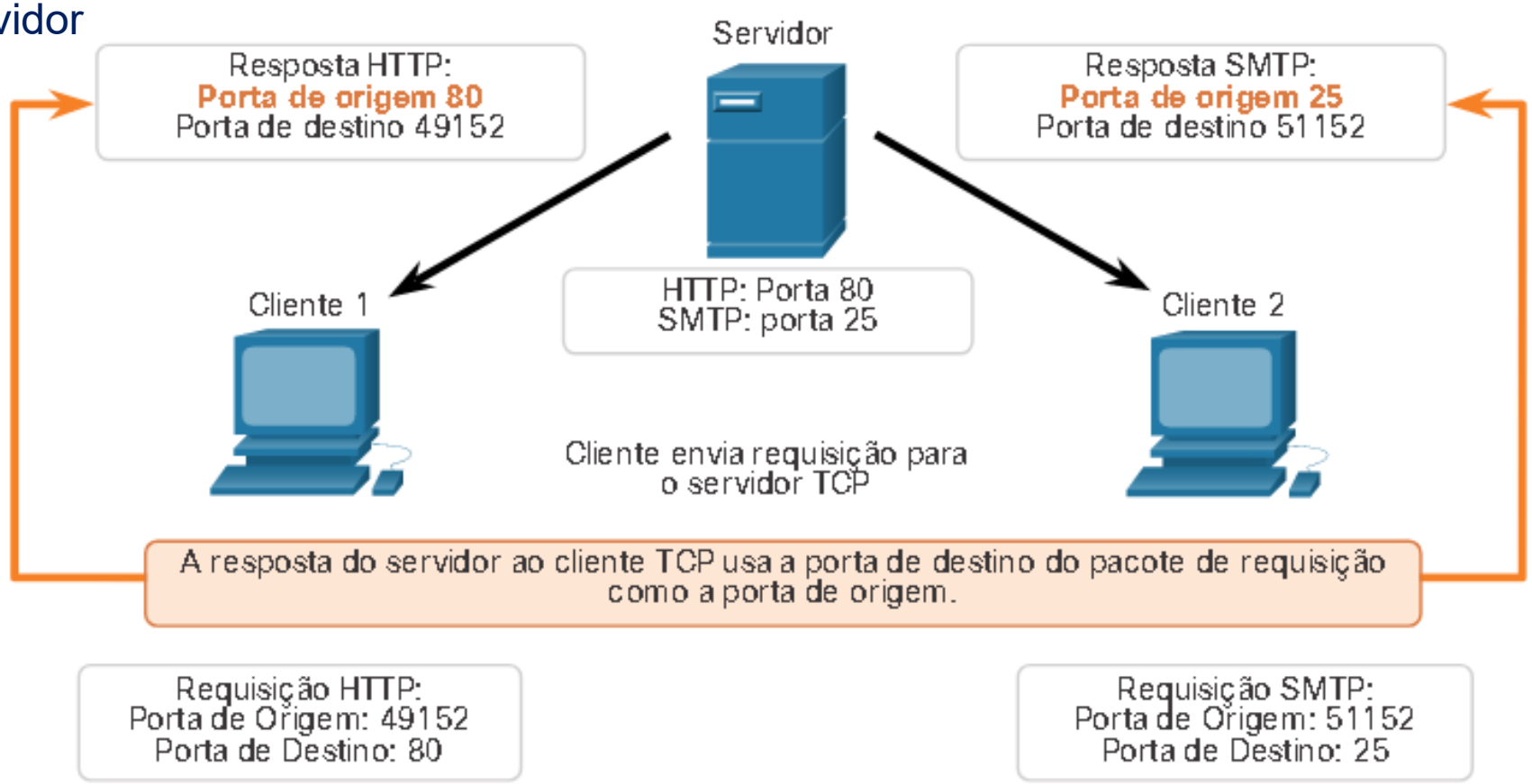
Fonte: Cisco

Processo de Comunicação TCP

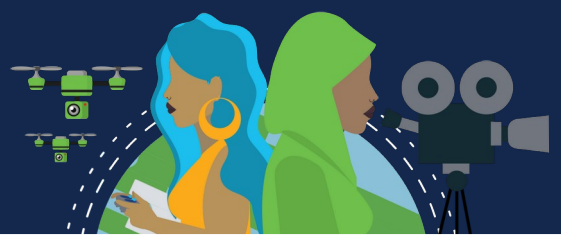
Processos em Servidores TCP

Portas de Origem das Respostas

A porta de origem na resposta do servidor é a porta de destino original nas solicitações iniciais.



Fonte: Cisco



Processo de Comunicação TCP

Estabelecimento de Conexão TCP

Nas conexões TCP, o cliente host estabelece a conexão com o servidor usando o processo de handshake de três vias.

Etapa 1. SYN

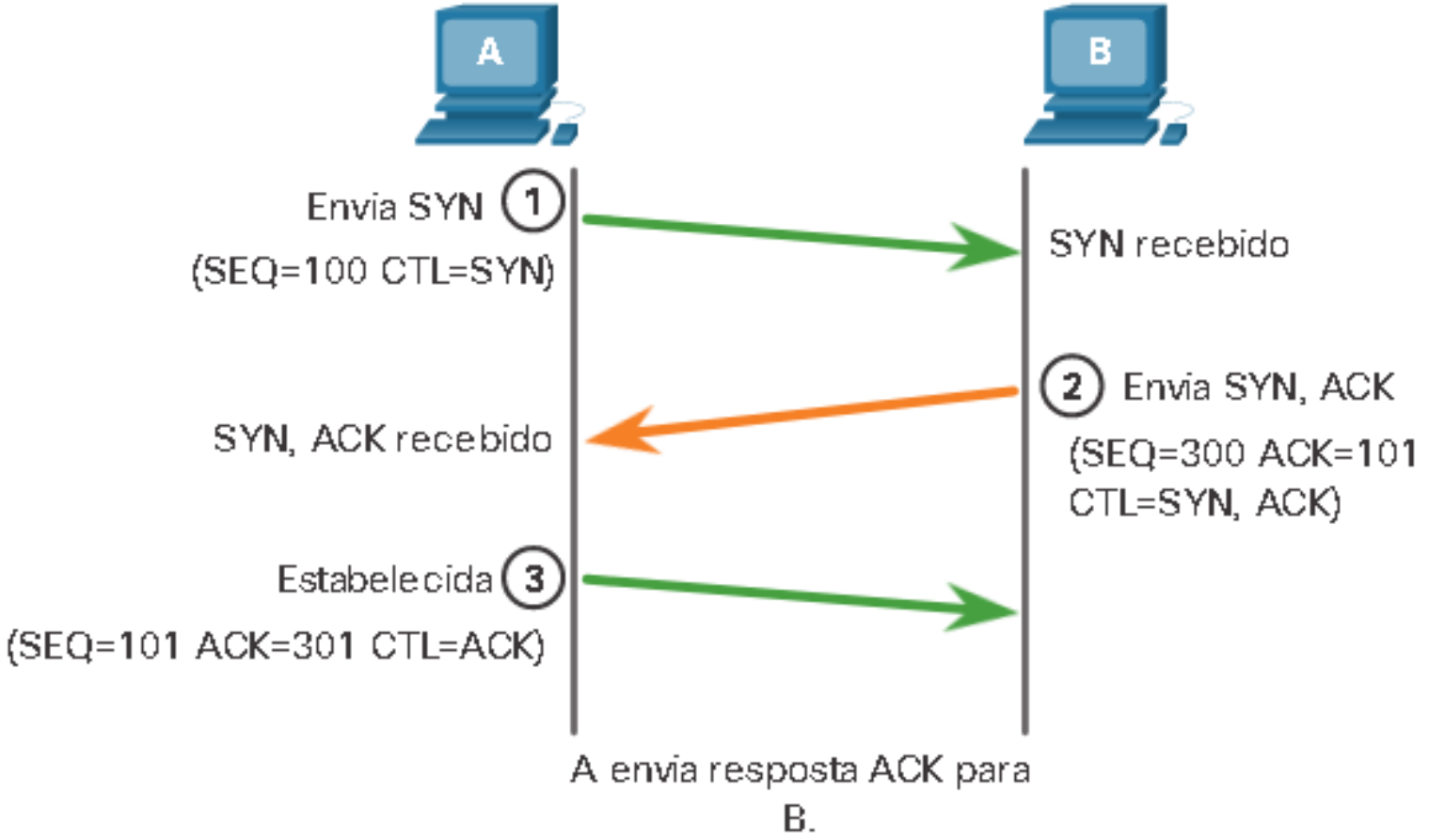
O cliente iniciador requisita uma sessão de comunicação cliente-servidor com o servidor.

Etapa 2. ACK e SYN

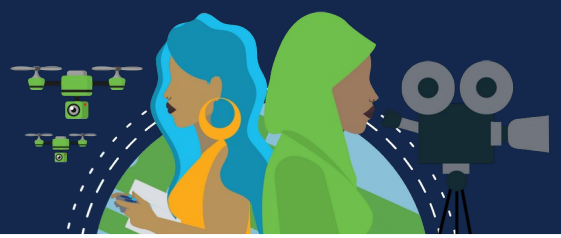
O servidor confirma a sessão de comunicação cliente-servidor e requisita uma sessão de comunicação de servidor-cliente.

Etapa 3. ACK

O cliente iniciador confirma a sessão de comunicação de servidor-cliente.



Fonte: Cisco



Processo de Comunicação TCP

Encerramento da Sessão

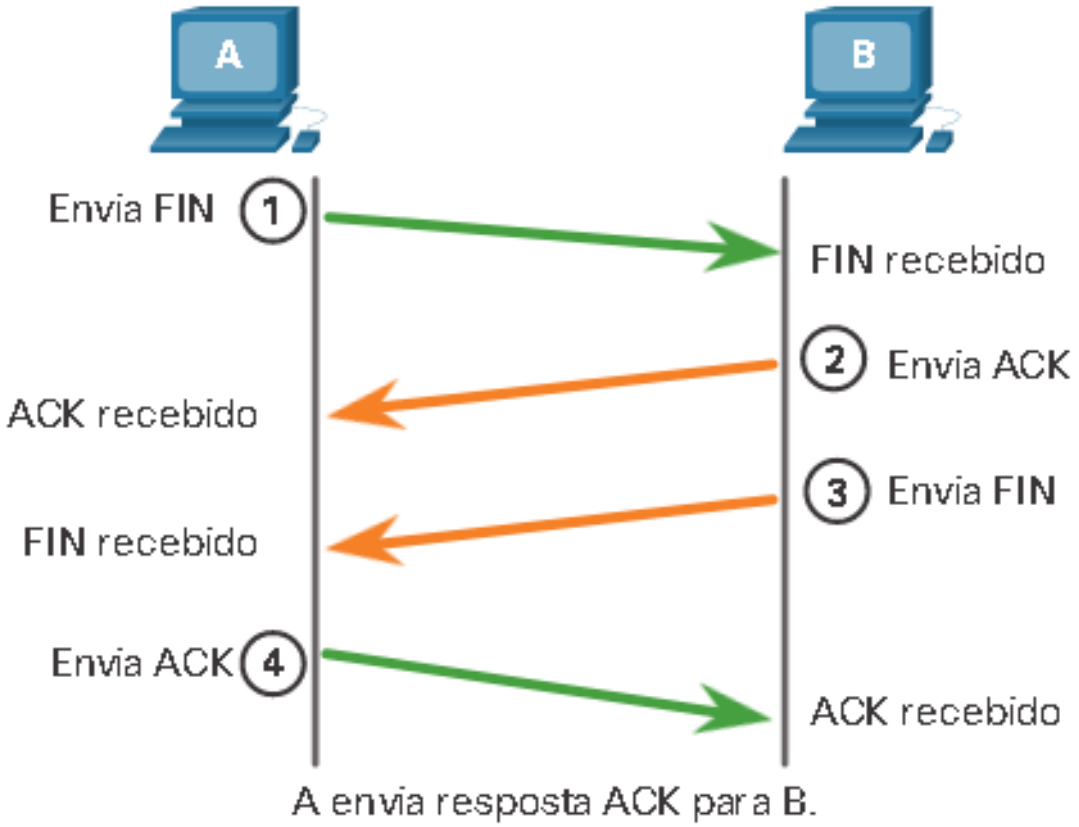
Para fechar uma conexão, o flag de controle Finish (FIN) deve ser ligado no cabeçalho do segmento. Para terminar cada sessão TCP de uma via, um handshake duplo, consistindo de um segmento FIN e um segmento ACK (Acknowledgment) é usado. Portanto, para terminar uma conversação única permitida pelo TCP, quatro trocas são necessárias para finalizar ambas as sessões. O cliente ou o servidor podem iniciar o encerramento.

Etapa 1. FIN: Quando o cliente não tem mais dados para enviar no fluxo, ele envia um segmento com um flag FIN ligado.

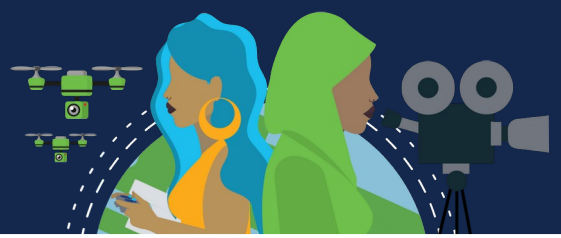
Etapa 2. ACK: O servidor envia ACK para confirmar o recebimento de FIN para encerrar a sessão do cliente com o servidor.

Etapa 3. FIN: O servidor envia um FIN ao cliente para encerrar a sessão do servidor-para-cliente.

Etapa 4. ACK: O cliente responde com um ACK para reconhecer o FIN do servidor.



Fonte: Cisco



Processo de Comunicação TCP

Análise do Handshake Triplo do TCP

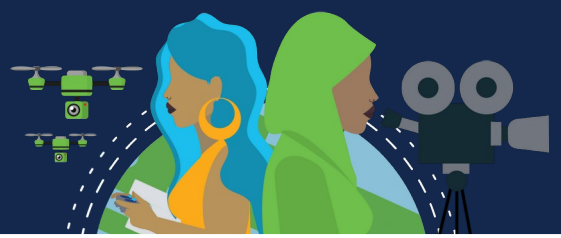
Os hosts mantêm o estado, rastreiam cada segmento de dados em uma sessão e trocam informações sobre quais dados são recebidos usando as informações no cabeçalho TCP. O TCP é um protocolo full-duplex, em que cada conexão representa duas sessões de comunicação unidirecional. Para estabelecer uma conexão, os hosts realizam um handshake triplo (three-way handshake). Os bits de controle no cabeçalho TCP indicam o progresso e o status da conexão.

Estas são as funções do handshake de três vias:

- Estabelece que o dispositivo de destino está presente na rede.
- Ele verifica se o dispositivo de destino possui um serviço ativo e está aceitando solicitações no número da porta de destino que o cliente inicial pretende usar.
- Ele informa ao dispositivo de destino que o cliente de origem pretende estabelecer uma sessão de comunicação nesse número de porta.

Após a conclusão da comunicação, as sessões são fechadas e a conexão é encerrada. Os mecanismos de conexão e sessão ativam a função de confiabilidade do TCP.

Fonte: Cisco



Processo de Comunicação TCP

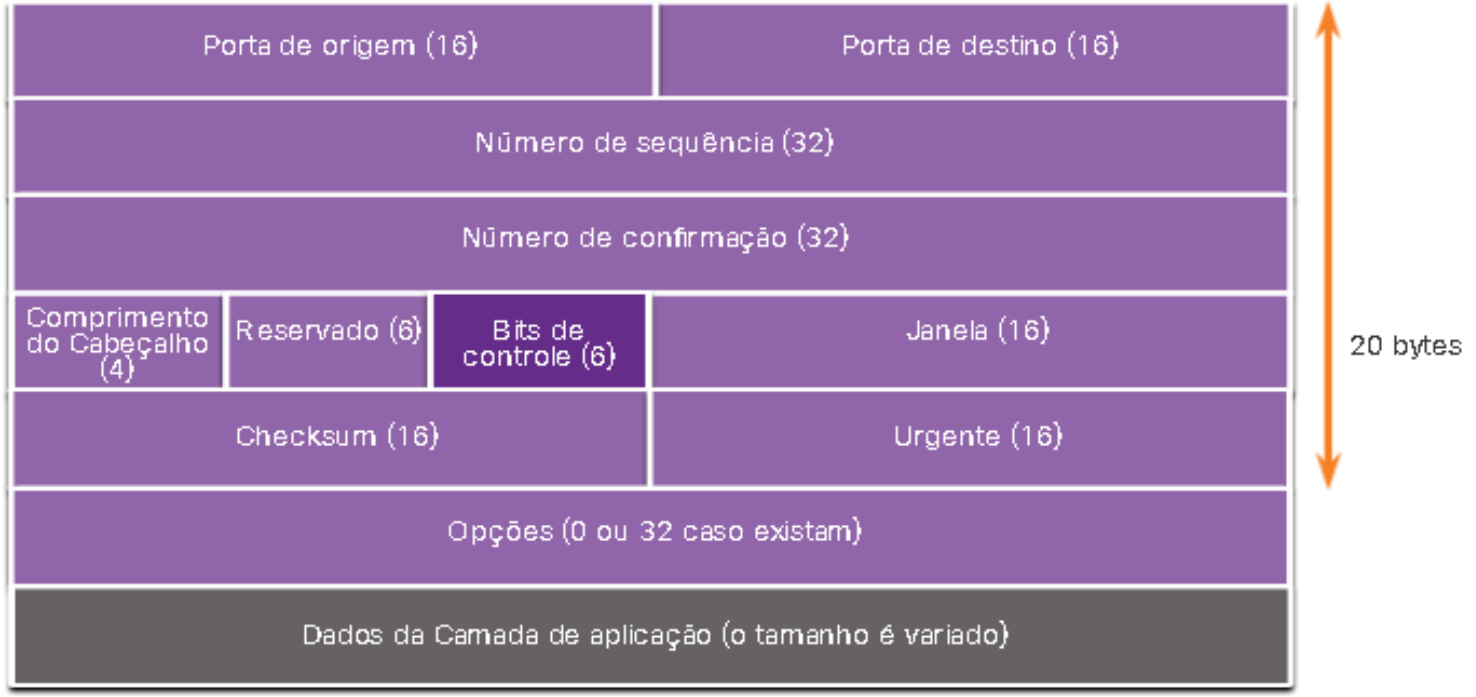
Análise do Handshake Triplo do TCP

Campo de bits de controle

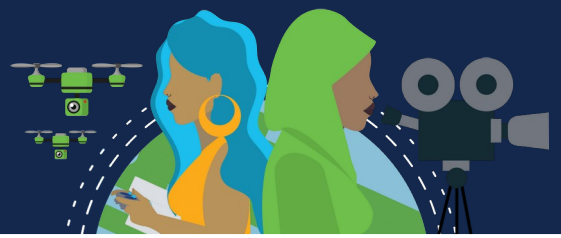
Os seis bits no campo Bits de Controle do cabeçalho do segmento TCP são também conhecidos como flags. Uma flag (sinalizador, bandeira) é um bit que é definido como ligado (1) ou desligado (0).

Os seis bits de controle sinalizadores são os seguintes:

- **URG:** Campo de ponteiro urgente significativo.
- **ACK:** Indicador de confirmação usado no estabelecimento de conexão e encerramento de sessão.
- **PSH:** Função Push.
- **RST:** Redefina a conexão quando ocorrer um erro ou tempo limite.
- **SYN:** Sincronizar números de sequência usados no estabelecimento de conexão.
- **FIN:** Não há mais dados do remetente e usados no encerramento da sessão.



Fonte: Cisco



Confiabilidade e controle de fluxo

Confiabilidade do TCP - Entrega garantida e solicitada

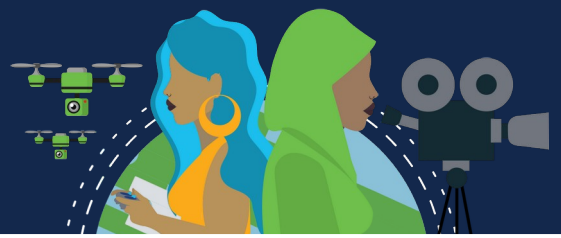
Pode haver momentos em que os segmentos TCP não chegam ao seu destino. Outras vezes, os segmentos TCP podem chegar fora de ordem. Para que a mensagem original seja entendida pelo destinatário, todos os dados devem ser recebidos e os dados nesses segmentos devem ser remontados na ordem original. Os números de sequência são atribuídos no cabeçalho de cada pacote para alcançar esse objetivo. O número de sequência representa o primeiro byte de dados do segmento TCP.

Durante o estabelecimento de uma sessão, um número de sequência inicial (ISN) é definido. Este ISN representa o valor inicial dos bytes que são transmitidos ao aplicativo receptor. À medida que os dados são transmitidos durante a sessão, número de sequência é incrementado do número de bytes que foram transmitidos. Esse rastreamento dos bytes de dados permite que cada segmento seja identificado e confirmado de forma única. Segmentos perdidos podem então, ser identificados.

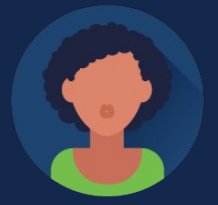
O ISN não começa em um, mas é efetivamente um número aleatório. Isso é para impedir determinados tipos de ataques maliciosos. Os números de sequência do segmento indicam como remontar e reordenar os segmentos recebidos.

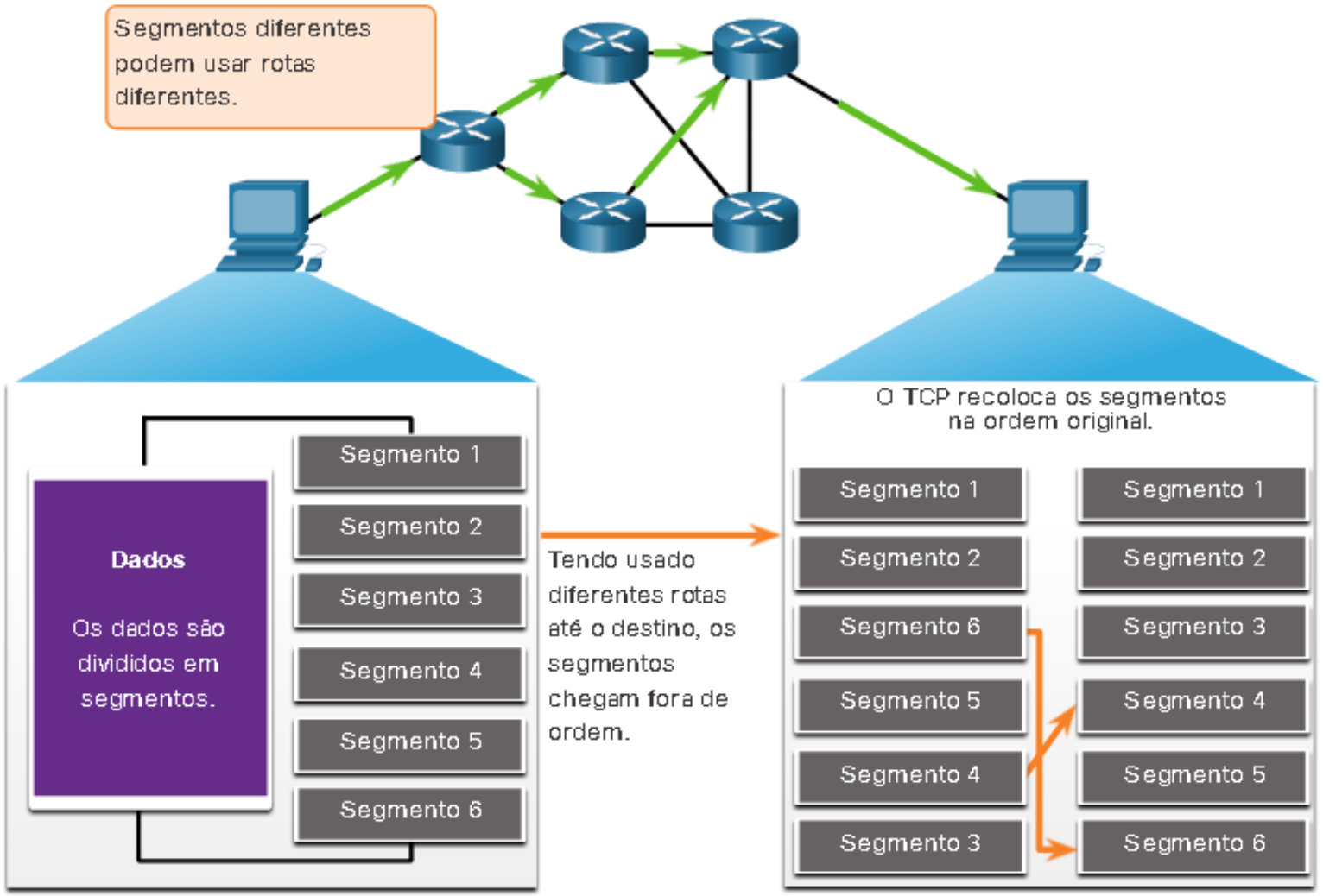
O processo TCP receptor coloca os dados de um segmento em um buffer receptor. Os segmentos são então colocados na ordem de sequência correta e passados para a camada de aplicativo quando remontados. Qualquer segmento que chegue com números de sequência fora de ordem são retidos para processamento posterior. Por isso, quando os segmentos com os bytes que faltavam chegam, esses segmentos são processados.

Fonte: Cisco



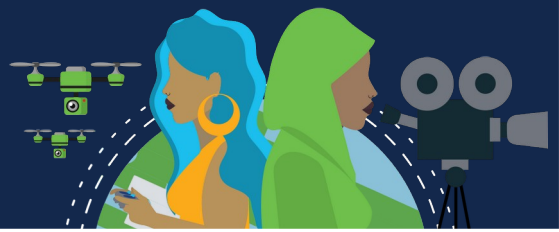
Confiabilidade e controle de fluxo





Fonte: Cisco

Confiabilidade e controle de fluxo

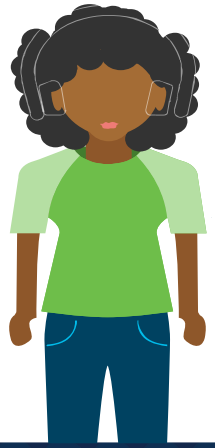


Confiabilidade do TCP - perda de dados e retransmissão

Não importa o quão bem projetada uma rede é, a perda de dados ocasionalmente ocorre. O TCP fornece métodos de gerenciamento dessas perdas de segmento. Entre esses métodos há um mecanismo que retransmite segmentos dos dados não confirmados.

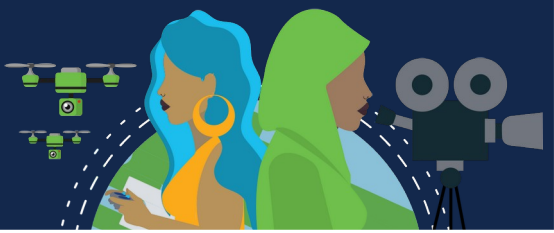
O número de sequência (SEQ) e o número de confirmação (ACK) são usados juntamente para confirmar o recebimento dos bytes de dados contidos nos segmentos. O número SEQ identifica o primeiro byte de dados no segmento que está sendo transmitido. O TCP usa o número de confirmação (ACK) enviado de volta à origem para indicar o próximo byte que o destino espera receber. Isto é chamado de confirmação antecipatória.

Antes de melhorias posteriores, o TCP só podia reconhecer o próximo byte esperado.



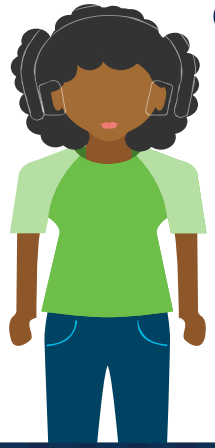
Fonte: Cisco

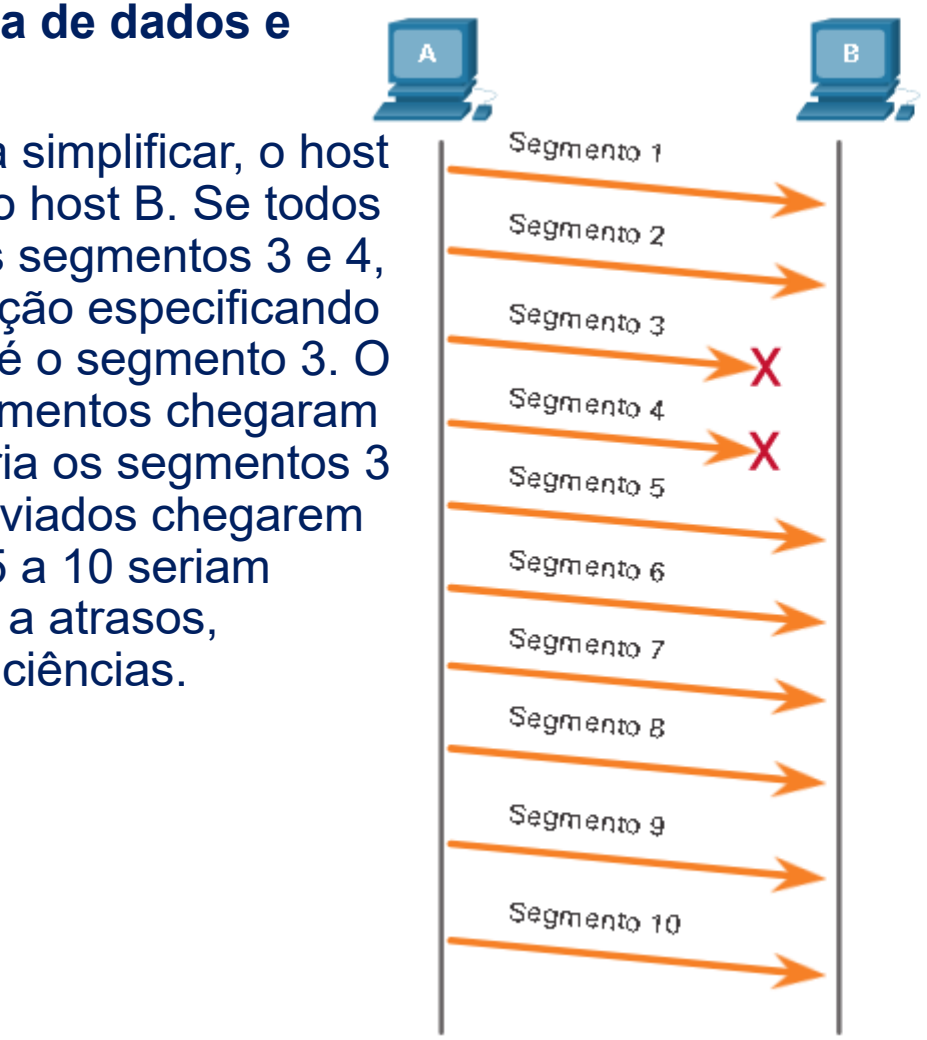
Confiabilidade e controle de fluxo

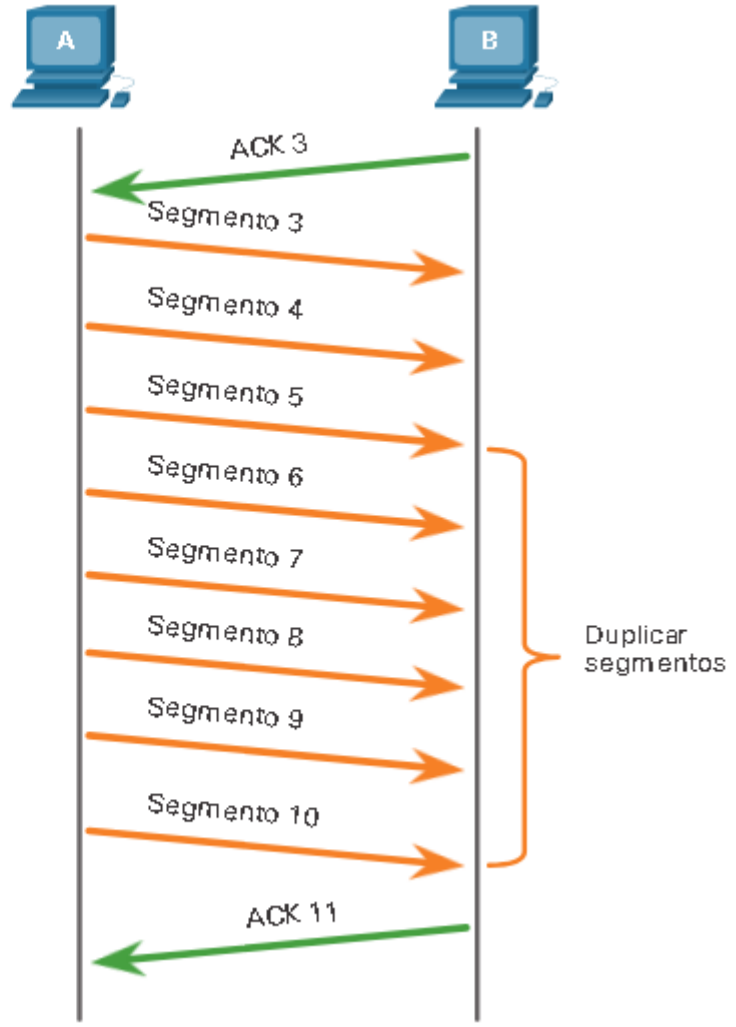


Confiabilidade do TCP - perda de dados e retransmissão

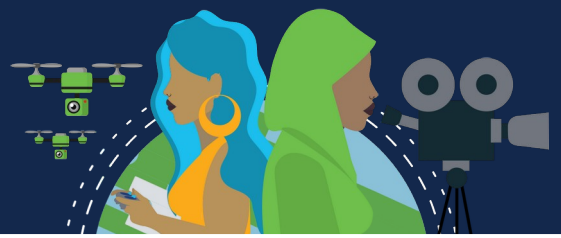
Usando números de segmento para simplificar, o host A envia os segmentos 1 a 10 para o host B. Se todos os segmentos chegarem, exceto os segmentos 3 e 4, o host B responderia com confirmação especificando que o próximo segmento esperado é o segmento 3. O Host A não tem idéia se outros segmentos chegaram ou não. O host A, portanto, reenviaria os segmentos 3 a 10. Se todos os segmentos reenviados chegarem com sucesso, os segmentos 5 a 10 seriam duplicados. Isso pode levar a atrasos, congestionamentos e ineficiências.







Fonte: Cisco



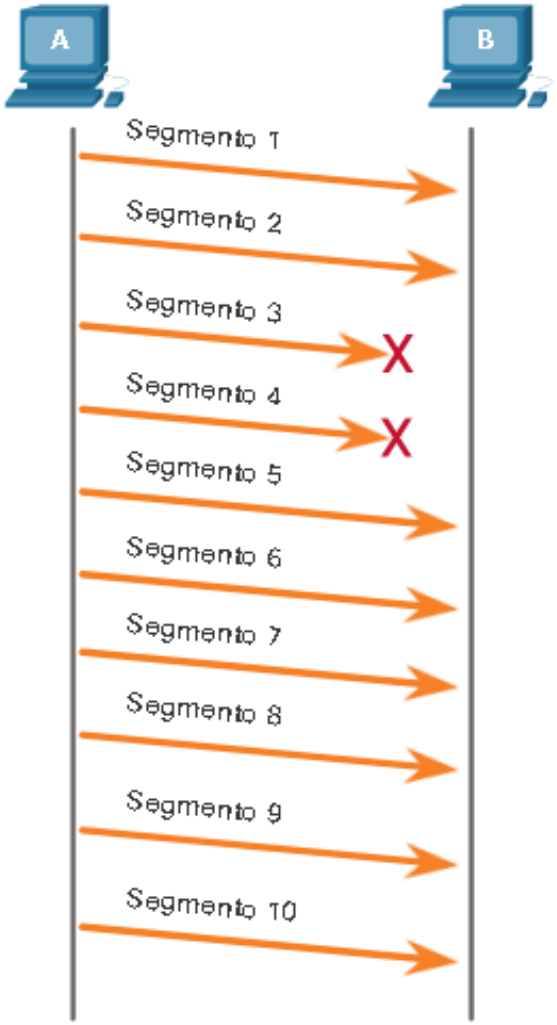
Confiabilidade e controle de fluxo

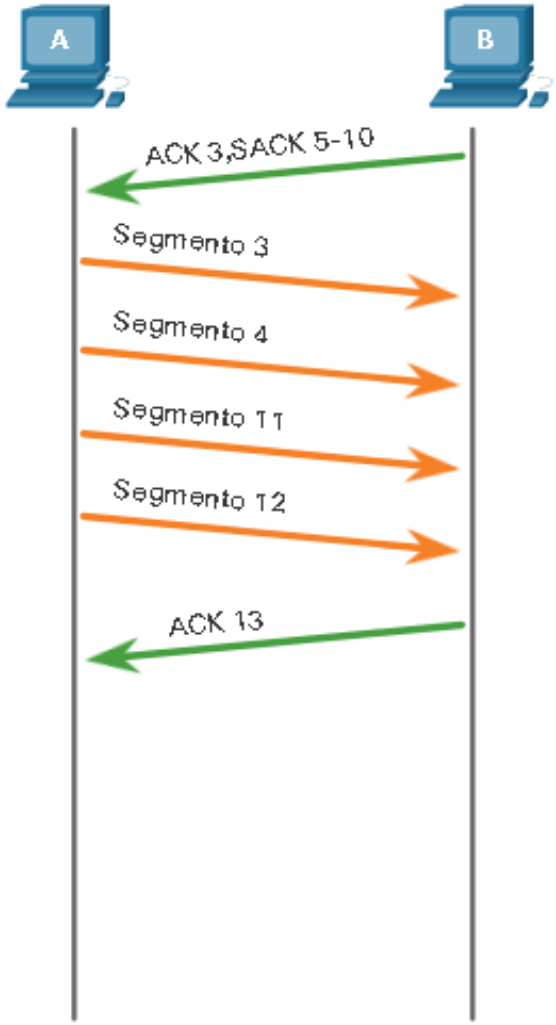
Confiabilidade do TCP - perda de dados e retransmissão

Hoje, os sistemas operacionais utilizam um recurso TCP opcional chamado reconhecimento seletivo (SACK), negociado durante o handshake de três vias. Se ambos os hosts suportarem SACK, o receptor pode reconhecer explicitamente quais segmentos (bytes) foram recebidos, incluindo quaisquer segmentos descontínuos. O host de envio, portanto, só precisa retransmitir os dados ausentes.

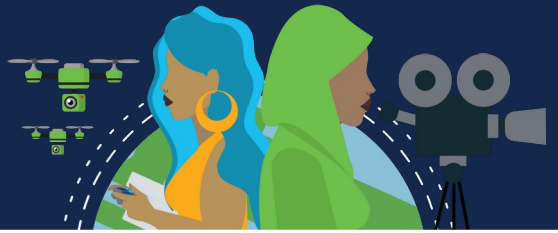
O host A envia segmentos 1 a 10 para o host B. Se todos os segmentos chegarem, exceto os segmentos 3 e 4, o host B pode reconhecer que recebeu segmentos 1 e 2 (ACK 3) e reconhecer seletivamente os segmentos 5 a 10 (SACK 5-10). O host A só precisaria reenviar os segmentos 3 e 4.

O TCP usa temporizadores para saber quanto tempo esperar antes de reenviar um segmento.





Fonte: Cisco

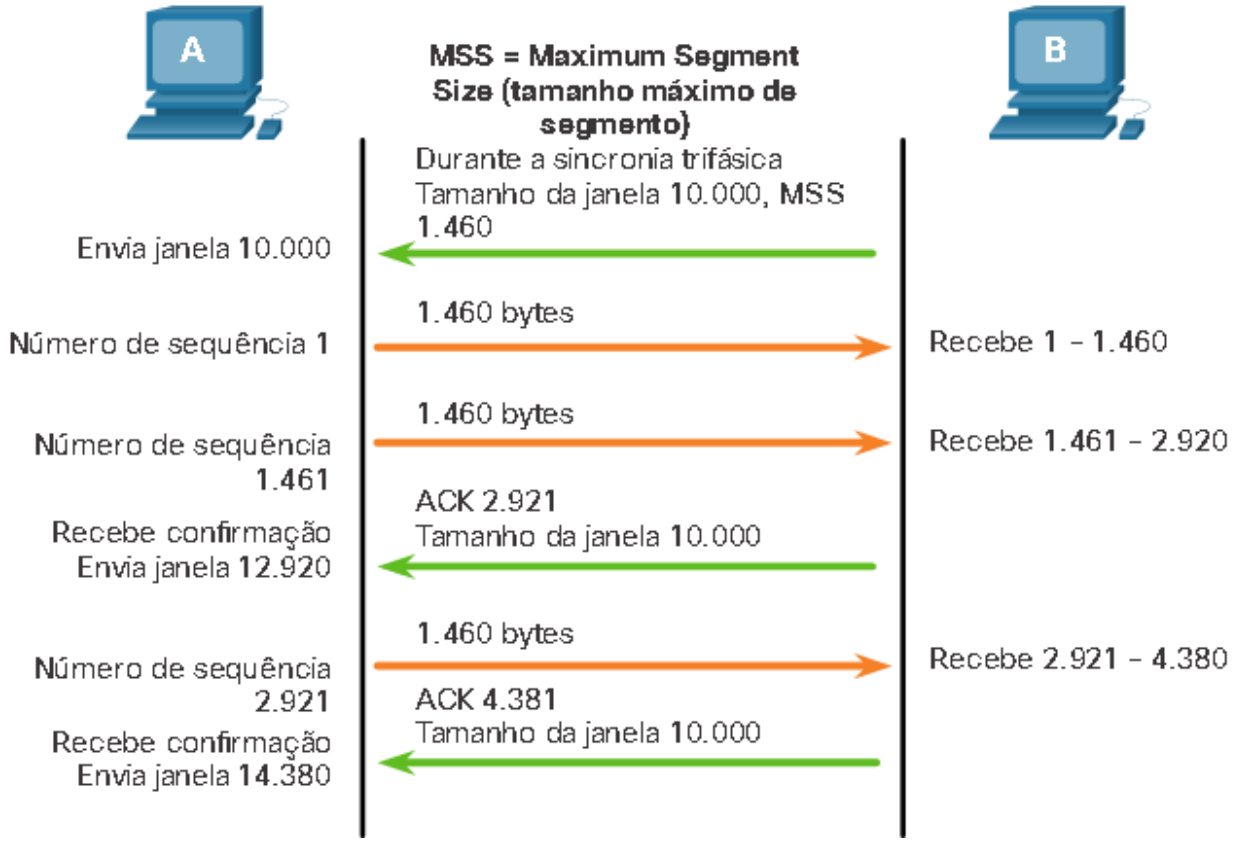


Confiabilidade e controle de fluxo

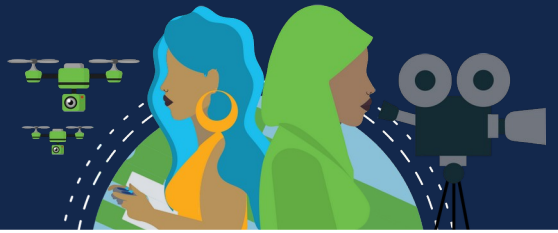
Controle de Fluxo TCP – Tamanho da Janela e Confirmações

Controle de fluxo é a quantidade de dados que o destino pode receber e processar de forma confiável. Ele ajuda a manter a confiabilidade da transmissão TCP definindo a taxa de fluxo de dados entre a origem e o destino em uma determinada sessão. Para realizar isso, o cabeçalho TCP inclui um campo de 16 bits chamado de tamanho da janela.

O tamanho da janela determina o número de bytes que podem ser enviados antes de esperar uma confirmação. O número de reconhecimento é o número do próximo byte esperado. É o número de bytes que o dispositivo de destino de uma sessão TCP pode aceitar e processar de uma vez. No exemplo, o tamanho da janela inicial do PC B para a sessão TCP é de 10.000 bytes. No caso do primeiro byte ser número 1, o último byte que PC A pode enviar sem receber uma confirmação é o byte 10.000. Isso é conhecido como janela de envio do PC A. O tamanho da janela é incluído em todos os segmentos TCP, para que o destino possa modificar o tamanho da janela a qualquer momento, dependendo da disponibilidade do buffer.



Fonte: Cisco



Confiabilidade e controle de fluxo

Controle de Fluxo TCP – Tamanho da Janela e Confirmações

O tamanho da janela inicial é determinado quando a sessão é estabelecida durante o handshake triplo. O dispositivo de origem limita o número de bytes enviados ao destino com base no tamanho da janela do destino. Somente depois que o dispositivo de origem receber uma confirmação de que os bytes foram recebidos, ele poderá continuar a enviar mais dados para a sessão. O destino não esperará que todos os bytes que a sua janela comporta sejam recebidos para responder confirmando. À medida que os bytes forem recebidos e processados, o destino enviará confirmações para informar à origem que pode continuar a enviar mais bytes. No exemplo, é típico que o PC B não espere até que todos os 10.000 bytes tenham sido recebidos antes de enviar uma confirmação. Isso significa que o PC A pode ajustar sua janela de envio ao receber confirmações do PC B. Quando o PC A recebe uma confirmação com o número de confirmação 2.921, que é o próximo byte esperado. A janela de envio do PC A irá incrementar 2.920 bytes. Isso altera a janela de envio de 10.000 bytes para 12.920. O PC A agora pode continuar enviando até outros 10.000 bytes para o PC B, desde que não envie mais do que sua nova janela de envio em 12.920. Um destino que envia confirmações enquanto processa os bytes recebidos e o ajuste contínuo da janela de envio de origem é conhecido como janelas deslizantes. No exemplo, a janela de envio do PC A incrementa ou desliza sobre outros 2.921 bytes de 10.000 para 12.920. Se a disponibilidade do espaço de buffer do destino diminui, ele pode reduzir o tamanho da sua janela para informar à origem que reduza o número de bytes que ela deveria enviar sem receber uma confirmação.

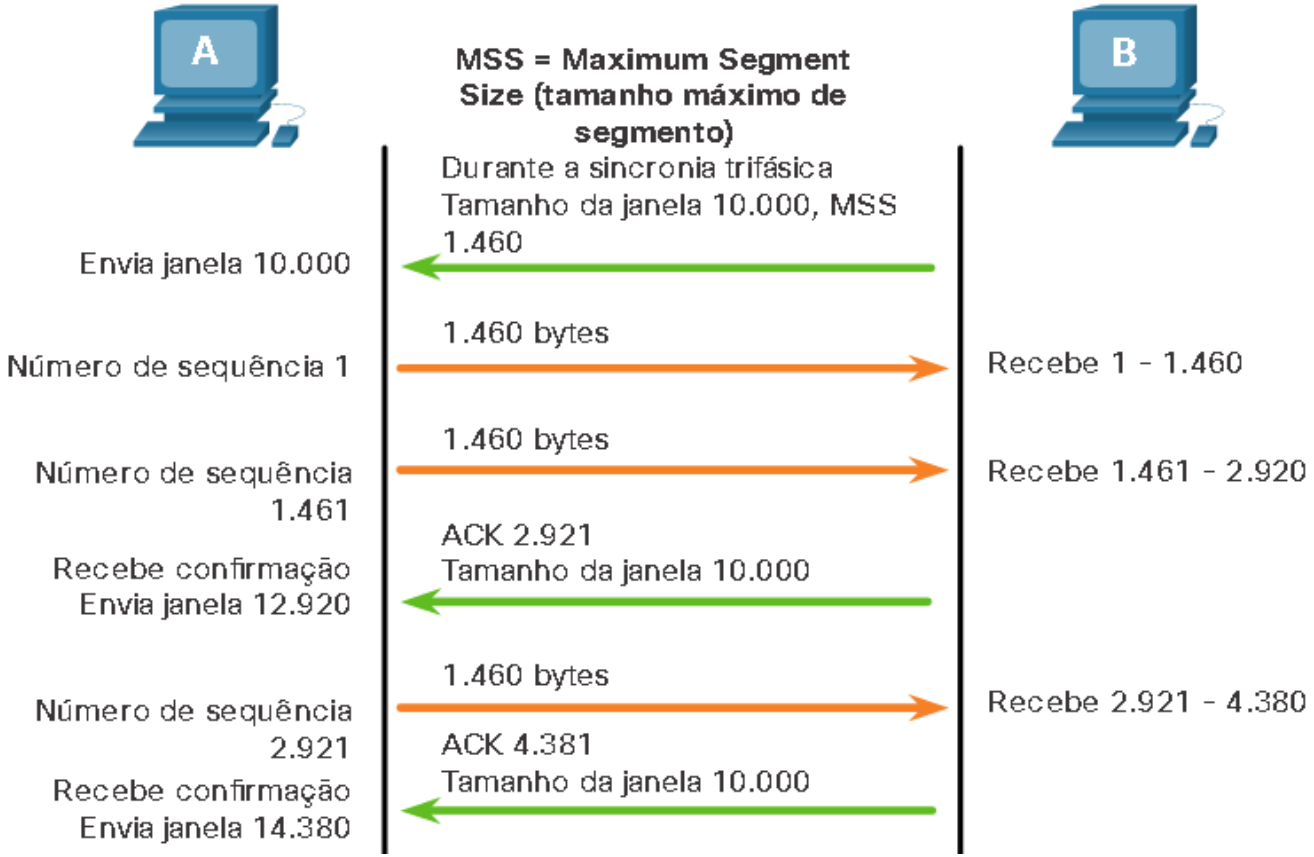
Com o uso de janelas deslizantes. O receptor normalmente envia uma confirmação após cada dois segmentos que recebe. O número de segmentos recebidos antes de ser confirmado pode variar. A vantagem é que permite que o emissor transmita continuamente segmentos, desde que o receptor esteja reconhecendo segmentos anteriores.

Fonte: Cisco

Confiabilidade e controle de fluxo

Controle de Fluxo TCP - Tamanho Máximo do Segmento (MSS)

Na figura, a fonte está transmitindo 1.460 bytes de dados dentro de cada segmento TCP. Normalmente, este é o tamanho máximo do segmento (MSS) que o dispositivo de destino pode receber. O MSS faz parte do campo de opções no cabeçalho TCP que especifica a maior quantidade de dados, em bytes, que um dispositivo pode receber em um único segmento TCP. O tamanho do MSS não inclui o cabeçalho TCP. O MSS é normalmente incluído durante o handshake de três vias.

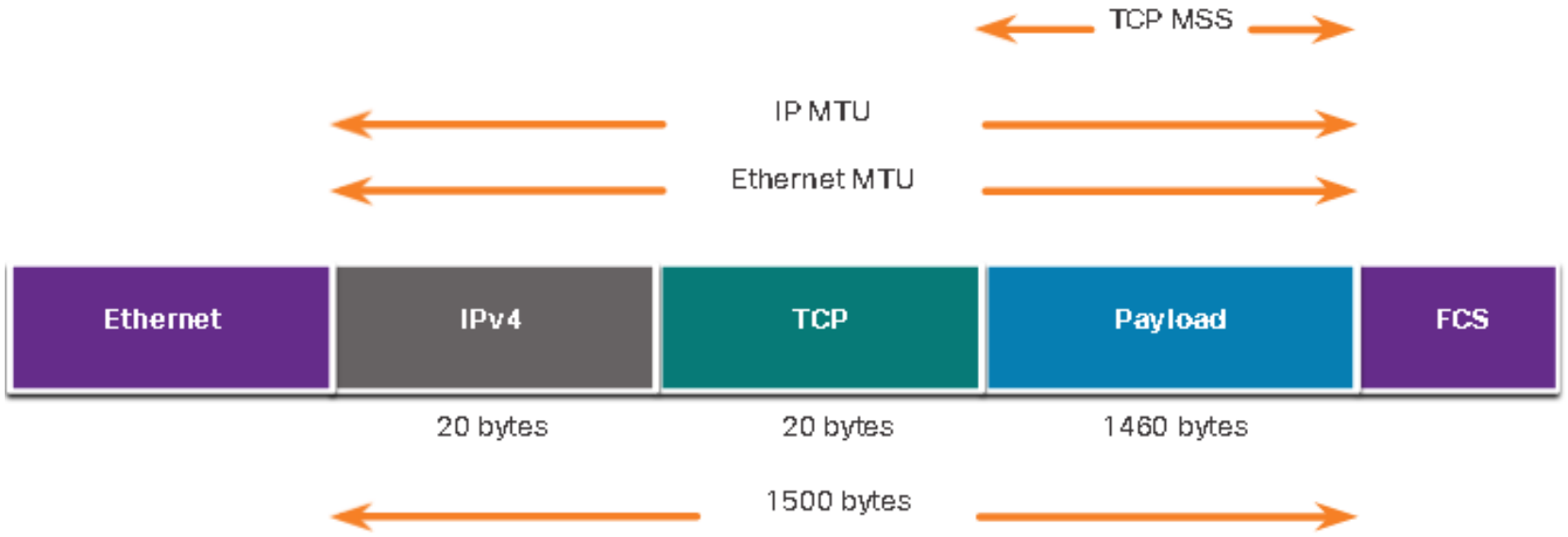


Fonte: Cisco

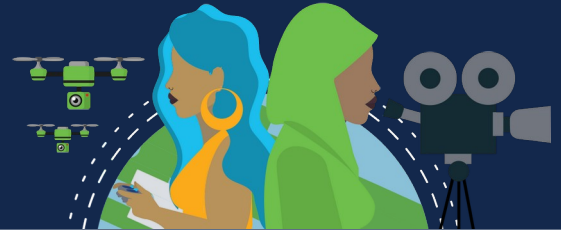
Confiabilidade e controle de fluxo

Controle de Fluxo TCP - Tamanho Máximo do Segmento (MSS)

Um MSS comum é 1.460 bytes ao usar IPv4. Um host determina o valor do campo de MSS subtraindo os cabeçalhos de IP e de TCP da MTU (Maximum transmission unit, Unidade máxima de transmissão) da Ethernet. Em uma interface Ethernet, a MTU padrão é 1500 bytes. Subtraindo o cabeçalho IPv4 de 20 bytes e o cabeçalho TCP de 20 bytes, o tamanho padrão do MSS será 1460 bytes, conforme mostrado na figura..



Fonte: Cisco



Confiabilidade e controle de fluxo

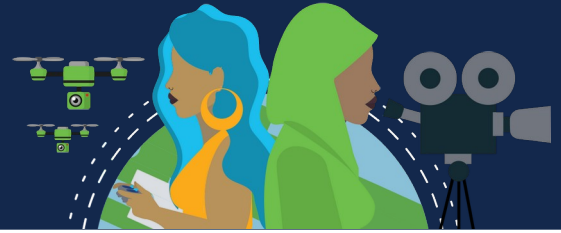
Controle de Fluxo TCP - Prevenção de Congestionamento

Quando ocorre um congestionamento em uma rede, resulta em pacotes sendo descartados pelo roteador sobrecarregado. Ao determinar a taxa na qual os segmentos TCP são enviados, mas não confirmados, a origem pode pressupor um certo nível de congestionamento da rede.

Sempre que ocorrer um congestionamento, ocorrerá a retransmissão de segmentos TCP perdidos por parte da origem. Se a retransmissão não for devidamente controlada, a retransmissão adicional dos segmentos TCP pode agravar o congestionamento. Não só novos pacotes com segmentos TCP são introduzidos na rede, como também o efeito de feedback dos segmentos retransmitidos que foram perdidos aumentarão o congestionamento. Para evitar e controlar o congestionamento, o TCP emprega alguns mecanismos para lidar com o congestionamento, temporizadores e algoritmos.

Se a origem determina que os segmentos TCP não são confirmados ou não são confirmados em tempo hábil, isso pode reduzir o número de bytes enviados antes do recebimento de uma confirmação.

Fonte: Cisco



Confiabilidade e controle de fluxo

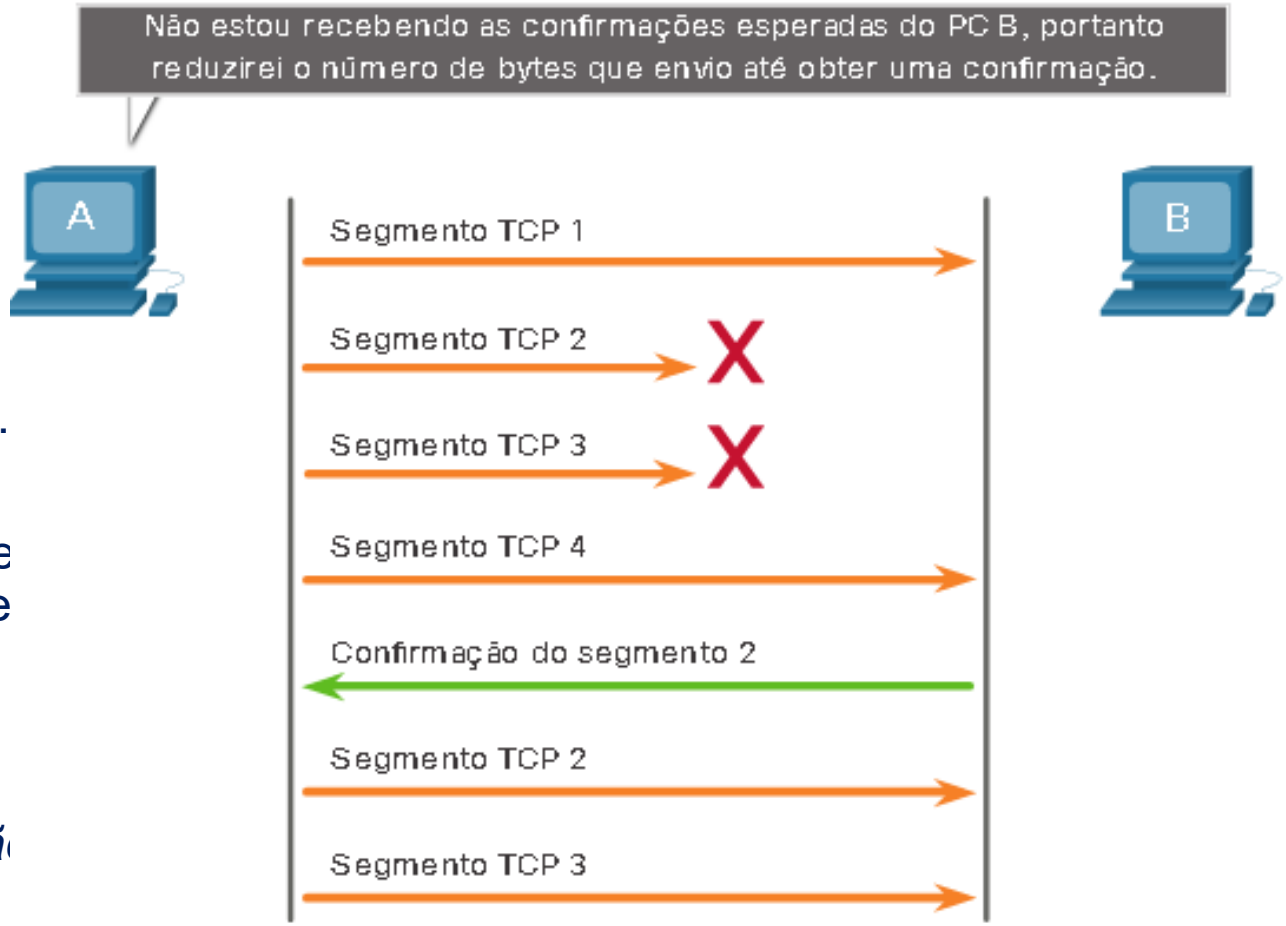
Controle de Fluxo TCP - Prevenção de Congestionamento

Na figura, o PC A detecta que há congestionamento e, portanto, reduz o número de bytes que envia antes de receber uma confirmação do PC B.

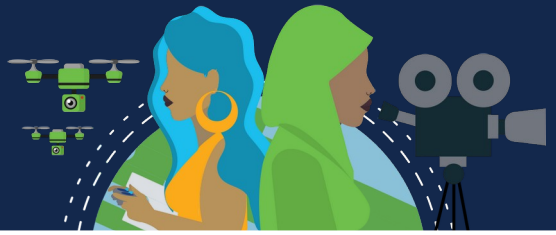
Os números de confirmação são para o próximo byte esperado e não para um segmento. Os números de segmento usados são simplificados para fins ilustrativos.

Observe que é a origem que está reduzindo o número de bytes não confirmados que envia e não o tamanho da jane determinado pelo destino.

As explicações sobre os mecanismos, cronômetros e algoritmos reais de tratamento de congestionamento estã além do escopo deste curso.



Fonte: Cisco



Comunicação UDP

Baixa Sobrecarga do UDP Versus Confiabilidade

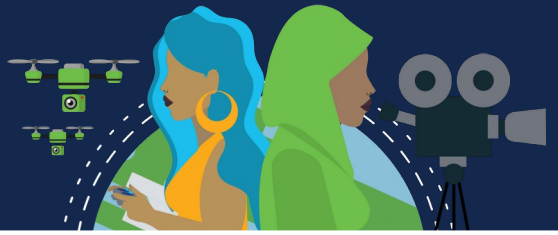
O UDP é perfeito para comunicações que precisam ser rápidas, como VoIP. O UDP não estabelece uma conexão. O UDP fornece transporte de dados de baixa sobrecarga, porque tem um cabeçalho de datagrama pequeno e nenhum tráfego de gerenciamento de rede.

Remontagem do Datagrama UDP

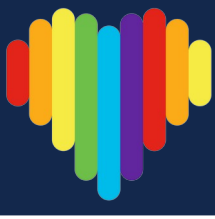
Como ocorre com segmentos TCP, quando múltiplos datagramas UDP são enviados a um destino, eles geralmente tomam caminhos diferentes e chegam na ordem errada. O UDP não rastreia os números de sequência da forma que o TCP faz. O UDP não tem como reordernar os datagramas na sua ordem de transmissão.

Portanto, o UDP simplesmente remonta os dados na ordem que eles foram recebidos e os encaminha para a aplicação. Se a sequência de dados for importante para a aplicação, a aplicação deverá identificar a sequência apropriada e determinar como os dados devem ser processados.

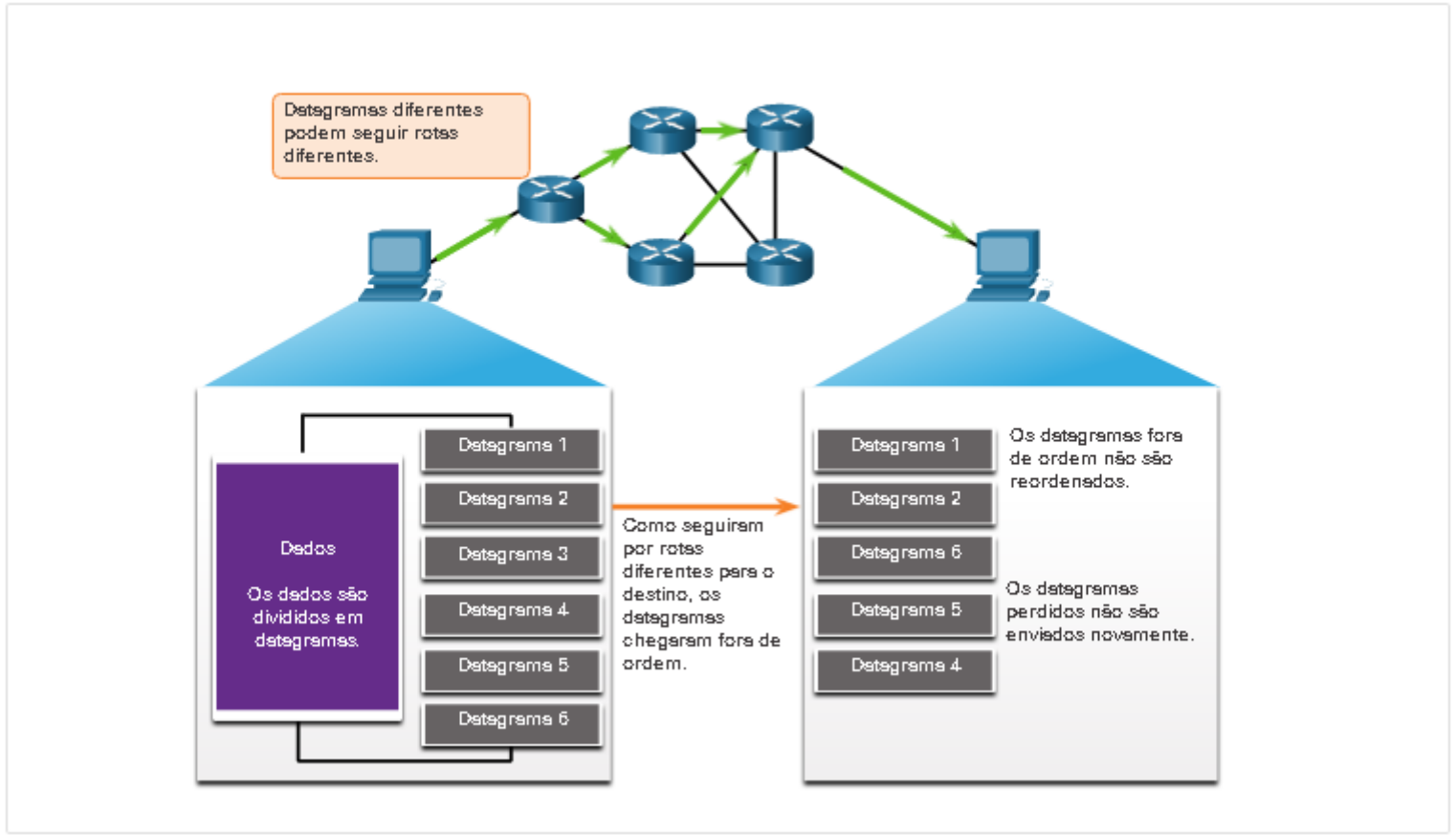
Fonte: Cisco



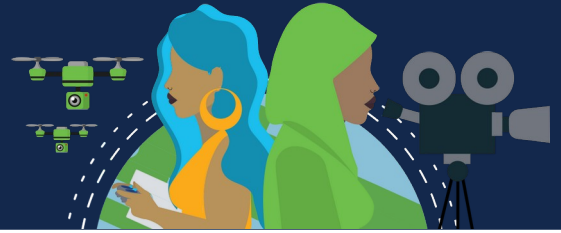
Comunicação UDP



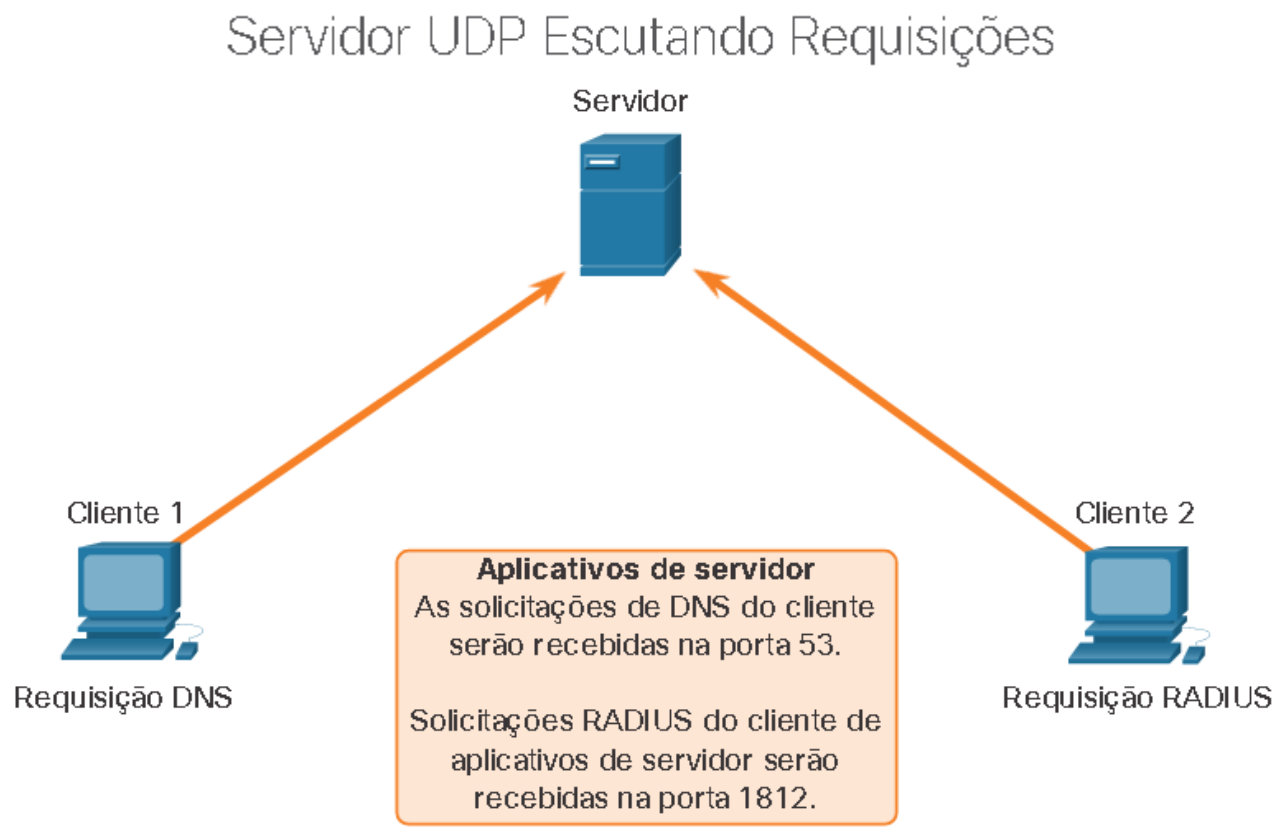
UDP: Sem Conexão e Não Confiável



Fonte: Cisco



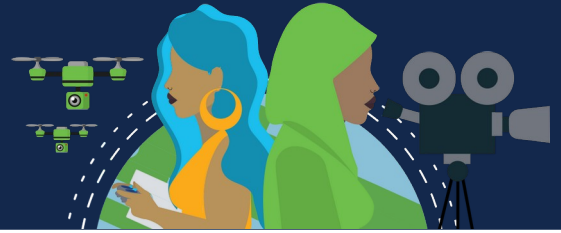
Comunicação UDP



Processos em Servidores e Requisições UDP

As aplicações de servidor baseadas em UDP também recebem números de portas bem conhecidas ou registradas. Quando as aplicações ou processos estão sendo executados, eles aceitarão os dados correspondentes ao número de porta atribuído. Quando o UDP recebe um datagrama destinado a uma destas portas, ele encaminha os dados à aplicação apropriada com base em seu número de porta.

Fonte: Cisco



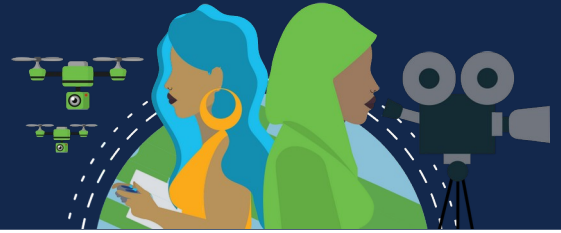
Comunicação UDP

Processos em Clientes UDP

A comunicação cliente servidor é iniciada por uma aplicação cliente que requisita dados de um processo em um servidor. O processo no cliente UDP seleciona dinamicamente um número de porta e a usa como a porta de origem para a conversa. A porta de destino será geralmente o número de porta muito conhecida ou registrada atribuído ao serviço no servidor.

Depois de selecionar as portas de origem e de destino, o mesmo par de portas é usado no cabeçalho de todos os datagramas na transação. Para dados que retornam para o cliente vindos do servidor, os números da porta de origem e de destino no cabeçalho do datagrama são invertidos.

Fonte: Cisco

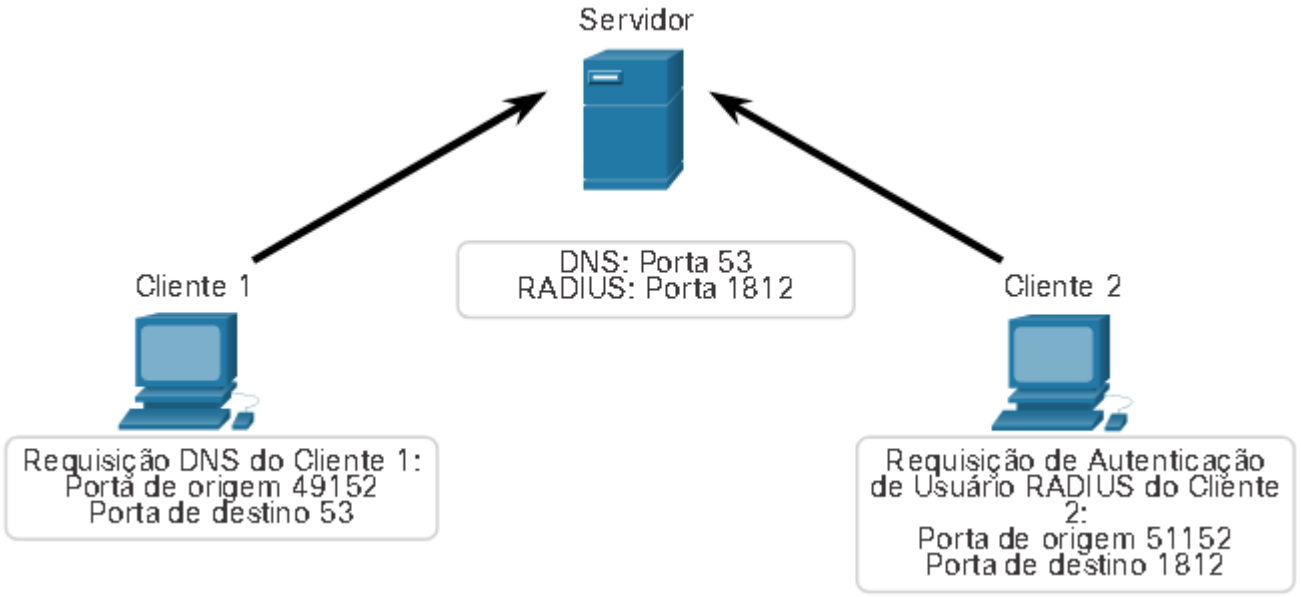


Comunicação UDP

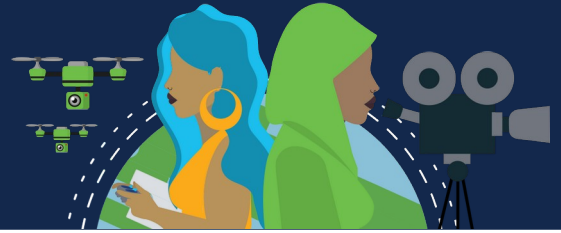
Processos em Clientes UDP

Clientes enviando solicitações UDP

O Cliente 1 está enviando uma solicitação DNS usando a conhecida porta 53 enquanto o Cliente 2 está solicitando serviços de autenticação RADIUS usando a porta registrada 1812.



Fonte: Cisco

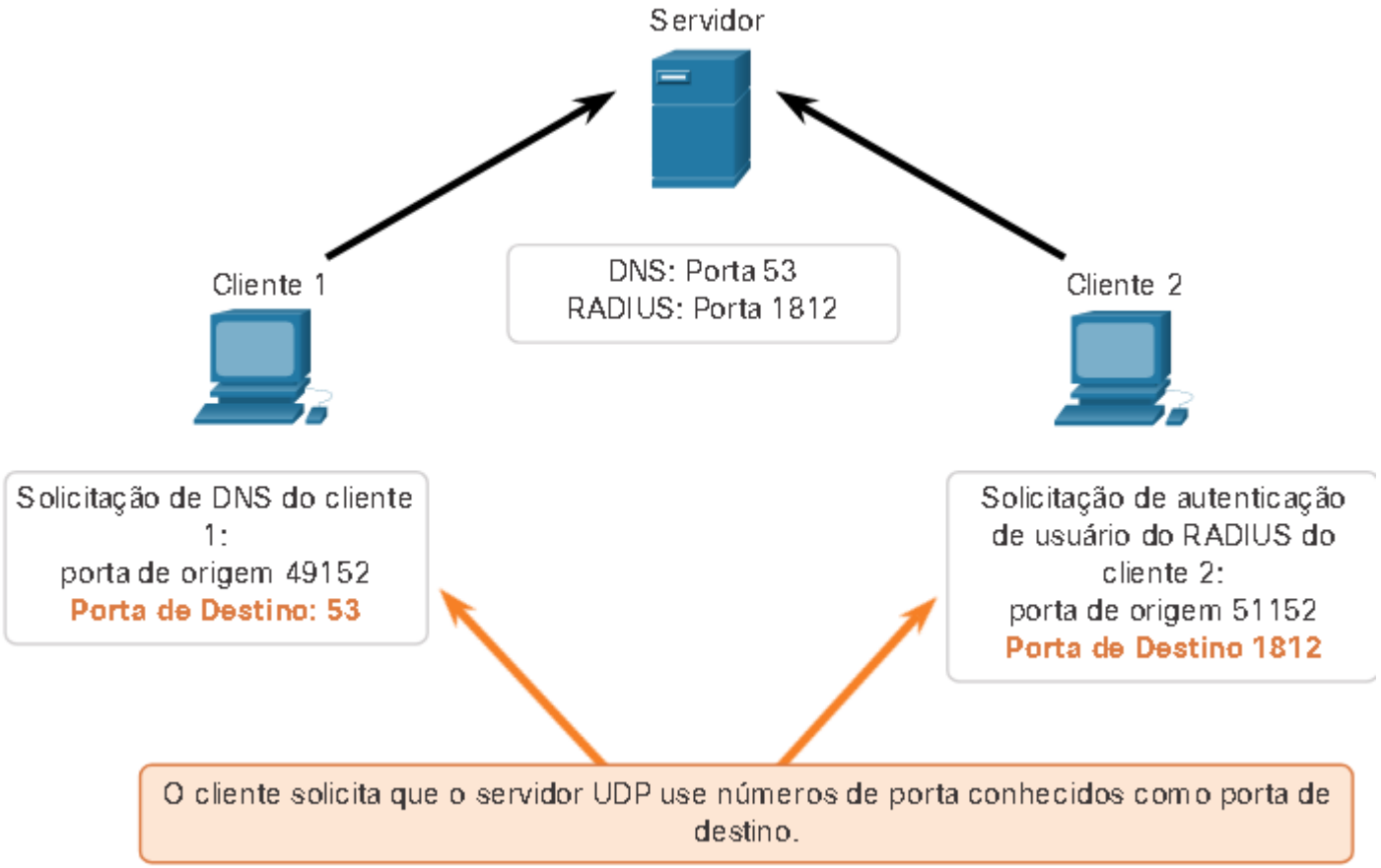


Comunicação UDP

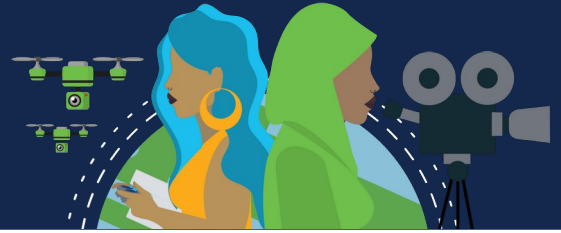
Processos em Clientes UDP

Portas de destino de solicitação UDP

As solicitações dos clientes geram dinamicamente números de porta de origem. Nesse caso, o cliente 1 está usando a porta de origem 49152 e o cliente 2 está usando a porta de origem 51152.



Fonte: Cisco

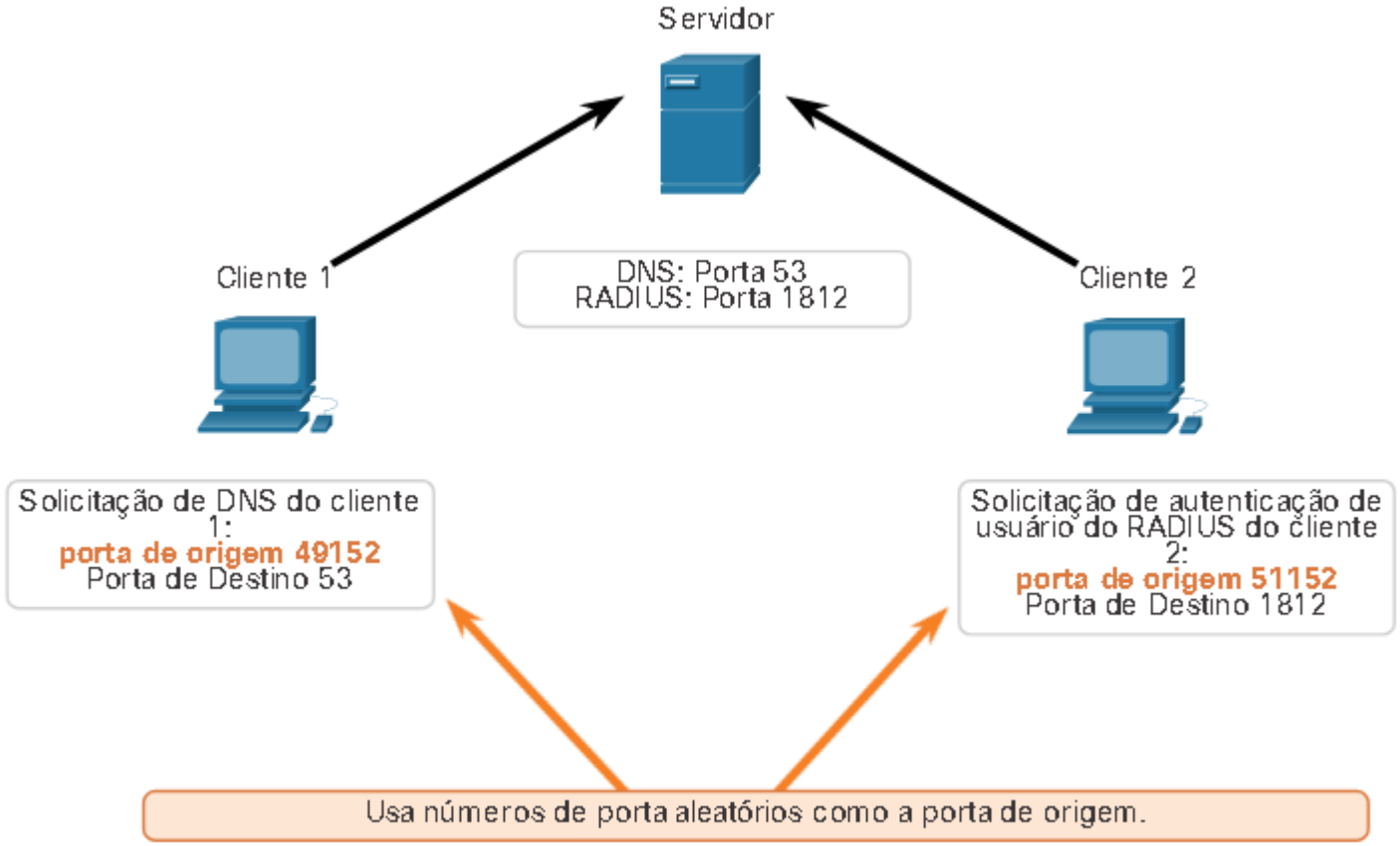


Comunicação UDP

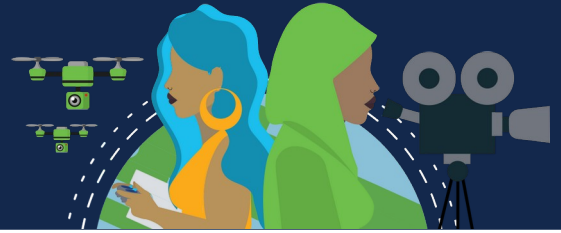
Processos em Clientes UDP

Portas de origem da solicitação UDP

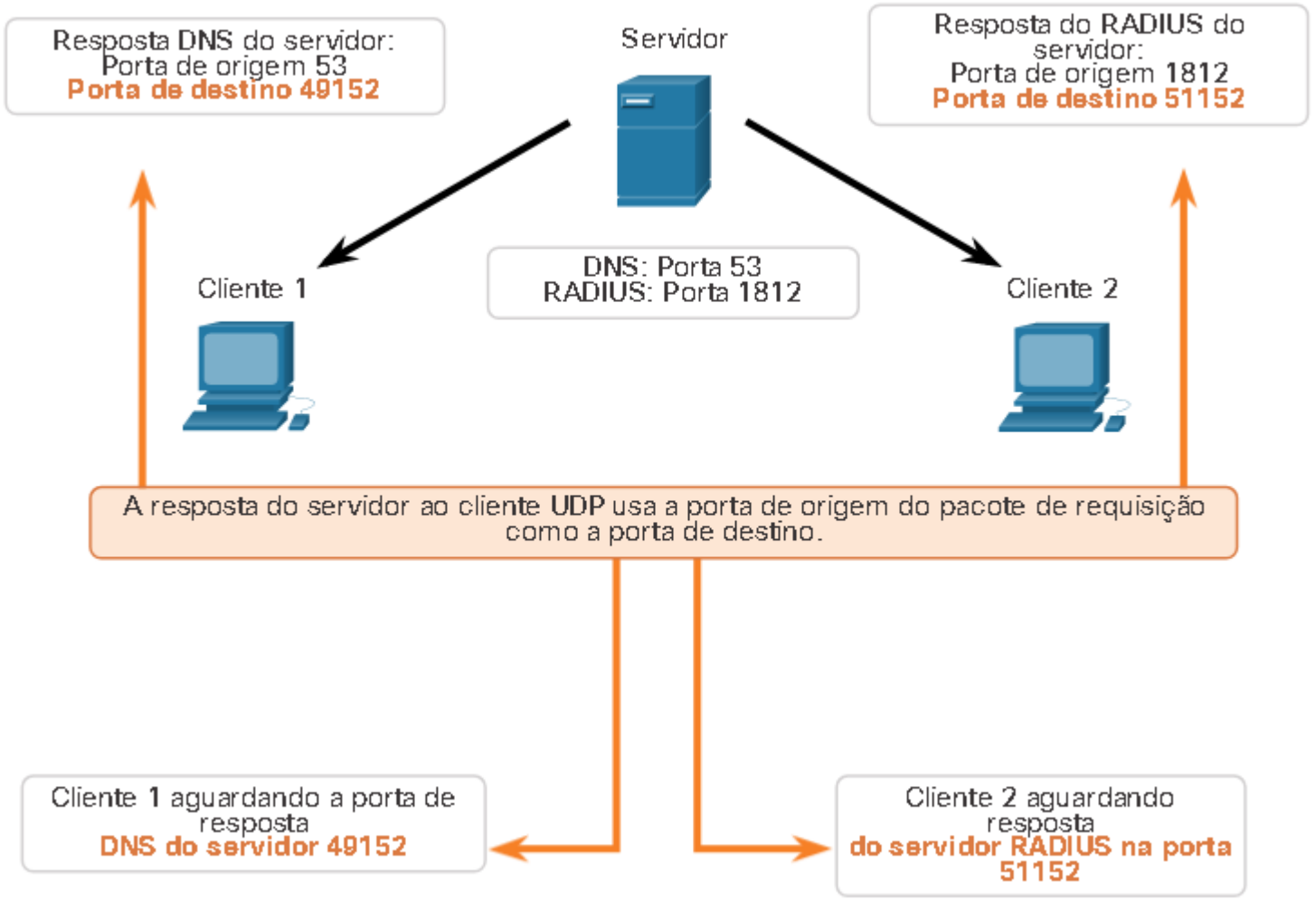
Quando o servidor responde às solicitações, ele reverte as portas de destino e de origem da solicitação inicial.



Fonte: Cisco



Comunicação UDP

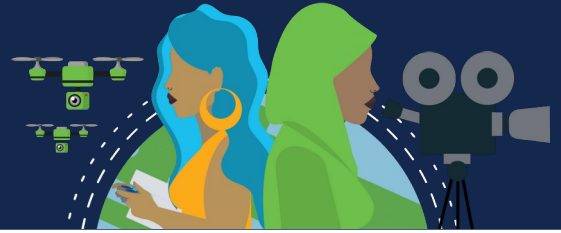


Processos em Clientes UDP

Destino de resposta UDP

Na resposta do servidor à solicitação DNS agora é a porta de destino 49152 e a resposta de autenticação RADIUS é agora a porta de destino 51152.

Fonte: Cisco

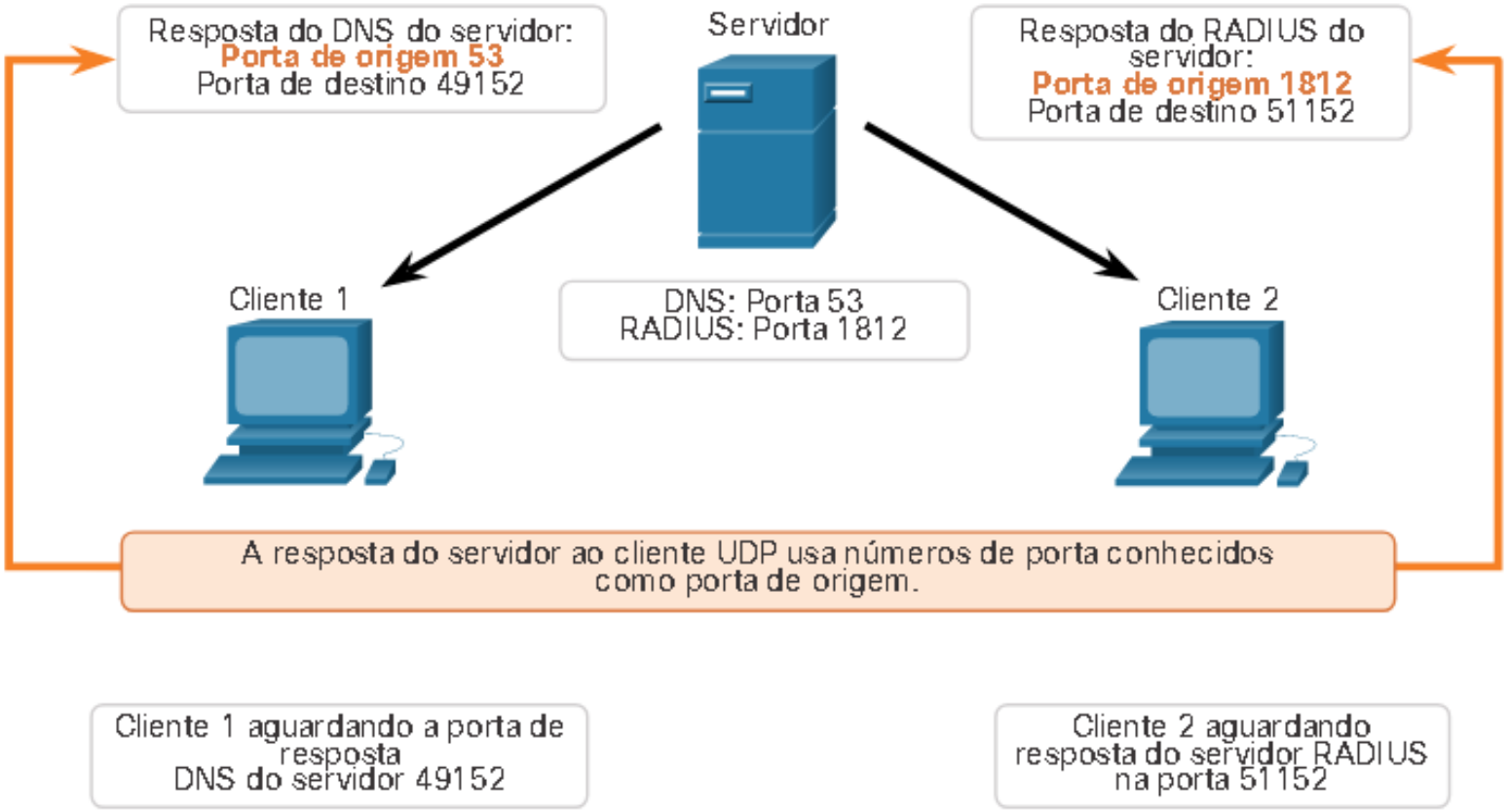


Comunicação UDP

Processos em Clientes UDP

Portas de origem de resposta UDP

As portas de origem na resposta do servidor são as portas de destino originais nas solicitações iniciais.



Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

CCNAv7 – ITN – Camada de Aplicação

Módulo 15

Embaixadores do Programa 2020, 2021 & 2022:

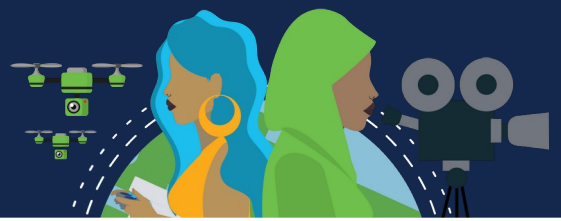
Organizadoras Cisco: Eliana Silva, Veruska Clednev

Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

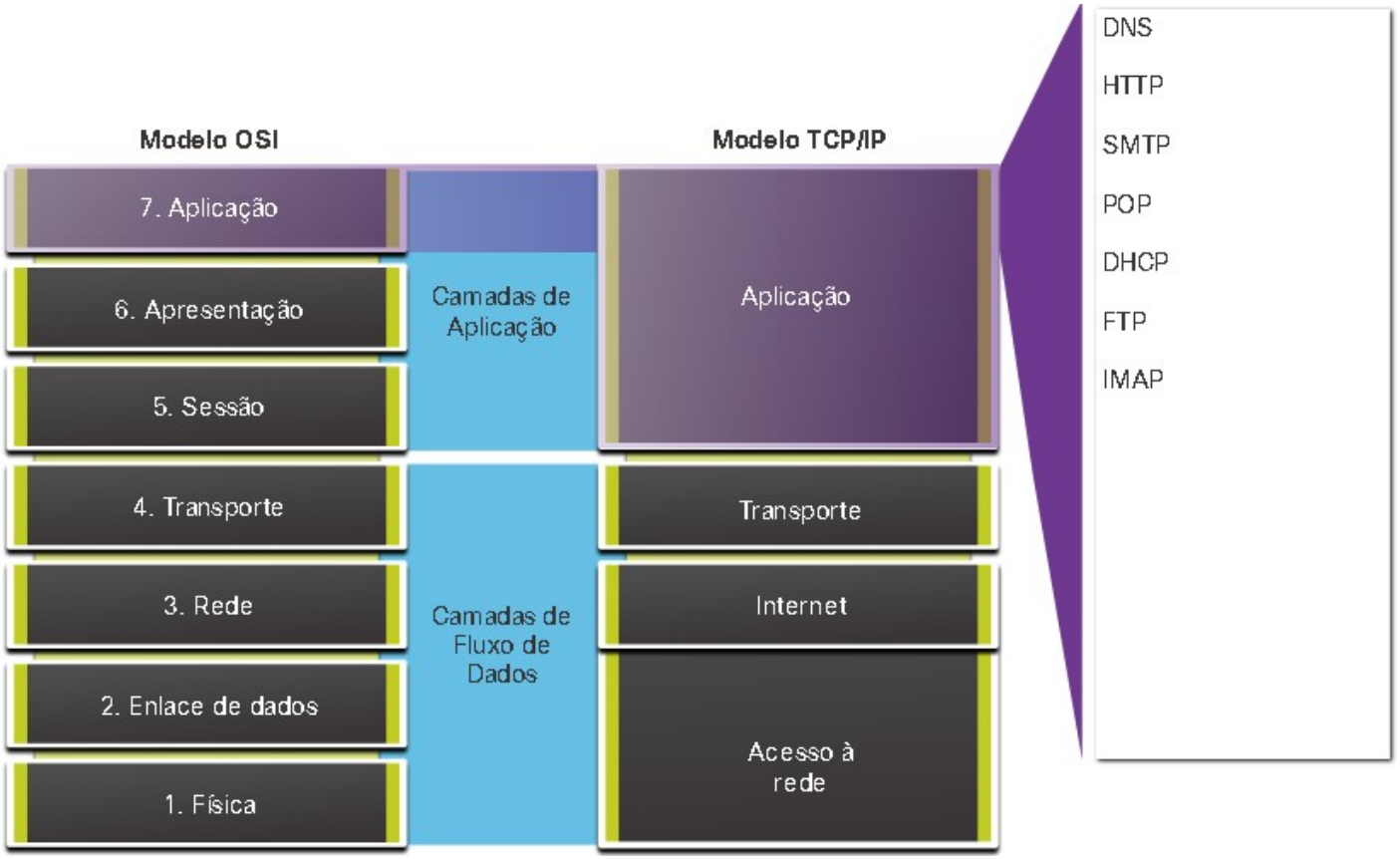
WOMENROCK-IT
Brasil 2021

Networking Academy

Camada de Aplicação



Aplicação, Apresentação e Sessão



Camada de Aplicação

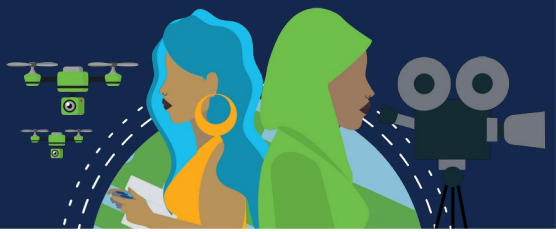
É a camada mais próxima do usuário final, que fornece a interface entre os aplicativos usados e a rede subjacente pela qual as mensagens são transmitidas. Os protocolos da camada de aplicação são utilizados para troca de dados entre programas executados nos hosts de origem e destino.

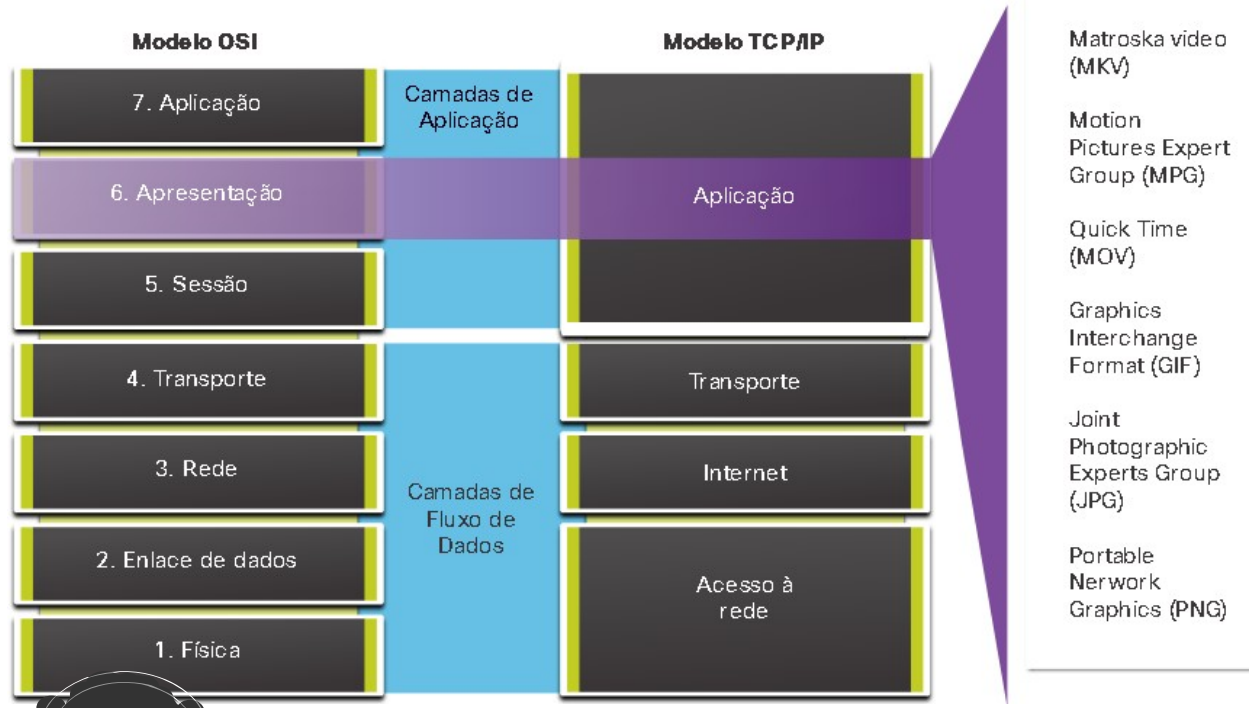
Com base no modelo TCP / IP, as três camadas superiores do modelo OSI (aplicativo, apresentação e sessão) definem funções da camada de aplicativo TCP / IP.

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

Fonte: Cisco

Aplicação, Apresentação e Sessão





Matroska video (MKV)

Motion Pictures Expert Group (MPG)

Quick Time (MOV)

Graphics Interchange Format (GIF)

Joint Photographic Experts Group (JPG)

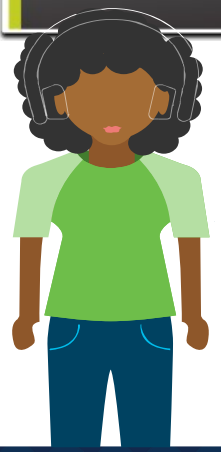
Portable Nerwork Graphics (PNG)

Camada de Apresentação

Possui três funções principais:

- Formatar dados no dispositivo de origem em um formato compatível para recebimento no host destino.
- Comprimir dados de uma maneira que possa ser descompactada pelo host destino.
- Criptografar dados para transmissão e descriptografar dados após o recebimento.

Ela formata dados para a camada de aplicação e define padrões para formatos de arquivo. Alguns padrões para vídeo incluem; *Matroska Video (MKV), Motion Picture Experts Group (MPG) e QuickTime Video (MOV)*.

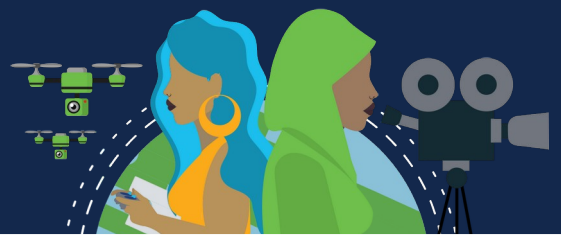


Alguns formatos de imagem são; *Graphics Interchange Format (GIF), o Joint Photographic Experts Group (JPG)* e *Portable Network Graphics (PNG)*.

Camada de sessão

As funções na camada de sessão criam e mantêm diálogos entre as aplicações origem e destino. Ela processa a troca de informações para iniciar diálogos, mantê-los ativos e reiniciar sessões interrompidas ou ociosas por um longo período.

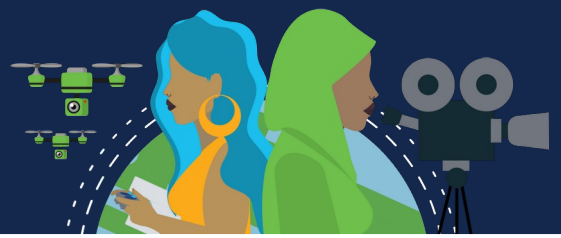
Fonte: Cisco



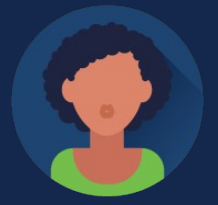
Aplicação, Apresentação e Sessão

Protocolos TCP/IP da Camada de Aplicação

Especificam o formato e as informações de controle necessárias para muitas funções comuns de comunicação da Internet. Os protocolos da camada de aplicação são utilizados pelos dispositivos de origem e destino durante uma sessão de comunicação. Para que as comunicações sejam bem-sucedidas, os protocolos da camada de aplicativo implementados no host de origem e destino devem ser compatíveis.



Aplicação, Apresentação e Sessão

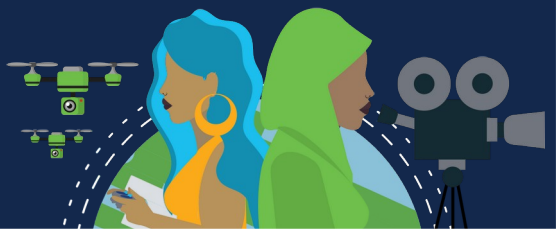


Protocolos TCP/IP da Camada de Aplicação

Tipo	Protocolo	Porta	Descrição
Sistemas de Nomes	DNS – Sistema de Nomes de Domínio (ou Serviço)	TCP, cliente UDP 53	Converte nomes de domínio, como cisco.com, em endereços IP.
Configuração do host	BOOTP – Protocolo de Bootstrap	Cliente UDP 68 Servidor 67	Permite que uma estação de trabalho sem disco descubra seu próprio endereço IP e carregue um arquivo na memória para inicializar a máquina. Em substituição pelo DHCP.
	DHCP – Protocolo de configuração de host dinâmico	Cliente UDP 68 Servidor 67	Atribui dinamicamente endereços IP.
Email	SMTP – Protocolo Simples de Transferência de Correio	TCP 25	Usado para envio de e-mails para um servidor de e-mail.
	POP3 – Protocolo da agência postal	TCP 110	Usado para recebimento de e-mails. Transfere o e-mail do servidor para a aplicação de correio local do cliente.
	IMAP – Protocolo de Acesso à Mensagem na Internet	TCP 143	Permite que os clientes acessem e-mails armazenados em um servidor de e-mail, mas mantém o e-mail no servidor.
Transferência de arquivo	FTP – Protocolo de Transferência de Arquivos	TCP 20 a 21	Protocolo de entrega de arquivos confiável, orientado à conexão. Permite que um usuário em um host acesse e transfira arquivos para outro host em uma rede.
	TFTP – Protocolo de Transferência de Arquivos Trivial	Cliente* UDP 69	Protocolo de transferência de arquivos simples e sem conexão, sem confirmação e de melhor esforço. Usa menos sobrecarga que o FTP.
WEB	HTTP – Protocolo de transferência de hipertexto	TCP 80, 8080	Conjunto de regras para a troca de texto, imagens gráficas, som, vídeo e outros arquivos multimídia na World Wide Web.
	HTTPS – HTTP seguro	TCP, UDP 443	O navegador usa criptografia para proteger conversações HTTP. Autentica o site ao qual você conecta o seu navegador.

Fonte: Cisco

Ponto a ponto

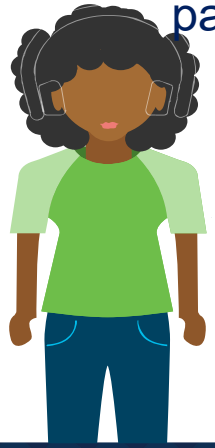


Modelo Cliente-Servidor

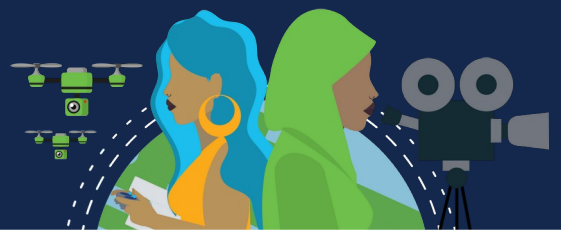
No modelo cliente / servidor, o dispositivo que solicita as informações é chamado de cliente e o dispositivo que responde à solicitação é chamado de servidor.

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

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



Fonte: Cisco



Ponto a ponto

Redes Ponto a ponto

No modelo ponto a ponto (P2P), os dados são acessados de um dispositivo sem usar um servidor exclusivo.

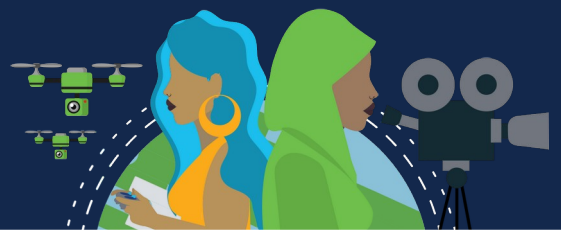
Inclui duas partes, com características semelhantes, mas que funcionam de maneira diferente: *redes P2P e aplicações P2P.*

Em uma rede P2P, dois ou mais computadores são conectados via rede e podem compartilhar recursos (como impressoras e arquivos) sem ter um servidor exclusivo. Cada dispositivo final conectado (conhecido como peer) pode funcionar como cliente ou servidor. Um computador pode assumir o papel de servidor para uma transação ao mesmo tempo em que é o cliente de outra. As funções de cliente e servidor são definidas de acordo com a requisição.

Além de compartilhar arquivos, uma rede como essa permitiria aos usuários ativar jogos em rede ou compartilhar uma conexão com a Internet.

Em uma comunicação peer-to-peer, ambos os dispositivos são considerados iguais no processo de comunicação. O ponto 1 tem arquivos compartilhados com o ponto 2 e pode acessar a impressora compartilhada diretamente conectada ao ponto 2 para imprimir arquivos. O ponto 2 está compartilhando a impressora conectada diretamente com o Peer 1 ao acessar os arquivos compartilhados no Peer 1.

Fonte: Cisco

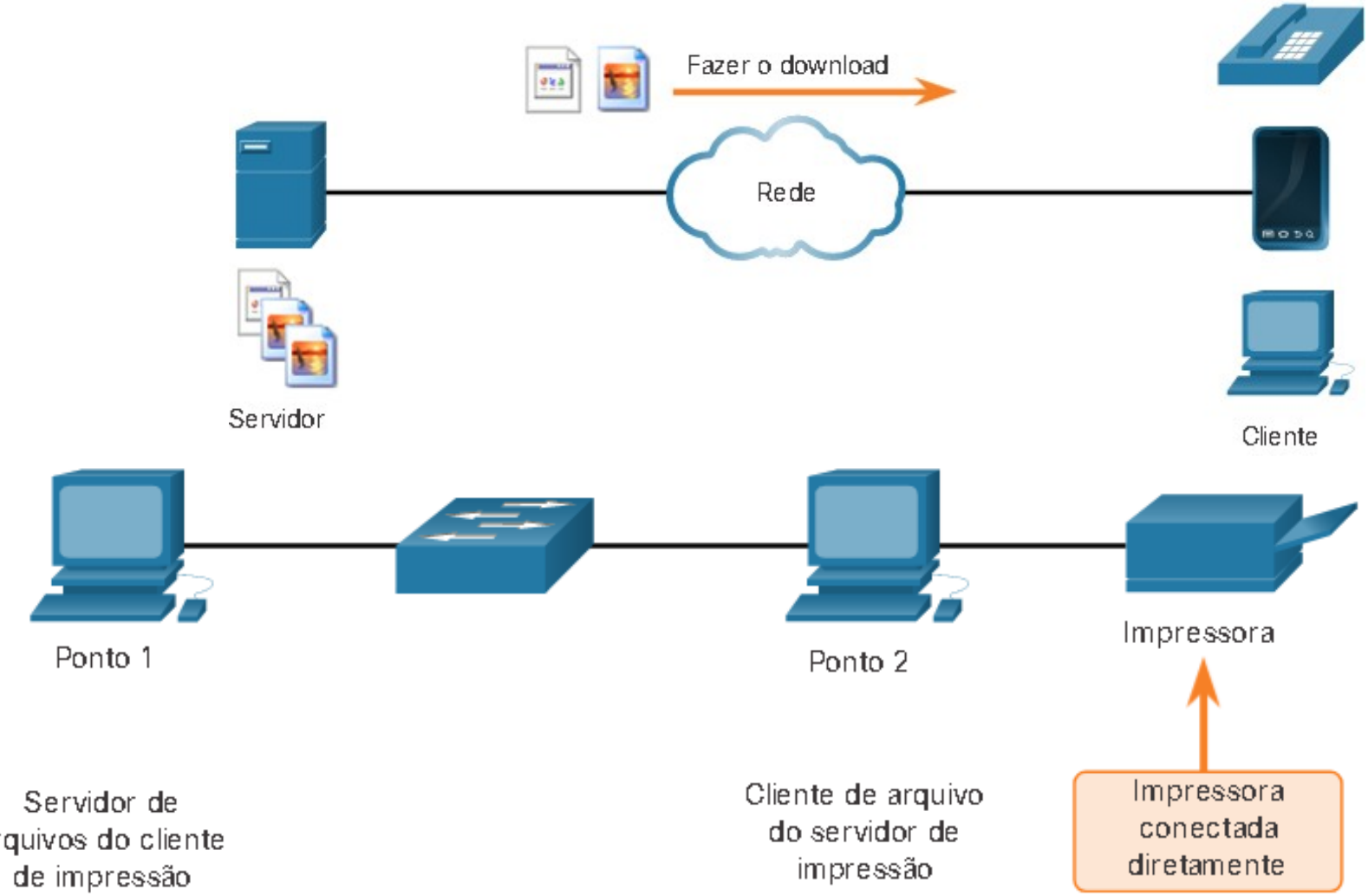


Ponto a ponto

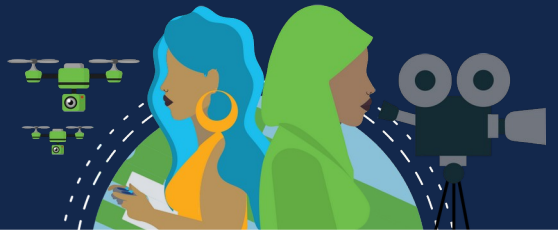
Modelo Cliente-Servidor

Redes Ponto a ponto

Redes Ponto a ponto



Fonte: Cisco

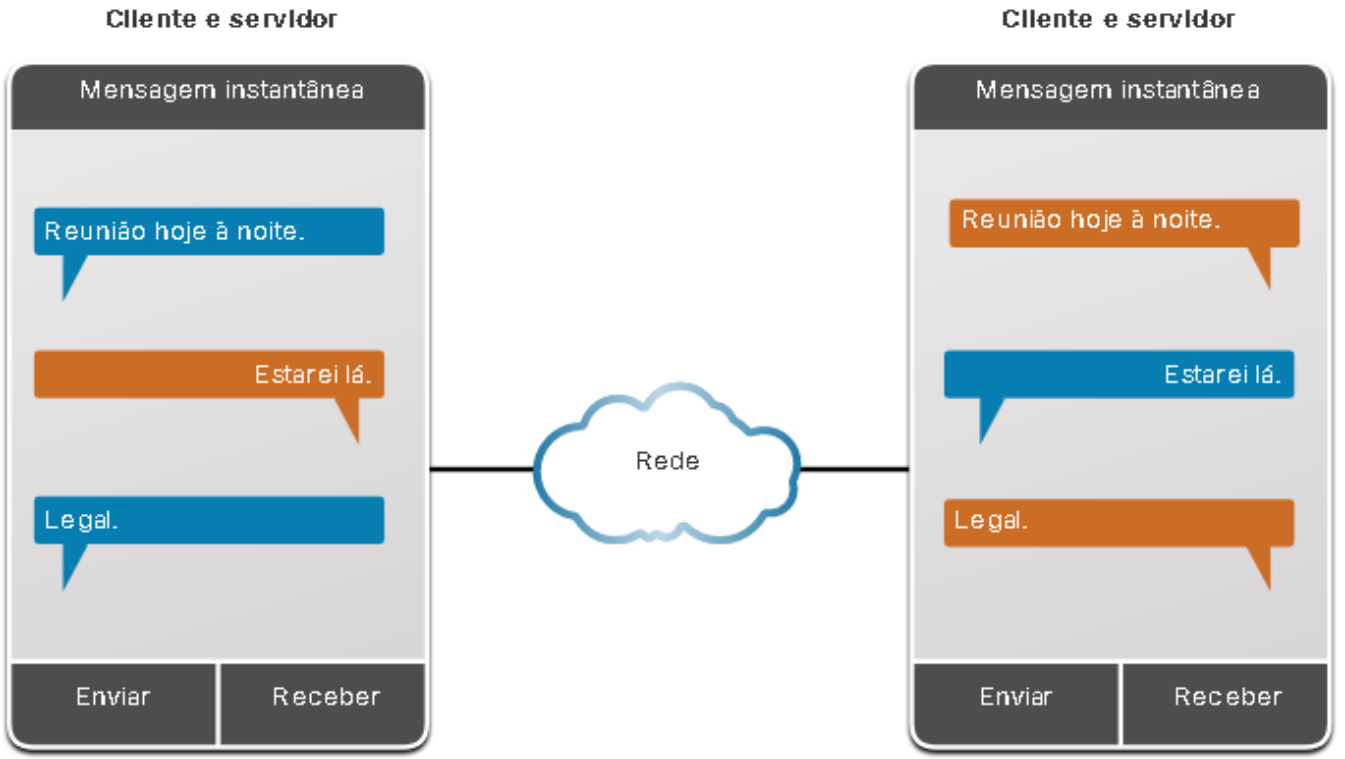


Ponto a ponto

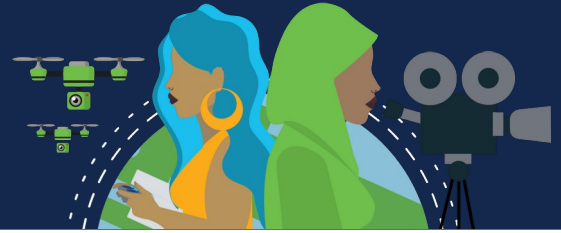
Aplicação entre pares (peer-to-peer)

Um aplicação P2P permite que um dispositivo atue como cliente e servidor na mesma comunicação. Todo cliente é um servidor e todo servidor é um cliente. Aplicações P2P exigem que cada dispositivo final forneça uma interface de usuário e execute um serviço em segundo plano.

Algumas aplicações P2P utilizam um sistema híbrido no qual o compartilhamento de recursos é descentralizado, mas os índices que apontam para as localizações de recursos são armazenados em um diretório centralizado. Em um sistema híbrido, cada peer acessa um servidor de índice para obter a localização de um recurso armazenado em outro peer.



Fonte: Cisco



Ponto a ponto

Aplicações P2P Comuns

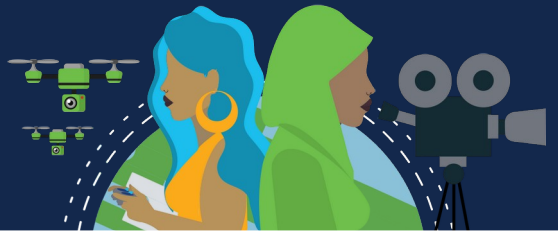
Aplicações P2P; cada computador na rede executando o aplicativo pode atuar como cliente ou servidor para os outros computadores que também estão executando o aplicativo, como*; BitTorrent, Direct Connect, eDonkey e Freenet.*

Alguns usam o protocolo **Gnutella**, que permite que os usuários compartilhem arquivos completos com outros usuários. O software cliente compatível com Gnutella permite que os usuários se conectem aos serviços Gnutella pela Internet e localizem e acessem recursos compartilhados por outros colegas Gnutella. Muitos aplicativos cliente Gnutella estão disponíveis, incluindo *µTorrent, BitComet, DC++, Deluge e emule*.

Alguns permitem que os usuários compartilhem trechos de vários arquivos entre si ao mesmo tempo. Os clientes usam um arquivo torrent para localizar outros usuários com as peças de que precisam, para que possam se conectar diretamente a eles. Este arquivo também contém informações sobre os computadores rastreadores que controlam quais usuários possuem partes específicas de determinados arquivos. Os clientes solicitam peças de vários usuários ao mesmo tempo. Isso é conhecido como enxame e a tecnologia é chamada **BitTorrent**. BitTorrent tem seu próprio cliente. Mas existem muitos outros clientes BitTorrent, incluindo *uTorrent, Deluge e qBittorrent*.

Qualquer tipo de arquivo pode ser compartilhado entre usuários. Muitos desses arquivos são protegidos por direitos autorais, o que significa que apenas o autor tem o direito de distribuí-lo. É ilegal baixar ou distribuir arquivos protegidos por direitos autorais, sem a permissão do detentor desses direitos. A violação dos direitos autorais pode resultar em ações criminais e cíveis.

Fonte: Cisco



Protocolos de E-mail e Web

HTTP e HTML

Protocolos específicos da camada de aplicativo são projetados para usos comuns, como navegação na Web e e-mail. Quando uma URL é digitada em um navegador, ele estabelece uma conexão com o serviço da Web em execução em um servidor utilizando o protocolo HTTP. URLs *(Uniform Resource Locator)* e URIs *(Uniform Resource Identifiers)* são os nomes associados aos endereços da Web.

Interação entre navegador e o servidor da web para abrir a página web http://www.cisco.com/index.html.

Etapa 1: O navegador interpreta como três partes da URL:

- http (o protocolo ou esquema)
- www.cisco.com (o nome do servidor)
- index.html (o nome do arquivo específico solicitado)

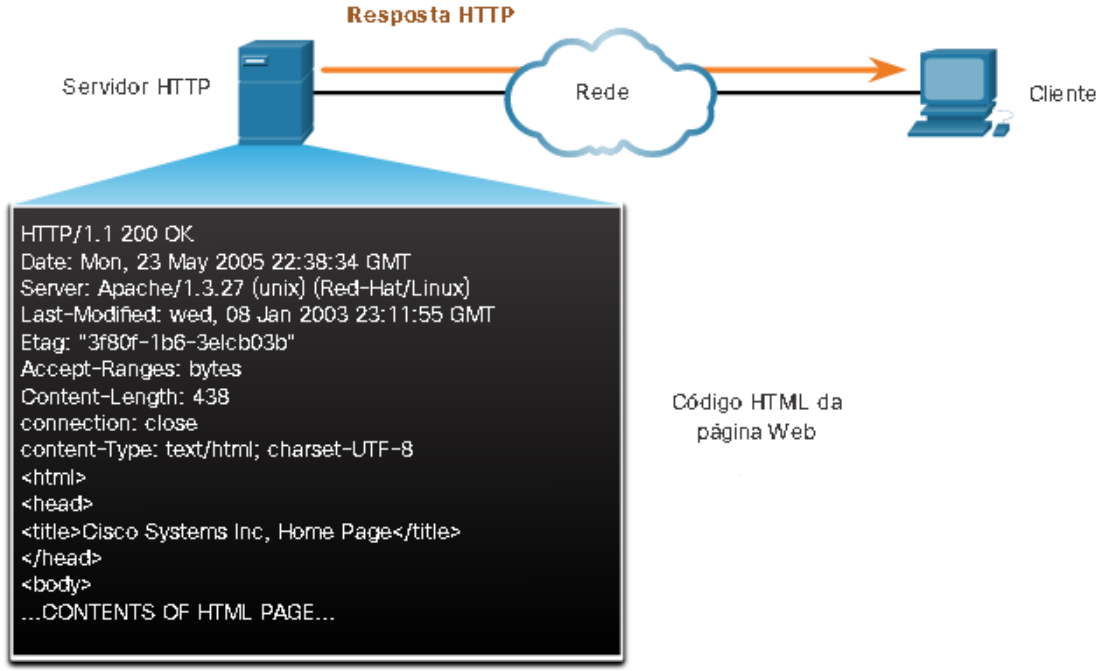
Etapa 2: O navegador verifica com um servidor de nomes para converter www.cisco.com em um endereço IP numérico, usado para conectar-se ao servidor. O cliente inicia uma solicitação HTTP para um servidor enviando uma solicitação GET para o servidor e solicita o arquivo index.html.

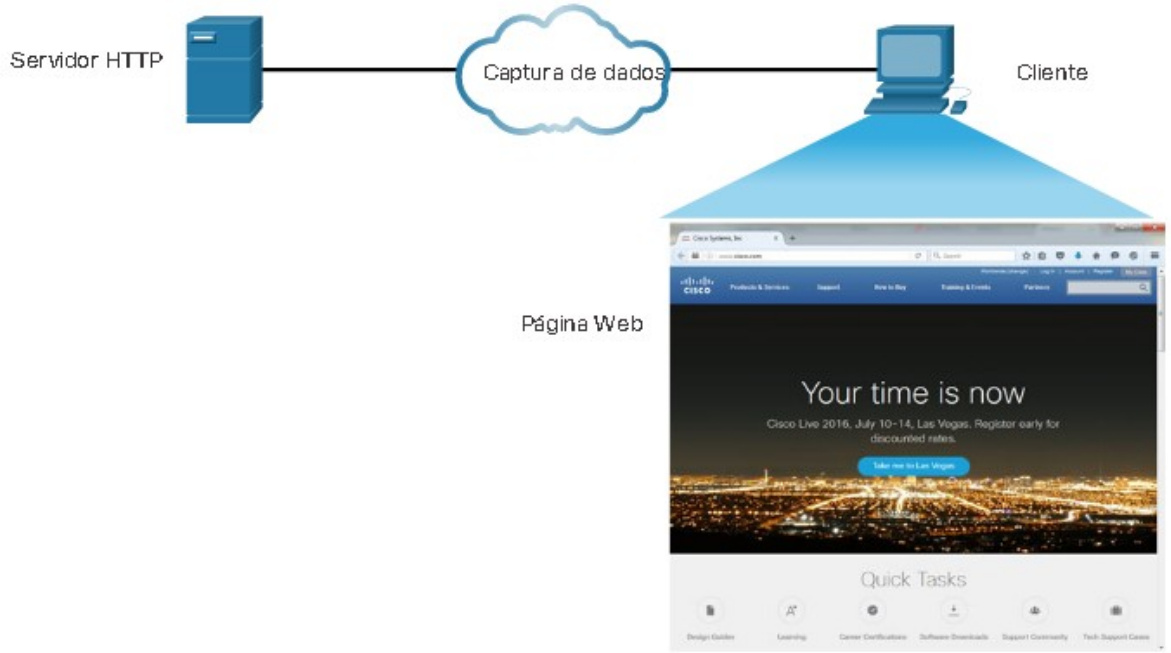
Fonte: Cisco

Protocolos de E-mail e Web

HTTP e HTML

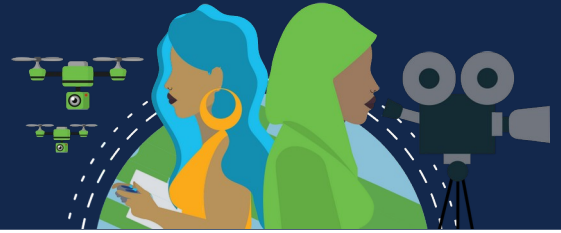
Etapa 3: Em resposta à solicitação, o servidor envia o código HTML para esta página da Web para o navegador.





Etapa 4: O navegador decifra o código HTML e formata a página da janela do navegador.

Fonte: Cisco



Protocolos de E-mail e Web

HTTP e HTTPS

O HTTP é um protocolo de requisição/resposta. Ao enviar uma requisição a um servidor Web, é o HTTP quem especifica os tipos de mensagem usados nessa conversação. Os três tipos de mensagens comuns são:

GET: Um cliente (navegador Web) envia a mensagem GET ao servidor Web para requisitar páginas HTML.

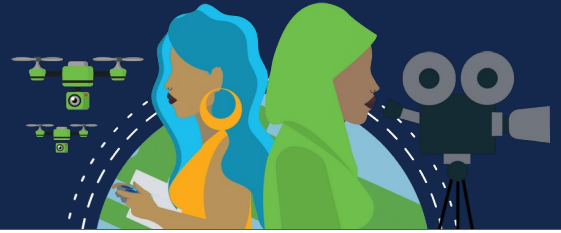
POST: Carrega arquivos de dados no servidor da web, como dados do formulário.

PUT: Carrega conteúdo para o servidor da web, como uma imagem.

Embora o HTTP seja notavelmente flexível, não é um protocolo seguro. As mensagens de solicitação enviam informações ao servidor em texto sem formatação que podem ser interceptadas e lidas. As respostas do servidor, normalmente páginas HTML, também não são criptografadas.

Para comunicação segura na Internet, é usado o protocolo HTTP Secure (HTTPS). O HTTPS utiliza autenticação e criptografia para proteger dados durante o trajeto entre o cliente e o servidor. O HTTPS usa o mesmo processo de requisição do cliente, resposta do servidor do HTTP, mas o fluxo de dados é criptografado com SSL antes de ser transportado através da rede.

Fonte: Cisco



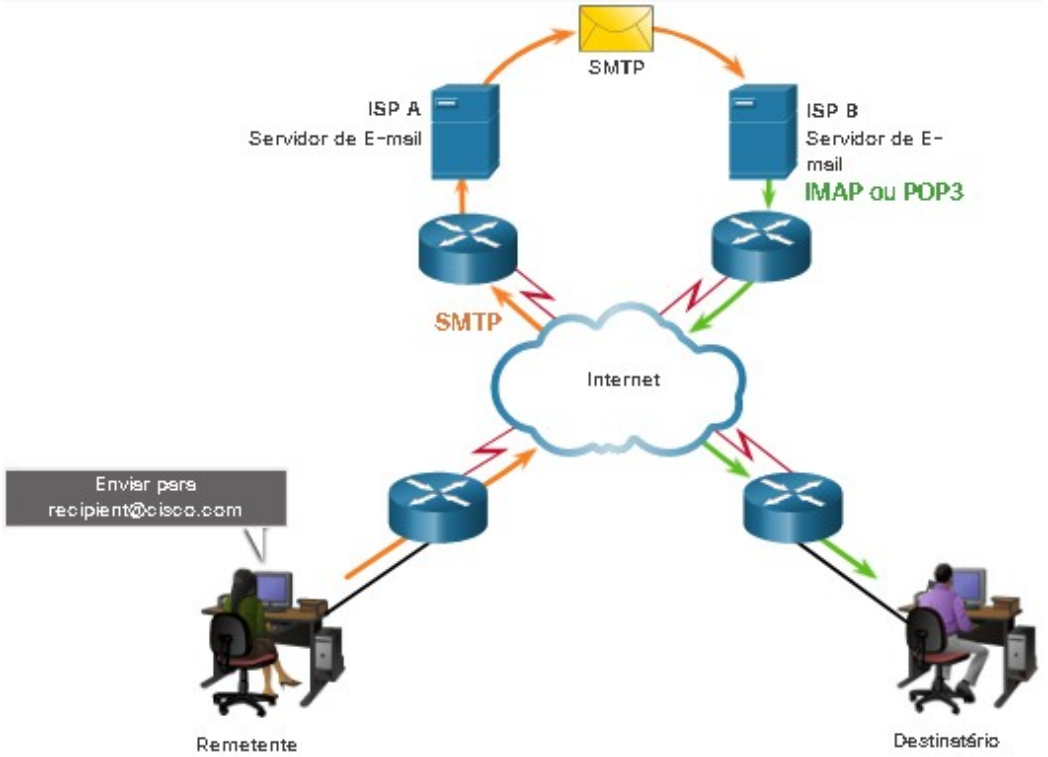
Protocolos de E-mail e Web

Protocolos de E-mail

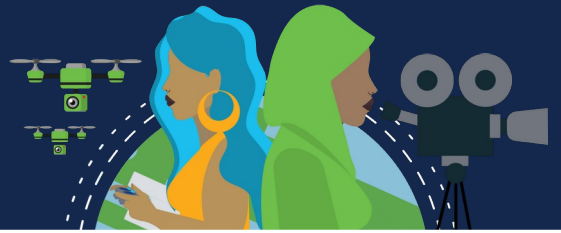
Um dos serviços básicos oferecidos por um ISP é a hospedagem de e-mails. O e-mail é um método de armazenar e encaminhar, de enviar e de recuperar mensagens eletrônicas em uma rede. Mensagens de e-mail são armazenadas nos bancos de dados em servidores de e-mail.

Clientes de e-mail se comunicam com servidores de e-mail para enviar e receber e-mails. Servidores de e-mail se comunicam com outros servidores de e-mail para transportar mensagens de um domínio para outro. Um cliente de e-mail não se comunica diretamente com outro, eles precisam dos servidores para transportar mensagens.

Três protocolos separados são usados para a operação: **SMTP, POP** e **IMAP**. O processo da camada de aplicação que envia e-mail usa o SMTP. Um cliente recupera e-mails usando os protocolos *POP* ou *IMAP*.



Fonte: Cisco



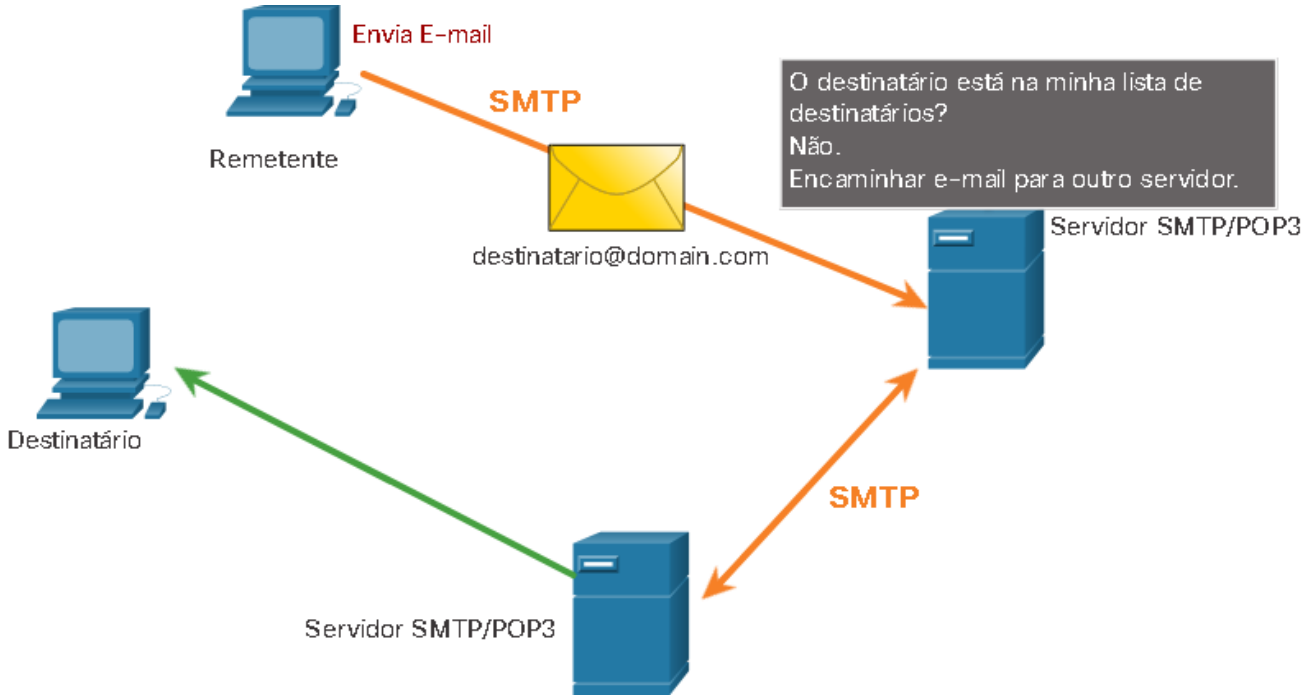
Protocolos de E-mail e Web

SMTP, POP e IMAP

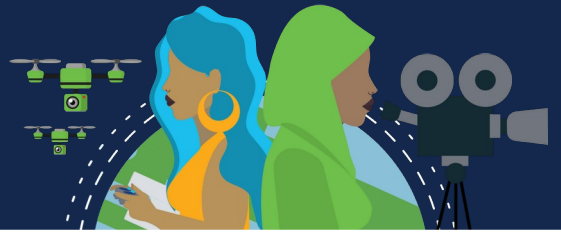
SMTP: O formato de mensagens SMTP exige um cabeçalho e um corpo de mensagem. O corpo da mensagem pode conter qualquer tamanho, o cabeçalho deve ter um endereço de e-mail do destinatário e um endereço do remetente.

Ao enviar um e-mail, o processo SMTP do cliente se conecta com o processo SMTP do servidor na porta 25. A mensagem é enviada ao servidor depois que a conexão é feita. Ao receber a mensagem, ou o servidor a coloca em uma conta local, ou encaminha a mensagem para outro servidor de correio para entrega.

Quando o servidor de e-mail de destino estiver off-line ou ocupado, o SMTP armazenará as mensagens para envio e periodicamente, verificará se há mensagens na fila para novo envio. Se a mensagem não for entregue após um período pré-determinado de expiração, ela é devolvida ao remetente como não entregue.



Fonte: Cisco



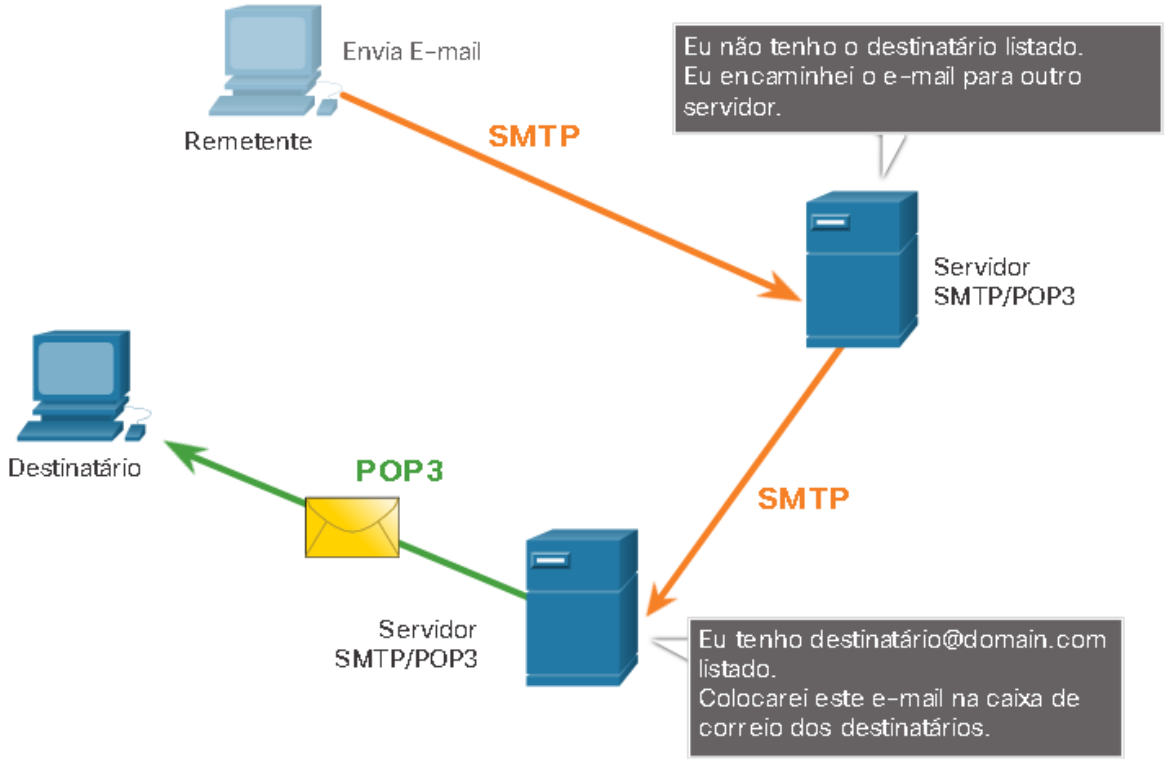
Protocolos de E-mail e Web

SMTP, POP e IMAP

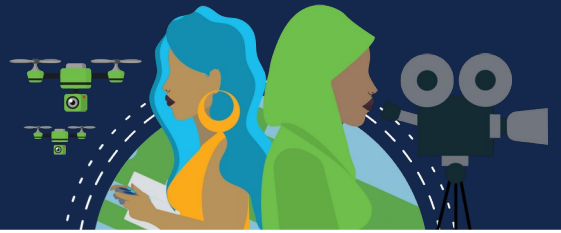
POP: É usado para recuperar e-mails de um servidor de e-mail. Após ser transferido do servidor ao cliente o e-mail é excluído do servidor. Esta é a operação padrão do POP.

O servidor inicia o serviço POP ao escutar de forma passiva a porta TCP 110 por requisições de conexão dos clientes. Quando um cliente deseja fazer uso do serviço, ele envia uma solicitação para estabelecer uma conexão TCP com o servidor. Ao estabelecer a conexão, o servidor POP envia uma saudação. O cliente e o servidor POP trocam comandos e respostas até que a conexão seja encerrada ou cancelada.

As mensagens de e-mail são baixadas para o cliente e removidas do servidor, portanto não há um local centralizado onde as mensagens de e-mail sejam mantidas. POP3 é a versão mais usada.



Fonte: Cisco

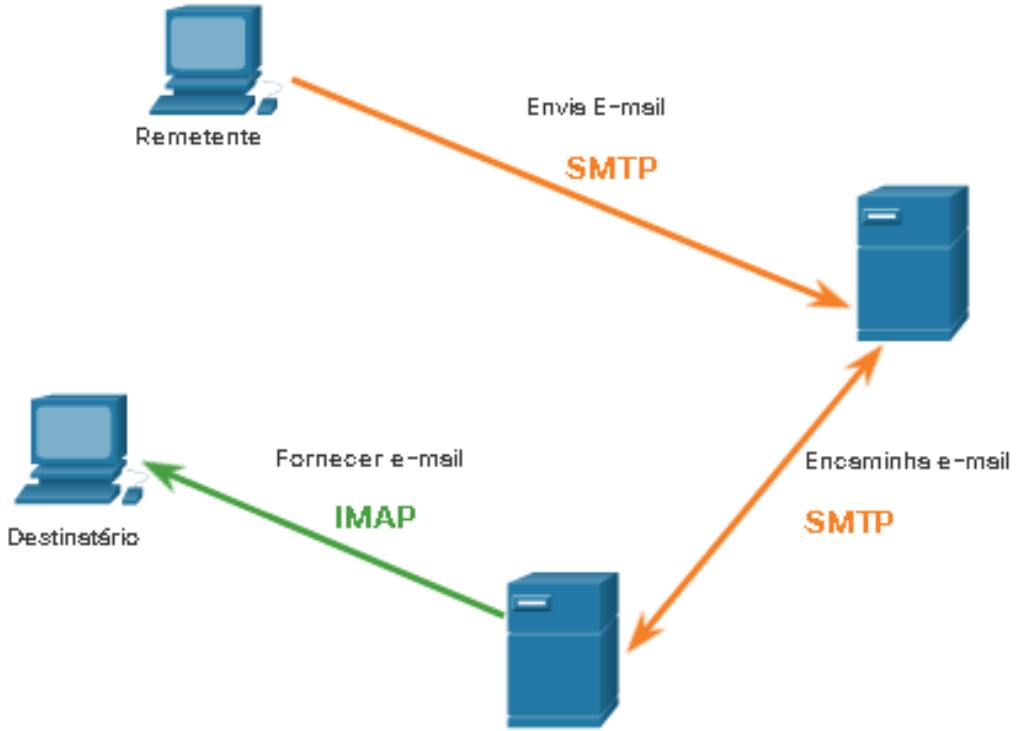


Protocolos de E-mail e Web

SMTP, POP e IMAP

IMAP: Ao contrário do POP, quando o usuário se conecta a um servidor IMAP, cópias das mensagens são baixadas para o aplicativo cliente e as mensagens originais são mantidas no servidor até que sejam excluídas manualmente.

Os usuários podem criar uma hierarquia de arquivos no servidor para organizar e armazenar o e-mail. A estrutura de arquivos é duplicada no cliente de e-mail também. Quando um usuário decide excluir uma mensagem, o servidor sincroniza essa ação e exclui a mensagem do servidor.



Fonte: Cisco

Serviços de Endereçamento IP

Serviço de Nomes de Domínio (DNS)

Em redes de dados, os dispositivos são rotulados com endereços IP numéricos para enviar e receber dados pelas redes. Os *nomes de domínio* foram criados para converter o endereço numérico em um nome simples e reconhecível.

Na internet, nomes de domínio totalmente qualificados (FQDNs), como (http://www.cisco.com), são muito mais fáceis de lembrar do que 198.133.219.25. Se a Cisco decidir alterar o endereço numérico de www.cisco.com, ele será transparente ao usuário, porque o nome de domínio permanecerá o mesmo. O novo endereço é simplesmente vinculado ao nome de domínio atual e a conectividade é mantida.

O protocolo DNS define um serviço automatizado que compara nomes de recursos com o endereço de rede numérico requisitado. Ele inclui o formato para consultas, respostas e dados. As comunicações do protocolo DNS utilizam um único formato, chamado de mensagem, utilizado para todos os tipos de consultas de cliente e respostas de servidor, mensagens de erro e transferência de informações de registro de recursos entre servidores.

Fonte: Cisco

Serviços de Endereçamento IP

Serviço de Nomes de Domínio (DNS)

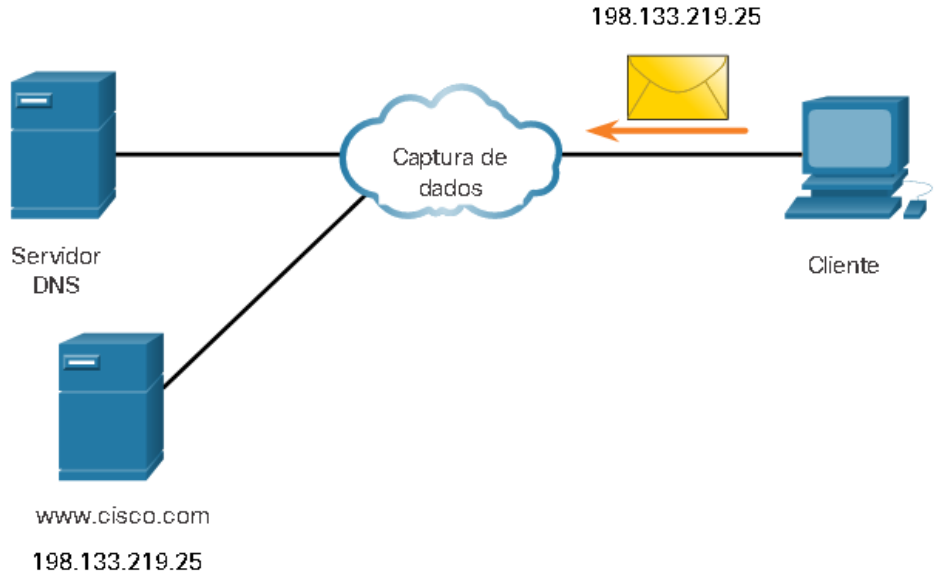
Etapa 1: O usuário digita um FQDN em um campo Endereço do aplicativo do navegador.

Etapa 2: Uma consulta DNS é enviada para o servidor DNS designado para o computador cliente.

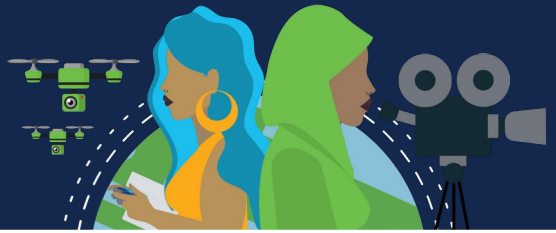
Etapa 3: O servidor DNS corresponde ao FQDN com seu endereço IP.

Etapa 4: A resposta da consulta DNS é enviada de volta ao cliente com o endereço IP do FQDN.

Etapa 5: O computador cliente usa o endereco IP para fazer solicitações do servidor.



Fonte: Cisco



Serviços de Endereçamento IP

Formato de Mensagem DNS

O servidor DNS armazena diferentes tipos de registros usados para resolver nomes. Esses registros contêm o nome, endereço e tipo de registro;

A: Um endereço IPv4 do dispositivo final.
NS: Um servidor de nomes com autoridade.
AAAA: Um endereço IPv6 do dispositivo final (pronunciado quad-A).
MX: Um registro de mail exchange.

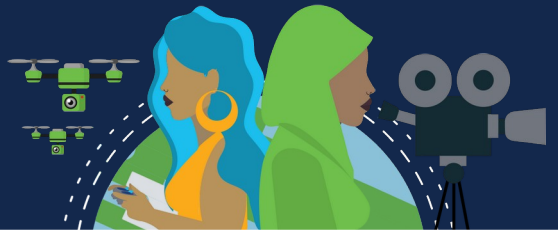
Ao receber uma consulta, o processo DNS do servidor primeiro examina seus próprios registros para resolver o nome. Se não conseguir, ele entrará em contato com outros servidores. Ao encontrar uma correspondência o servidor temporariamente armazena o número do endereço em questão, no caso do mesmo nome ser requisitado outra vez.

O serviço de DNS do Windows também armazena nomes resolvidos. O comando **ipconfig /displaydns** exibe todas as entradas DNS em cache.

O DNS usa o mesmo formato de mensagem entre servidores, consistindo em uma pergunta, resposta, autoridade e informações adicionais para todos os tipos de consultas de cliente e respostas de servidor, mensagens de erro e transferência de informações de registro de recursos.

DNS message section	Description
Question	The question for the name server
Answer	Resource Records answering the question
Authority	Resource Records pointing toward an authority
Additional	Resource Records holding additional information

Fonte: Cisco



Serviços de Endereçamento IP

Hierarquia DNS

O protocolo DNS usa um sistema hierárquico para criar um banco de dados para fornecer resolução de nomes.

A estrutura de nomenclatura é dividida em zonas pequenas, gerenciáveis. Cada servidor DNS mantém um arquivo de banco de dados específico e só é responsável por gerenciar os mapeamentos de nome para IP para essa pequena parte da estrutura DNS. Quando um servidor DNS recebe uma requisição para a conversão de um nome que não faça parte da sua zona DNS, o servidor DNS a encaminha para outro servidor DNS na zona apropriada para a tradução. O DNS é escalável porque a resolução do nome do host está espalhada por vários servidores.

Os diferentes domínios de nível superior representam o tipo de organização ou país de origem. Exemplos de domínios de nível superior são os seguintes:

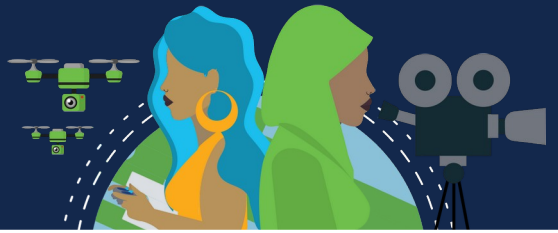
.com: uma empresa ou indústria

.org: uma organização sem fins lucrativos

.au: Austrália

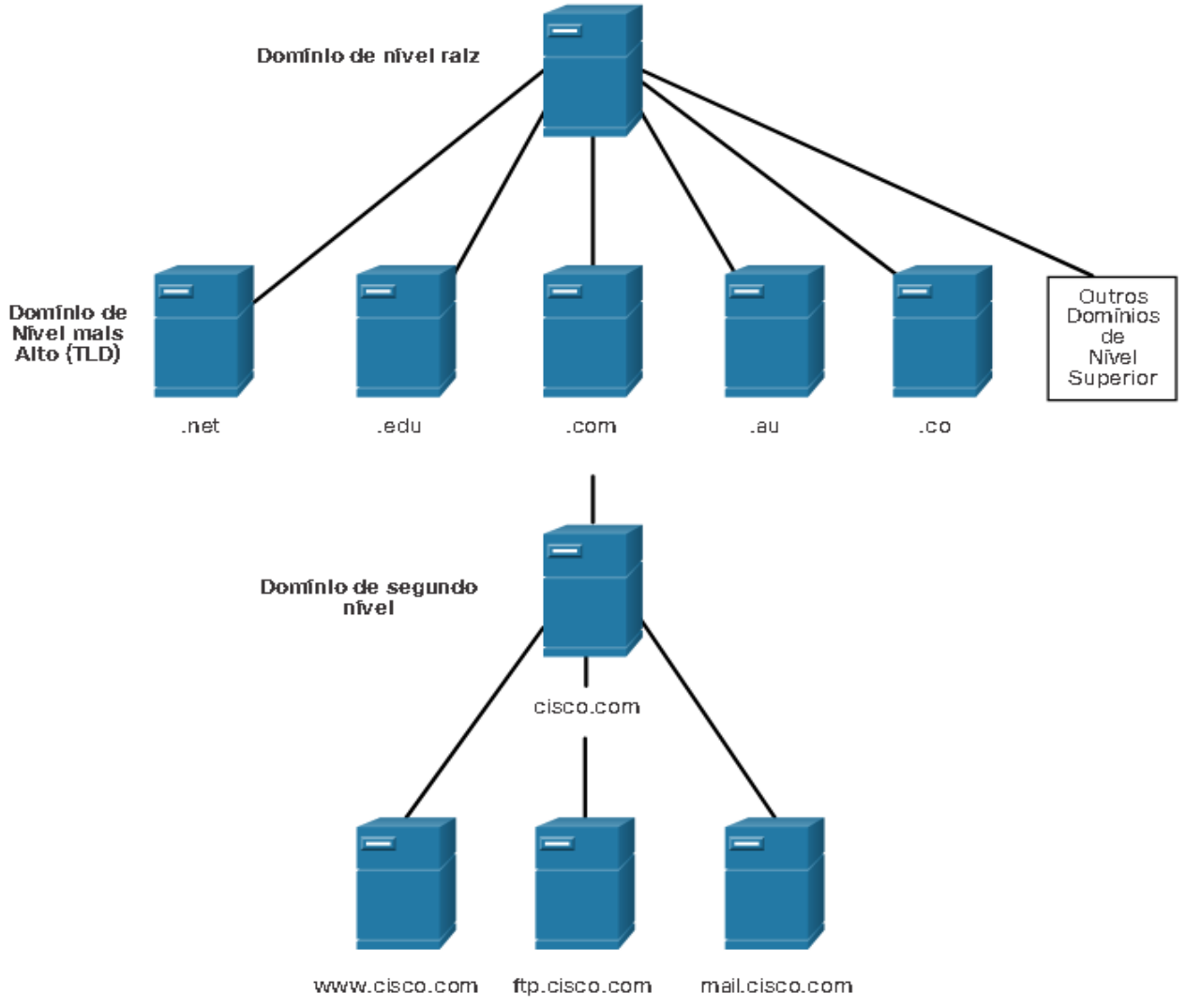
.co: Colômbia

Fonte: Cisco

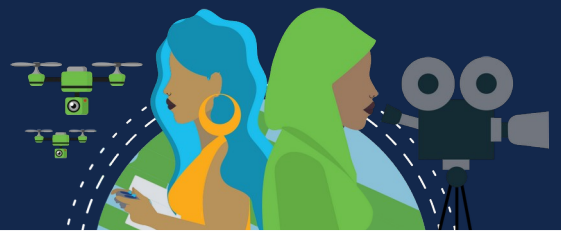


Serviços de Endereçamento IP

Hierarquia DNS



Fonte: Cisco



Serviços de Endereçamento IP

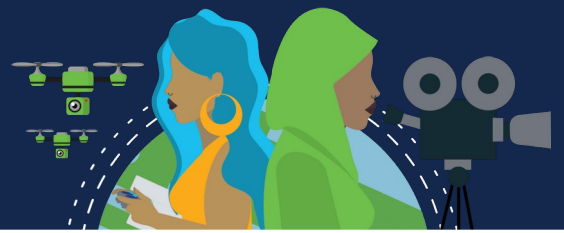
O Comando nslookup

Ao configurar um dispositivo de rede, um ou mais endereços de servidor DNS são fornecidos para que o cliente DNS possa usá-los na resolução de nomes. O ISP fornece os endereços a serem usados nos servidores DNS. Quando um aplicativo de usuário solicita a conexão a um dispositivo remoto por nome, o cliente DNS solicitante consulta o servidor de nomes para resolver o nome para um endereço numérico.

O utilitário **Nslookup** permite ao usuário consultar manualmente os servidores de nomes para resolver um determinado nome de host. Também usado para corrigir problemas de resolução de nomes e verificar o status atual dos servidores de nomes, com muitas opções para testes e verificações extensivas do processo DNS.

```
C:\Users> nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183
> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    origin-www.cisco.com
Addresses:  2001:420:1101:1::a
          173.37.145.84
Aliases:  www.cisco.com
> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    cisco.netacad.net
Address:  72.163.6.223
```

Fonte: Cisco



Serviços de Endereçamento IP

Protocolo de Configuração Dinâmica de Host (DHCP)

Endereçamento dinâmico: O serviço DHCP para IPv4 torna automática a atribuição de endereços IPv4, máscaras de sub-rede, gateways e outros parâmetros de rede IPv4.

Endereçamento estático: O administrador de redes insere manualmente informações de endereço IP em hosts.

Quando um host está conectado à Internet, o servidor DHCP é contatado e um endereço é requisitado. O servidor DHCP escolhe um endereço de uma lista configurada de endereços chamada **pool** e o atribui ao host por um período de tempo configurável, chamado **período de concessão**. Quando o período de concessão expira ou uma mensagem DHCPRELEASE é recebida, o endereço é retornado ao pool DHCP para reutilização.

O servidor DHCP na maioria das redes médias a grandes normalmente é um PC com um serviço dedicado. Em redes residenciais o serviço é localizado no roteador local que conecta a rede residencial ao ISP.

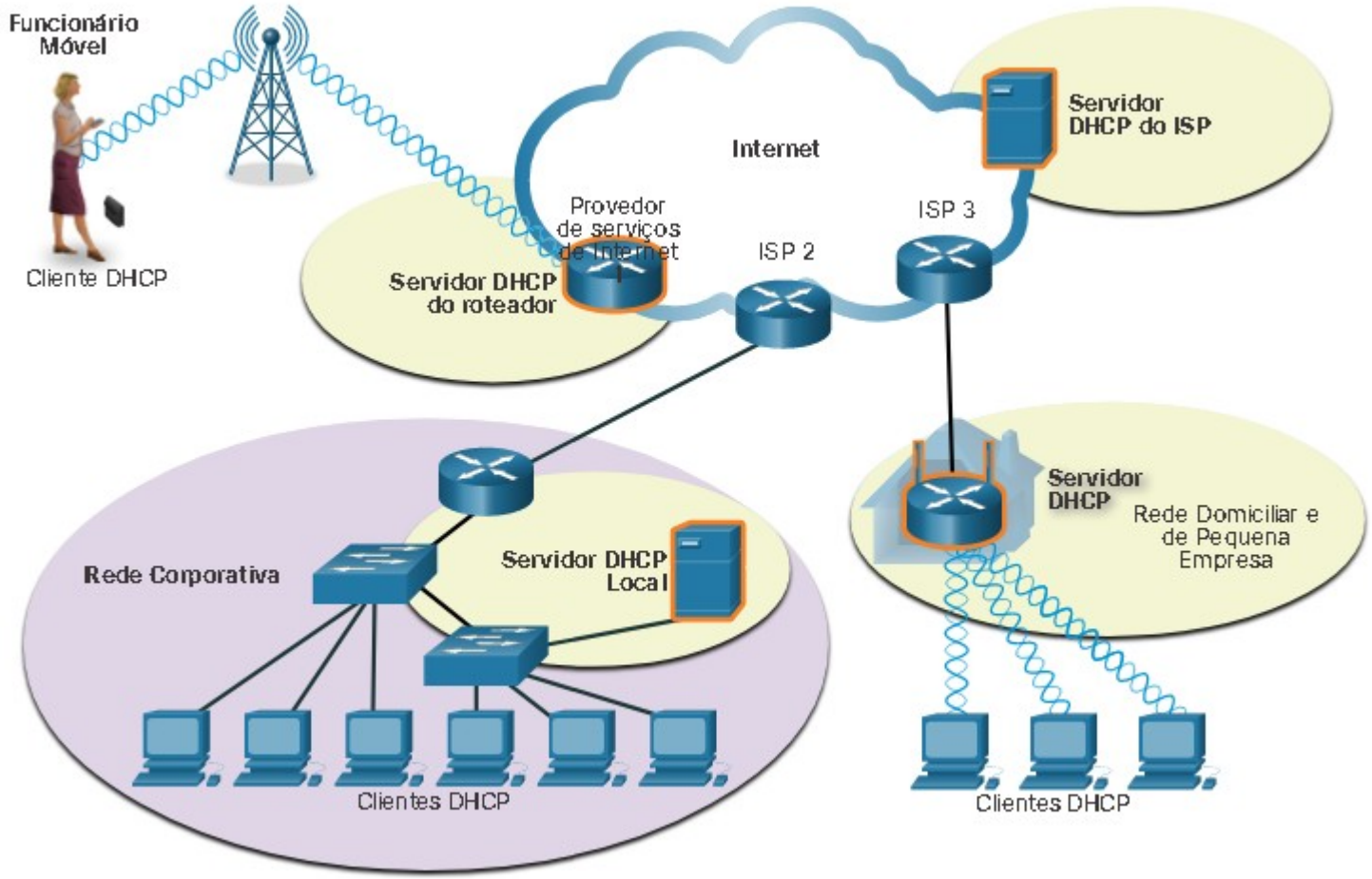
Muitas redes utilizam DHCP e endereçamento estático. O DHCP é usado para hosts de uso geral, como dispositivos de usuário final. O endereçamento estático é usado para dispositivos de rede, como roteadores de gateway, comutadores, servidores e impressoras.

O DHCP para IPv6 (DHCPv6) fornece serviços semelhantes para clientes IPv6. Uma diferença importante é que o DHCPv6 não fornece o endereço do gateway padrão. Isso só pode ser obtido dinamicamente a partir da mensagem Anúncio do roteador.

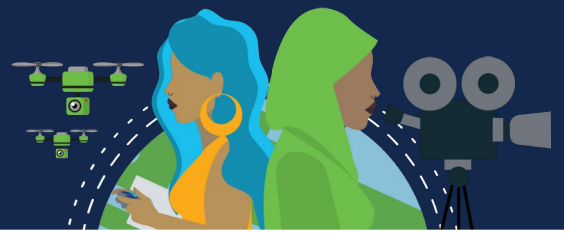
Fonte: Cisco

Serviços de Endereçamento IP

Protocolo de Configuração Dinâmica de Host (DHCP)



Fonte: Cisco



Serviços de Endereçamento IP

Operação do DHCP

Quando um dispositivo IPv4 configurado com DHCP inicia ou se conecta à rede, o cliente transmite uma mensagem de descoberta DHCP (DHCPDISCOVER) para identificar qualquer servidor DHCP disponível na rede. Um servidor DHCP responde com uma mensagem de oferta DHCP (DHCPOFFER), que oferece uma locação ao cliente. A mensagem de oferta contém o endereço IPv4 e a máscara de sub-rede a serem atribuídos, o endereço IPv4 do servidor DNS e o endereço IPv4 do gateway padrão. A oferta de locação também inclui a duração da locação.

O cliente pode receber várias mensagens DHCPOFFER, caso exista mais de um servidor DHCP na rede local. Portanto, deve escolher entre eles e transmitir uma mensagem de requisição de DHCP (DHCPREQUEST) que identifique o servidor explícito e a oferta de locação que o cliente está aceitando. Um cliente também pode decidir requisitar um endereço que já havia sido alocado pelo servidor.

Presumindo que o endereço IPv4 requisitado pelo cliente, ou oferecido pelo servidor, ainda seja válido, o servidor retornará uma mensagem de confirmação DHCP (DHCPACK) que confirma para o cliente que a locação foi finalizada. Se a oferta não é mais válida, o servidor selecionado responde com uma mensagem de confirmação negativa DHCP (DHCPNAK). Se uma mensagem DHCPNAK for retornada, o processo de seleção deverá recomeçar com a transmissão de uma nova mensagem DHCPDISCOVER. Quando o cliente tiver a locação, ela deverá ser renovada por outra mensagem DHCPREQUEST antes do vencimento.

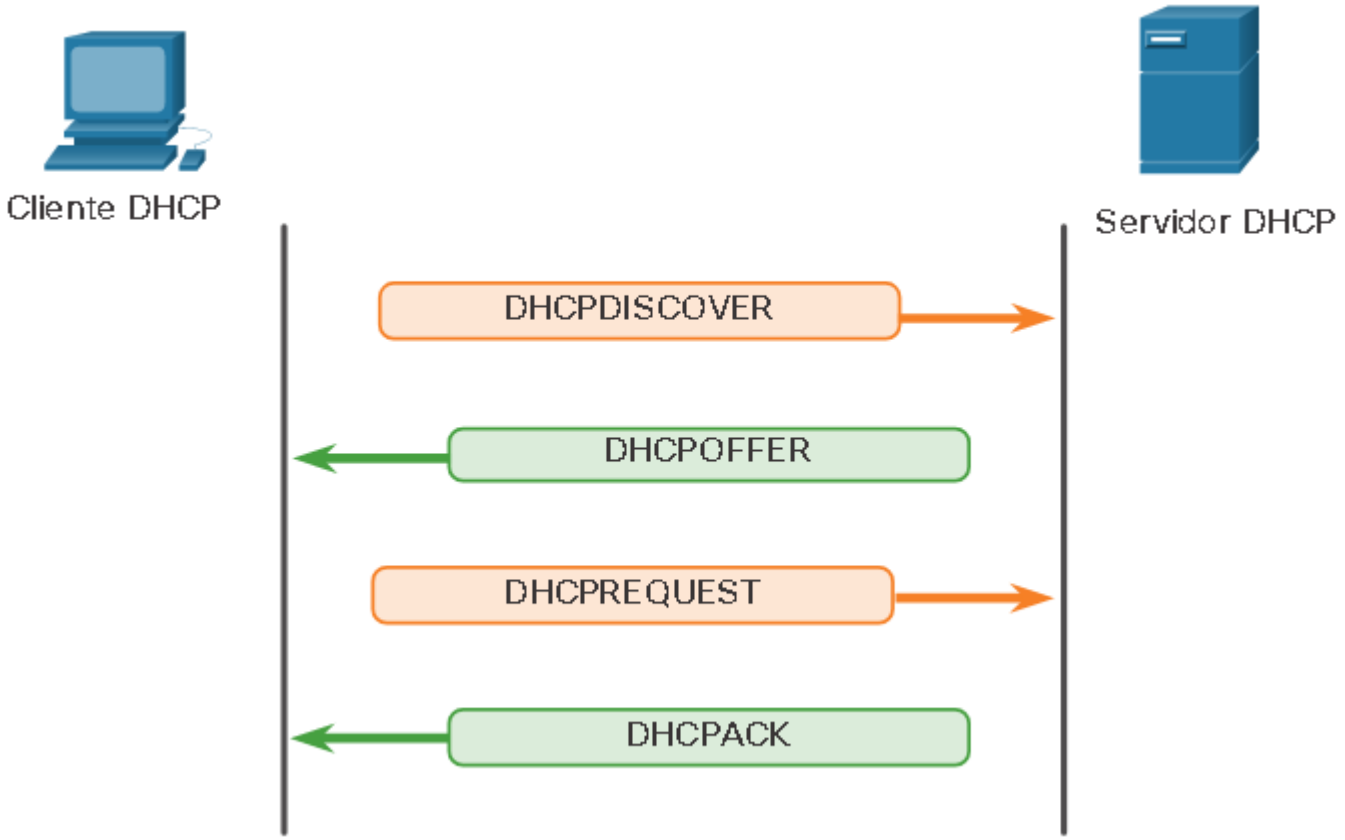
Fonte: Cisco

Serviços de Endereçamento IP

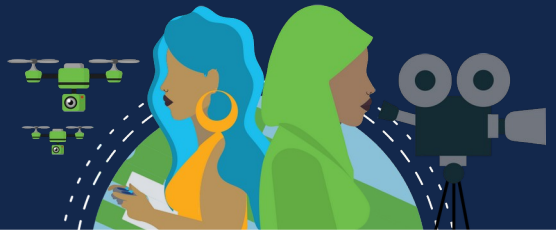
Operação do DHCP

O servidor DHCP garante que todos os endereços IP sejam exclusivos (um mesmo endereço IP não pode ser atribuído a dois dispositivos de rede diferentes simultaneamente). A maioria dos ISPs usa o DHCP para alocar endereços para seus clientes.

O DHCPv6 possui um conjunto de mensagens semelhantes às do DHCPv4. As mensagens DHCPv6 são SOLICIT, ADVERTISE, INFORMATION REQUEST, e REPLY.



Fonte: Cisco



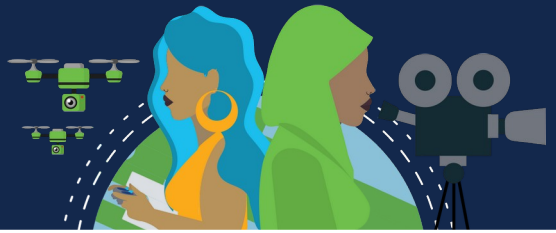
Serviços de Compartilhamento de Arquivos

Protocolo FTP

No modelo cliente/servidor, o cliente pode carregar dados para um servidor e baixar dados de um servidor, se ambos os dispositivos estiverem usando um protocolo de transferência de arquivos (FTP). Como HTTP, e-mail e protocolos de endereçamento, FTP é comumente usado protocolo de camada de aplicativo.

O FTP foi desenvolvido para possibilitar transferências de arquivos entre um cliente e um servidor. Um cliente FTP é um aplicativo que é executado em um computador que está sendo usado para enviar e receber dados de um servidor FTP.

Fonte: Cisco



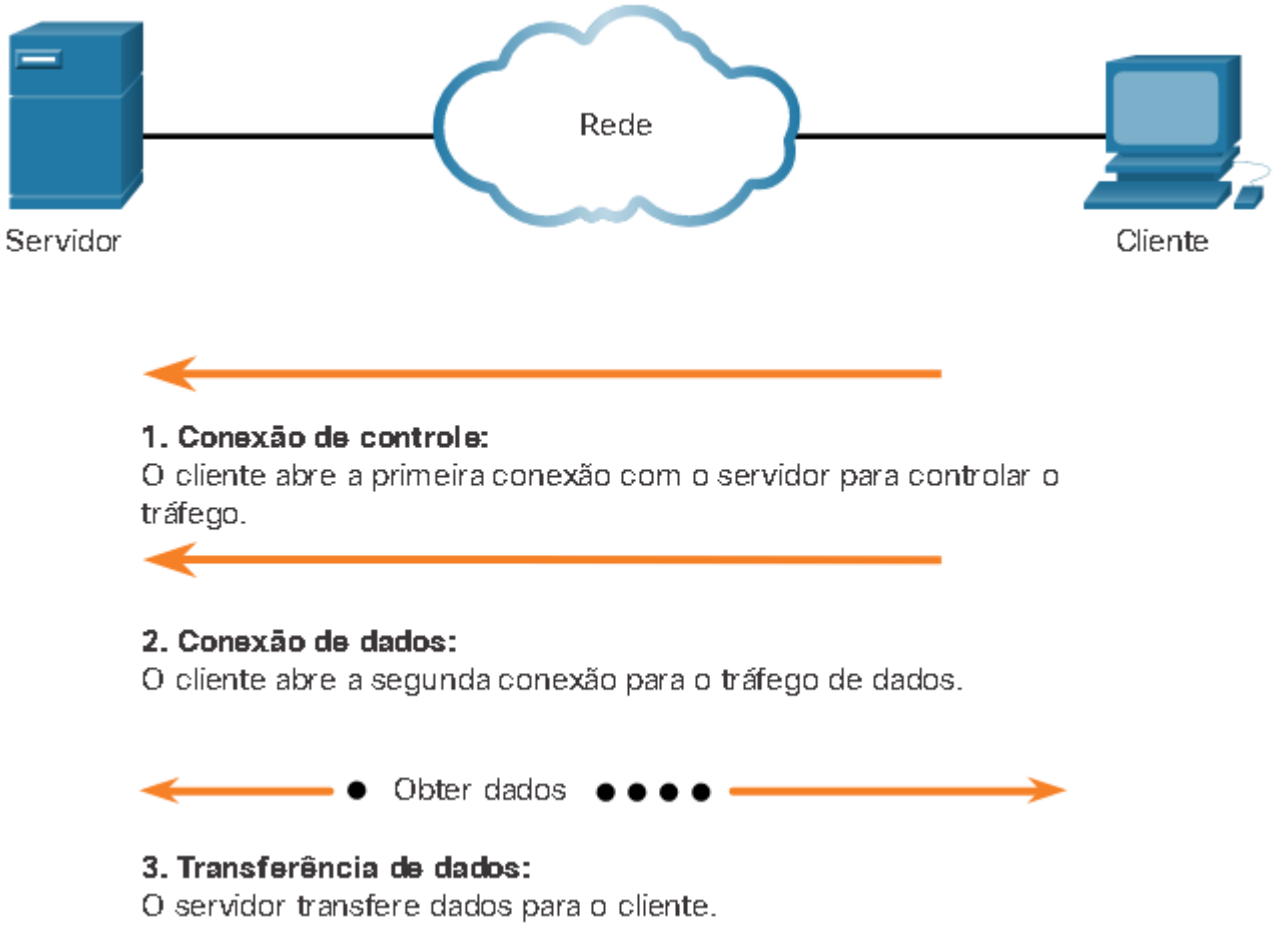
Serviços de Compartilhamento de Arquivos

Protocolo FTP

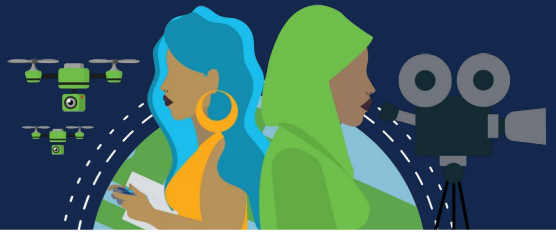
O cliente estabelece a primeira conexão com o servidor para o tráfego de controle usando a porta TCP 21. O tráfego consiste em comandos do cliente e respostas do servidor.

O cliente estabelece a segunda conexão com o servidor para transferência de dados propriamente dita, usando a porta TCP 20. Essa conexão é criada toda vez que houver dados a serem transferidos.

A transferência de dados pode acontecer em ambas as direções. O cliente pode baixar dados do servidor ou o cliente pode fazer upload (enviar) de dados para o servidor.



Fonte: Cisco



Serviços de Compartilhamento de Arquivos

Protocolo SMB

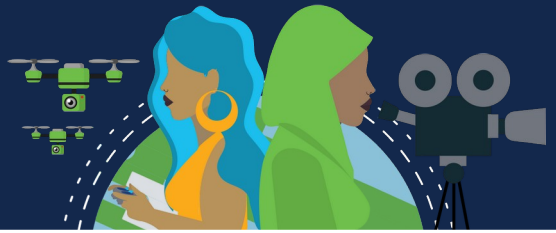
O Server Message Block (SMB) é um protocolo de compartilhamento de arquivos cliente/servidor, que descreve a estrutura de recursos de rede compartilhados, como diretórios, arquivos, impressoras e portas seriais. É um protocolo de requisição/resposta. Todas as mensagens SMB têm um formato em comum. Esse formato utiliza um cabeçalho com tamanho fixo seguido por um parâmetro de tamanho variável e componente de dados.

Aqui estão três funções de mensagens SMB:

- Iniciar, autenticar e encerrar sessões.Iniciar, autenticar e encerrar sessões.
- Arquivo de controle e acesso à impressora.
- Permitir que um aplicativo envie ou receba mensagens para ou de outro dispositivo.

Os serviços de compartilhamento de arquivos e impressão do SMB se tornaram o sustentáculo das redes Microsoft. Com a introdução da série de software Windows 2000, a Microsoft mudou a estrutura subjacente para uso do SMB. Nas versões anteriores de produtos Microsoft, os serviços SMB não utilizavam o protocolo TCP/IP para implementar a resolução de nomes. A partir do Windows 2000, todos os produtos Microsoft subsequentes usam a nomeação DNS, que permite que os protocolos TCP / IP suportem diretamente o compartilhamento de recursos SMB.

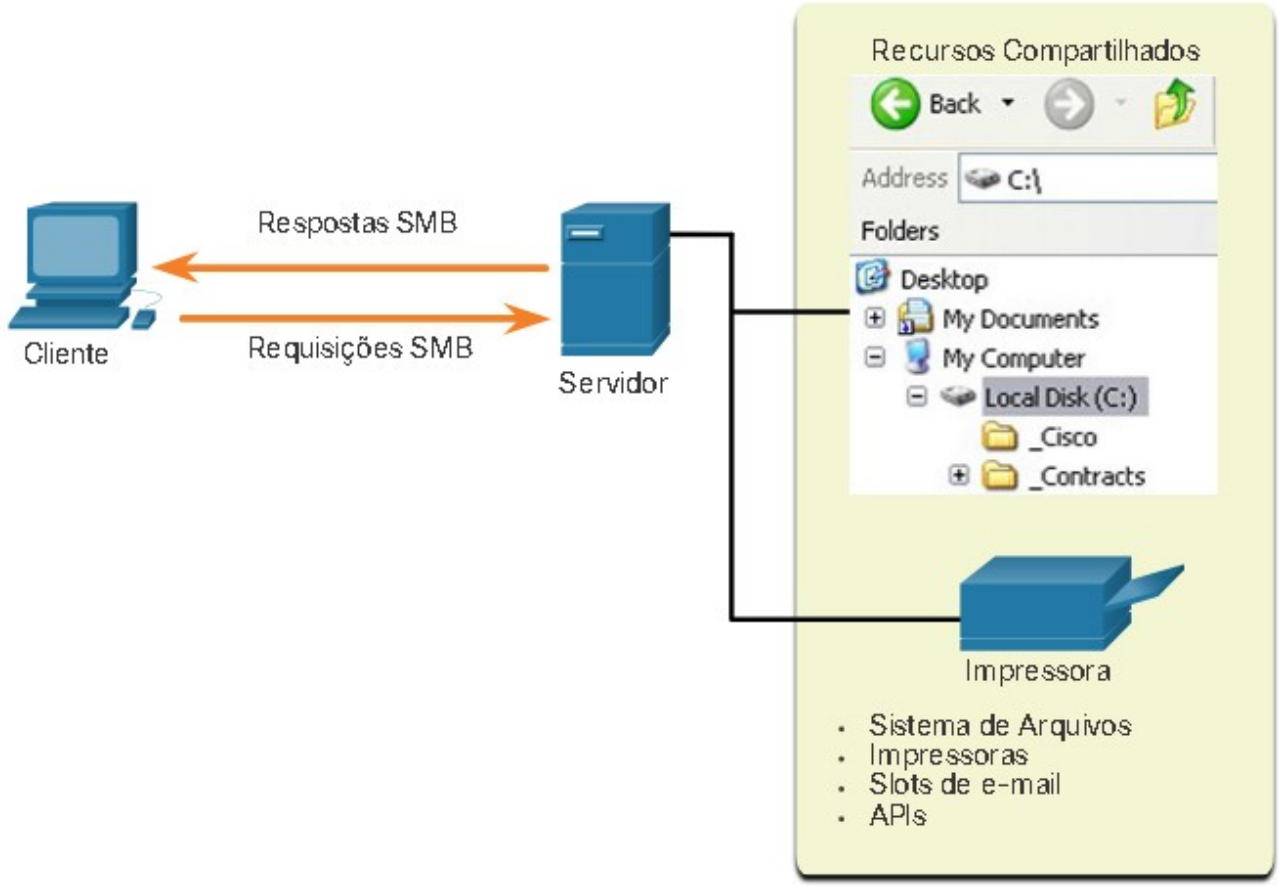
Fonte: Cisco



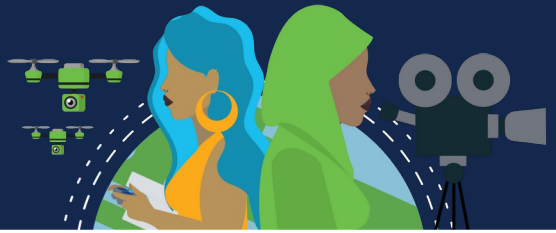
Serviços de Compartilhamento de Arquivos

Protocolo SMB

SMB é um cliente / servidor, protocolo de solicitação-resposta. Os servidores podem disponibilizar seus próprios recursos para os clientes na rede.



Fonte: Cisco

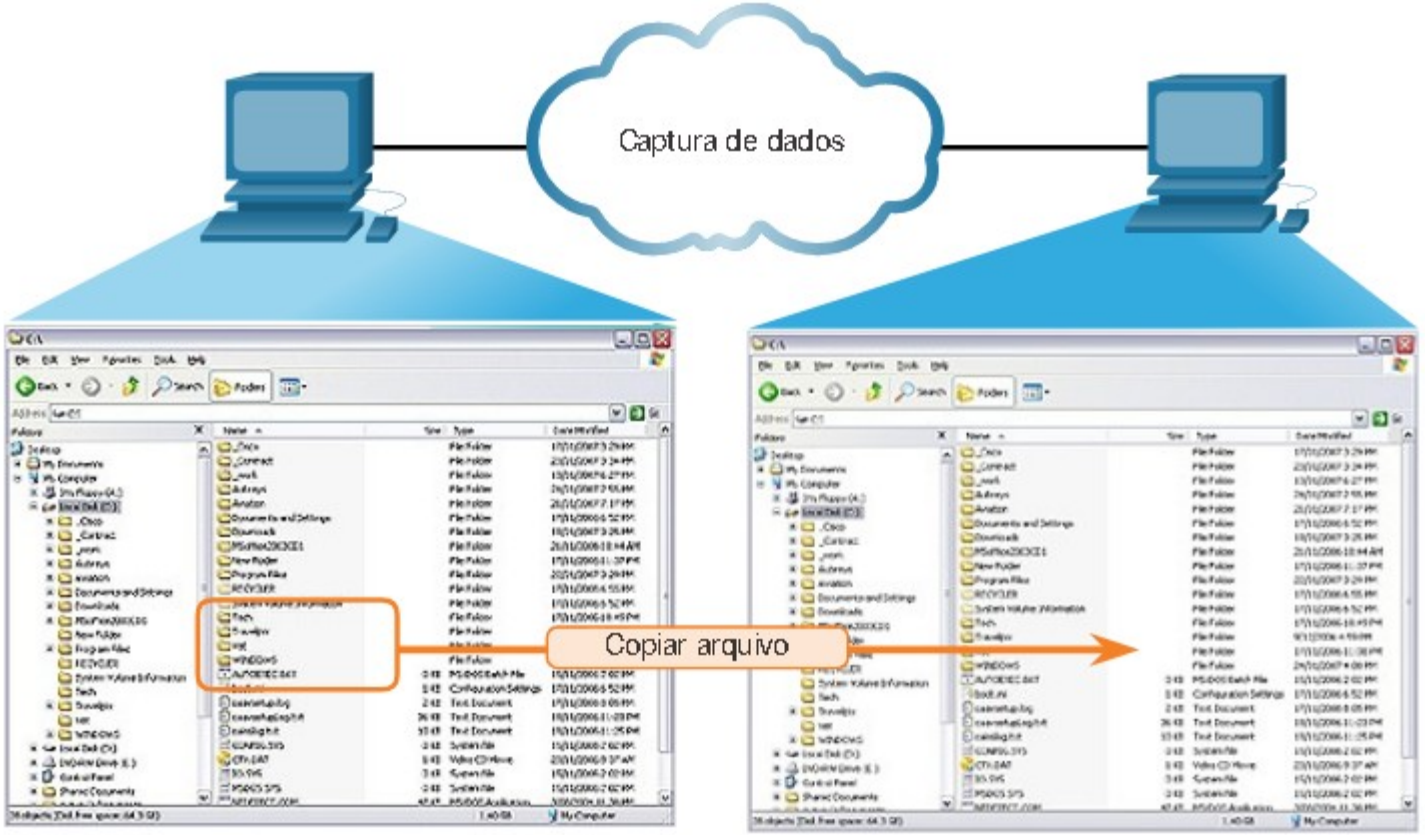


Serviços de Compartilhamento de Arquivos

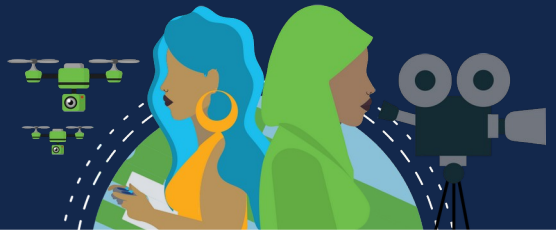
Protocolo SMB

Processo de troca de arquivos SMB entre PCs com Windows.

Um arquivo pode ser copiado de um computador para outro com o Windows Explorer usando o protocolo SMB.



Fonte: Cisco



Serviços de Compartilhamento de Arquivos

Protocolo SMB

Diferentemente do compartilhamento de arquivos permitido pelo FTP, os clientes estabelecem uma conexão de longo prazo com os servidores. Depois que a conexão é estabelecida, o usuário do cliente pode acessar os recursos no servidor como se o recurso fosse local para o host do cliente.

Os sistemas operacionais LINUX e UNIX também fornecem um método de compartilhamento de recursos com redes Microsoft usando uma versão do SMB chamada SAMBA. Os sistemas operacionais Apple Macintosh também oferecem suporte ao compartilhamento de recursos usando o protocolo SMB.

Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

CCNAv7 – ITN – Fundamentos de segurança de rede

Módulo 16

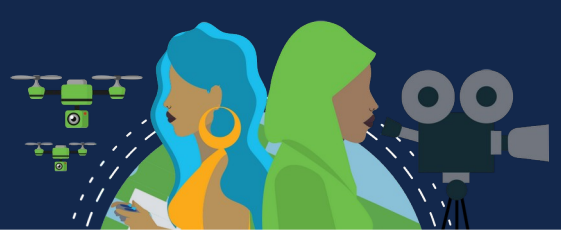
Embaixadores do Programa 2020, 2021 & 2022:

Organizadoras Cisco: Eliana Silva, Veruska Clednev
Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

WOMENROCK-IT
Brasil 2021

Networking Academy

Fundamentos de segurança de rede



Ameaças à Segurança e Vulnerabilidades

Tipos de Ameaças

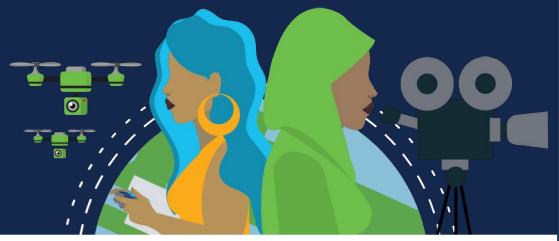
Os invasores podem obter acesso a uma rede através de vulnerabilidades de software, ataques de hardware ou adivinhando o nome de usuário e a senha de alguém. Os invasores que obtêm acesso modificando o software ou explorando vulnerabilidades são chamados de agentes de ameaças.

Depois que o agente da ameaça obtém acesso à rede, quatro tipos de ameaças podem surgir.

- **Roubo de informações:** Invasão com intenção de obter informações confidenciais, ou proprietárias de uma organização, como dados de pesquisa e desenvolvimento, que possam ser usadas ou vendidas para diversas finalidades.
- **Perda e manipulação de dados:** Invasão com intenção de destruir ou alterar registros de dados, através de um vírus que reformata o disco rígido do computador, ou que manipule dados invadindo um sistema de registros para alterar informações, como o preço de um item.
- **Roubo de identidade:** Roubo de informações pessoais com o objetivo de assumir a identidade de alguém. Um agente de ameaças pode obter documentos legais, solicitar crédito e fazer compras on-line não autorizadas. É um problema crescente que custa bilhões de dólares por ano.
- **Interrupção de serviços:** Impede que usuários legítimos acessem serviços aos quais têm direito. Como ataques de negação de serviço (DoS) em servidores, dispositivos de rede ou links de comunicação de rede.

Fonte: Cisco

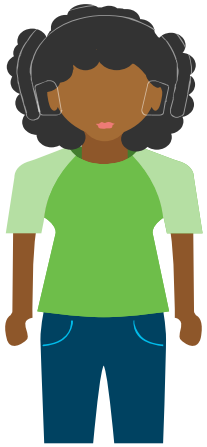
Ameaças à Segurança e Vulnerabilidades



Tipos de Vulnerabilidades

Vulnerabilidade é o grau de fraqueza em uma rede ou dispositivo. Algum grau de vulnerabilidade é inerente a roteadores, switches, desktops, servidores e até dispositivos de segurança. Normalmente, o foco são endpoints como servidores e desktops.

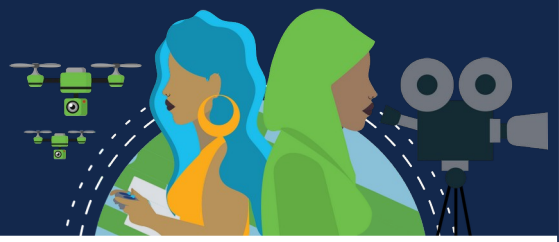
Existem três principais vulnerabilidades: política tecnológica, configuração e segurança. Todas essas podem deixar uma rede ou dispositivo aberto a outros ataques, como ataques de código malicioso e ataques de rede.



Tipo	Vulnerabiidade	Descrição
Tecnológica	Ponto fraco do protocolo TCP/IP	• Os Protocolos HTTP, FTP e ICMP são inerentemente inseguros. • Protocolo SNMP e SMTP estão relacionados à estrutura inerentemente insegura em que o TCP foi projetado.
	Pontos fracos dos sistemas operacionais	• Todo sistema operacional tem problemas de segurança que devem ser tratados. • Eles estão documentados na Equipe de resposta a emergências de computadores (CERT) arquivados em http://www.cert.org
	Pontos fracos dos equipamentos de rede	Equipamentos de rede, como roteadores, firewalls e switches possuem falhas de segurança que devem ser reconhecidas e protegidas. Como proteção por senha, falta de autenticação, protocolos de roteamento e falhas de firewall.
De configuração	Contas de usuário não protegidas	Informações de conta de usuário podem ser transmitidas de forma insegura através da rede, expondo nomes de usuário e senhas a atores ameaçadores.
	Contas de sistema com senhas facilmente descobertas	Esse problema comum é o resultado de senhas de usuários mal criadas.
	Serviços de Internet mal configurados	Ativar JavaScript em navegadores da Web permite ataques ao acessar sites não confiáveis. Outras fontes de falhas incluem serviços mal configurados como FTP ou servidores Web como IIS e Apache HTTP Server.

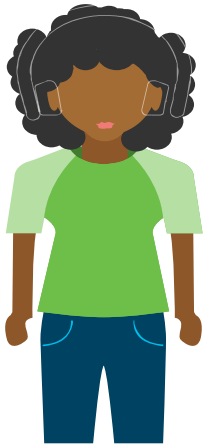
Fonte: Cisco

Ameaças à Segurança e Vulnerabilidades

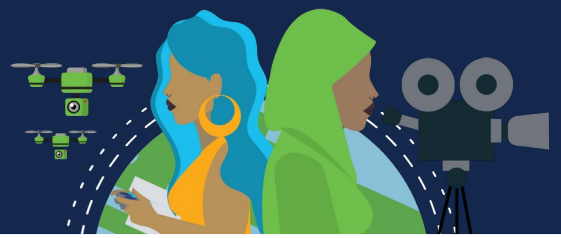


Tipos de Vulnerabilidades

Tipo	Vulnerabiidade	Descrição
De configuração	Configurações padrão não seguras.	Muitos produtos têm configurações padrão que criam ou habilitam falhas de segurança.
	Equipamento de rede configurado incorretamente	Configurações incorretas causam problemas significativos. Como; listas de acesso mal configuradas, protocolos de roteamento ou strings de comunidade SNMP podem criar ou habilitar falhas na segurança.
De política	Falta de uma política de segurança por escrito	Uma política de segurança não pode ser aplicada ou aplicada de forma consistente se for não escrita.
	Política	Batalhas políticas e guerras territoriais podem dificultar a implementação de um política de segurança consistente.
	Falta de continuidade da autenticação	Senhas mal escolhidas, facilmente quebradas ou padrão podem permitir acesso não autorizado à rede.
	Controles de acesso lógico não aplicados	O monitoramento e auditoria inadequados permitem ataques e uso não autorizado contínuo, desperdiçando recursos da empresa. Isso pode resultar em ação judicial ou rescisão contra técnicos de TI, gerenciamento de TI ou até mesmo contra empresas que permitem que essas condições inseguras persistam.
	Instalação e alterações de hardware e de software que não seguem a política	Alterações não autorizadas na topologia de rede ou instalação de aplicativos não aprovados cria ou habilita falhas na segurança.
	Plano de recuperação de desastres inexistente	A falta de um plano de recuperação de desastres permite o caos, pânico e confusão quando ocorre um desastre natural ou um ator ameaçador ataca o empreendimento.



Fonte: Cisco



Ameaças à Segurança e Vulnerabilidades

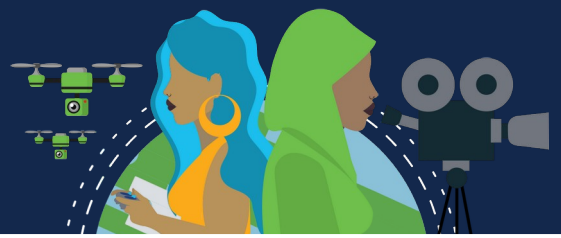
Segurança Física

Uma área vulnerável da rede igualmente importante a considerar é a segurança física dos dispositivos. Se os recursos de rede puderem ser fisicamente comprometidos, um agente de ameaça poderá negar o uso de recursos de rede.

As quatro classes de ameaças físicas são as seguintes:

- **Ameaças de hardware:** Inclui danos físicos a servidores, roteadores, switches, instalações de cabeamento e estações de trabalho.
- **Ameaças ambientais:** Inclui extremos de temperatura (muito quente ou muito frio) ou extremos de umidade (muito úmido ou muito seco).
- **Ameaças elétricas:** Inclui picos de tensão, tensão de alimentação insuficiente (quedas de energia), energia não condicionada (ruído) e perda total de energia.
- **Ameaças à manutenção:** Inclui o uso dos principais componentes elétricos (descarga eletrostática), falta de peças de reposição críticas, cabeamento incorreto e rotulagem inadequada.

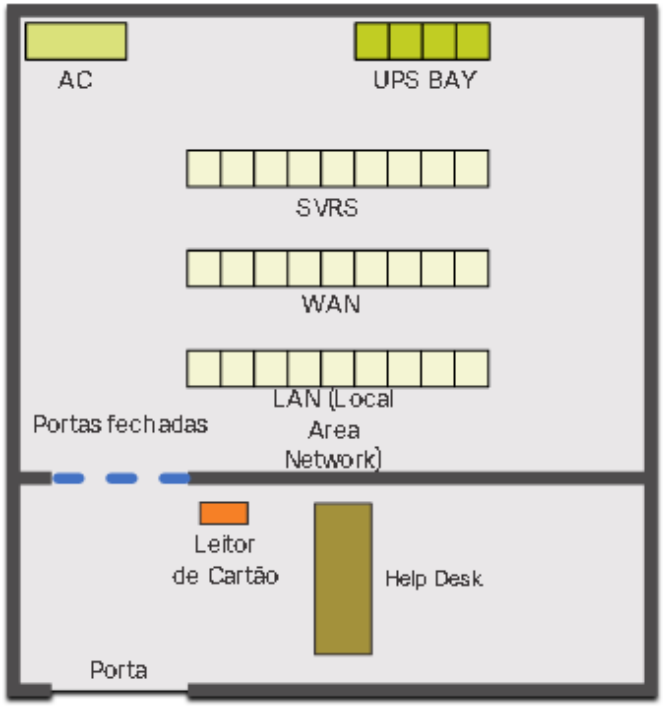
Um bom plano de segurança física deve ser criado e implementado para resolver esses problemas.



Ameaças à Segurança e Vulnerabilidades

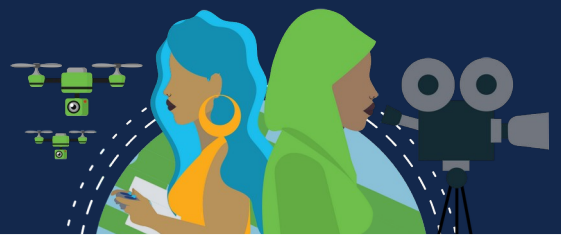
Segurança Física

Planejar a segurança física para limitar os danos ao equipamento



Etapa 1. Bloqueie os equipamentos e impeça o acesso não autorizado por meio de portas, teto, piso elevado, janelas, canais e fendas de ventilação.
Etapa 2. Monitore e controle a entrada com logs eletrônicos.
Etapa 3. Use câmeras de segurança.

Fonte: Cisco



Ataques à Rede

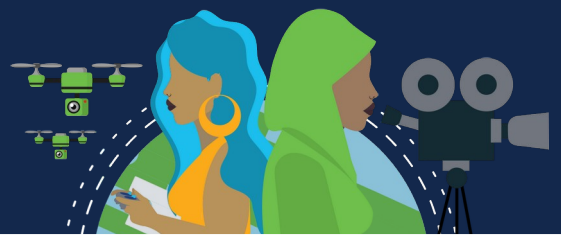
Tipos de Malware

Malware é a abreviação de software malicioso. É um código ou software projetado especificamente para danificar, interromper, roubar ou infligir ações “ruins” ou ilegítimas em dados, hosts ou redes. Vírus, worms e cavalos de Tróia são tipos de malware.

Vírus: É um tipo de malware que se propaga inserindo uma cópia de si mesmo dentro de outro programa e se tornando parte dele. Ele se dissemina de um computador para outro, deixando infecções por onde passa. Os vírus podem variar em gravidade, causando efeitos levemente irritantes, danificando dados ou software e causando condições de negação de serviço (DoS). Quase todos os vírus estão anexados a um arquivo executável, o que significa que o vírus pode existir em um sistema, mas não estar ativo ou ser capaz de se disseminar até que o usuário execute ou abra o arquivo ou o programa hospedeiro mal-intencionado. Quando o código hospedeiro é executado, o código viral é executado também. Normalmente, o programa host continua funcionando depois que o vírus o infecta. No entanto, alguns vírus sobrescrevem outros programas com cópias deles mesmos, o que destrói todo o programa hospedeiro. Os vírus se espalham quando o software ou documento ao qual estão conectados é transferido de um computador para outro usando a rede, um disco, compartilhamento de arquivos ou anexos de e-mail infectados.

Worms: Similares aos vírus na reprodução de cópias funcionais de si mesmos e podem causar o mesmo tipo de dano. Ao contrário dos vírus, que necessitam que um arquivo infectado se espalhe, worms são softwares independentes e não necessitam de um programa hospedeiro ou ajuda humana para se propagarem. Um worm não precisa estar anexado a um programa para infectar um hospedeiro e entrar em um computador usando uma vulnerabilidade no sistema. Os worms utilizam os recursos do sistema para viajar pela rede sem ajuda.

Fonte: Cisco



Ataques à Rede

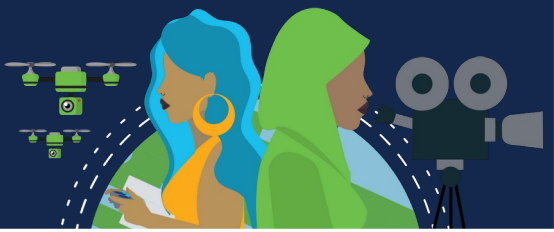
Tipos de Malware

Cavalos de Tróia: É outro tipo de malware que recebeu o nome do cavalo de madeira usado pelos gregos para invadirem Troia. É uma parte perigosa do software que parece legítima. Os usuários são, em geral, enganados carregando e executando-os em seus sistemas. Depois de ativado, ele pode causar vários ataques ao host, desde irritar o usuário (com janelas pop-up excessivas ou alterar a área de trabalho) até danificá-lo (excluir arquivos, roubar dados ou ativar e espalhar outros malwares, como vírus). Cavalos de Troia também são conhecidos por criarem portas dos fundos (back doors) que permitem o acesso de usuários mal-intencionados ao sistema.

Ao contrário de vírus e worms, os cavalos de Tróia não se reproduzem infectando outros arquivos. Eles se auto-replicam. Os cavalos de Tróia devem se espalhar pela interação do usuário, como abrir um anexo de e-mail ou fazer o download e executar um arquivo da Internet.

Fonte: Cisco

Ataques à Rede

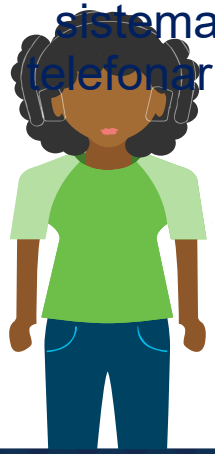


Ataques de Reconhecimento

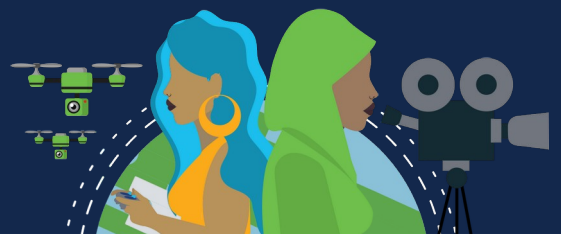
Os ataques à rede podem ser classificados em três categorias principais:

- **Ataques de reconhecimento:** Descoberta e mapeamento de sistemas, serviços ou vulnerabilidades.
- **Ataques de acesso:** Manipulação não autorizada de dados, acesso ao sistema ou privilégios do usuário.
- **Negação de serviço:** Desativação ou corrupção de redes, sistemas ou serviços.

Para ataques de reconhecimento, os atores externos de ameaças podem usar ferramentas da Internet, como *nslookup* e *whois*, para determinar facilmente o espaço de endereço IP atribuído a uma determinada corporação ou entidade. Após a determinação do espaço de endereço IP, um agente de ameaça pode executar *ping* nos endereços IP disponíveis ao público para identificar os endereços que estão ativos. Para ajudar a automatizar essa etapa, um agente de ameaça pode usar uma ferramenta de *varredura de ping*, como **fping** ou **gping**. Isso envia sistematicamente todos os endereços de rede em um determinado intervalo ou sub-rede. Isso se assemelha a telefonar para cada um dos contatos de uma agenda telefônica para ver quem atende. Seguido de uma varredura de porta nos endereços IP ativos descobertos.



Fonte: Cisco



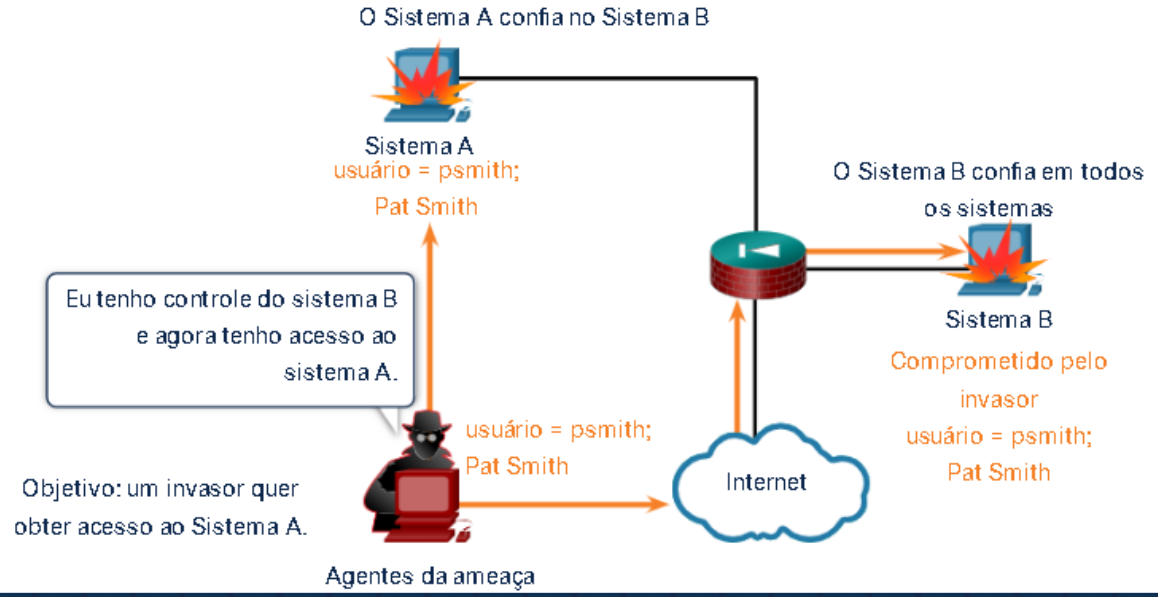
Ataques à Rede

Ataques de Acesso

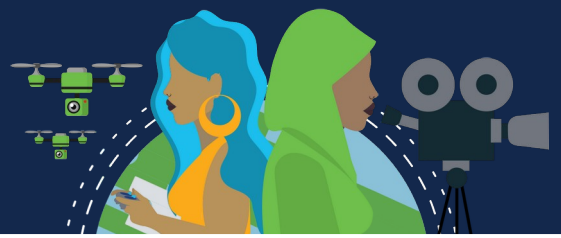
Os ataques de acesso exploram vulnerabilidades conhecidas em serviços de autenticação, serviços de FTP e serviços da Web para obter acesso a contas da Web, bancos de dados e outras informações confidenciais.

São classificados em quatro tipos:

- **Ataques de senha:** Implantados usando vários métodos diferentes, como:*Ataques de força bruta, Ataques de cavalo de Tróia e Sniffers de pacotes*
  - **Exploração de Confiança:** Privilégios não autorizados são usados para obter acesso a um sistema, comprometendo o alvo.



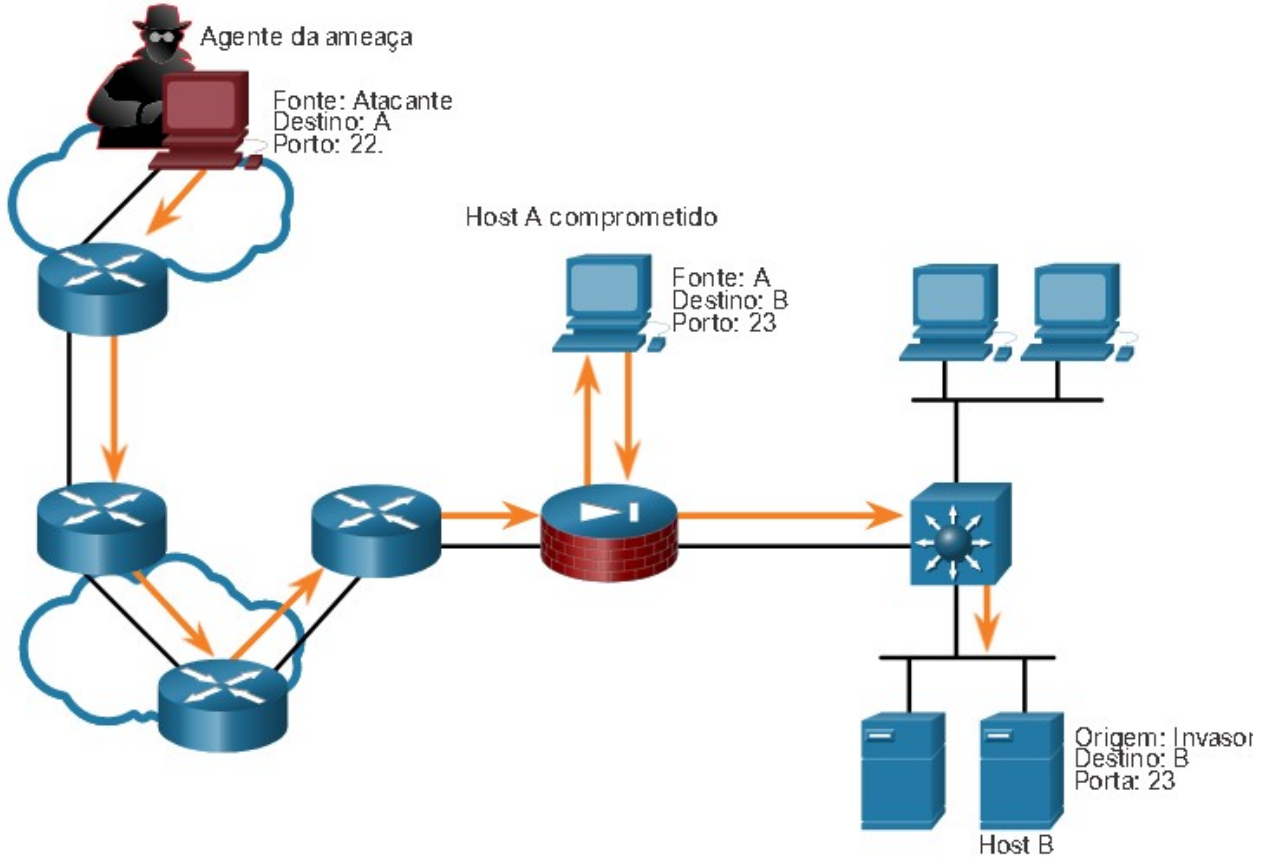
Fonte: Cisco



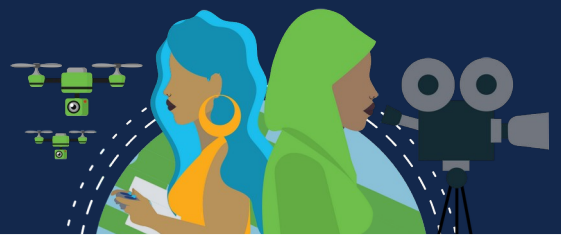
Ataques à Rede

Ataques de Acesso

- **Redirecionamento de porta:** Um agente de ameaça usa um sistema comprometido como base para ataques contra outros alvos.



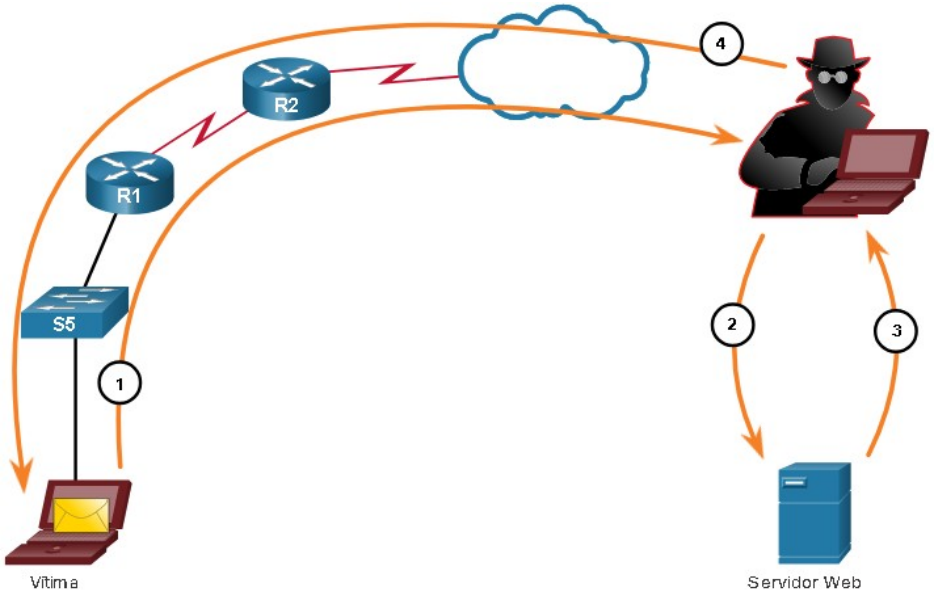
Fonte: Cisco



Ataques à Rede

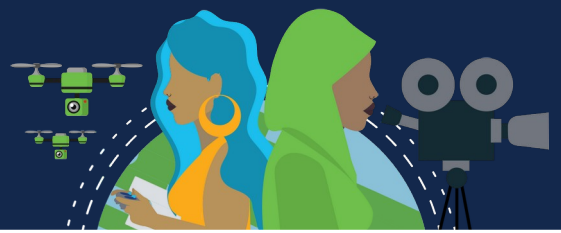
Ataques de Acesso

- **Man-in-the-Middle:** O agente da ameaça é posicionado entre duas entidades legítimas para ler ou modificar os dados que passam entre as duas partes.



Etapa 1. Uma vítima solicita uma página da Web, a solicitação é direcionada ao computador do agente da ameaça.
Etapa 2. O computador do agente da ameaça recebe a solicitação e recupera a página real do site legítimo.
Etapa 3. O ator ameaçador pode alterar a página da Web legítima e fazer alterações nos dados.
Etapa 4. O ator da ameaça encaminha a página solicitada à vítima.

Fonte: Cisco



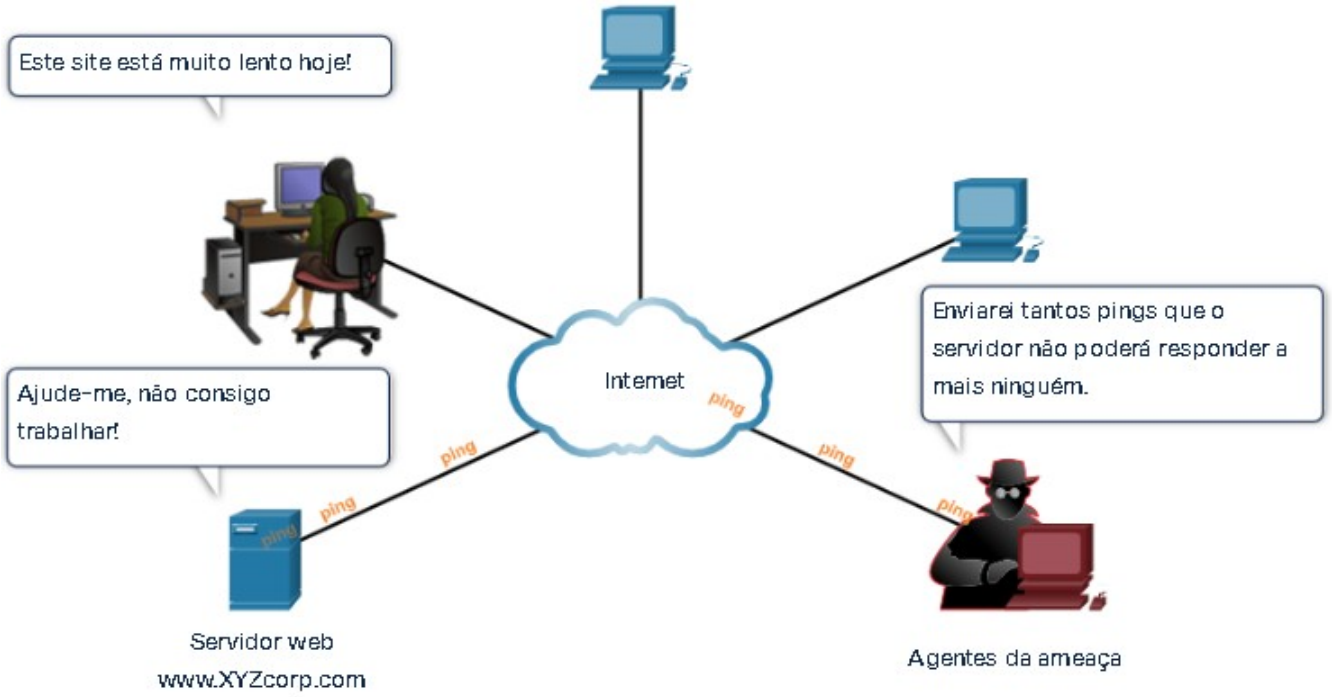
Ataques à Rede

Ataques de Negação de Serviços

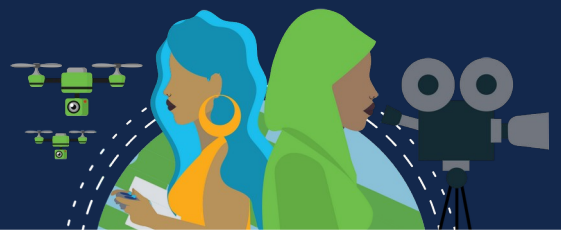
Os ataques de negação de serviço (DoS) são a forma de ataque mais divulgada e uma das mais difíceis de eliminar. No entanto, devido à facilidade de implementação e danos potencialmente significativos, os ataques de negação de serviço merecem atenção especial dos administradores de segurança.

Os ataques DoS assumem muitas formas. E, por fim, impedem que pessoas autorizadas usem um serviço ao consumir recursos do sistema. Para prevenir ataques (DoS) é importante manter em dia as mais recentes atualizações de segurança para sistemas operacionais e aplicações.

Ataque DoS: Os ataques de DoS são um grande risco, porque interrompem a comunicação e causam perda significativa de tempo e dinheiro. Esses ataques são relativamente simples de conduzir, mesmo por um invasor não capacitado.



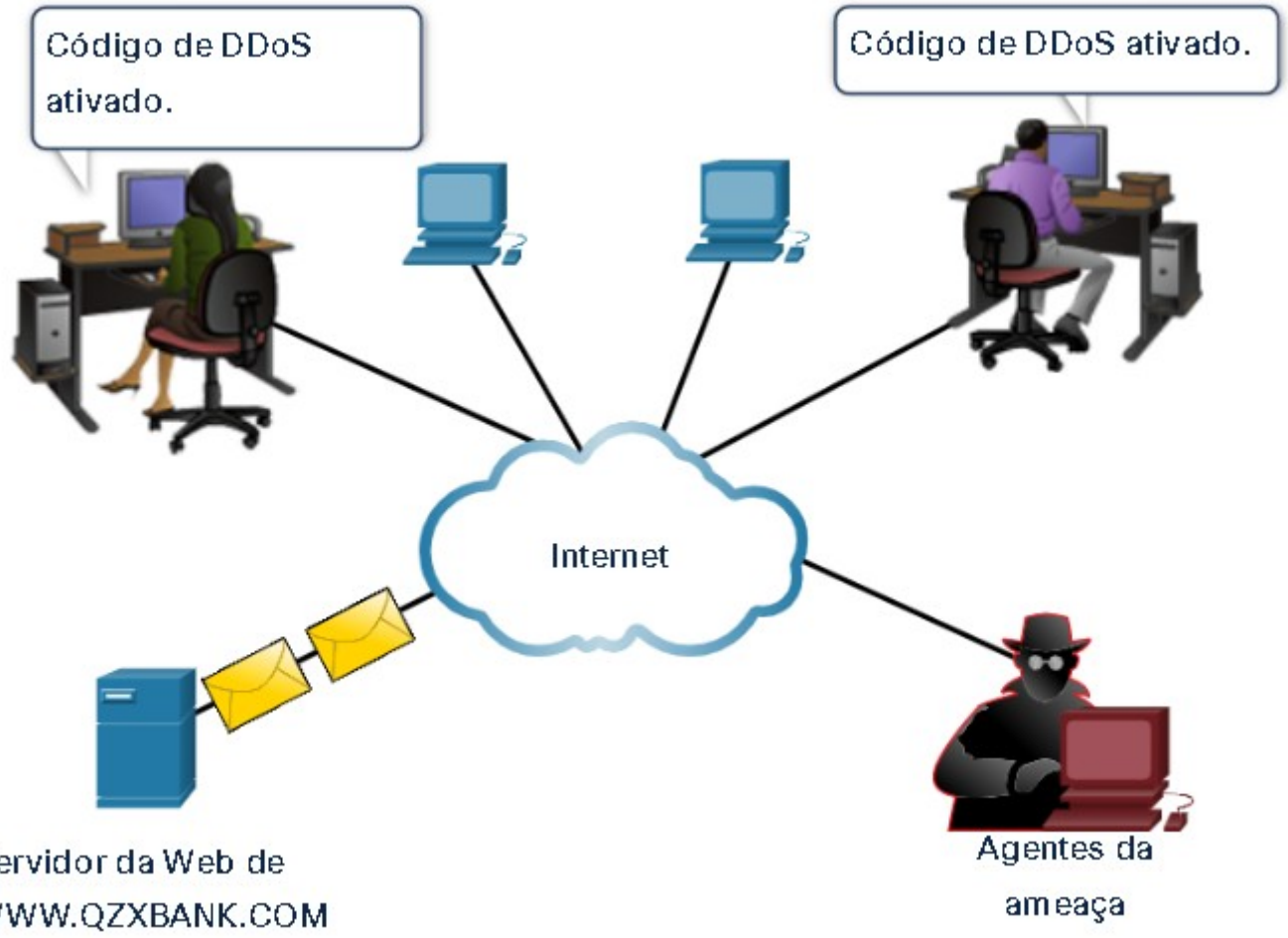
Fonte: Cisco



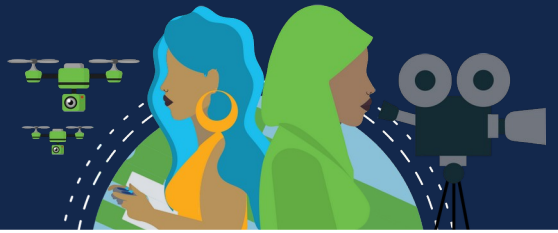
Ataques à Rede

Ataques de Negação de Serviços

Ataque DDoS: Um DDoS (DoS distribuído) é semelhante a um ataque de DoS, mas é originado de várias fontes coordenadas. Por exemplo, um agente de ameaça cria uma rede de hosts infectados, conhecidos como zumbis. Uma rede de zumbis é chamada de botnet. O ator ameaça usa um programa de comando e controle (CNC) para instruir o botnet de zumbis para realizar um ataque DDoS.



Fonte: Cisco



Mitigações de ataque à rede

A abordagem de defesa em camadas

Para atenuar os ataques de rede, primeiro você deve proteger dispositivos, incluindo roteadores, switches, servidores e hosts. A maioria das organizações emprega uma abordagem de defesa profunda (também conhecida como abordagem em camadas) à segurança. Isso requer uma combinação de dispositivos e serviços de rede trabalhando em conjunto.

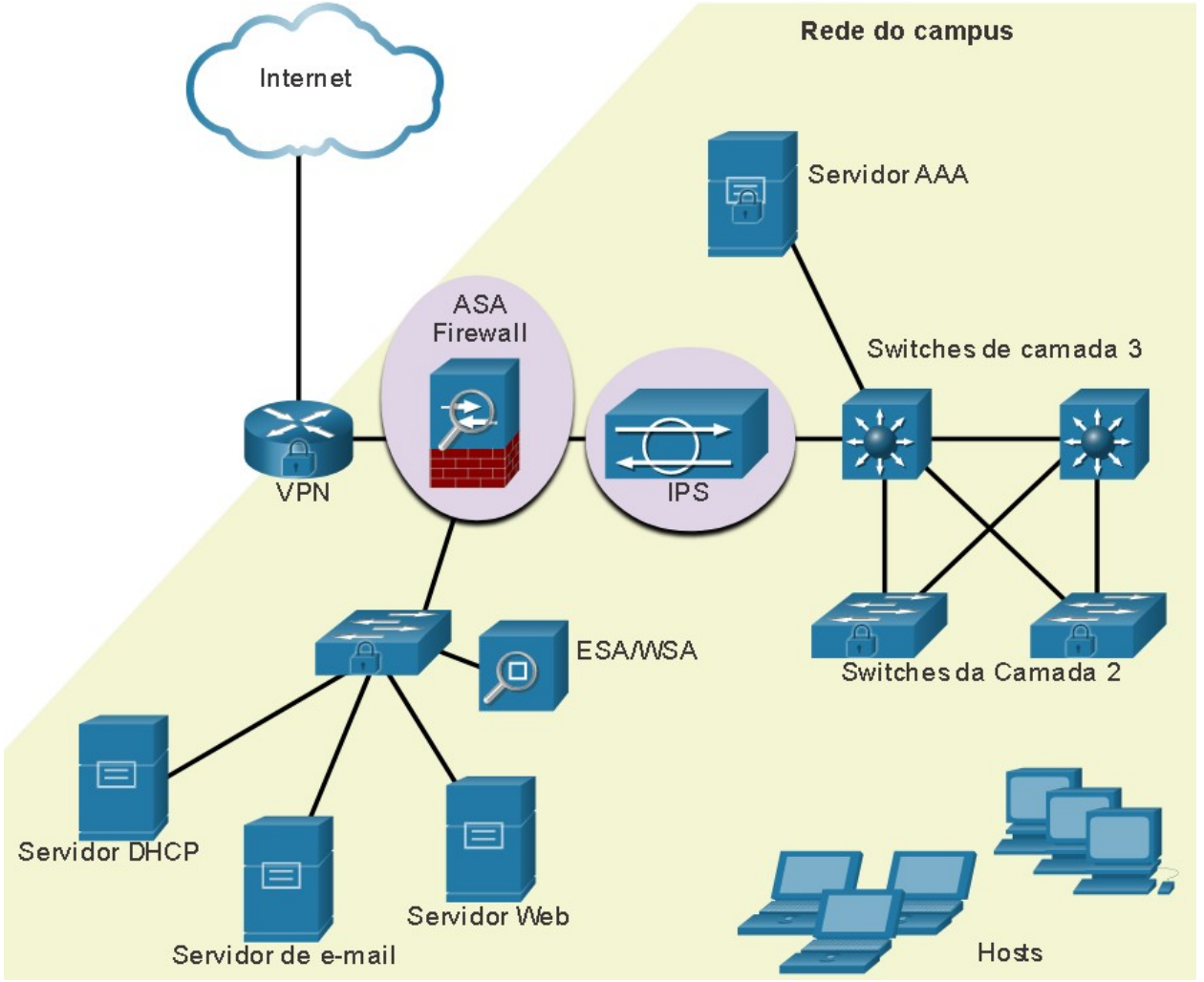
Vários dispositivos e serviços de segurança são implementados para proteger os usuários e ativos de uma organização contra ameaças TCP / IP.

- **VPN:** Um roteador é usado para fornecer serviços VPN seguros com sites corporativos e suporte a acesso remoto para usuários remotos usando túneis criptografados seguros.
- **ASA Firewall:** Este dispositivo dedicado fornece serviços de firewall com estado. Ele garante que o tráfego interno possa sair e voltar, mas o tráfego externo não pode iniciar conexões com hosts internos.
- **IPS:** Um sistema de prevenção contra intrusões (IPS) monitora o tráfego de entrada e saída procurando malware, assinaturas de ataques à rede e muito mais. Se reconhecer uma ameaça, ela poderá imediatamente pará-la.
- **ESA/WSA:** O dispositivo de segurança de e-mail (ESA) filtra spam e e-mails suspeitos. O WSA (Web Security Appliance) filtra sites de malware conhecidos e suspeitos na Internet.
- **Servidor AAA**: Este servidor contém um banco de dados seguro de quem está autorizado a acessar e gerenciar dispositivos de rede. Os dispositivos de rede autenticam usuários administrativos usando esse banco de dados.

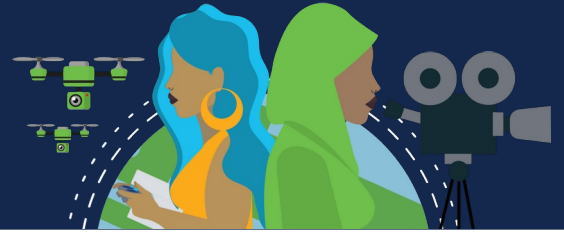
Fonte: Cisco

Mitigações de ataque à rede

A abordagem de defesa em camadas



Fonte: Cisco



Mitigações de ataque à rede

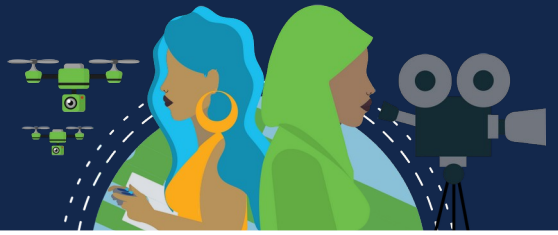
Manter Backups

Fazer backup de configurações e dados do dispositivo é uma das maneiras mais eficazes de se proteger contra a perda de dados. O backup de dados armazena uma cópia das informações de um computador em uma mídia removível de backup que pode ser guardada em um local seguro. Os dispositivos de infraestrutura devem ter backups de arquivos de configuração e imagens IOS em um servidor de arquivos FTP ou similar. Se o computador ou um hardware de roteador falhar, os dados ou a configuração podem ser restaurados usando a cópia de backup.

Os backups devem ser realizados regularmente, conforme identificado na política de segurança. Os backups de dados são, normalmente, armazenados em outro local, para proteger a mídia de backup, se algo acontecer com a instalação principal. Hosts Windows têm um utilitário de backup e restauração. É importante que os usuários façam backup de seus dados em outra unidade ou em um provedor de armazenamento baseado em nuvem.

Considerações	Descrição
Frequência	• Realizar backups regularmente, conforme identificado na política de segurança de TI da empresa. • Backups completos podem ser demorados, portanto, executar mensalmente ou backups semanais com backups parciais frequentes de arquivos alterados.
Armazenamento	Valide sempre os backups para garantir a integridade dos dados e os procedimentos de restauração de arquivos.
Segurança	Os backups devem ser transportados para um armazenamento externo aprovado em uma rotação diária, semanal ou mensal, conforme exigido pelo política de segurança.
Validação	Os backups devem ser protegidos usando senhas fortes. A senha é necessário para restaurar os dados.

Fonte: Cisco



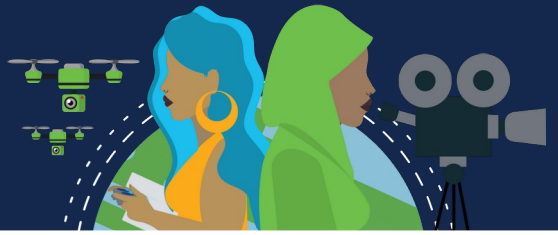
Mitigações de ataque à rede

Atualização, atualização e patch

O meio mais eficaz de reduzir um ataque de worm é baixar as atualizações de segurança do sistema operacional do fornecedor e corrigir todos os sistemas vulneráveis. A administração de vários sistemas envolve a criação de uma imagem de software padrão (sistema operacional e aplicações com autorização para uso nos sistemas do cliente) que é implantada em sistemas novos ou atualizados. No entanto, os requisitos de segurança são alterados e os sistemas já implantados podem precisar ter patches de segurança atualizados instalados.

Uma solução para o gerenciamento de patches críticos de segurança é garantir que todos os sistemas finais baixem atualizações automaticamente, sem a intervenção do usuário.

Fonte: Cisco



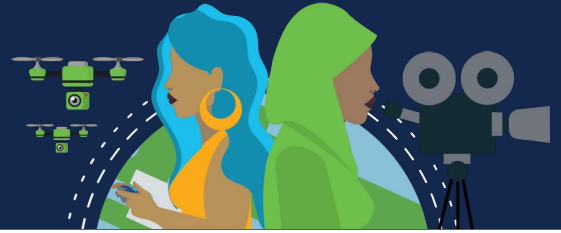
Mitigações de ataque à rede

Autenticação, autorização e auditoria

Todos os dispositivos de rede devem ser configurados de forma segura para fornecer acesso apenas a indivíduos autorizados. Os serviços de segurança de rede de autenticação, autorização e auditoria (AAA ou "triplo A") fornecem a estrutura principal para configurar o controle de acesso nos dispositivos de rede.

O AAA é uma maneira de controlar quem tem permissão para acessar uma rede (autenticar), quais ações eles executam enquanto acessam a rede (autorizar) e fazer um registro do que foi feito enquanto eles estão lá (auditoria/ contabilização).

Fonte: Cisco



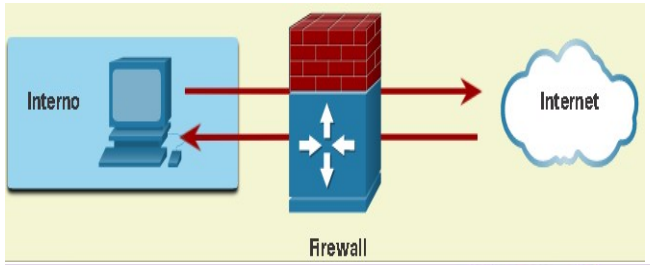
Mitigações de ataque à rede

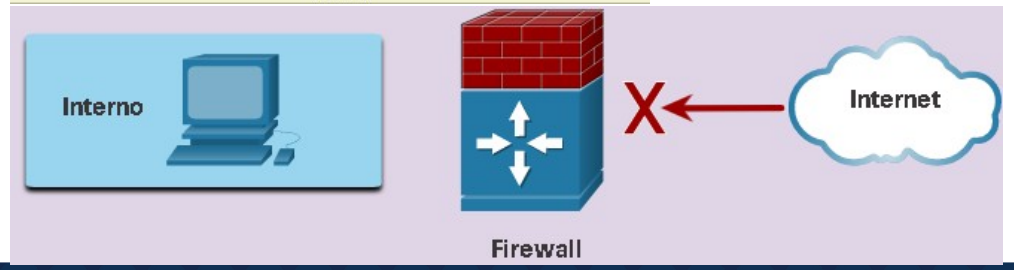
Firewalls

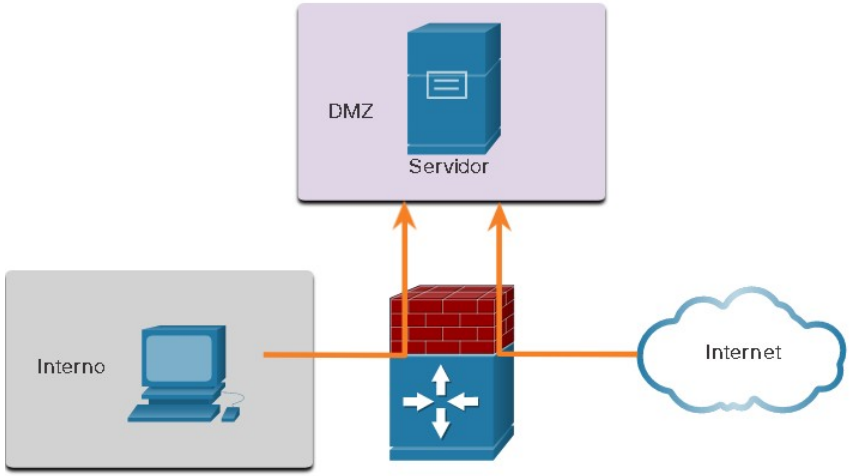
Um firewall é uma das ferramentas de segurança disponíveis mais eficazes na proteção dos usuários contra ameaças externas. Um firewall protege computadores e redes impedindo que tráfego indesejável entre em redes internas.

Os firewalls de rede estão localizados entre duas ou mais redes, e controlam o tráfego entre elas, além de ajudar a evitar o acesso não autorizado. Permitindo que o tráfego de um host de rede interno saia da rede e retorne à rede interna, ou que o tráfego iniciado pela rede externa (ou seja, a Internet) tenha acesso negado à rede interna.

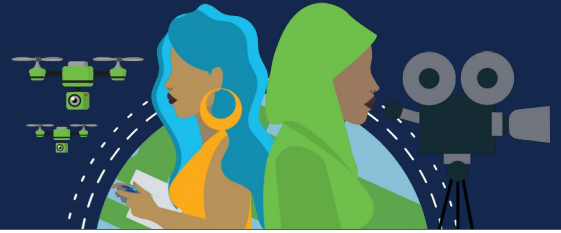
Um firewall poderia permitir que usuários externos controlassem o acesso a serviços específicos. Servidores acessíveis a usuários externos geralmente estão localizados em uma rede especial referida como a zona desmilitarizada (DMZ). Um administrador de rede deve aplicar políticas específicas para hosts conectados a essa rede.







Fonte: Cisco



Mitigações de ataque à rede

Tipos de Firewalls

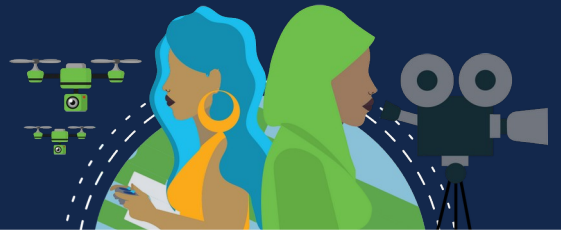
Várias técnicas diferentes são usadas para determinar o que será permitido ou negado o acesso a uma rede.

- **Filtragem de pacotes:** Impede ou permite o acesso com base em endereços IP ou MAC;
- **Filtragem de aplicativos:** Impede ou permite o acesso por tipos de aplicativos específicos com base nos números de porta;
- **Filtragem de URL:** Impede ou permite o acesso a sites com base em URLs ou palavras-chave específicas;
- **Inspeção de pacotes com estado (SPI):** Os pacotes recebidos devem ter respostas legítimas às solicitações dos hosts internos. Pacotes não solicitados são bloqueados, a menos que especificamente permitidos. O SPI também pode incluir o recurso de reconhecer e filtrar tipos específicos de ataques, como negação de serviço (DoS).

Segurança de Endpoints

Um endpoint é um sistema de computador individual ou um dispositivo que atua como um cliente da rede. Os endpoints comuns são laptops, desktops, servidores, smartphones e tablets. A segurança de dispositivos de endpoint é uma das tarefas mais desafiadoras de um administrador de rede, porque envolve a natureza humana. Uma empresa deve ter obrigatoriamente as políticas em vigor bem documentadas e os funcionários devem conhecer essas regras. Os funcionários devem ser treinados para usarem corretamente a rede. As políticas em geral incluem o uso de software antivírus e prevenção contra invasões. Soluções de segurança de endpoints mais abrangentes baseiam-se no controle de acesso à rede.

Fonte: Cisco



Segurança de dispositivos

AutoSecure Cisco

As configurações de segurança são definidas com os valores padrão quando um novo sistema operacional é instalado em um dispositivo. Na maioria dos casos, esse nível de segurança é inadequado. Para roteadores Cisco, o recurso Cisco AutoSecure pode ser usado para ajudar a proteger o sistema.

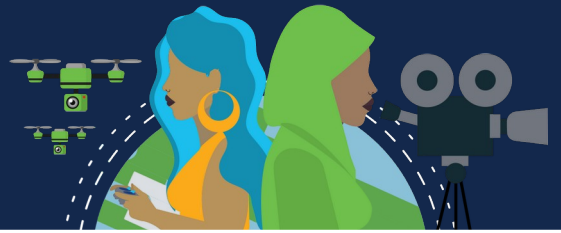
```
Router# auto secure
                --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router but it will not make router absolutely secure
from all security attacks ***
```

Além disso, existem algumas etapas simples que podem ser executadas e que se aplicam à maioria dos sistemas:

- Nomes de usuário e senhas padrão devem ser trocados imediatamente.
- O acesso aos recursos do sistema deve ser restrito apenas aos indivíduos que estão autorizados a usá-los.
- Todos os serviços e aplicações desnecessários devem ser desativados e desinstalados assim que possível.

Em geral, dispositivos vindos de fábrica ficaram estocados em um depósito por um período e não têm os patches mais atuais instalados. É importante atualizar todos os programas e instalar todos os patches de segurança antes da implementação.

Fonte: Cisco



Segurança de dispositivos

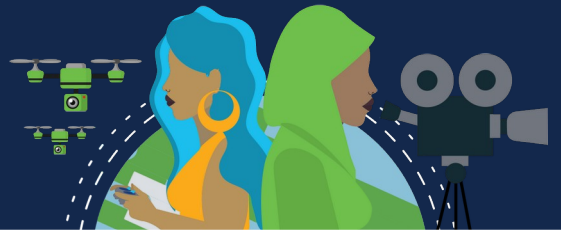
Senhas

É importante usar senhas fortes para proteger dispositivos de rede. Estas são as diretrizes padrão a serem seguidas:

- Use um comprimento de senha de pelo menos oito caracteres, de preferência 10 ou mais caracteres. Uma senha mais longa é uma senha mais segura.
- Use senhas complexas. Inclua uma combinação de letras maiúsculas e minúsculas, números, símbolos e espaços, se permitido.
- Evite as senhas com base em repetição, palavras comuns de dicionário, sequências de letras ou números, nomes de usuário, nomes de parentes ou de animais de estimação, informações biográficas, como datas de nascimento, números de identificação, nomes de antepassados ou outras informações facilmente identificáveis.
- Deliberadamente, soletre errado uma senha. Por exemplo, Smith = Smyth = 5mYth ou Security = 5ecur1ty.
- Altere as senhas periodicamente. Se uma senha for inconscientemente comprometida, a janela de oportunidade para o agente de ameaças usar a senha é limitada.

Não anote as senhas e muito menos as deixe em locais óbvios, como em sua mesa ou no monitor.

Fonte: Cisco



Segurança de dispositivos

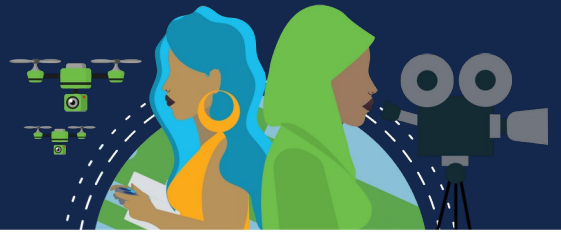
Senhas

Senha Fraca	Por que ela é fraca?
secret	Senha simples de dicionário
smith	Nome de solteira da mãe
toyota	Fabricante de um carro
bob1967	Nome e data de nascimento do usuário
Blueleaf23	Palavras e números simples

Senha Forte	Por que ela é forte?
b67n42d39c	Combina caracteres alfanuméricos
12^h u4@1p7	Combina caracteres alfanuméricos, símbolos e inclui um espaço

Nos roteadores Cisco, os espaços à esquerda são ignorados em senhas, mas os espaços após o primeiro caractere não são ignorados. Portanto, um método para criar uma senha forte é utilizar a barra de espaço e criar uma frase feita de muitas palavras. Isso se chama. Uma frase secreta geralmente mais fácil de lembrar do que uma senha simples. Também é maior e mais difícil de ser descoberta.

Fonte: Cisco



Segurança de dispositivos

Segurança de Senha Adicional

Senhas fortes são úteis apenas se forem secretas. Existem várias etapas que podem ser tomadas para ajudar a garantir que as senhas permaneçam secretas em um roteador e switch Cisco, incluindo estes:

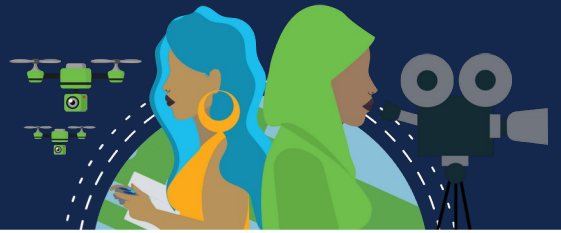
- Criptografando todas as senhas de texto sem formatação;
- Definindo um tamanho mínimo aceitável de senha;
- Impedir ataques força bruta de adivinhação de senha;
- Desativando um acesso de modo EXEC privilegiado inativo após um período especificado.

O comando de configuração global **service password-encryption** impede que indivíduos não autorizados visualizem senhas em texto sem formatação no arquivo de configuração.

O comando de configuração global **security passwords min-length length** garante que todas as senhas configuradas tenham no mínimo o comprimento especificado.

Software de quebra de senha é usado para realizar um ataque de força bruta em um dispositivo de rede. Tentando continuamente adivinhar as senhas válidas até que uma funcione. O comando de configuração global **login block-for # attempts # within #** impede esse tipo de ataque, bloqueando as tentativas de login por X segundos se houver X tentativas de login com falha dentro de X segundos.

Fonte: Cisco



Segurança de dispositivos

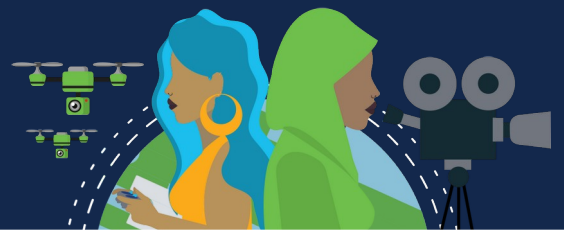
Segurança de Senha Adicional

Os administradores de rede podem se distrair e acidentalmente deixar uma sessão de modo EXEC privilegiada aberta em um terminal. Isso pode permitir que um ator de ameaça interno tenha acesso para alterar ou apagar a configuração do dispositivo.

Por padrão, os roteadores Cisco farão logout de uma sessão EXEC após 10 minutos de inatividade. No entanto, você pode reduzir essa tempo, usando o comando **exec-timeout** *[minutos][segundos]* na configuração das linhas de acesso. Esse comando pode ser aplicado na line console, auxiliares e linhas vty.

```
R1(config)# service password-encryption
R1(config)# security passwords min-length 8
R1(config)# login block-for 120 attempts 3 within 60
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# exec-timeout 5 30
R1(config-line)# transport input ssh
R1(config-line)# end
R1#
R1# show running-config | section line vty
line vty 0 4
 password 7 094F471A1A0A
 exec-timeout 5 30
 login
 transport input ssh
```

Fonte: Cisco



Segurança de dispositivos

Ativação do SSH

O Telnet simplifica o acesso remoto ao dispositivo, mas não é seguro. Um pacote Telnet é transmitido sem criptografia. É altamente recomendável ativar o Secure Shell (SSH) em dispositivos para acesso remoto seguro, usando as seis etapas a seguir:

Etapa 1: Configure um nome de host de dispositivo exclusivo, diferente do padrão.

Etapa 2: Configure o nome do domínio IP usando o comando modo de configuração global **ip-domain name**.

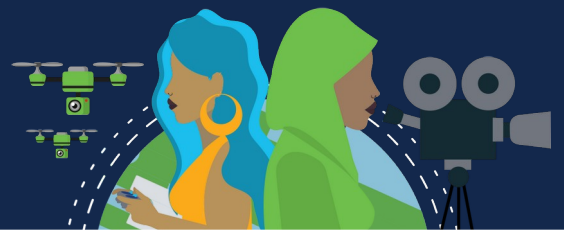
Etapa 3: Gere uma chave para criptografar o tráfego SSH entre a origem e o destino com o comando de configuração global **crypto key generate rsa general-keys modulus** *bits*. O módulo *bits* determina o tamanho da chave e pode ser configurado de 360 bits a 2048 bits. Quanto maior o valor de bit, mais segura a chave. No entanto, valores de bits maiores também levam mais tempo para criptografar e descriptografar. O mínimo recomendado é 1024 bits.

Etapa 4: Crie uma entrada de nome de usuário no banco de dados local usando o comando de configuração global **username,** o parâmetro secret é usado para que a senha seja criptografada usando MD5.

Etapa 5: Autentique a linha vty no banco de dados local com o comando de configuração de linha **login local.**

Etapa 6: Habilite as sessões SSH de entrada vty. Por padrão, nenhuma sessão de entrada é permitida em linhas vty. Use o comando **transport input** *[ssh | telnet].*

Fonte: Cisco

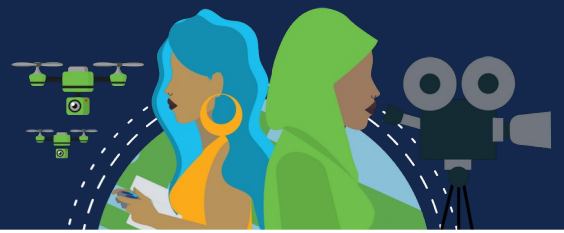


Segurança de dispositivos

Ativação do SSH

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com % The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Fonte: Cisco



Segurança de dispositivos

Desativar serviços não utilizados

Os roteadores e switches Cisco começam com uma lista de serviços ativos que podem ou não ser necessários em sua rede. Desative todos os serviços não utilizados para preservar os recursos do sistema, como ciclos de CPU e RAM, e impedir que os atores ameaçadores explorem esses serviços. O tipo de serviços que estão ativados por padrão varia dependendo da versão do IOS. Por exemplo, o IOS-XE normalmente terá apenas portas HTTPS e DHCP abertas. Você pode verificar isso com o comando **show ip ports all**.

```
Router# show ip ports all
Proto Local Address              Foreign Address            State       PID/Program Name
TCB       Local Address              Foreign Address            (state)
tcp    :::443                    :::*                       LISTEN      309/[IOS]HTTP CORE
tcp    *:443                     *:*                        LISTEN      309/[IOS]HTTP CORE
udp    *:67                       0.0.0.0:0                              387/[IOS]DHCPD Receive
```

Versões anteriores do IOS ao IOS-XE usam o comando **show control-plane host open-ports**. A saída é semelhante. No entanto, observe que este roteador mais antigo tem um servidor HTTP inseguro e Telnet em execução. Ambos os serviços devem ser desativados com o comando de configuração global **no ip http server** e especificando apenas SSH no comando de configuração de linha, **transport input ssh**.

```
Router# show control-plane host open-ports
Active internet connections (servers and established)
Prot        Local Address      Foreign Address                Service    State
 tcp                *:23                *:0                    Telnet   LISTEN
 tcp                *:80                *:0                 HTTP CORE   LISTEN
 udp                *:67                *:0             DHCPD Receive   LISTEN
Router# configure terminal
Router(config)# no ip http server
Router(config)# line vty 0 15
Router(config-line)# transport input ssh
```

Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy

Networking Academy

WOMENROCK-IT

CCNAv7 – ITN – Criação de uma rede pequena

Módulo 17

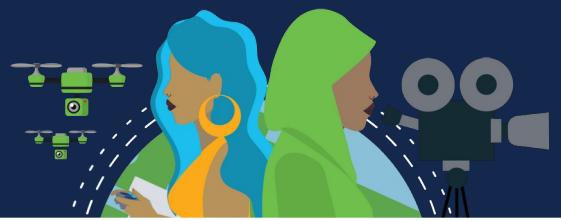
Embaixadores do Programa 2020, 2021 & 2022:

Organizadoras Cisco: Eliana Silva, Veruska Clednev
Professores Coordenadores: Marissol Barros, Moisés Nisenbaum

WOMENROCK-IT
Brasil 2021

Networking Academy

Criação de uma rede pequena



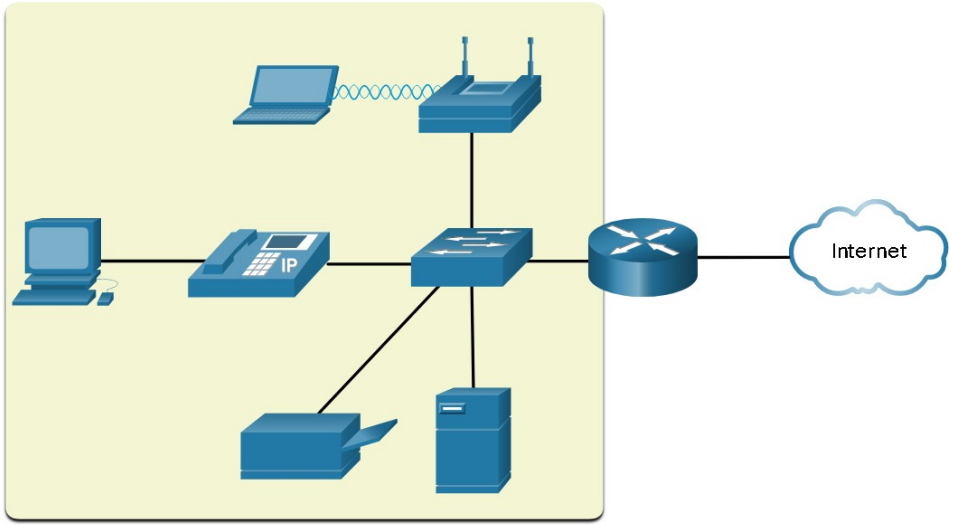
Dispositivos em uma Rede Pequena

Topologias de Redes Pequenas

A maioria das empresas são pequenas; portanto, a maioria das redes empresariais também são pequenas.

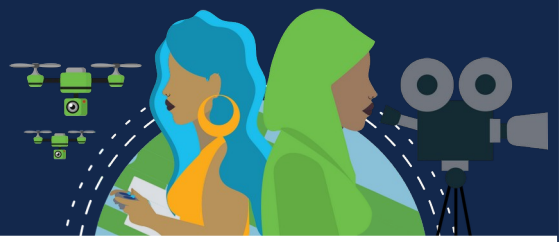
Um pequeno design de rede geralmente é simples. Uma pequena rede requer um roteador, um switch e um ponto de acesso sem fio para conectar usuários com fio e sem fio, um telefone IP, uma impressora e um servidor. Redes pequenas geralmente têm uma única conexão WAN fornecida por DSL, cabo ou conexão Ethernet.

Redes grandes exigem que um departamento de TI mantenha, proteja e solucione problemas de dispositivos de rede e proteja dados organizacionais. O gerenciamento de uma rede pequena exige muitas das mesmas qualificações profissionais exigidas para o gerenciamento de uma rede grande. Pequenas redes são gerenciadas por um técnico de TI local ou por um profissional contratado.



Fonte: Cisco

Dispositivos em uma Rede Pequena

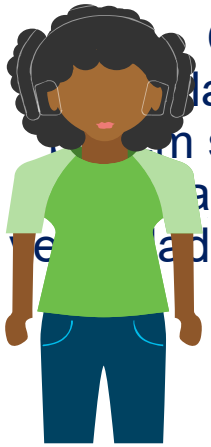


Seleção de Dispositivos para uma Rede Pequena

Redes pequenas também exigem planejamento e design para atender aos requisitos do usuário, assegurando que todos os fatores de custo e opções de implantação recebam a devida consideração. Uma das primeiras considerações de design é o tipo de dispositivos intermediários a serem usados.

Custo: É determinado pela capacidade e recursos dos dispositivos, incluindo o número, os tipos de portas e a velocidade do backplane. Recursos de gerenciamento de rede, tecnologias de segurança incorporadas, tecnologias de comutação avançadas opcionais e despesas com o cabeamento necessário à conexão de cada dispositivo na rede também devem ser considerados, assim como a quantidade de redundância a ser incorporada no design.

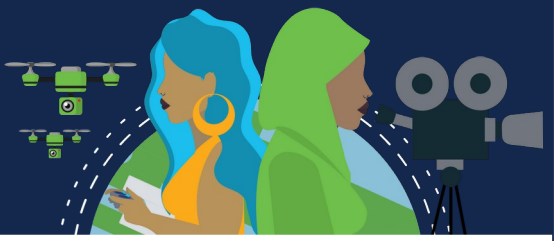
Velocidade e tipos de interfaces: Computadores mais novos possuem NICs de 1 Gbps incorporadas. Alguns servidores podem até ter portas de 10 Gbps. Embora seja mais caro, a escolha de dispositivos da Camada 2 que podem acomodar velocidades maiores permite que a rede evolua sem substituir os dispositivos centrais.



Capacidade de expansão: Os dispositivos de rede estão disponíveis em configurações físicas fixas e dulares. Os dispositivos de configuração fixa têm um número e tipo específico de portas ou interfaces e não m ser expandidos. Os dispositivos modulares possuem slots de expansão para adicionar novos módulos à a que os requisitos evoluem. Os switches são disponibilizados com portas adicionais para uplinks de alta de. Roteadores podem ser usados para conectar diferentes tipos de redes. Deve-se ter cuidado ao selecionar os módulos e interfaces apropriados para as mídias específicas.

Fonte: Cisco

Dispositivos em uma Rede Pequena

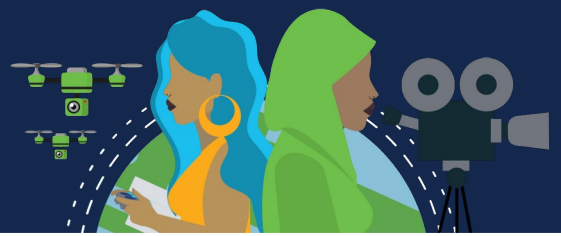


Seleção de Dispositivos para uma Rede Pequena

Recursos e serviços do sistema operacional: Os dispositivos de rede devem ter sistemas operacionais que possam suportar os requisitos da organização, como os seguintes:

- Switching de Camada 3
- Tradução de Endereço de Rede (NAT)
- Protocolo de Configuração Dinâmica de Host (DHCP)
- Segurança
- Qualidade de Serviço (QoS – Quality-of-Service).
- VoIP (Voice over IP)

Fonte: Cisco



Dispositivos em uma Rede Pequena

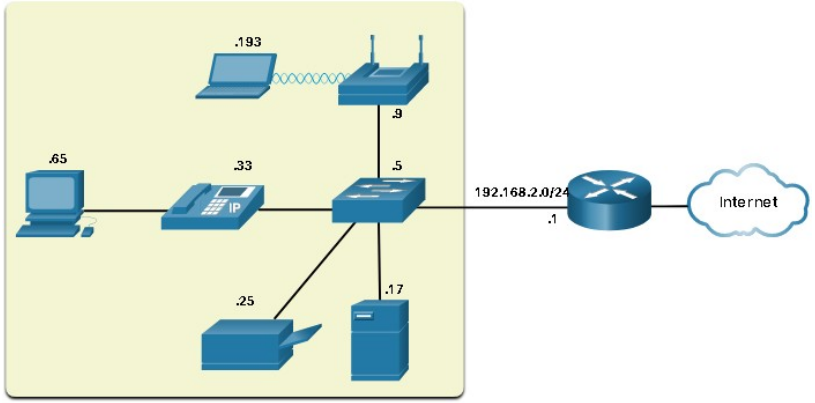
Endereçamento IP para uma rede pequena

Ao implementar uma rede, crie um esquema de endereçamento IP e use-o. Todos os hosts e dispositivos em uma rede devem ter um endereço exclusivo.

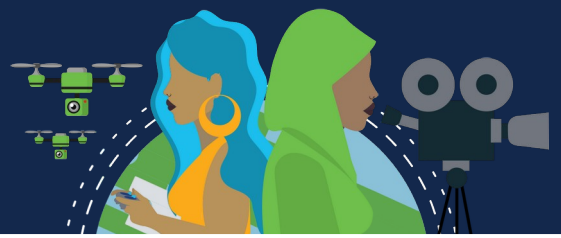
Os dispositivos que serão fatoriais no esquema de endereçamento IP incluem o seguinte:

- **Dispositivos do usuário final:** O número e o tipo de conexão (ou seja, com fio, sem fio, acesso remoto)
- **Servidores e dispositivos periféricos** (por exemplo, impressoras e câmeras de segurança)
- **Dispositivos intermediários:** Incluindo switches e pontos de acesso

É recomendável planejar, documentar e manter um esquema de endereçamento IP baseado no tipo de dispositivo. O uso de um esquema de endereçamento IP planejado facilita a identificação de um tipo de dispositivo e a solução de problemas, como por exemplo, ao solucionar problemas de tráfego de rede com um analisador de protocolo.



Fonte: Cisco



Dispositivos em uma Rede Pequena

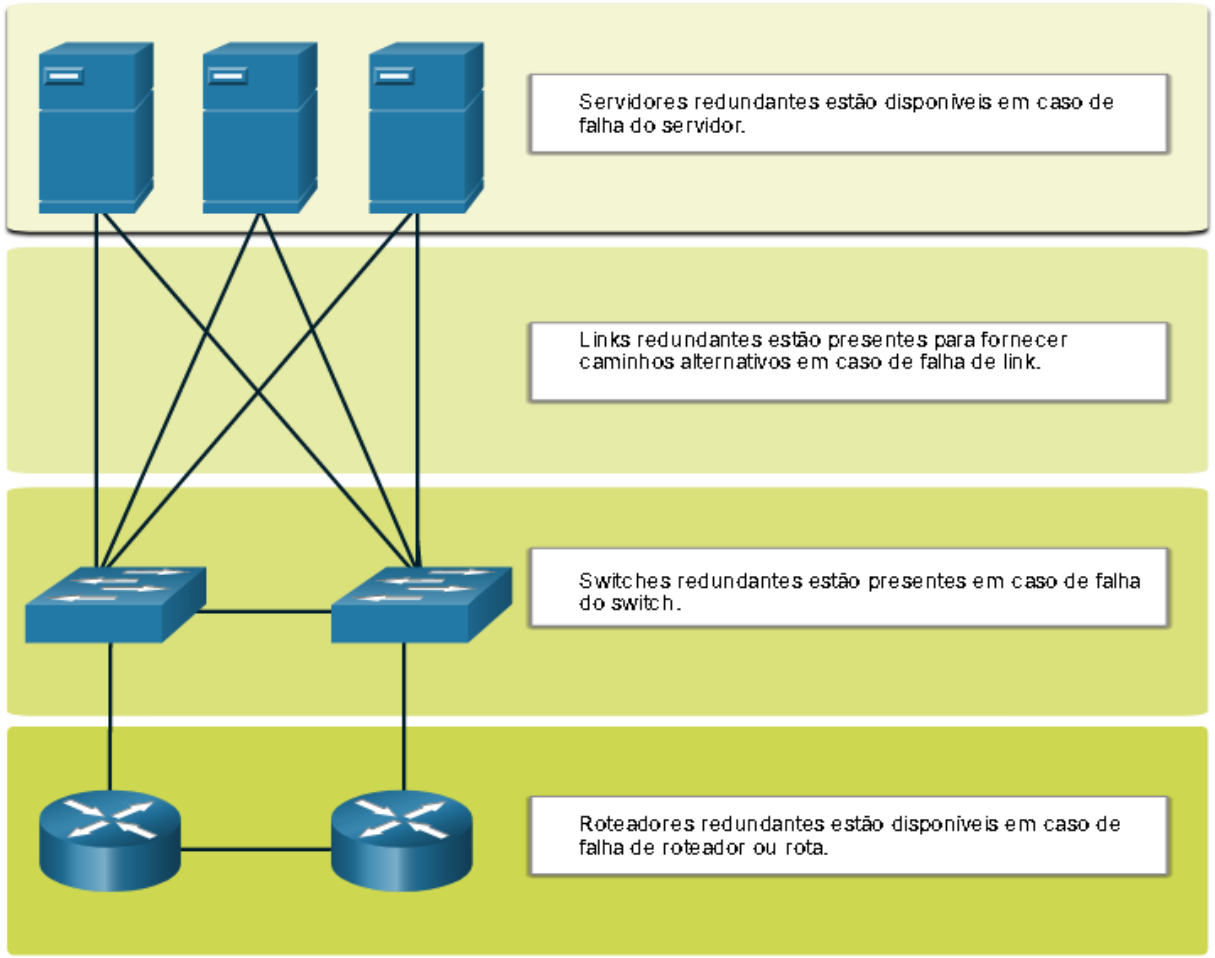
Redundância em uma Rede Pequena

Outra parte importante no projeto de rede é a confiabilidade. Em geral, mesmo as pequenas empresas confiam muito em suas redes para operações comerciais. Uma falha na rede pode sair bem cara.

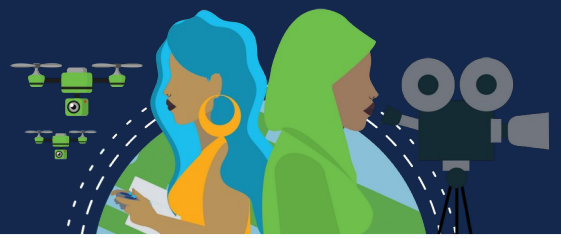
Para manter um alto grau de confiabilidade, redundância é necessária no design da rede. A redundância ajuda a eliminar os pontos únicos de falha.

Há várias maneiras de se efetuar redundância em uma rede. A redundância pode ser efetuada com a instalação de equipamento duplicado, mas também com o fornecimento de links de rede duplicados para áreas críticas.

Redes pequenas geralmente fornecem um único ponto de saída para a Internet por meio de um ou mais gateways padrão. Se o roteador falhar, a rede inteira perderá a conectividade com a Internet. Por essa razão, pode ser aconselhável para pequenas empresas contratar um segundo provedor de serviços como backup.



Fonte: Cisco

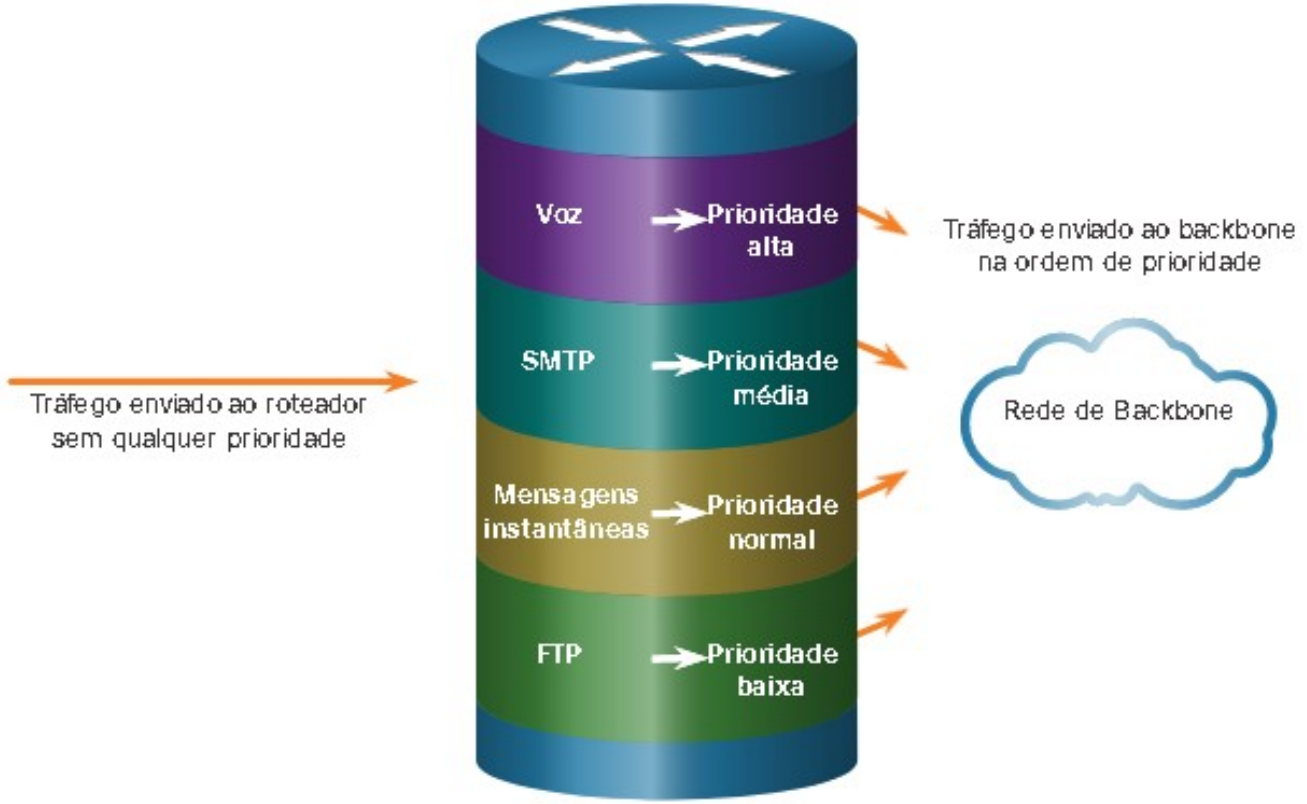


Dispositivos em uma Rede Pequena

Gerenciamento de Tráfego

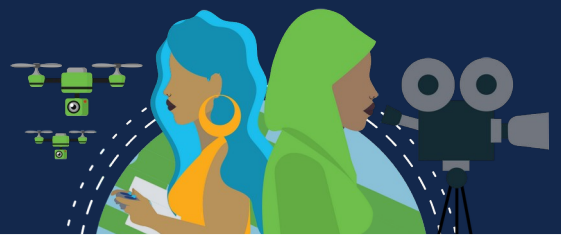
O objetivo de um bom design de rede, mesmo para uma pequena rede, é aumentar a produtividade dos funcionários e minimizar o tempo de inatividade da rede. O administrador de redes deve considerar os vários tipos de tráfego e o tratamento deles no projeto de rede.

Os roteadores e comutadores em uma rede pequena devem ser configurados para rastrear o tráfego em tempo real, como voz e vídeo, de maneira possível em relação a outro tráfego de dados. De fato, um bom design de rede implementará qualidade de serviço (QoS) para classificar o tráfego cuidadosamente de acordo com a prioridade.



O enfileiramento com prioridade tem quatro filas. A fila de prioridade alta é sempre esvaziada primeiro.

Fonte: Cisco



Aplicações e Protocolos de Redes Pequenas

Aplicações Comuns

Uma rede é tão útil quanto as aplicações que estão nela. Há duas formas de programas de software ou processos que fornecem acesso à rede: *aplicações de rede* e *serviços da camada de aplicação*.

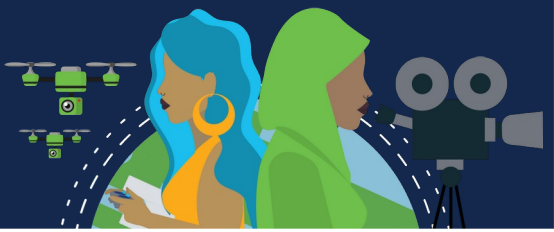
Aplicações de rede: Softwares usados para comunicação pela rede. Algumas aplicações de usuário final reconhecem a rede, o que significa que elas implementam protocolos da camada de aplicação e conseguem se comunicar diretamente com as camadas inferiores da pilha de protocolos. *Clientes de e-mail e navegadores são exemplos desse tipo de aplicação.*

Serviços de camada de aplicação: Outros programas precisam de assistência dos serviços da camada de aplicação para utilizar recursos da rede, como *transferência de arquivos ou spooling de impressão em rede*. Embora transparentes para um funcionário, esses serviços são os programas que fazem interface com a rede e preparam os dados para transferência. Diferentes tipos de dados (texto, gráficos ou vídeo), exigem serviços de rede diferentes para garantir que sejam preparados adequadamente para processamento pelas funções que ocorrem nas camadas inferiores do modelo OSI.

Cada aplicação ou serviço de rede utiliza protocolos que definem os padrões e formatos de dados a serem utilizados. Sem protocolos, a rede de dados não teria uma maneira comum de formatar e direcionar os dados. Para entender a função de vários serviços de rede, é necessário se familiarizar com os protocolos subjacentes que regem sua operação.

Fonte: Cisco

Aplicações e Protocolos de Redes Pequenas



Protocolos Comuns

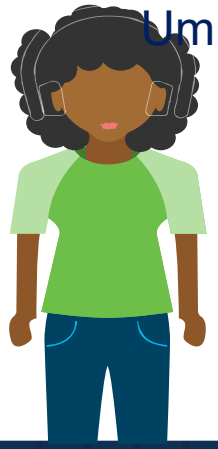
Protocolos de rede dão suporte às aplicações e serviços usados por funcionários em uma rede pequena.

Dispositivos e servidores de rede exigem acesso remoto. As duas soluções mais comuns são Telnet e Secure Shell (SSH). **Dispositivos de rede** e **Servidores** devem suportar SSH para estabelecer uma conexão de acesso remoto segura . Os administradores também devem oferecer suporte a servidores e protocolos de rede comuns;

Servidor web: Usa HTTP (Hypertext Transfer Protocol) e Hypertext Transfer Protocol Secure (HTTPS).

Servidor de e-mail: Usa SMTP (Simple Mail Transfer Protocol) para enviar e-mails, POP3 (Protocolo de correio eletrônico) ou o IMAP (Internet Message Access Protocol) para receber o e-mail.

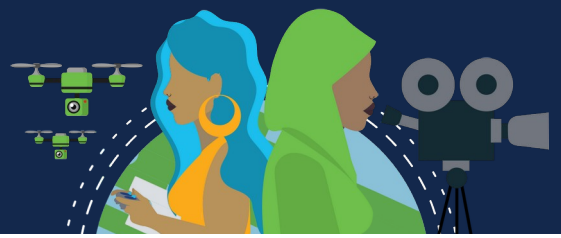
Servidor FTP: Usa File Transfer Protocol (FTP), FTP Secure (FTPS) e Secure FTP (SFTP) para transferência de arquivos.



Um servidor pode fornecer vários serviços de rede e sempre que possível deve usar as versoes seguras como SSH, SFTP e HTTPS. Cada um desses protocolos de rede define:

- Processos em cada extremidade de uma sessão de comunicação
- Tipos de mensagens
- Sintaxe das mensagens
- Significado dos campos de informação
- Como as mensagens são enviadas e a resposta esperada
- Interação com a próxima camada inferior

Fonte: Cisco



Aplicações e Protocolos de Redes Pequenas

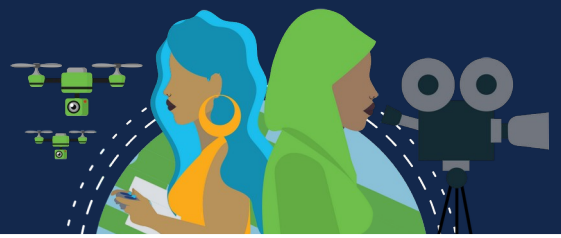
Aplicações de Voz e Vídeo

As empresas cada vez mais usam telefonia IP e streaming de mídia para se comunicar com os clientes e parceiros de negócios. Muitas organizações estão permitindo que seus funcionários trabalhem remotamente. Usuários ainda precisam de acesso a software e arquivos corporativos, bem como suporte para aplicativos de voz e vídeo.

O administrador de redes deve assegurar que o equipamento adequado foi instalado na rede e que os dispositivos de rede foram configurados para garantir entrega prioritária.

Infraestrutura	• A infra-estrutura de rede deve suportar os aplicativos em tempo real. • Os dispositivos e cabos existentes devem ser testados e validados. • Produtos de rede mais recentes podem ser necessários.
VoIP	• Os dispositivos de VoIP convertem sinais telefônicos analógicos em pacotes IP digitais. • O VoIP é mais barato que uma solução de telefonia IP, mas a qualidade não atende aos mesmos padrões. • Voz e vídeo podem ser resolvidos usando versões Skype e não empresariais do Cisco WebEx em redes menores.
Telefonia IP	• Realiza conversão de voz para IP com o uso de um servidor dedicado para controle de chamadas e sinalização. • Há soluções de telefonia IP para pequenas empresas, como os produtos Cisco Business Edition 4000 Series.
Aplicações de Voz e Vídeo	• A rede deve suportar mecanismos de qualidade de serviço (QoS) para minimizar problemas de latência para aplicativos de streaming em tempo real. • O Protocolo de Transporte em Tempo Real (RTP) e o Protocolo de Controle de Transporte em Tempo Real (RTCP) são dois protocolos que atendem à essa exigência.

Fonte: Cisco



Escalar para Redes Maiores

Crescimento das Redes Pequenas

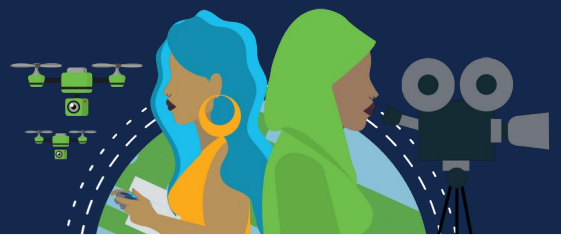
O crescimento é um processo natural para muitas empresas de pequeno porte, e suas redes devem acompanhá-lo. Idealmente, o administrador da rede deve ter tempo de entrega suficiente para tomar decisões inteligentes sobre o crescimento da rede alinhado com o crescimento da empresa.

Para escalonar uma rede, vários elementos são necessários:

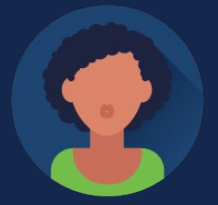
- **Documentação de rede:** Topologia física e lógica.
- **Inventário de dispositivos:** Lista de dispositivos que usam ou compreendem a rede.
- **Orçamento:** Orçamento de TI detalhado, incluindo orçamento de compra de equipamentos do ano fiscal.
- **Análise de tráfego:** Protocolos, aplicativos e serviços e seus respectivos requisitos de tráfego devem ser documentados.

Esses elementos são usados para subsidiar a tomada de decisão que acompanha o crescimento de uma rede pequena.

Fonte: Cisco



Escalar para Redes Maiores



Análise de Protocolos

À medida que a rede cresce, torna-se importante determinar como gerenciar o tráfego de rede. É importante entender o tipo de tráfego que está atravessando a rede, bem como o fluxo de tráfego atual. Existem várias ferramentas de gerenciamento de rede que podem ser usadas para esse fim. No entanto, um analisador de protocolo simples, como o Wireshark, também pode ser usado.

Executar o Wireshark em vários hosts principais pode revelar os tipos de tráfego de rede que flui através da rede.

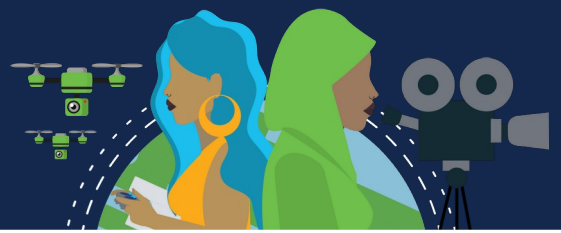
Para determinar os padrões de fluxo de tráfego, é importante fazer o seguinte:

- Capturar o tráfego durante as horas de pico de utilização para obter uma boa ideia dos diferentes tipos de tráfego.
- Realize a captura em diferentes segmentos e dispositivos de rede, pois algum tráfego será local para um segmento específico.

As informações reunidas pelo analisador de protocolos são avaliadas com base na origem e destino do tráfego, bem como no tipo de tráfego que é enviado. Essa análise pode ser usada para tomar uma decisão sobre como gerenciar o tráfego com mais eficiência. Isso pode ser feito com a redução de fluxos de tráfego desnecessários ou alterando totalmente os padrões de fluxo com a mudança de um servidor, por exemplo.

Algumas vezes, a simples mudança de um servidor ou serviço para outro segmento de rede melhora o desempenho da rede e acomoda as necessidades do tráfego crescente. Outras vezes, a otimização do desempenho da rede exige uma maior intervenção e um novo projeto da rede.

Fonte: Cisco



Verificar a conectividade

Verificar conectividade com ping

O comando **ping** é a maneira mais eficaz de testar rapidamente a conectividade da Camada 3 entre um endereço IP de origem e de destino. O comando também exibe várias estatísticas de tempo de ida e volta.

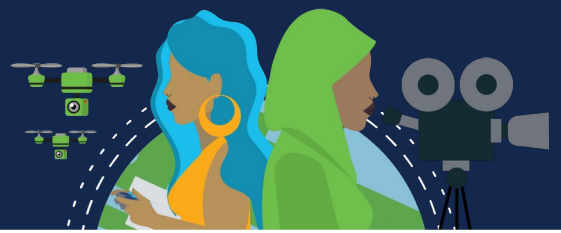
O ping usa as mensagens ICMP echo (ICMP Type 8) e echo reply (ICMP Type 0) e está disponível na maioria dos sistemas operacionais.

Em um host Windows 10, o comando ping envia quatro mensagens de eco ICMP consecutivas e espera quatro respostas de eco ICMP consecutivas do destino.

Em um Cisco IOS, o ping envia cinco mensagens de eco ICMP. O ping IOS exibe um indicador para cada resposta de eco ICMP recebida. A tabela lista os caracteres de saída mais comuns do comando ping .

!	• O ponto de exclamação indica o recebimento bem-sucedido de uma resposta de eco. • Ele valida uma conexão de Camada 3 entre origem e destino.
.	• Um período significa que o tempo expirou esperando por uma mensagem de resposta de eco. • Isso indica que ocorreu um problema de conectividade em algum lugar ao longo do caminho.
U	• “U” indica que um roteador, ao longo do caminho, respondeu com um destino ICMP Tipo 3 “ inacessível”. • Possíveis razões incluem que o roteador não sabe a direção para a rede de destino ou não foi possível localizar o host na rede de destino.

Fonte: Cisco



Verificar a conectividade

Utilização da Rede Pelos Funcionários

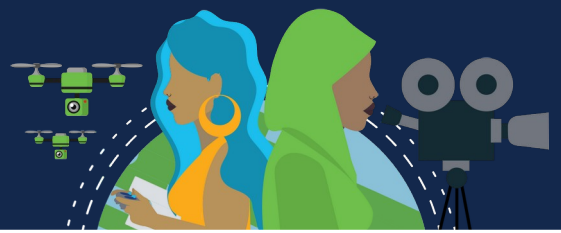
Além de entender as mudanças nas tendências de tráfego, um administrador de rede deve estar ciente de como o uso da rede está mudando. Muitos sistemas operacionais fornecem ferramentas integradas para exibir essas informações. O Windows fornece ferramentas como o Gerenciador de Tarefas, Visualizador de Eventos e Ferramentas de Uso de Dados que podem ser usadas para consultar o estado atual de informações e processos, como as seguintes:

- Sistema Operacional e a versão desse sistema;
- Utilização da CPU;
- Utilização da memória RAM;
- Utilização das unidades de disco;
- Aplicativos que não são de rede;
- Aplicações de rede.

Documentar snapshots para funcionários em uma pequena rede por um período de tempo é muito útil para identificar requisitos de protocolo em evolução e fluxos de tráfego associados. Uma mudança na utilização dos recursos pode requerer que o administrador de redes ajuste a alocação de recursos da rede proporcionalmente.

A ferramenta de uso de dados do Windows 10 é especialmente útil para determinar quais aplicativos estão usando serviços de rede em um host. A ferramenta de uso de dados é acessada usando **Settings > Network & Internet > Data usage > network interface** (dos últimos 30 dias).

Fonte: Cisco



Verificar a conectividade

Ping Estendido

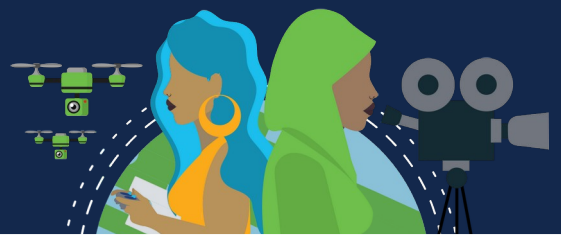
Um ping padrão usa o endereço IP da interface mais próxima da rede de destino como a origem do ping.

O Cisco IOS oferece um modo "estendido" do comando ping, que permite ao usuário ajustar parâmetros relacionados à operação de comando.

O ping estendido é inserido no modo EXEC privilegiado, digitando apenas ping sem um endereço IP de destino. Em seguida, você receberá vários prompts para personalizar o ping estendido. Ao pressionar *Enter* os valores padrão indicados são aceitos.

```
R1# ping
Protocol [ip]:
Target IP address: 10.1.1.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Ingress ping [n]:
Source address or interface: 192.168.10.1
DSCP Value [0]:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0x0000ABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Fonte: Cisco



Verificar a conectividade

Verifique a conectividade com o Traceroute

Traceroute ajuda a localizar áreas problemáticas da Camada 3 em uma rede, retornando uma lista dos saltos no roteamento de um pacote pela rede. Identifica o ponto ao longo do caminho onde pode existir um problema.

A sintaxe do comando varia entre sistemas operacionais.

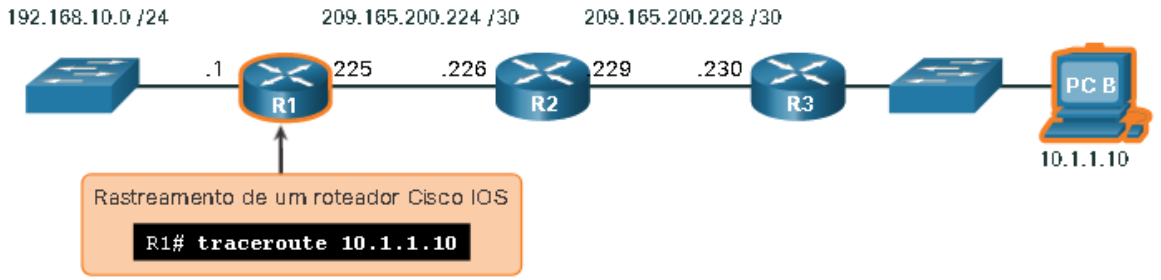
Solicitações de rastreamento para o próximo salto expiradas são indicadas pelo asterisco (*), significa que o próximo salto não respondeu. Indicam que há uma falha na rede ou que esses roteadores foram configurados para não responder às solicitações de eco usadas no rastreamento.

Use *Ctrl-Shift-6* para interromper um traceroute no Cisco IOS.

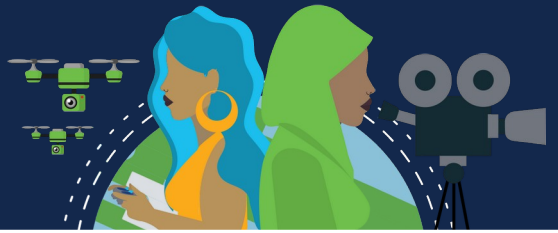
Observação: A implementação do traceroute (tracert) do Windows envia solicitações de eco do ICMP. Cisco IOS e Linux usam UDP com um número de porta inválido. O destino final retornará uma mensagem de porta ICMP inacessível.

```
C:\Users\PC-A> tracert 10.1.1.10
Tracing route to 10.1.10 over a maximum of 30 hops:
  1     2 ms     2 ms     2 ms  192.168.10.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
^C
```

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 mseg 0 mseg 1 mseg
  2 209.165.200.230 1 mseg 0 mseg 1 mseg
  3 10.1.1.10 1 ms 0 ms
```



Fonte: Cisco

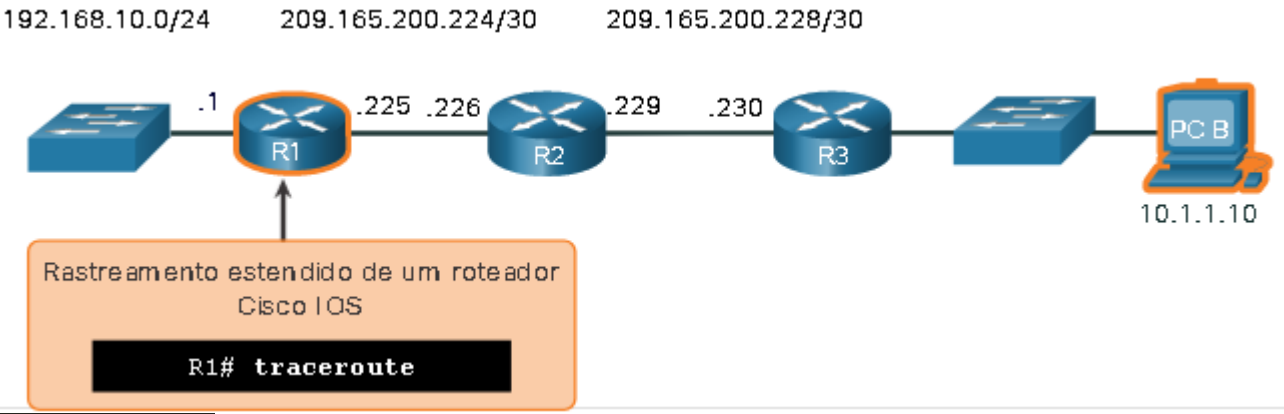


Verificar a conectividade

Traceroute estendido

Como o ping comando estendido, há também um comando **traceroute** estendido. Útil para solucionar loops de roteamento, determinar o roteador do próximo salto exato ou determinar onde os pacotes estão sendo descartados ou negados por um roteador ou firewall.

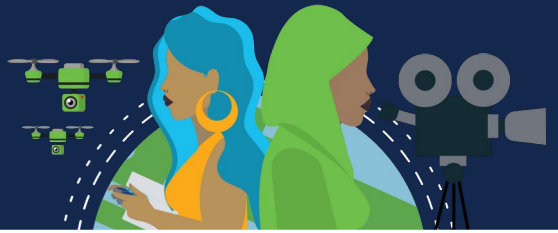
O comando **tracert** do Windows também permite a entrada de vários parâmetros, mas não é interativo como o comando encontrado no IOS.




```
R1# traceroute
Protocol [ip]:
Target IP address: 10.1.1.10
Ingress traceroute [n]:
Source address: 192.168.10.1
DSCP Value [0]:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.10.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 1 msec 1 msec
  2 209.165.200.230 0 msec 1 msec 0 msec
  3  *
    10.1.1.10 2 msec 2 msec
```

```
C:\Users\PC-A> tracert /?
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                  Do not resolve addresses to hostnames.
    -h maximum_hops     Maximum number of hops to search for target.
    -j host-list        Loose source route along host-list (IPv4-only).
    -w timeout          Wait timeout milliseconds for each reply.
    -R                  Trace round-trip path (IPv6-only).
    -S srcaddr          Source address to use (IPv6-only).
    -4                  Force using IPv4.
    -6                  Force using IPv6.
```

Fonte: Cisco



Verificar a conectividade

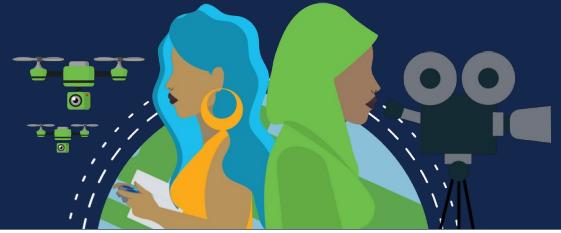
Linha de Base da Rede

Uma das ferramentas mais eficazes para o monitoramento e a solução de problemas de desempenho de rede é estabelecer uma linha de base da rede. A criação de uma linha de base de desempenho eficaz é realizada ao longo de um período de tempo. Medir o desempenho em momentos e cargas variados ajudará a criar uma imagem melhor do desempenho geral da rede.

O resultado derivado dos comandos de rede contribui com dados para a linha de base da rede. Um método para iniciar uma linha de base é copiar e colar os resultados de um comando executando ping, tracert (ou traceroute) ou outros comandos relevantes em um arquivo de texto. Esses arquivos de texto podem ser marcados com a data e salvos em um arquivo para posterior recuperação e comparação.

Entre itens a serem considerados estão mensagens de erro e os tempos de resposta host a host. Se houver um aumento considerável nos tempos de resposta, pode existir um problema de latência a ser resolvido.

Redes corporativas devem possuir linhas de base extensas, mais extensas do que podemos descrever neste curso. Ferramentas profissionais de software estão disponíveis para armazenamento e manutenção das informações de linha de base.



Host e comandos IOS

Configuração de IP em um host do Windows

Os comandos Host e IOS podem ajudá-lo a determinar se o problema é com o endereçamento IP dos seus dispositivos, o que é um problema comum de rede.

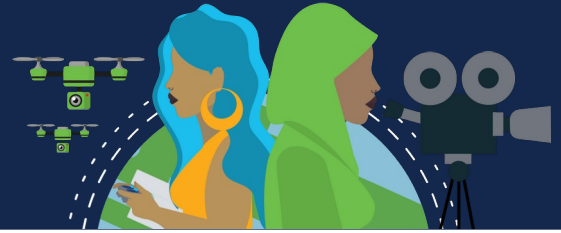
Verificar o endereçamento IP em dispositivos host é uma prática comum em rede para verificar e solucionar problemas de conectividade de ponta a ponta. No Windows 10, você pode acessar os detalhes do endereço IP do **Network and Sharing Center**, para visualizar rapidamente as quatro configurações importantes: *endereço, máscara, roteador* e *DNS.* O comando **ipconfig** na linha de comando de um computador Windows exibe as mesmas informações.

Use **ipconfig /all** para visualizar o endereço MAC, bem como vários detalhes sobre o endereçamento da Camada 3 do dispositivo.

Se um host estiver configurado como um cliente DHCP, a configuração do endereço IP poderá ser renovada usando **ipconfig /release** e **ipconfig /renew**.

O serviço Cliente DNS nos computadores com Windows também otimiza o desempenho da decisão do nome DNS ao armazenar nomes previamente definidos na memória. O comando **ipconfig /displaydns** exibe todas as entradas DNS armazenadas em cache em um sistema de computador Windows.

Fonte: Cisco



Host e comandos IOS

Configuração de IP em um host do Windows

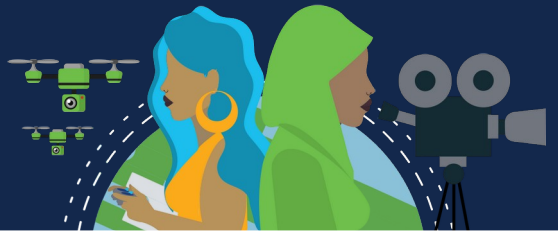
```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```

```
C:\Users\PC-A> ipconfig /release
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   Default Gateway . . . . . . . . . :
(Output omitted)
C:\Users\PC-A> ipconfig /renew
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.1.124
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
(Output omitted)
```

```
C:\Users\PC-A> ipconfig /displaydns
Windows IP Configuration
(Output omitted)
    netacad.com
    ----------------------------------------
    Record Name . . . . . : netacad.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 602
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 54.165.95.219
(Output omitted)
```

```
C:\Users\PC-A> ipconfig /all
Windows IP Configuration
   Host Name . . . . . . . . . . . . : PC-A-00H20
   Primary Dns Suffix  . . . . . . . : cisco.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cisco.com
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : F8-94-C2-E4-C5-0A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : August 17, 2019 1:20:17 PM
   Lease Expires . . . . . . . . . . : August 18, 2019 1:20:18 PM
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 100177090
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
   DNS Servers . . . . . . . . . . . : 192.168.10.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Fonte: Cisco



Host e comandos IOS

Configuração de IP em um host Linux

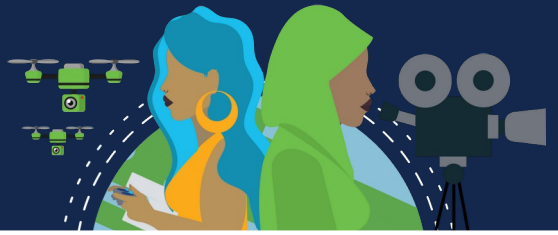
A verificação das configurações de IP usando a GUI em uma máquina Linux será diferente dependendo da distribuição Linux (distro) e da interface de desktop. No Ubuntu temos Connection Information que mostra o *endereço IP, máscara, gateway e DNS.*

O comando **ifconfig** também é usado para exibir o status das interfaces ativas no momento e sua configuração IP.

O comando Linux **ip address** é usado para exibir endereços e suas propriedades. Ele também pode ser usado para adicionar ou excluir endereços IP.

```
[analyst@secOps ~]$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:b5:d6:cb
          inet addr: 10.0.2.15  Bcast:10.0.2.255  Mask: 255.255.255.0
          inet6 addr: fe80::57c6:ed95:b3c9:2951/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1332239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105910 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1855455014 (1.8 GB)  TX bytes:13140139 (13.1 MB)
lo: flags=73  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Fonte: Cisco



Host e comandos IOS

Configuração de IP em um host macOS

Na GUI de um host Mac, abra *Network Preferences* > *Advanced* para obter as informações de endereçamento IP.

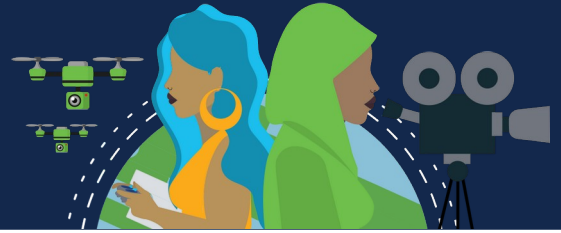
O comando **ifconfig** também pode ser usado para verificar a configuração IP da interface.

Outros comandos úteis do macOS para verificar as configurações de IP do host incluem **networksetup -listallnetworkservices** e o **networksetup -getinfo *<network service>*.**

```
MacBook-Air:~ Admin$ ifconfig en0
en0: flags=8863 mtu 1500
        ether c4:b3:01:a0:64:98
        inet6 fe80::c0f:1bf4:60b1:3adb%en0 prefixlen 64 secured scopeid 0x5
        inet 10.10.10.113 netmask 0xffffff00 broadcast 10.10.10.255
        nd6 options=201
        media: autoselect
        status: active
```

```
MacBook-Air:~ Admin$ networksetup -listallnetworkservices
An asterisk (*) denotes that a network service is disabled.
iPhone USB
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
MacBook-Air:~ Admin$
MacBook-Air:~ Admin$ networksetup -getinfo Wi-Fi
DHCP Configuration
IP address: 10.10.10.113
Subnet mask: 255.255.255.0
Router: 10.10.10.1
Client ID:
IPv6: Automatic
IPv6 IP address: none
IPv6 Router: none
Wi-Fi ID: c4:b3:01:a0:64:98
MacBook-Air:~ Admin$
```

Fonte: Cisco



Host e comandos IOS

O Comando arp

O comando **arp** é executado a partir do prompt de comando do Windows, Linux ou Mac. Ele lista todos os dispositivos atualmente no cache ARP do host, incluindo o endereço IPv4, endereço físico e o tipo de endereçamento (estático / dinâmico) para cada dispositivo.

O comando **arp -a** exibe o endereço IP conhecido e a ligação de endereço MAC que foram acessados recentemente.

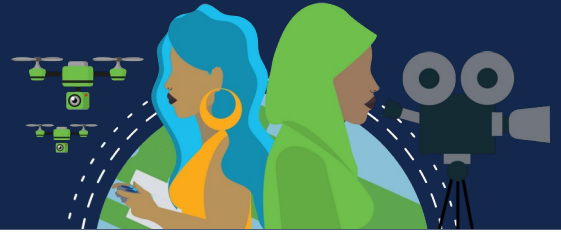
Use o **ping** para que um dispositivo tenha uma entrada na tabela ARP.

O cache pode ser limpo usando o comando **netsh interface ip delete arpcache**.

Você pode precisar de acesso de administrador no host para usar o comando netsh interface ip delete arpcache .

```
C:\Users\PC-A> arp -a
Interface: 192.168.93.175 --- 0xc
  Internet Address      Physical Address      Type
  10.0.0.2              d0-67-e5-b6-56-4b     dynamic
  10.0.0.3              78-48-59-e3-b4-01     dynamic
  10.0.0.4              00-21-b6-00-16-97     dynamic
  10.0.0.254            00-15-99-cd-38-d9     dynamic
```

Fonte: Cisco



Host e comandos IOS

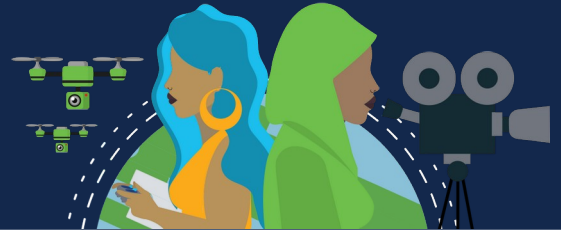
Comandos show Comuns Revisitados

O Cisco IOS fornece comandos para verificar a operação de interfaces de roteador e switch.

Os comandos **show** do Cisco IOS são usados extensivamente para exibir arquivos de configuração, verificar o status operacional do dispositivo, das interfaces e processos.

show running-config	Mostra a configuração atual.
show interfaces	Mostra o estado da interface e mensagens de erro.
show ip interface	Mostra informações da camada 3 na interface.
show arp	Mostra a lista de nós conhecidos na rede local.
show ip route	Mostra a tabela de rota e suas informações, na camada 3.
show protocols	Mostra quais protocolos estão operacionais.
show version	Mostra memória, interfaces e a licença do dispositivo.

Fonte: Cisco



Host e comandos IOS

Comandos show Comuns Revisitados

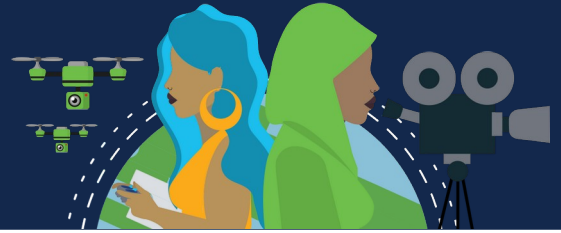
```
R1# show running-config

(Output omitted)

!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
interface GigabitEthernet0/0/0
 description Link to R2
 ip address 209.165.200.225 255.255.255.252
 negotiation auto
!
interface GigabitEthernet0/0/1
 description Link to LAN
 ip address 192.168.10.1 255.255.255.0
 negotiation auto
!
router ospf 10
 network 192.168.10.0 0.0.0.255 area 0
 network 209.165.200.224 0.0.0.3 area 0
!
banner motd ^C Authorized access only! ^C
!
line con 0
 password 7 14141B180F0B
 login
line vty 0 4
 password 7 00071A150754
 login
 transport input telnet ssh
!
end
```

```
R1# show interfaces
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 R2
  Internet address is 209.165.200.225/30
  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 00:00:21, 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
     5127 packets input, 590285 bytes, 0 no buffer
     Received 29 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 5043 multicast, 0 pause input
     1150 packets output, 153999 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 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
GigabitEthernet0/0/1 is up, line protocol is up
```

```
R1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1           -   a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  192.168.10.10         95   c07b.bcc4.a9c0  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.225         -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.226       138   a03d.6fe1.9d90  ARPA   GigabitEthernet0/0/0
```

```
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
O*E2  0.0.0.0/0 [110/1] via 209.165.200.226, 02:19:50, GigabitEthernet0/0/0
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/3] via 209.165.200.226, 02:05:42, GigabitEthernet0/0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 3 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/0
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/0
O        209.165.200.228/30
           [110/2] via 209.165.200.226, 02:07:19, GigabitEthernet0/0/0
```

Fonte: Cisco



Host e comandos IOS

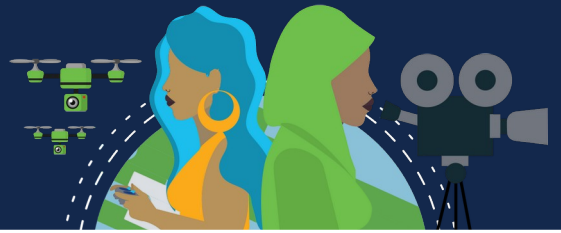
Comandos show Comuns Revisitados

```
R1# show version
Cisco IOS XE Software, Version 03.16.08.S - Extended Support Release
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5(3)S8, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 08-Aug-18 10:48 by mcpre

(Output omitted)

ROM: IOS-XE ROMMON
R1 uptime is 2 hours, 25 minutes
Uptime for this control processor is 2 hours, 27 minutes
System returned to ROM by reload
System image file is "bootflash:/isr4300-universalk9.03.16.08.S.155-3.S8-ext.SPA.bin"
Last reload reason: LocalSoft

(Output omitted)

Technology Package License Information:
------------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
------------------------------------------------------------------
appxk9        appxk9        RightToUse    appxk9
uck9          None          None          None
securityk9    securityk9    Permanent     securityk9
ipbase        ipbasek9      Permanent     ipbasek9
cisco ISR4321/K9 (1RU) processor with 1647778K/6147K bytes of memory.
Processor board ID FLM2044W0LT
2 Gigabit Ethernet interfaces
2 Serial interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
978928K bytes of USB flash at usb0:.
Configuration register is 0x2102
```

```
R1# show protocols
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 209.165.200.225/30
GigabitEthernet0/0/1 is up, line protocol is up
  Internet address is 192.168.10.1/24
Serial0/1/0 is down, line protocol is down
Serial0/1/1 is down, line protocol is down
GigabitEthernet0 is administratively down, line protocol is down
```

```
R1# show ip interface
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 209.165.200.225/30
  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
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  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
GigabitEthernet0/0/1 is up, line protocol is up
```

Fonte: Cisco



Host e comandos IOS

O Comando show cdp neighbors

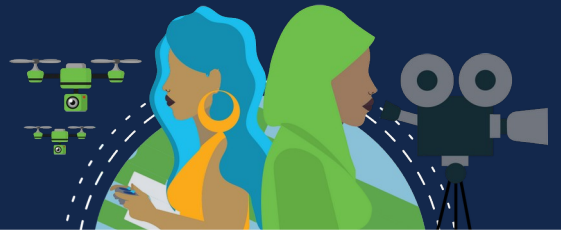
O *Cisco Discovery Protocol (CDP)* é um protocolo proprietário da Cisco que é executado na camada de enlace de dados. É ativo por padrão e descobre automaticamente dispositivos Cisco adjacentes com o CDP habilitado, independentemente de qual protocolo de Camada 3 esteja em execução. O CDP troca informações de hardware e software do dispositivo com seus vizinhos CDP diretamente conectados.

- **Identificadores de dispositivo:** Informa o nome do host configurado de um switch, roteador ou outro dispositivo.
- **Lista de endereços:** Até um endereço de camada de rede para cada protocolo suportado.
- **Identificador de porta:** O nome da porta local e remota na forma de uma cadeia de caracteres ASCII.
- **Lista de capacidades:** Informa se um dispositivo específico é um switch de Camada 2 ou um switch de Camada 3.
- **Plataforma:** Modelo de hardware do dispositivo.

O comando **show cdp neighbors detail** revela o endereço IP de um dispositivo vizinho, independentemente de você poder ou não executar ping nesse vizinho. Ajuda a determinar se um dos vizinhos do CDP possui um erro de configuração de IP.

O CDP, também pode ser um risco à segurança, por fornecer informações úteis aos agentes de ameaças. Por padrão muitas versões do IOS enviam anúncios CDP por todas as portas habilitadas. Entretanto, as melhores práticas sugerem que o CDP seja habilitado apenas em interfaces que se conectam a outros dispositivos Cisco e devem ser desativados em portas de usuário. Para desativar o CDP globalmente, use o comando **no cdp run**. Para desativar o CDP em uma interface, use o comando interface **no cdp enable**.

Fonte: Cisco

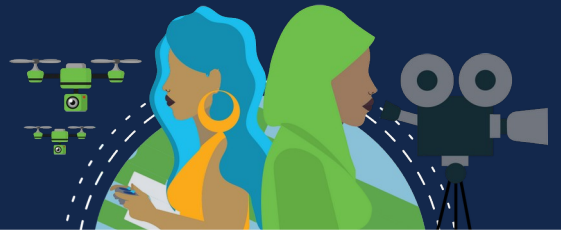


Host e comandos IOS

O Comando show cdp neighbors

```
R3# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S3               Gig 0/0/1         122              S I   WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#
```

Fonte: Cisco



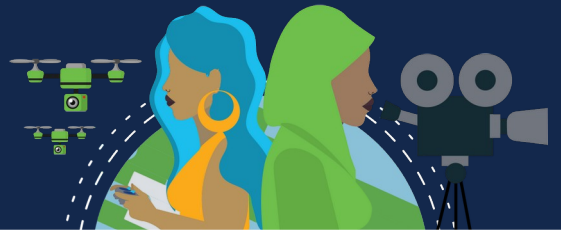
Host e comandos IOS

O Comando show ip interface brief

Um dos comandos mais frequentemente usados é o comando **show ip interface brief** . Este comando fornece uma saída mais abreviada que o comando **show ip interface**. Exibe um resumo das principais informações para todas as interfaces de rede em um roteador.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```

Fonte: Cisco



Metodologias de solução de problemas

Abordagens de solução de problemas básica

Os problemas de rede podem ser simples ou complexos e podem resultar de uma combinação de problemas de hardware, software e conectividade. Os técnicos precisam conseguir analisar o problema e identificar a causa do erro para poderem resolver a falha na rede. Esse processo é chamado de solução de problemas.

Para avaliar o problema, determine quantos dispositivos na rede estão enfrentando o problema. Se apenas um dispositivo na rede estiver enfrentando o problema, inicie o processo de solução de problemas por ele. Se todos os dispositivos na rede estiverem enfrentando o problema, inicie o processo de solução de problemas pelo dispositivo onde todos os outros dispositivos estiverem conectados. Você deve desenvolver um método lógico e consistente para diagnosticar problemas de rede eliminando um problema de cada vez.

Etapa 1: Identificar o problema é o primeiro passo no processo de solução de problemas. Ferramentas são usadas nessa etapa e uma conversa com o usuário é normalmente muito útil.

Etapa 2: Estabelecer uma lista de causas prováveis.

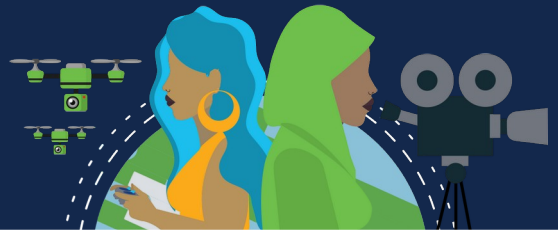
Etapa 3: Testar cada uma das causas prováveis para determinar o motivo exato.

Etapa 4: Estabelecer um plano de ação e implementar a solução.

Etapa 5: Verifique a solução e implemente medidas preventivas.

Etapa 6: Documentar descobertas, ações e resultados para referência futura.

Fonte: Cisco

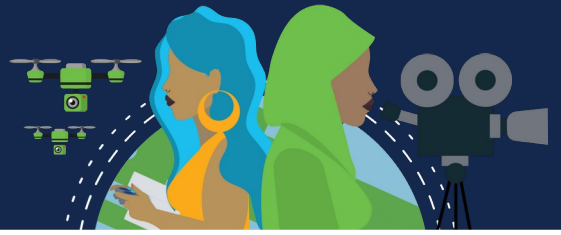


Metodologias de solução de problemas

Resolver ou escalonar?

Em algumas situações, talvez não seja possível resolver o problema imediatamente. O problema deve ser escalado quando requer uma decisão do gerente, algum conhecimento específico ou nível de acesso à rede indisponível para o técnico de solução de problemas ou abertura de chamado com provedores de serviços, como substituição de um módulo de roteador em garantia ou queda de um link WAN.

Uma política da empresa deve indicar claramente quando e como um técnico deve escalar um problema.



Metodologias de solução de problemas

O comando de debug

Processos, protocolos, mecanismos e eventos do SO geram mensagens para comunicar seu status, com informações valiosas para solucionar problemas ou verificar operações do sistema. O comando IOS **debug** exibe essas mensagens em tempo real para análise. É uma ferramenta muito importante para monitorar eventos em um dispositivo Cisco IOS.

Comando inserido no modo EXEC privilegiado. O Cisco IOS permite restringir a saída para “debugar” apenas o recurso ou funcionalidade relevante. Isso é importante porque a depuração da saída recebe alta prioridade no processo da CPU e pode travar o sistema. Use o debug apenas para solucionar problemas específicos.

Para monitorar o status das mensagens ICMP em um roteador Cisco, use **debug ip icmp**.

Para listar uma breve descrição de todas as opções de comando de depuração, use o comando **debug ?**.

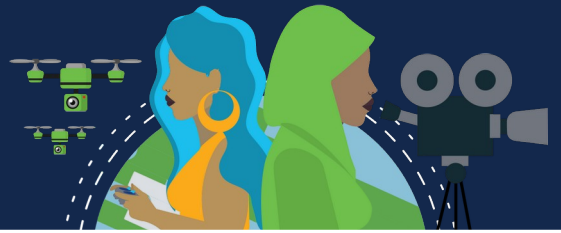
Para desativar um recurso de depuração específico, adicione **no** na frente do debug comando, **no debug ip icmp**.

Como alternativa, você pode inserir o comando **undebug**.

Para desativar todos os comandos de depuração ativos de uma só vez, use o comando **undebug all**.

Comandos **como debug all** e **debug ip packet** geram uma quantidade substancial de saída e podem usar uma grande parte dos recursos do sistema. O uso dessas opções de comando não é recomendável e deve ser evitado.

Fonte: Cisco

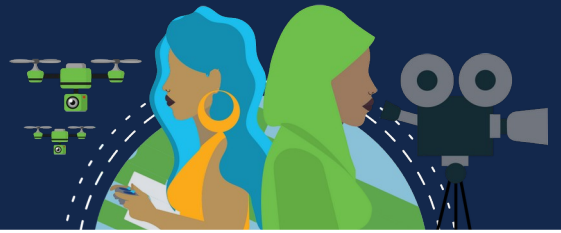


Metodologias de solução de problemas

O comando de debug

```
R1# debug ip icmp
ICMP packet debugging is on
R1#
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 14:18:59.605: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.606: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.608: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.609: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.611: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
```

Fonte: Cisco



Metodologias de solução de problemas

O Comando terminal monitor

As conexões para conceder acesso à interface da linha de comandos do IOS podem ser estabelecidas das seguintes maneiras:

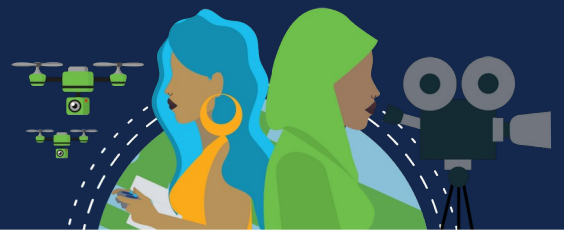
Localmente: As conexões locais (ou seja, a conexão do console) requerem acesso físico à porta do console do roteador ou do switch usando um cabo de sobreposição.

Remotamente: As conexões remotas exigem o uso de Telnet ou SSH para estabelecer uma conexão com um dispositivo configurado por IP.

Determinadas mensagens IOS são exibidas automaticamente em uma conexão de console, mas não em uma conexão remota. A saída debug é exibida por padrão em conexões de console, mas não em conexões remotas. Isso ocorre porque as mensagens debug são mensagens de log, que são impedidos de serem exibidas em linhas vty.

Para exibir mensagens de log em um terminal (console virtual), use o comando **terminal monitor** no modo EXEC privilegiado. Para parar de registrar mensagens em um terminal, use o comando **terminal no monitor**

. Observação: A intenção do comando debug é capturar a saída imediata de um retorno de um processo (comando na memória), por um curto período de tempo (ou seja, alguns segundos a um minuto ou mais). Desative sempre debug quando não for necessário.



Cenários de solução de problemas

Problemas de operação duplex e incompatibilidade

Nas comunicações de dados, **duplex** refere-se à direção da transmissão de dados entre dois dispositivos. São dois modos de comunicação duplex:

Half-duplex: A comunicação é restrita à troca de dados em uma direção por vez.

Full-duplex: As comunicações podem ser enviadas e recebidas simultaneamente.

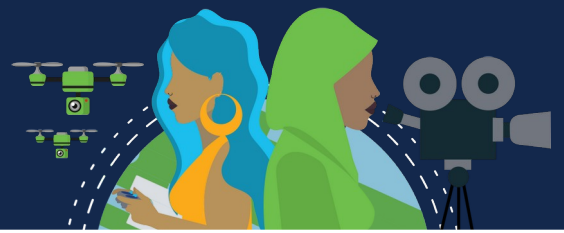
As interfaces Ethernet de interconexão devem operar no mesmo modo duplex para obter melhor desempenho de comunicação e evitar ineficiência e latência no link.

O recurso de negociação automática Ethernet facilita a configuração, minimiza problemas e maximiza o desempenho do link entre dois links Ethernet interconectados. Primeiramente, os dispositivos conectados anunciam seus recursos de compatibilidade e, depois, escolhem o modo de desempenho mais alto, compatível com as duas extremidades.

Se um dos dois dispositivos conectados estiverem operando no modo full-duplex e o outro no modo half-duplex, ocorrerá uma incompatibilidade de duplex. Já que a comunicação de dados ocorre por meio de um link físico, no caso de uma incompatibilidade de duplex o desempenho do link físico seria muito ruim.

As incompatibilidades duplex são normalmente causadas por uma interface mal configurada ou, em casos raros, por uma negociação automática com falha. As incompatibilidades de duplex podem ser difíceis de resolver, visto que a comunicação entre os dispositivos continua ocorrendo.

Fonte: Cisco



Cenários de solução de problemas

Problemas de endereçamento IP em dispositivos IOS

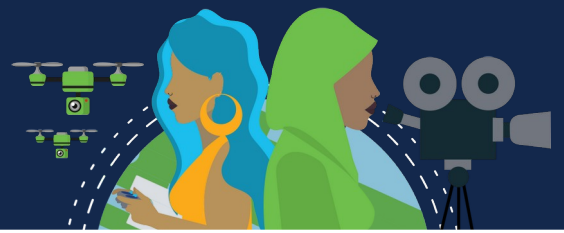
Os problemas relacionados ao endereço IP provavelmente impedirão que os dispositivos de rede remota se comuniquem. Como os endereços IP são hierárquicos, qualquer endereço IP atribuído a um dispositivo de rede deve estar em conformidade com esse intervalo de endereços nessa rede. Endereços IP atribuídos erroneamente geram diversos problemas, inclusive conflitos de endereços IP e problemas de roteamento.

Duas causas comuns de atribuição de IPv4 incorreta são os erros de atribuição manual ou problemas relacionados a DHCP.

Os administradores de rede normalmente precisam atribuir de forma manual os endereços IP aos dispositivos, como servidores e roteadores. Se for cometido um erro durante a atribuição, provavelmente ocorrerão problemas de comunicação com o dispositivo.

Em um dispositivo IOS, use os comandos **show ip interface** ou **show ip interface brief** para verificar quais endereços IPv4 estão atribuídos às interfaces de rede.

Fonte: Cisco



Cenários de solução de problemas

Problemas de endereçamento IP em dispositivos finais

Em máquinas com Windows, quando o dispositivo não consegue entrar em contato com um servidor DHCP, o Windows atribui automaticamente um endereço que pertence ao intervalo **169.254.0.0/16**. Esse recurso é chamado de endereçamento IP privado automático (**APIPA**) e foi projetado para facilitar a comunicação dentro da rede local. Pense nisso como o Windows dizendo: "Usarei esse endereço no intervalo 169.254.0.0/16 porque não consegui nenhum outro endereço".

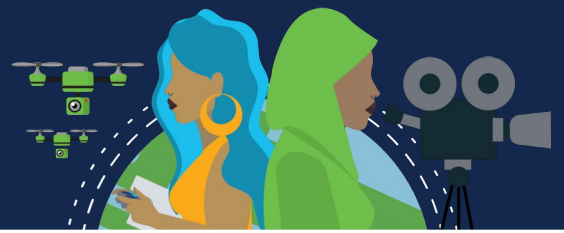
Frequentemente, um computador com um endereço APIPA não poderá comunicar-se com outros dispositivos na rede, porque esses dispositivos provavelmente não pertencerão à rede 169.254.0.0/16. Essa situação indica um problema de atribuição automática de endereço IPv4 que precisa ser corrigido.

Observação: Outros sistemas operacionais, como Linux e OS X, não atribuirão um endereço IPv4 à interface de rede se a comunicação com um servidor DHCP falhar.

A maioria dos dispositivos finais são configurados por um servidor DHCP para a atribuição automática de endereço IPv4. Se o dispositivo não puder comunicar-se com o servidor DHCP, o servidor não conseguirá atribuir um endereço IPv4 para a rede específica e o dispositivo não será capaz de comunicar-se.

Para verificar os endereços IP atribuídos a um computador com Windows, use o comando **ipconfig**.

Fonte: Cisco



Cenários de solução de problemas

Problemas de Gateway padrão

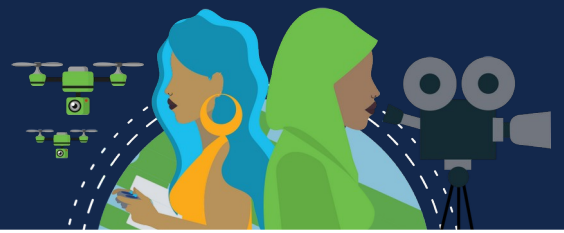
O gateway padrão de um dispositivo final é o dispositivo de rede mais próximo que pode encaminhar o tráfego para outras redes. Se um dispositivo tiver um endereço de gateway padrão errado ou inexistente, ele não conseguirá se comunicar com os dispositivos em redes remotas. Como o gateway padrão é o caminho para as redes remotas, seu endereço precisa pertencer à mesma rede que o dispositivo final.

O endereço do gateway padrão pode ser manualmente definido ou obtido de um servidor DHCP. Semelhantes aos problemas de endereçamento IPv4, os problemas de gateway padrão podem estar relacionados à configuração errada (no caso de atribuição manual) ou a problemas de DHCP (se a atribuição manual estiver em uso).

Para solucionar problemas de gateway padrão configurados incorretamente verifique se o endereço foi manualmente configurado e basta substituí-lo. Se o endereço de gateway padrão foi definido automaticamente, verifique se o dispositivo pode se comunicar com o servidor DHCP. Também é importante verificar se o endereço IPv4 e a máscara de sub-rede adequados foram configurados na interface do roteador e se a interface está ativa.

Em um roteador, use o comando **show ip route** para listar a tabela de roteamento e verifique se o gateway padrão, conhecido como rota padrão, foi definido. Essa rota é usada quando o endereço de destino do pacote não corresponde a nenhuma outra rota na tabela de roteamento.

Fonte: Cisco

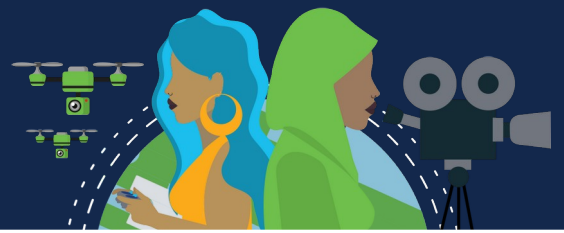


Cenários de solução de problemas

Problemas de Gateway padrão

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/1] via 209.165.200.226, 02:19:50, GigabitEthernet0/0/0
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/3] via 209.165.200.226, 02:05:42, GigabitEthernet0/0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 3 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/0
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/0
O        209.165.200.228/30
           [110/2] via 209.165.200.226, 02:07:19, GigabitEthernet0/0/0
```

Fonte: Cisco



Cenários de solução de problemas

Como solucionar problemas de DNS

É comum que os usuários relacionem por engano a operação de um link da Internet com a disponibilidade do DNS. As reclamações de usuários como "*a rede está inoperante*" ou "*a internet está inoperante*" geralmente são causadas por um servidor DNS inacessível. O roteamento de pacotes e todos os serviços de rede continuam em operação, mas falhas de DNS normalmente levam o usuário à conclusão errada.

Os endereços de servidor DNS podem ser atribuídos de forma manual ou automática.

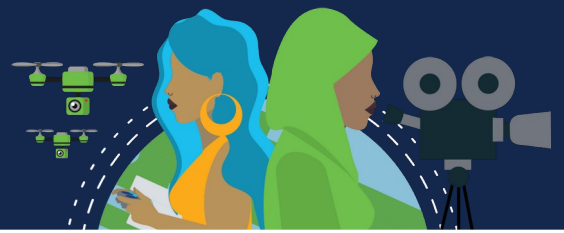
É comum as empresas gerenciarem seus próprios servidores DNS, qualquer servidor DNS alcançável pode ser usado para resolver nomes. Os usuários de SOHO (Small office and home office, pequeno escritório e escritório doméstico) normalmente contam com o servidor DNS mantido pelo seu ISP. O Google mantém um servidor DNS público que pode ser usado por qualquer pessoa e é muito útil para testes, endereços *8.8.8.8* e *2001:4860:4860::8888*.

A Cisco oferece *OpenDNS* que fornece serviço DNS seguro filtrando phishing e alguns sites de malware. Você pode alterar seu endereço DNS para *208.67.222.222* e *208.67.220.220*. Recursos avançados, como filtragem de conteúdo da Web e segurança, estão disponíveis para famílias e empresas.

Use o **ipconfig /all** como mostrado para verificar qual servidor DNS está sendo usado pelo computador Windows.

O comando **nslookup** é útil na solução de problemas DNS para PCs. Permitindo consultar e analisar manualmente as respostas DNS.

Fonte: Cisco



Cenários de solução de problemas

Como solucionar problemas de DNS

```
C:\Users\PC-A> nslookup
Default Server:  Home-Net
Address:  192.168.1.1
> cisco.com
Server:  Home-Net
Address:  192.168.1.1
Non-authoritative answer:
Name:    cisco.com
Addresses:  2001:420:1101:1::185
          72.163.4.185
> 8.8.8.8
Server:  Home-Net
Address:  192.168.1.1
Name:    dns.google
Address:  8.8.8.8
>
> 208.67.222.222
Server:  Home-Net
Address:  192.168.1.1
Name:    resolver1.opendns.com
Address:  208.67.222.222
>
```

```
C:\Users\PC-A> ipconfig /all
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : F8-94-C2-E4-C5-0A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : August 17, 2019 1:20:17 PM
   Lease Expires . . . . . . . . . . : August 18, 2019 1:20:18 PM
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 100177090
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
   DNS Servers . . . . . . . . . . . : 208.67.222.222
   NetBIOS over Tcpip. . . . . . . . : Enabled
(Output omitted)
```

Fonte: Cisco

Networking Academy
cisco

WOMEN ROCK-IT

Obrigade!

Networking Academy