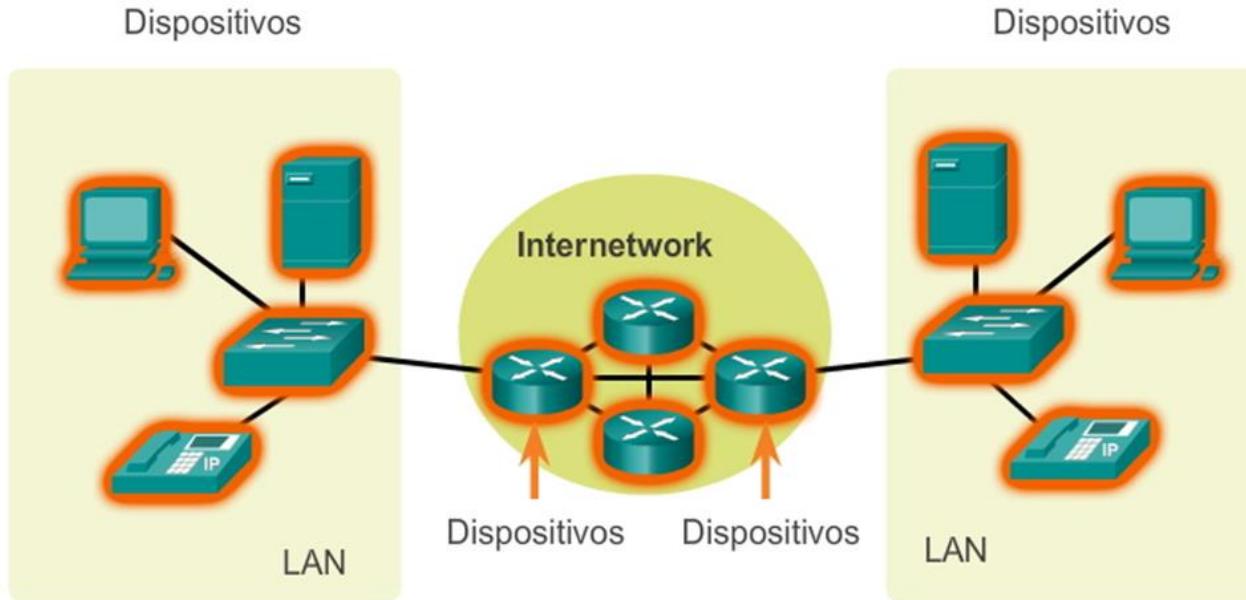


Capítulo 1

Introdução às Redes de Computadores

- Infraestrutura de redes
 - ✓ Equipamentos de rede (Switches, Routers, AP, . . .) e Meios de comunicação
 - ✓ LAN, WAN e interligação de redes
- Endereçamento IP
- Configuração de equipamentos de rede
 - ✓ Fundamentos do Sistema Operativo da CISCO – IOS
- O simulador de redes: Packet Tracer.

Equipamentos de rede e Meios de comunicação

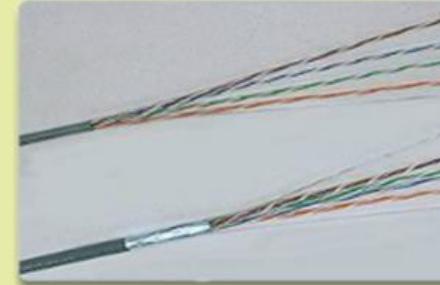


- Há duas categorias de componentes de rede:
 - ✓ Dispositivos
 - ✓ Meio físico

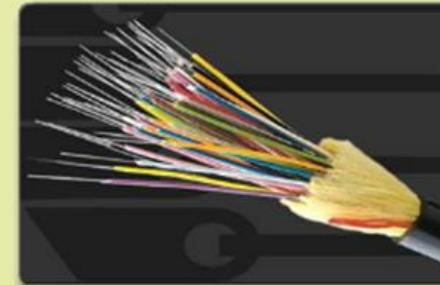
- Alguns exemplos de dispositivos finais são:
 - ✓ Computadores (estações de trabalho, laptops, servidores de ficheiros, servidores Web)
 - ✓ Impressoras de rede
 - ✓ Telefones VoIP
 - ✓ Terminais de TelePresença
 - ✓ Câmaras de segurança
 - ✓ Dispositivos móveis (como smartphones, tablets, PDAs, e também leitores de cartões de débito/crédito sem fios e scanners de código de barras)

- Exemplos de dispositivos intermediários de rede são:
 - ✓ Dispositivos de acesso à rede (switches e pontos de acesso sem fio)
 - ✓ Dispositivos de Redes Interligadas (routers)
 - ✓ Dispositivos de Segurança (firewalls)

Cobre



Fibra óptica



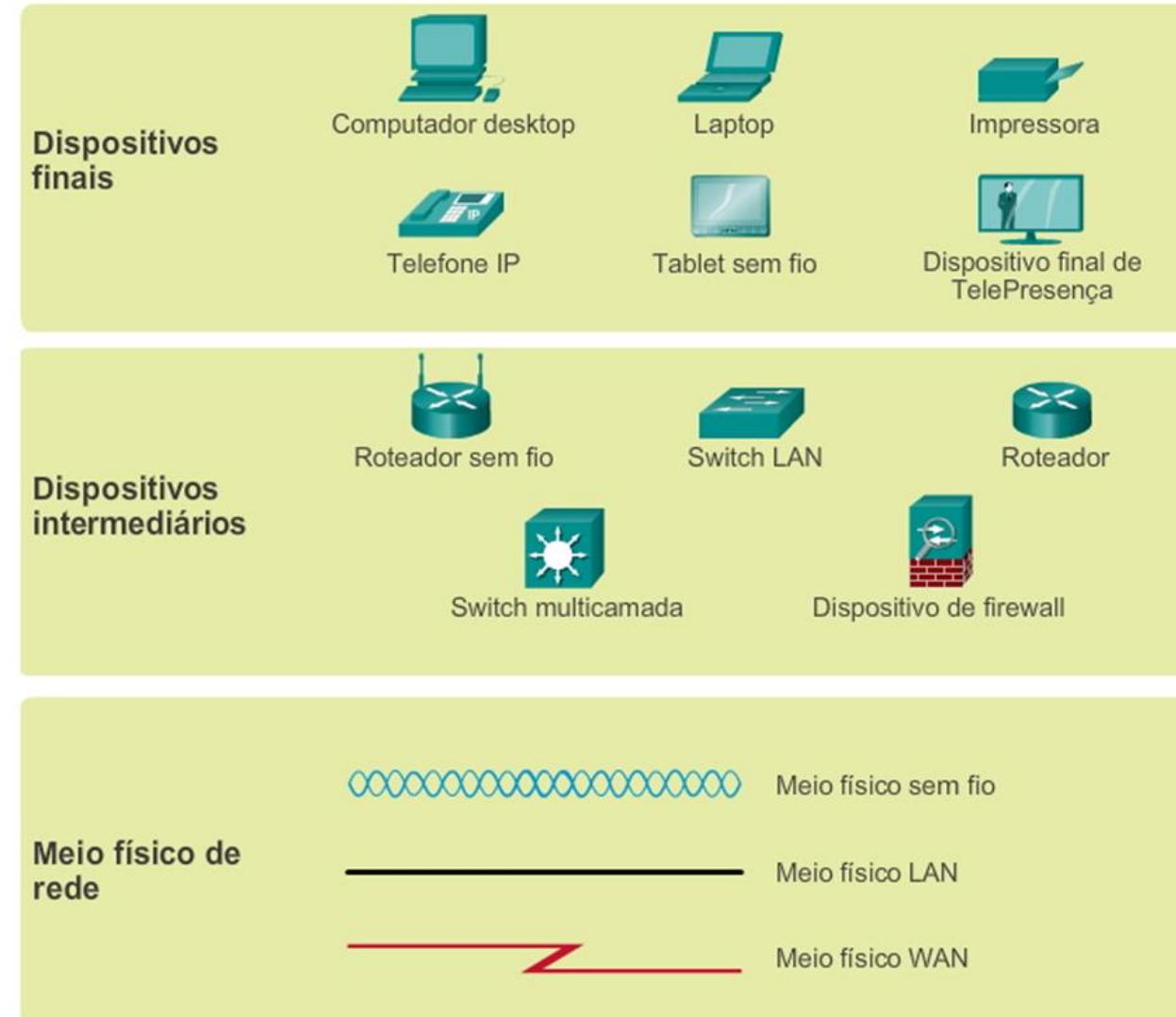
Sem fio

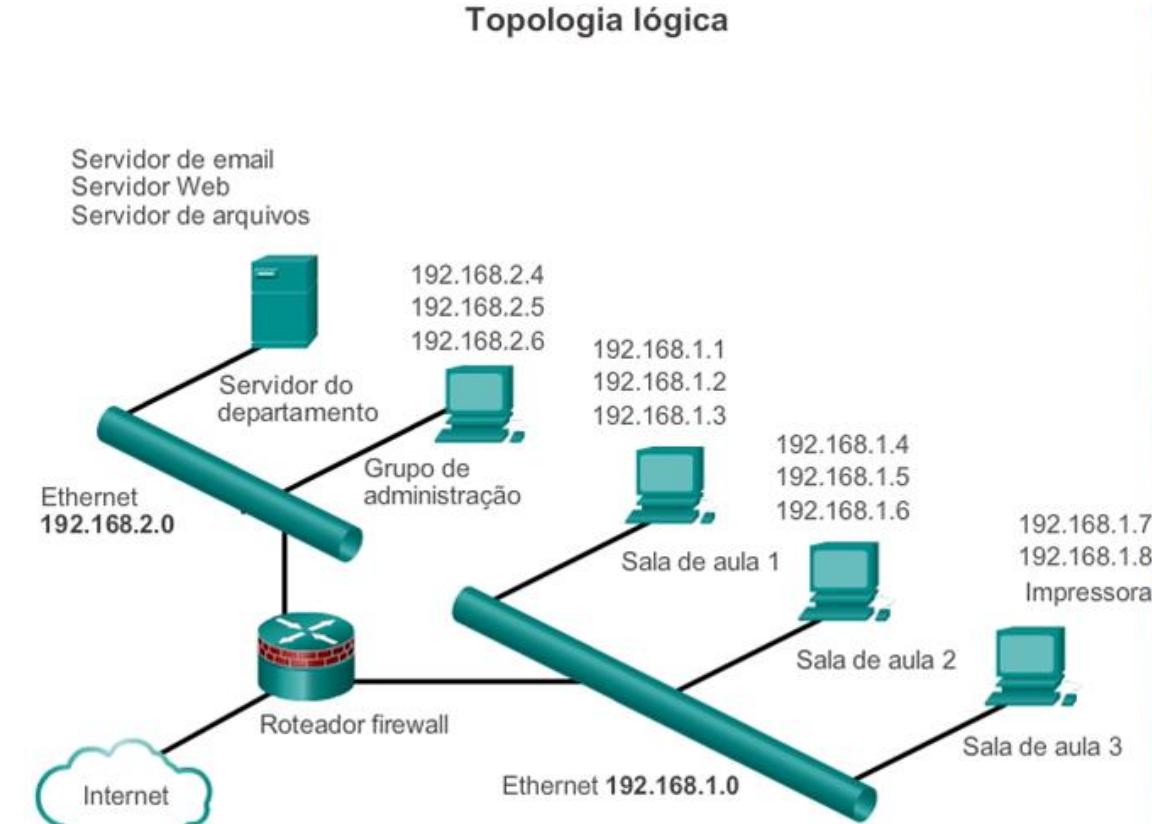
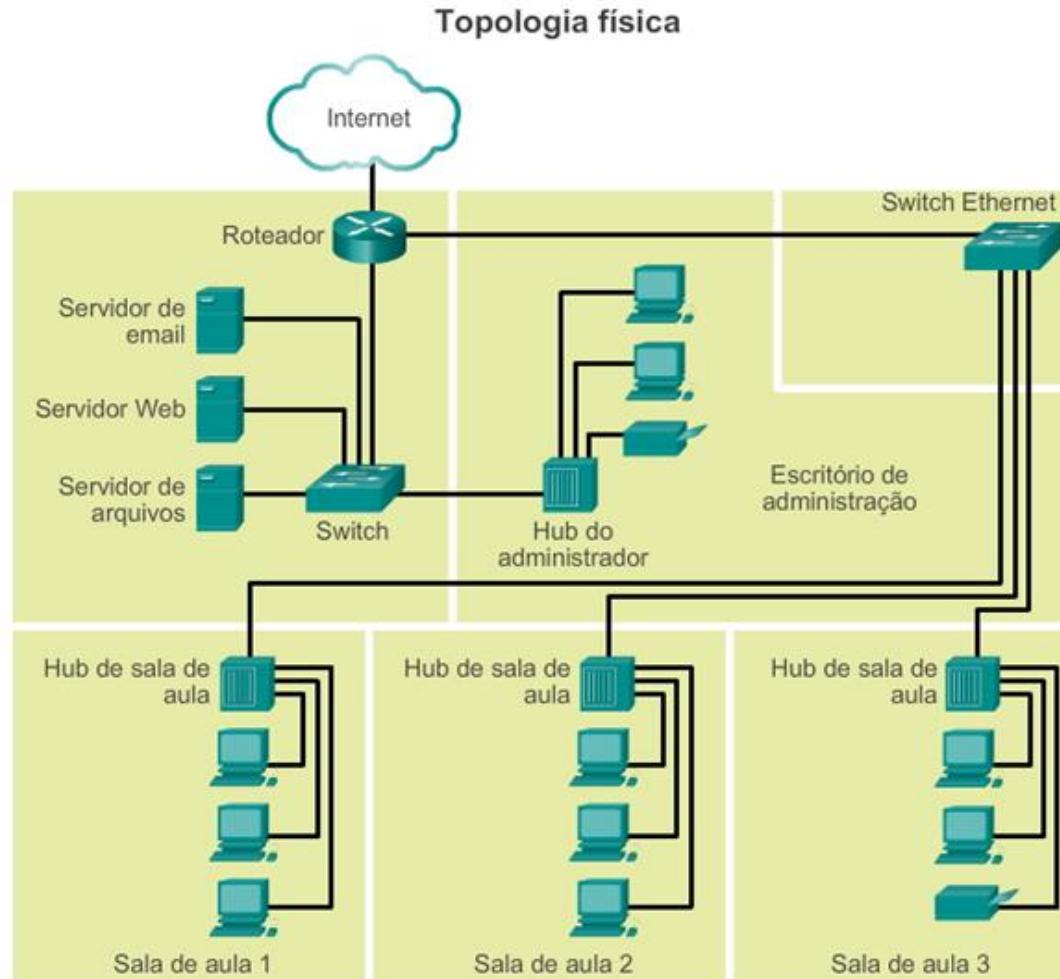


Problemas de implementação	Meio físico em cobre	Fibra ótica
Largura de banda suportada	10 Mbps – 10 Gbps	10 Mbps – 100 Gbps
Distância	Relativamente curto (1 – 100 metros)	Relativamente alto (1 – 100.000 metros)
Imunidade à interferência eletromagnética e à interferência da frequência de rádio	Baixa	Alta (Totalmente imune)
Imunidade a perigos elétricos	Baixa	Alta (Totalmente imune)
Custos do meio físico e conector	Menor	Maior
Habilidades necessárias para a instalação	Menor	Maior
Precauções de segurança	Menor	Maior

- Capacidade do meio físico para transportar dados
- Quantidade de dados que podem fluir de um ponto para outro por unidade de tempo

Unidades de Largura de Banda	Abreviação	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





LAN, WAN e interligação de redes



Small Home Networks



Small Office/Home Office Networks

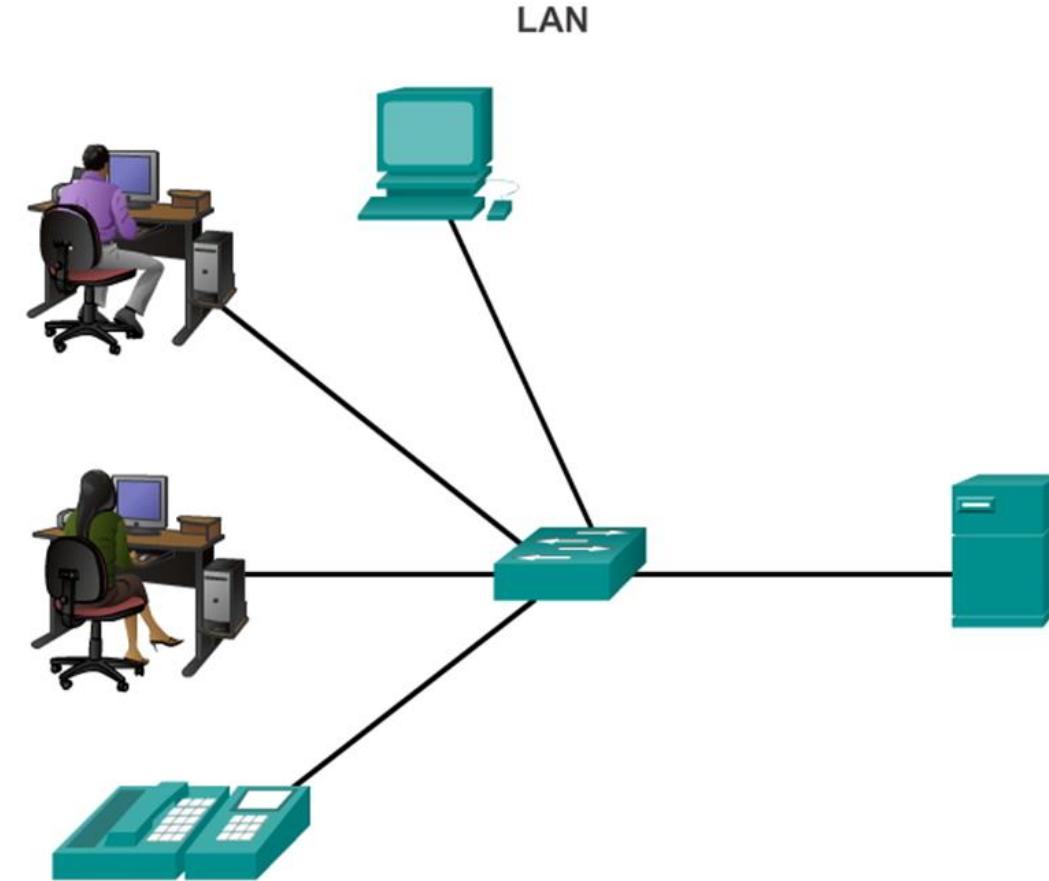


Medium to Large Networks



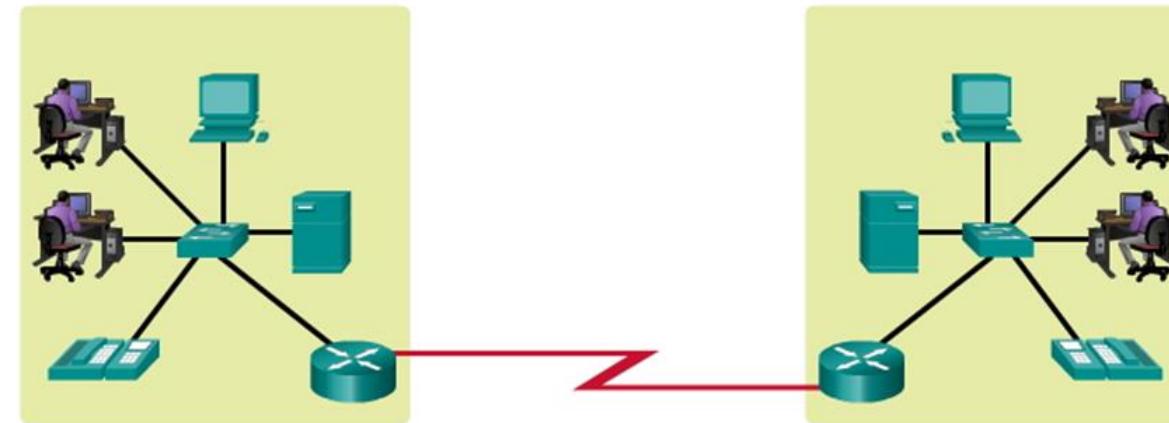
World Wide Networks

- Os dois tipos mais comuns de infraestruturas de rede são:
 - ✓ Rede Local (LAN)
 - ✓ Rede de Área Alargada (WAN).
- Outros tipos de redes incluem:
 - ✓ Rede de Área Metropolitana (MAN)
 - ✓ LAN sem fios (WLAN)
 - ✓ Rede de armazenamento (SAN - Storage Area Network)

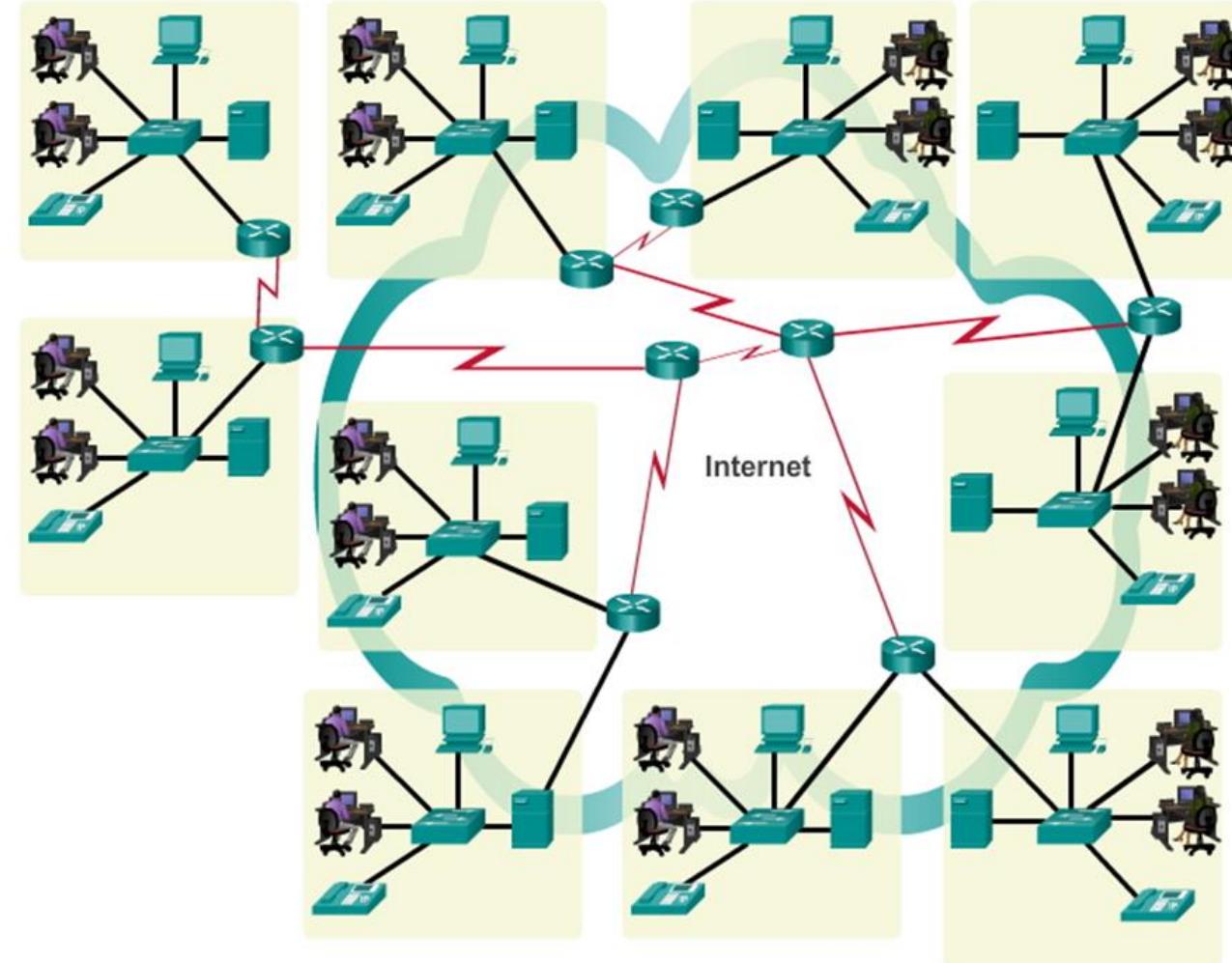


Uma rede que serve uma casa, um edifício ou um campus é considerada uma LAN.

WAN



As LANs separadas pela distância geográfica são conectadas por uma rede conhecida como WAN.

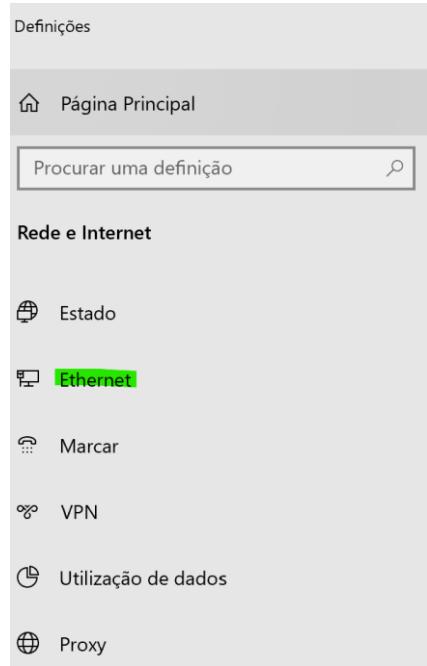


As LANs e as Wans podem ser conectadas em internetworks.

- Intranet e Extranet
- Tecnologias de acesso à Internet
 - ✓ Ligação remota de particulares à Internet
 - ✓ Ligação de organizações à Internet
- A rede convergente
- Suporte da rede para:
 - ✓ Tolerância a falhas
 - ✓ Escalabilidade
 - ✓ Qualidade do serviço (QoS)
 - ✓ Segurança
- Novas tendências
 - ✓ Traga seu próprio dispositivo (BYOD – Bring Your Own Device); Colaboração online; Vídeo e Computação em nuvem

- Cada dispositivo final numa rede deve ser configurado com um endereço IP
 - ✓ Configuração manual
 - ✓ Configuração automática
- A estrutura de endereços IPv4 é denominada notação decimal pontuada
- Os endereços IP são apresentados em notação decimal, com quatro números decimais entre 0 e 255
- Com o endereço IP, uma máscara de sub-rede também é necessária

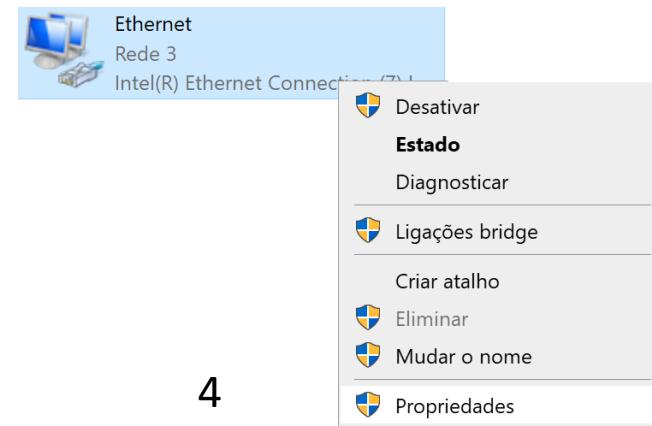
1



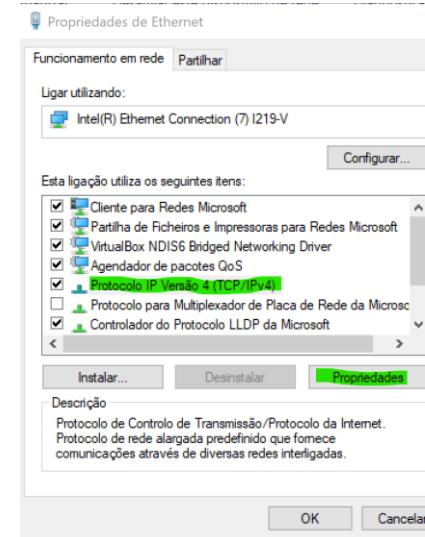
2

- Definições relacionadas
 - [Alterar opções do adaptador](#) (highlighted with a green box)
 - [Alterar opções de partilha avançadas](#)
- [Centro de Rede e Partilha](#)
- [Firewall do Windows](#)
- Tem dúvidas?
 - [Problemas de solução de problemas de conexão de rede](#)
 - [Obter ajuda](#)
 - [Enviar comentários](#)

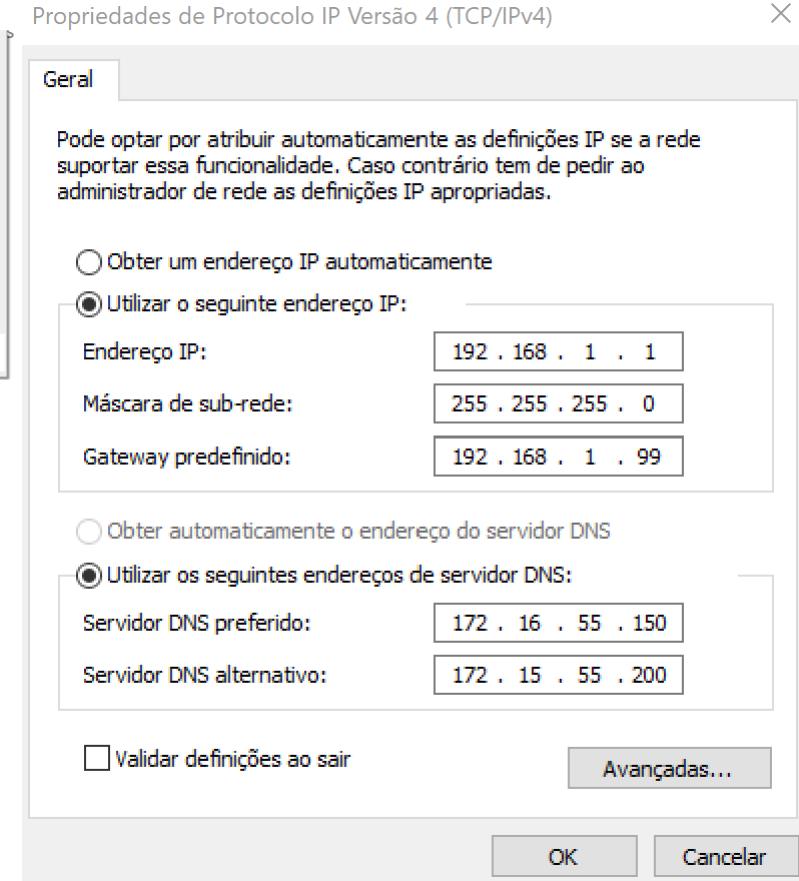
3



4

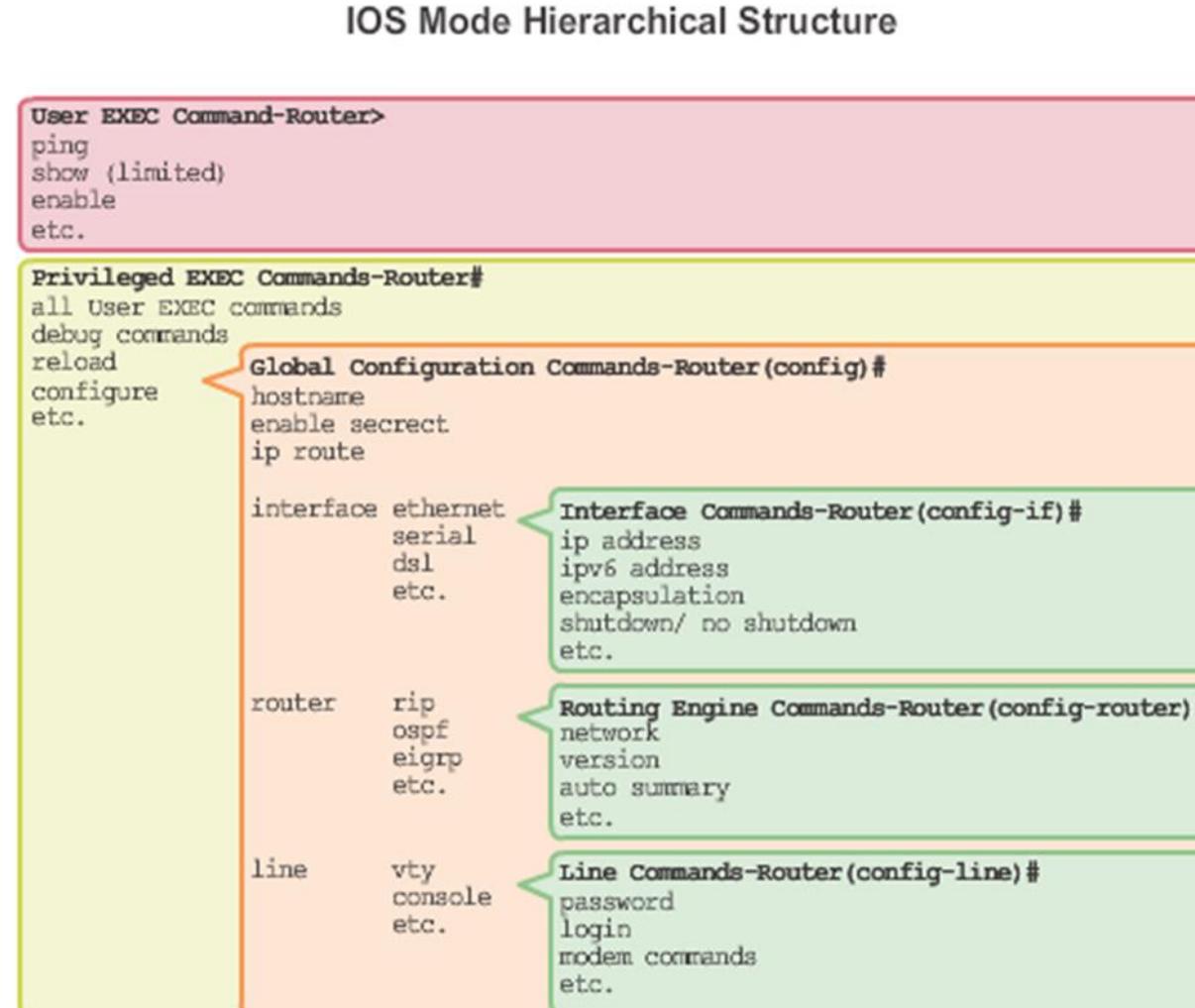


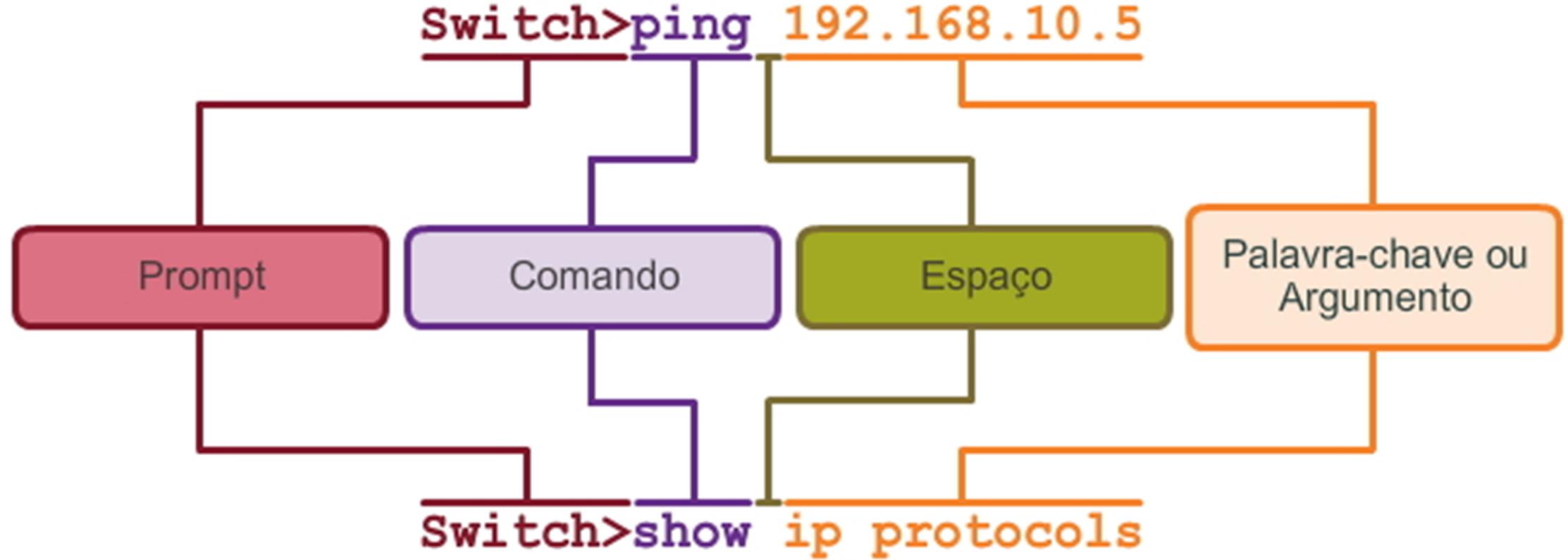
5



Configuração de equipamentos de rede

- IOS - Cisco Internetwork Operating System
 - ✓ O IOS é armazenado em memória flash
 - ✓ O IOS é copiado da memória flash para a RAM volátil
 - ✓ Métodos mais usados para aceder à CLI do equipamento
 - ❖ Console
 - ❖ Telnet ou SSH





- Criar uma rede com dois computadores conectados através de um switch
 - ✓ Definir um nome para o switch
 - ❖ Comando hostname
 - ✓ Limitar o acesso à configuração do dispositivo
 - ❖ Configurar passwords:
 - Limita o acesso ao modo EXEC privilegiado
 - Limita o acesso ao dispositivo usando a conexão de console
 - Limita o acesso ao dispositivo usando Telnet
 - Codificação da exibição das passwords
 - ✓ Configurar mensagens de banner
 - ✓ Salvar a configuração
 - ❖ Ficheiros de configuração

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=838ms TTL=35
Reply from 192.168.10.2: bytes=32 time=820ms TTL=35
Reply from 192.168.10.2: bytes=32 time=883ms TTL=36
Reply from 192.168.10.2: bytes=32 time=828ms TTL=36

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 820ms, Maximum = 883ms, Average = 842ms

C:\>ping 192.168.10.11

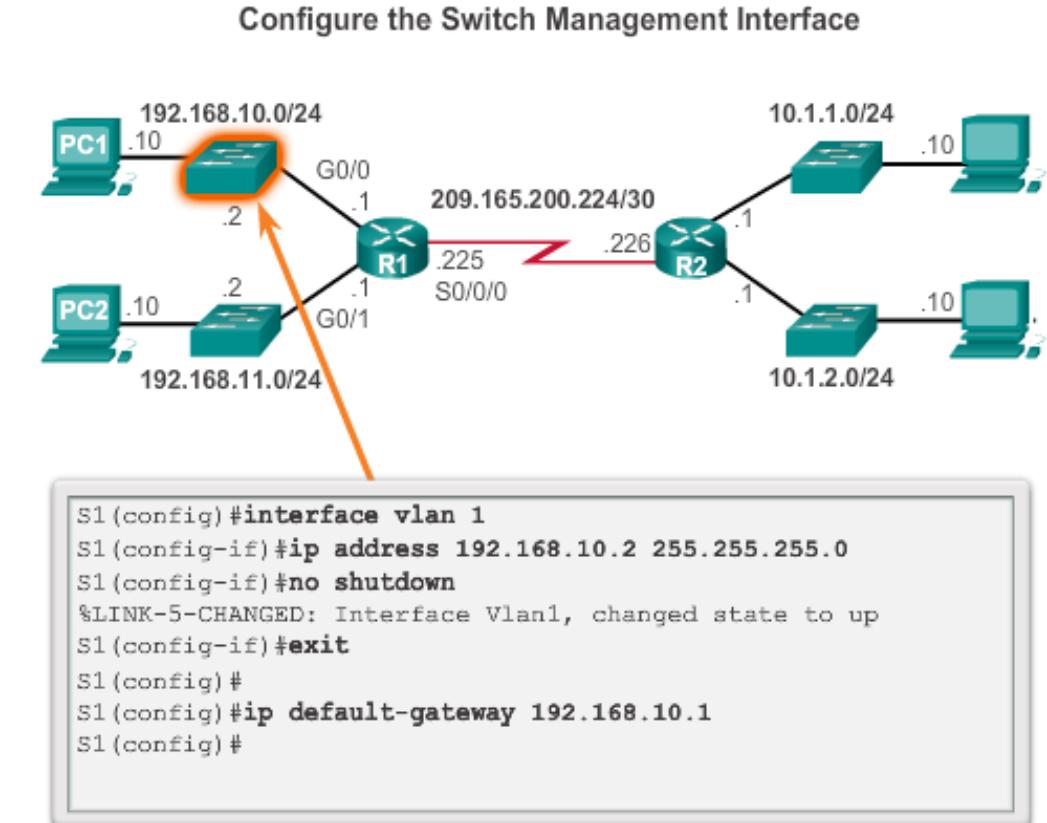
Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=838ms TTL=35
Reply from 192.168.10.11: bytes=32 time=820ms TTL=35
Reply from 192.168.10.11: bytes=32 time=883ms TTL=36
Reply from 192.168.10.11: bytes=32 time=828ms TTL=36

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 820ms, Maximum = 883ms, Average = 842ms

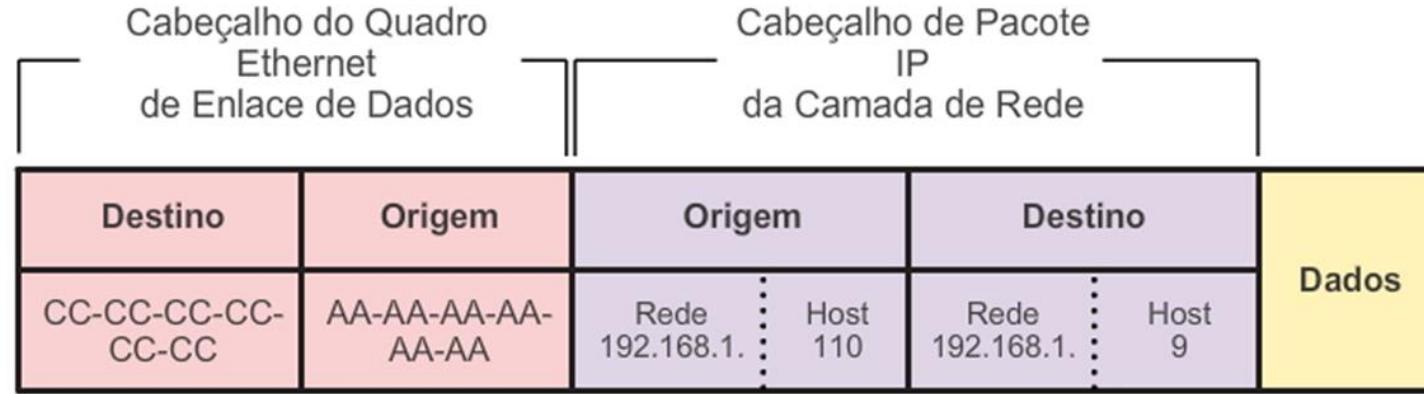
C:\>
```

- Dispositivos de infraestrutura de rede requerem endereços IP para permitir a gestão remota.
- Num switch, o endereço IP de gestão é atribuído a uma interface virtual

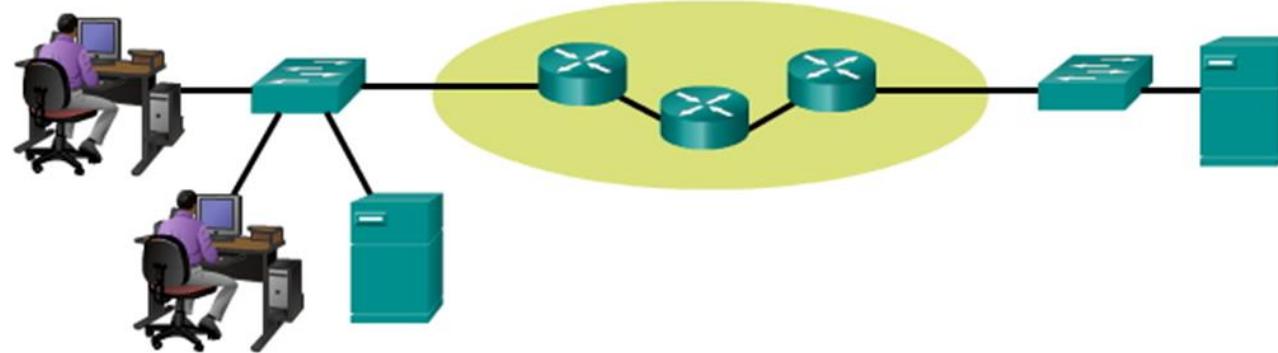
Configurar o endereço IP num Switch



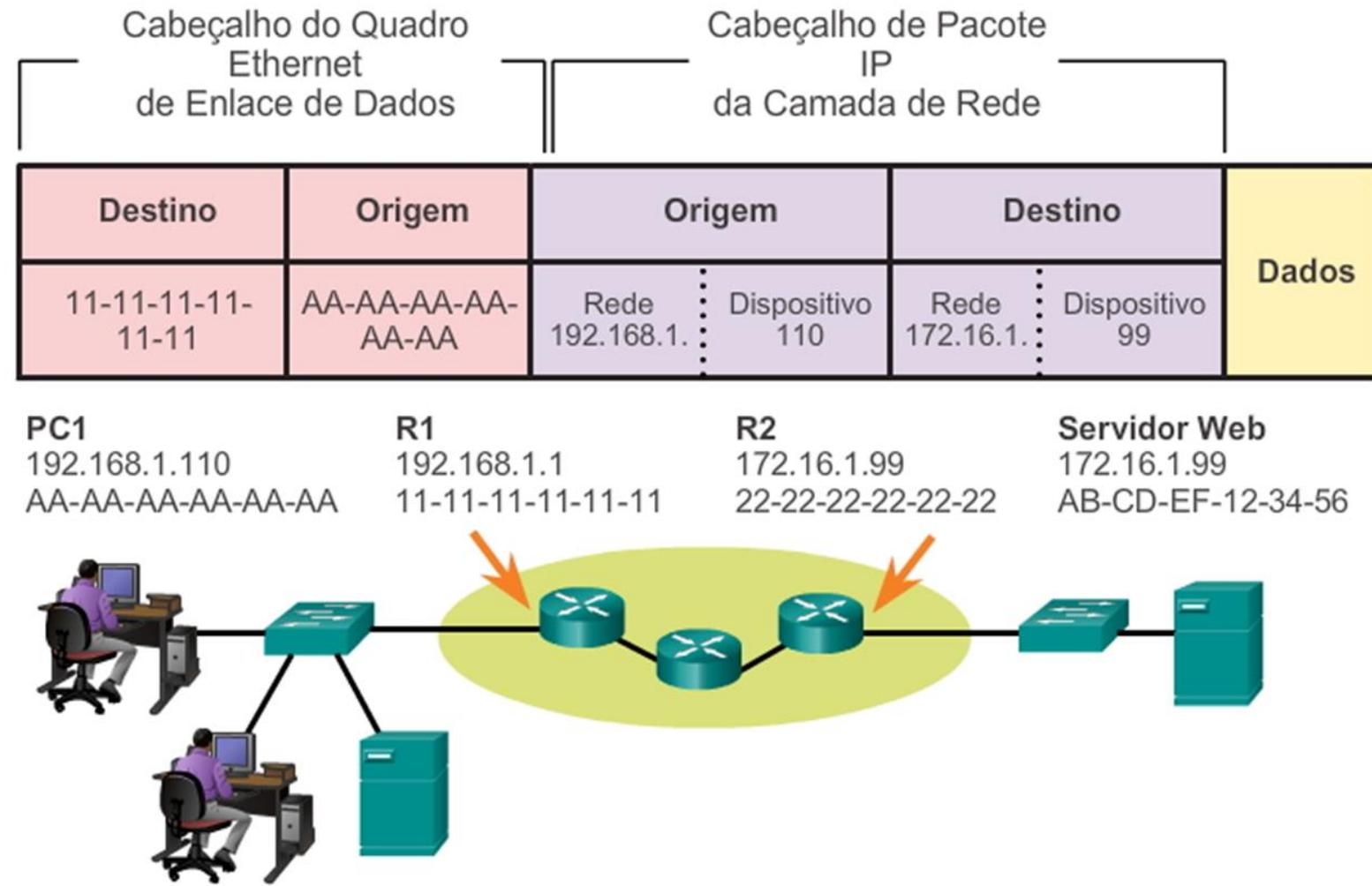
Exemplo - Comunicação com um dispositivo na mesma rede

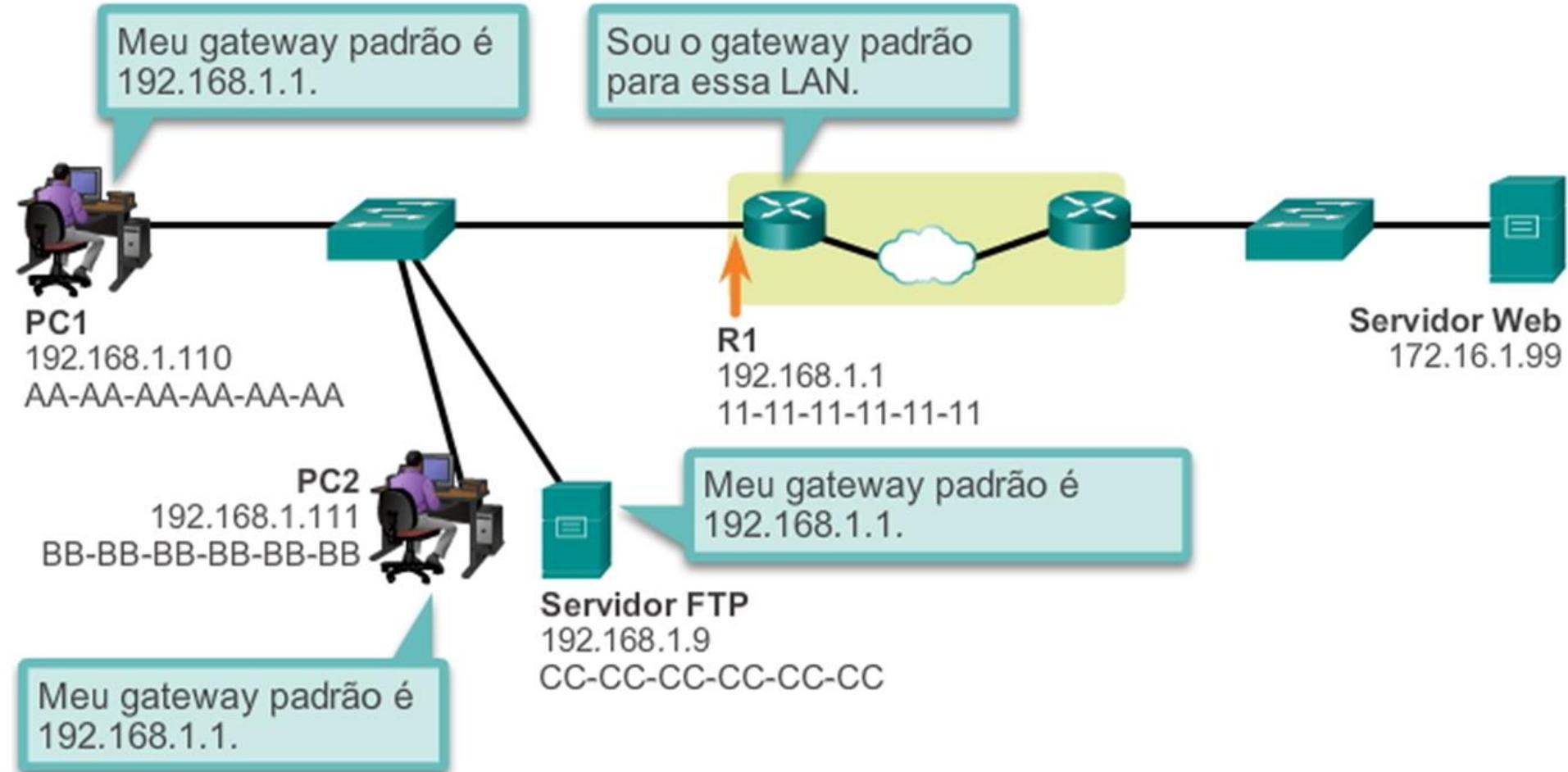


PC1
192.168.1.110
AA-AA-AA-AA-AA-AA



Servidor FTP
192.168.1.9
CC-CC-CC-CC-CC-CC

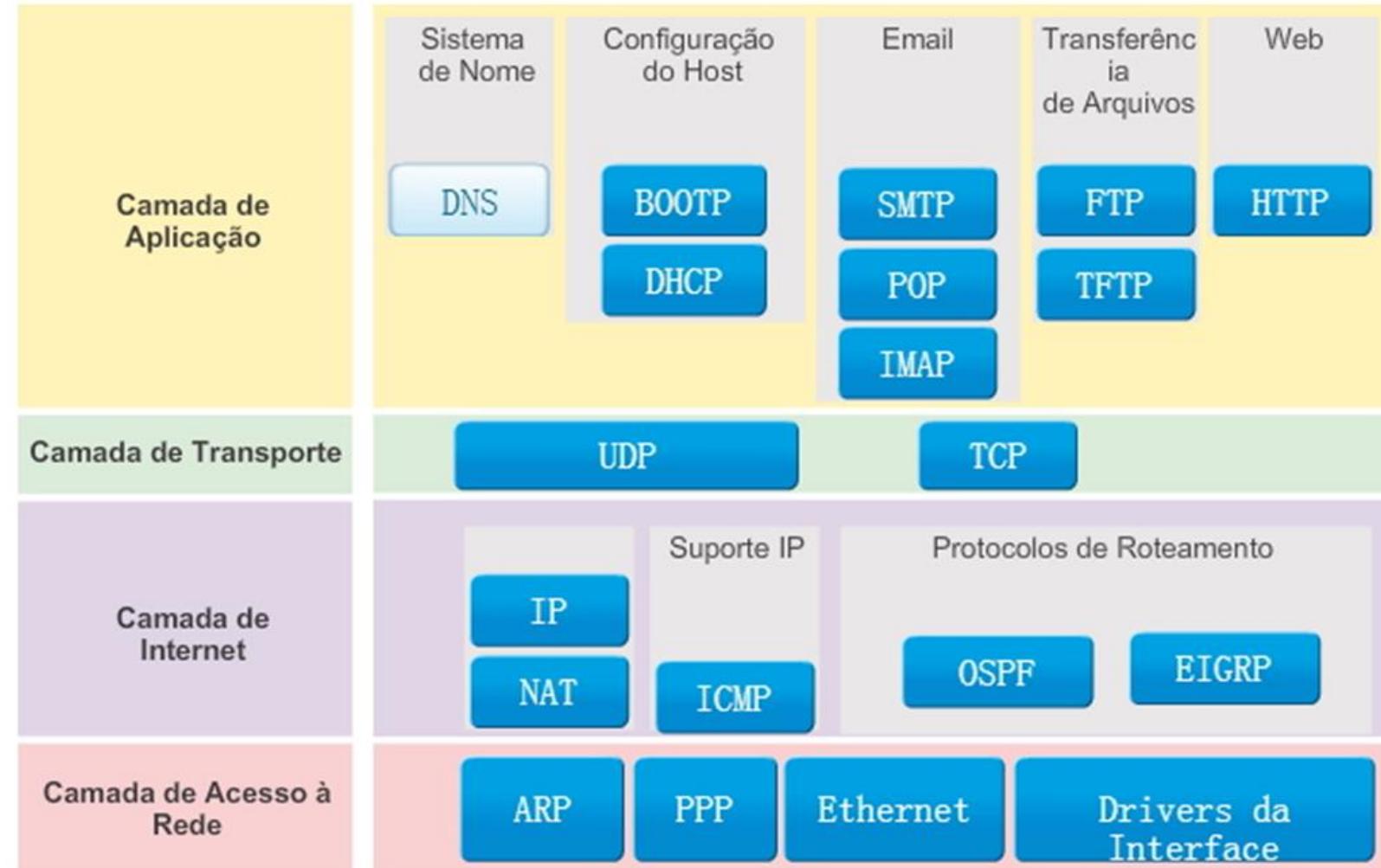


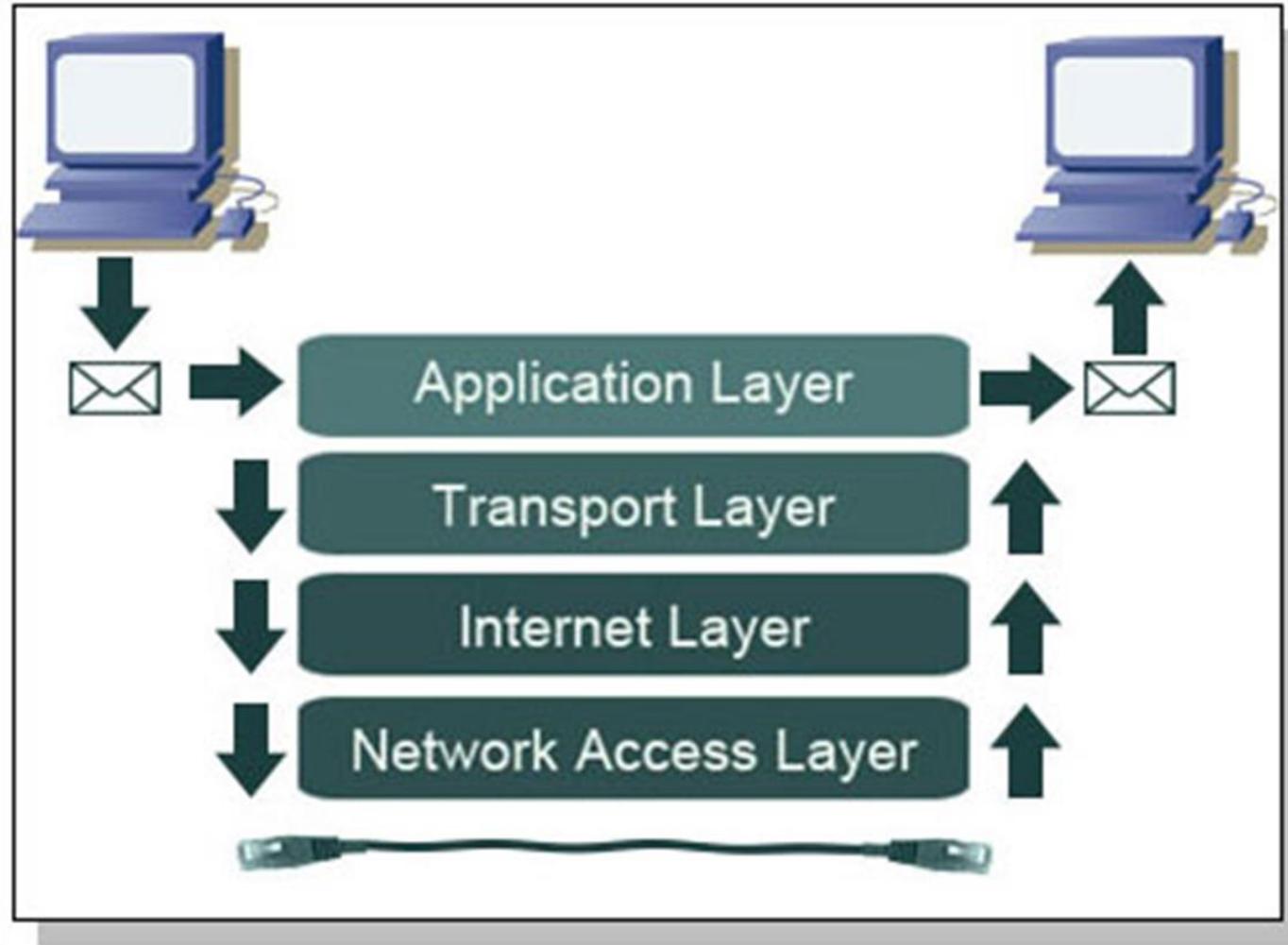


Comunicação e protocolos de rede

- Criar uma rede com dois computadores conectados através de um switch
 - ✓ Definir um nome para o switch
 - ❖ Comando hostname
 - ✓ Limitar o acesso à configuração do dispositivo
 - ❖ Configurar passwords:
 - Limita o acesso ao modo EXEC privilegiado
 - Limita o acesso ao dispositivo usando a conexão de console
 - Limita o acesso ao dispositivo usando Telnet
 - Codificação da exibição das passwords
 - ✓ Configurar mensagens de banner
 - ✓ Salvar a configuração
 - ❖ Ficheiros de configuração

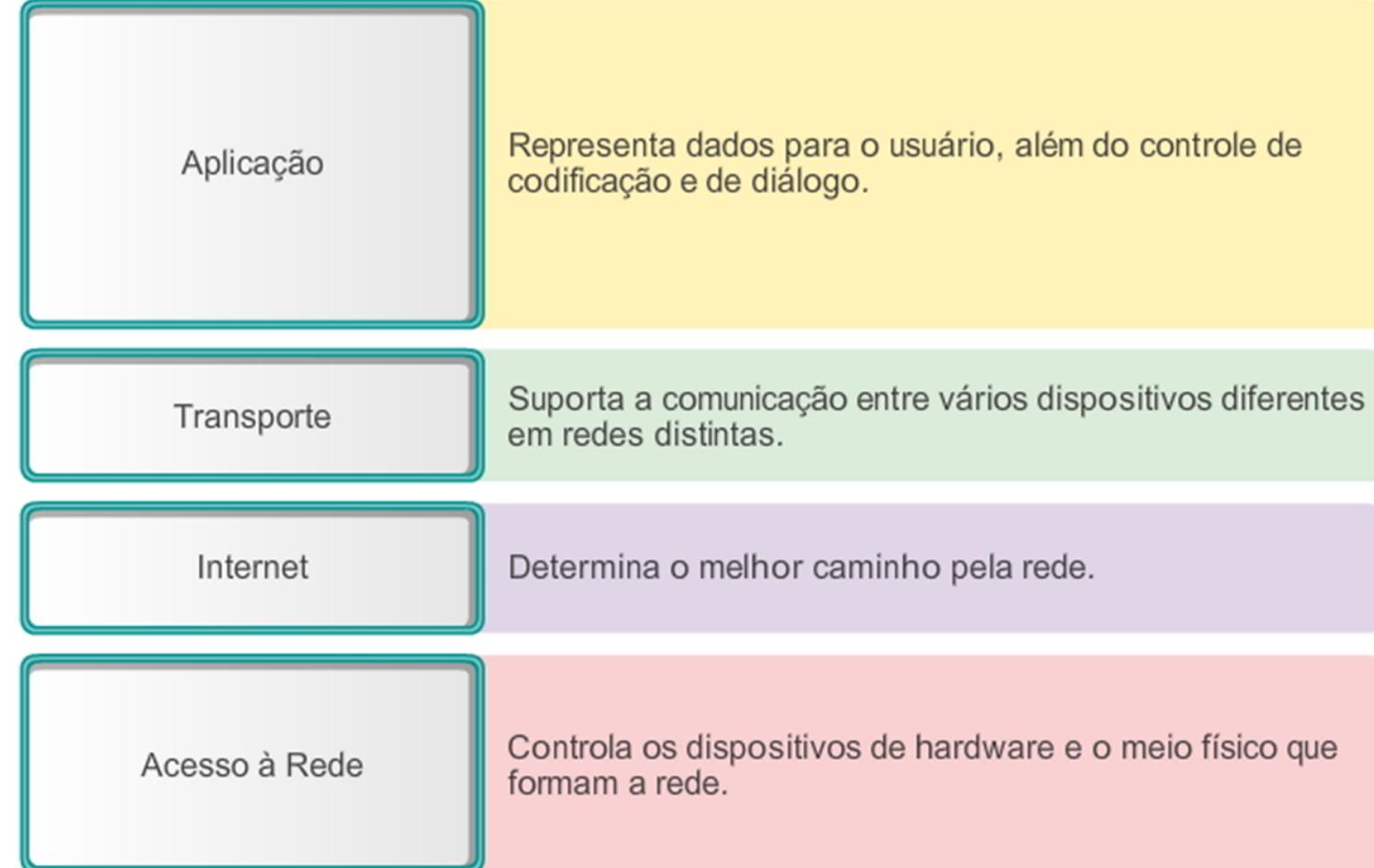
- Uma mensagem antes de ser enviada é convertida em dígitos binários (bits) que serão então codificados num sinal que possa ser transmitido num meio físico (cabo ou transmissão wireless)
- Formatação e encapsulamento da mensagem
 - ✓ Exemplo: a carta pessoal contém os seguintes elementos:
 - ❖ Identificação de destinatário
 - ❖ Uma saudação e/ou cumprimento
 - ❖ O conteúdo da mensagem
 - ❖ Uma frase de encerramento
 - ❖ Identificação de remetente
- Protocolos de rede definem
 - ✓ Como a mensagem é formatada ou estruturada

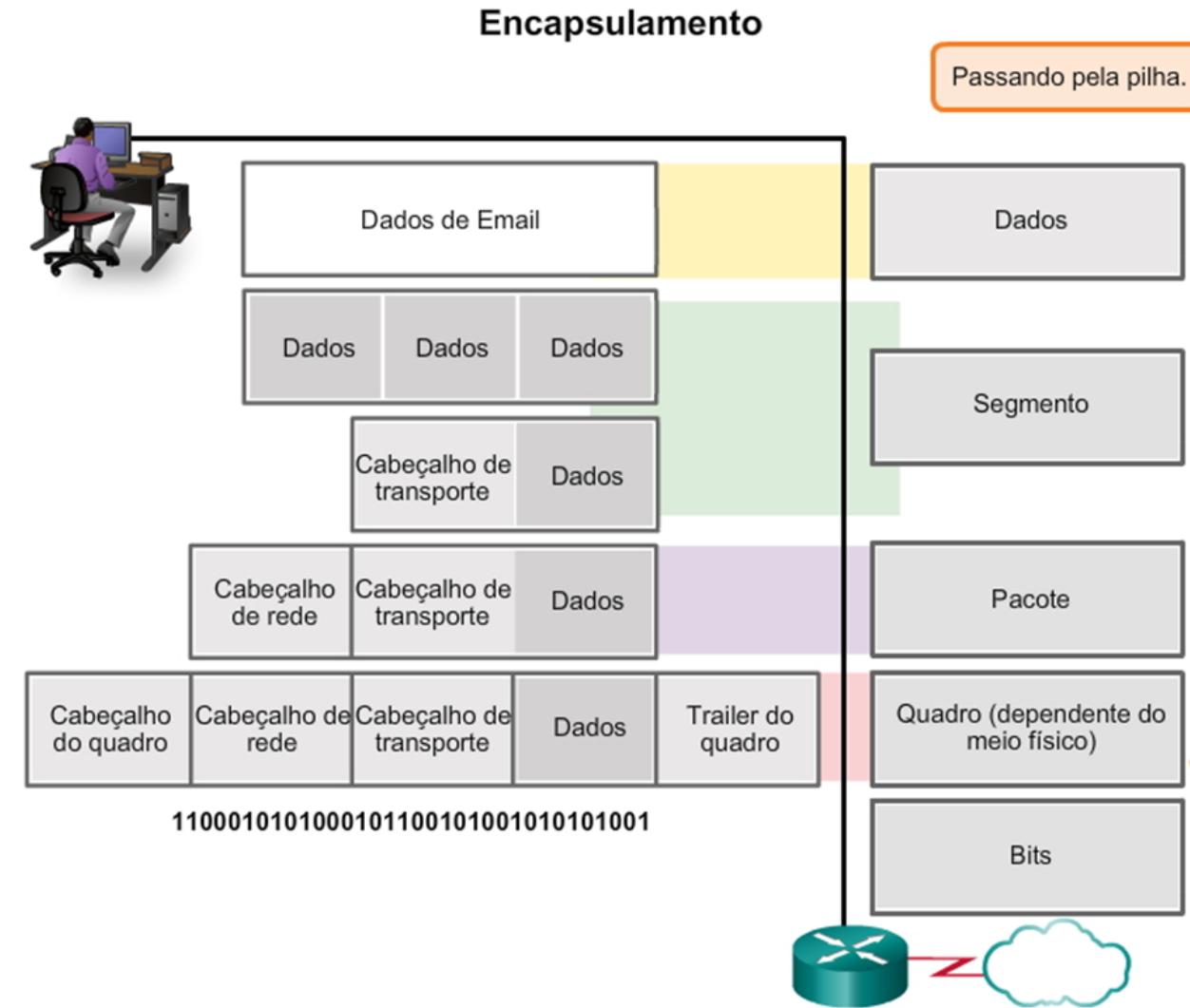




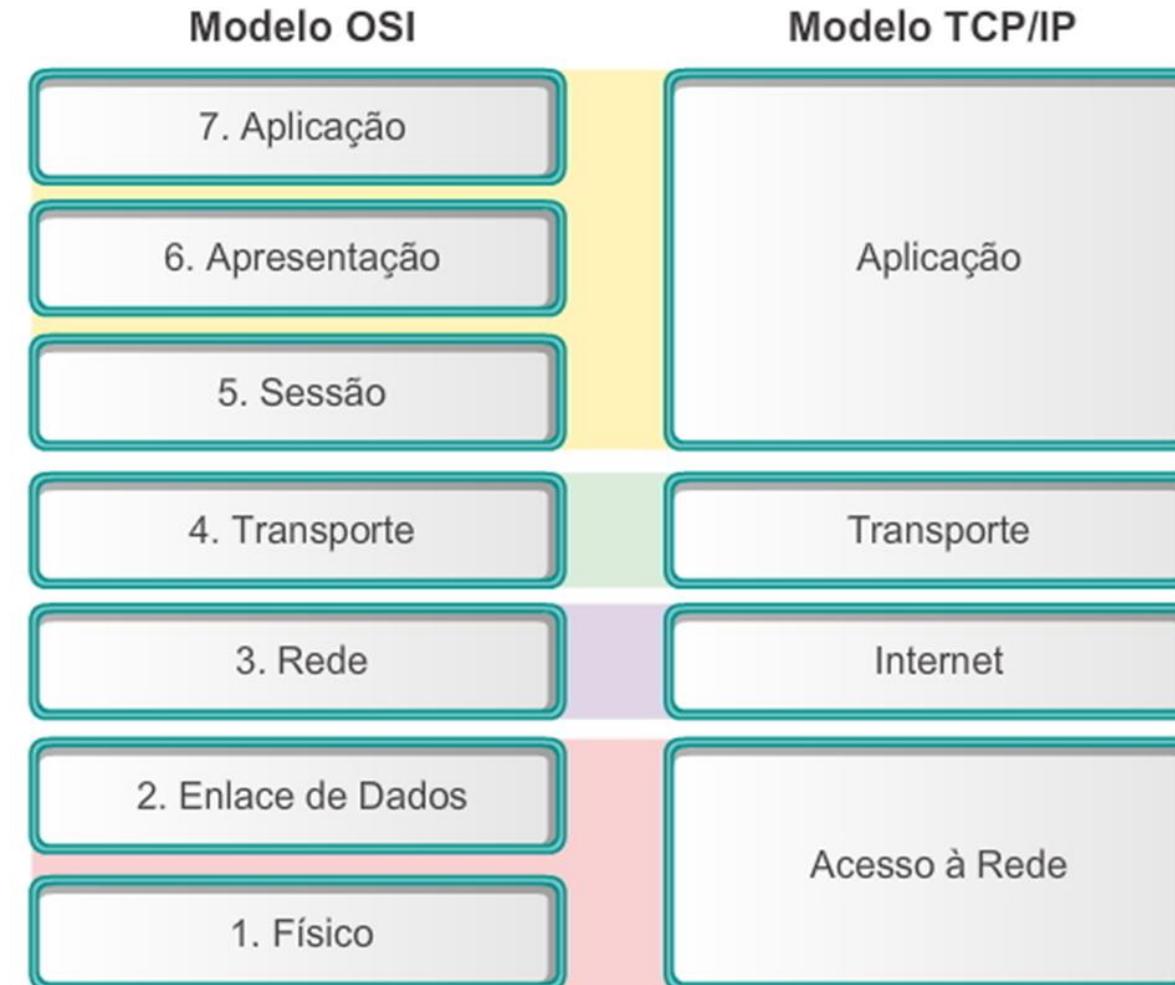
- Protocolo de aplicação – Protocolo HTTP
- Protocolo de transporte – Protocolo TCP
- Protocolo da Internet – Protocolo da Internet (IP)
- Protocolos de acesso à rede – Camada de Ligação de Dados e Camada Físicas

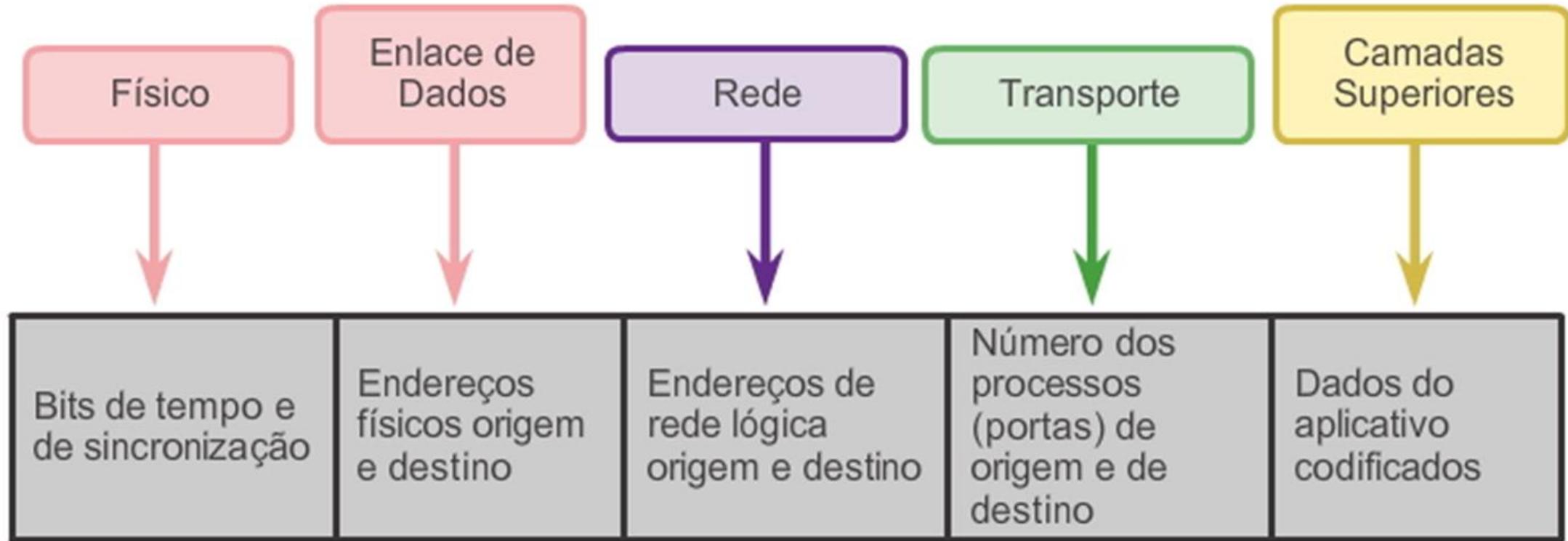
Modelo TCP/IP





Comparação dos modelos OSI e TCP/IP





- Enter privileged EXEC mode using the **enable** command
 - ❖ Switch> **enable**
 - ✓ Result ↵ Switch#
- Return to user EXEC mode using the **disable** command
 - ❖ Switch# **disable**
 - ✓ Result ↵ Switch>
- Enter global configuration mode using the **configure terminal** command.
 - ❖ Switch> **enable**
 - ❖ Switch# **configure terminal**
 - ✓ Result ↵ Switch(config)#
- Exit global configuration mode and return to privileged EXEC mode using the **exit** command
 - ❖ Switch(config)# **exit**
 - ✓ Result ↵ Switch#

- Re-enter global configuration mode
 - ❖ **Switch# configure terminal**
 - ✓ Result ↵ Switch(config)#
- Enter line subconfiguration mode for the console port using the **line console 0** command
 - ❖ **Switch(config)# line console 0**
 - ✓ Result ↵ Switch(config-line)#
- Enter the VLAN 1 interface subconfiguration mode using the **interface vlan 1** command
 - ❖ **Switch(config)# interface vlan 1**
 - ✓ Result ↵ Switch(config-if)#
- From interface configuration mode, switch to line console subconfiguration mode using the **line console 0** global configuration command
 - ❖ **Switch(config-if)# line console 0**
- Return to privileged EXEC mode using the **end** command
 - ❖ **Switch(config-if)# end**
 - ✓ Result ↵ Switch(config)#

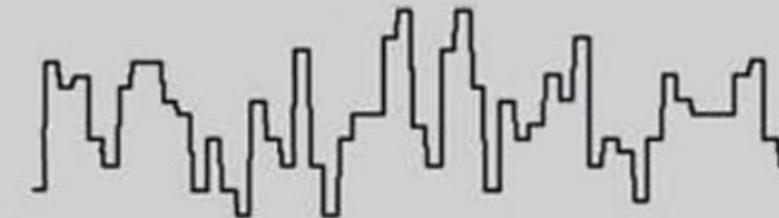
➤ Exercício 2

- Instalar uma rede Ethernet simples com um rooter e 2 PCs
 - O rooter deve estar ligado aos 2 PCs
 - No rooter deve fazer as seguintes configurações:
 - Entrar em modo administrador
 - Verificar como estão as interfaces
 - Dar nome ao rooter
 - Configurar as interfaces com 2 redes diferentes
 - Nos PCs deve fazer as seguintes configurações
 - Dar IPs estáticos aos 2 PCs

- Exercício do Packet Tracer
 - 2.5.5 - Configurações básicas num switch
 - 2.7.6 - Configurações básicas numa rede Ethernet simples
 - 2.9.1 – Desafio de consolidação de conhecimentos
 - 3.5.5 – Análise ao funcionamento do modelo TCP/IP e OSI
 - Casa: 2.3.7 - Navegando no IOS

Camada de acesso à rede

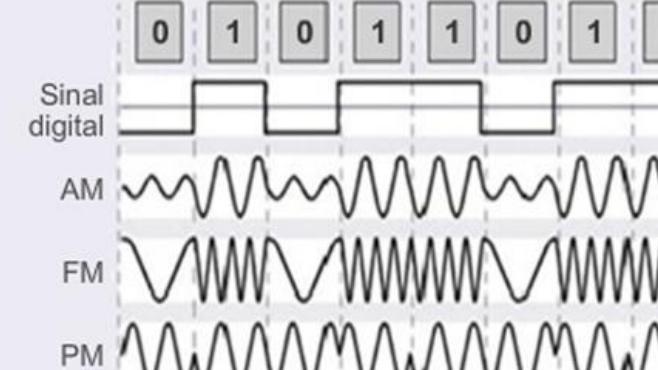
Sinal de saída (Tx)



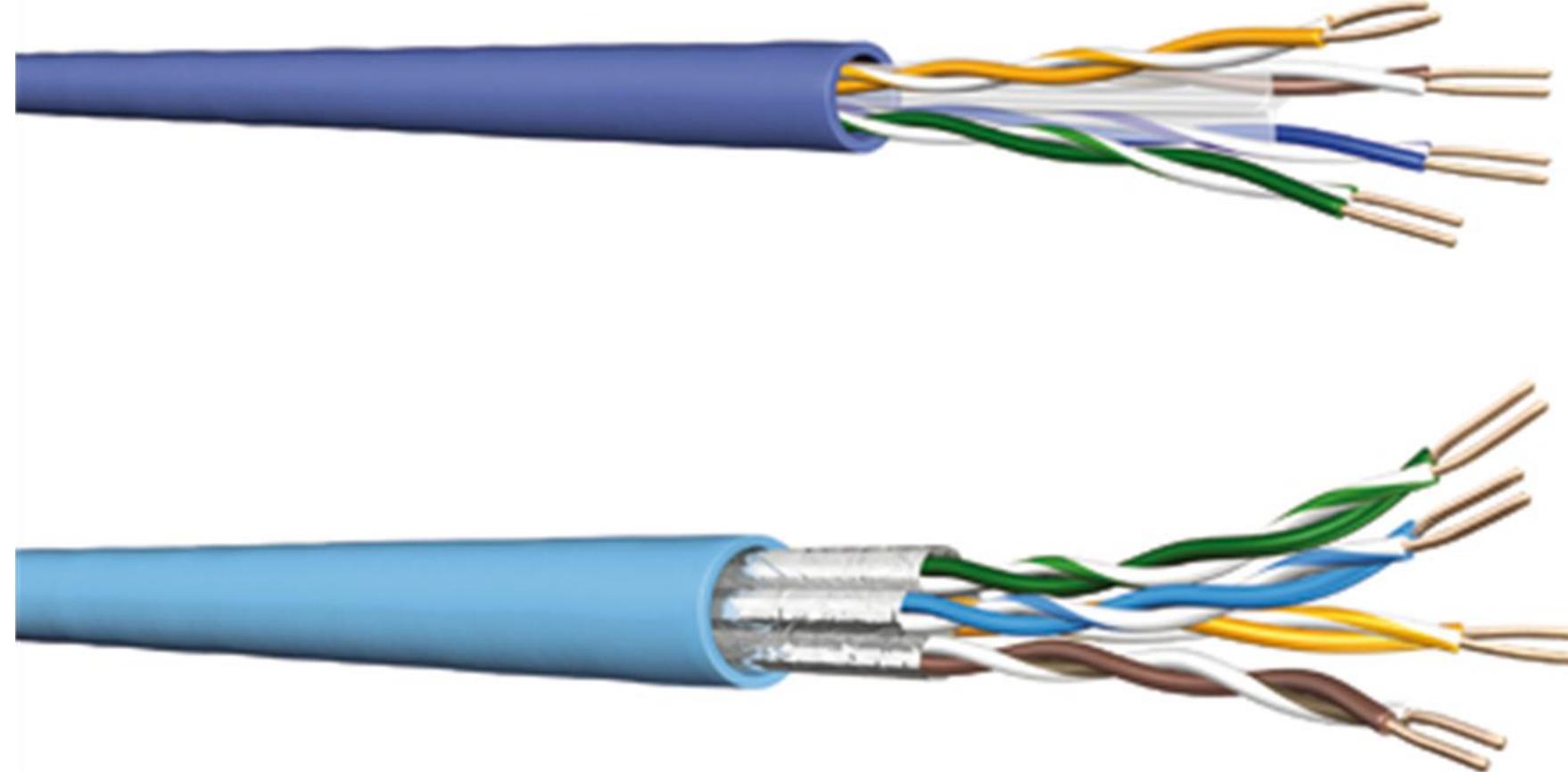
Sinais Elétricos –
Cabo de cobre

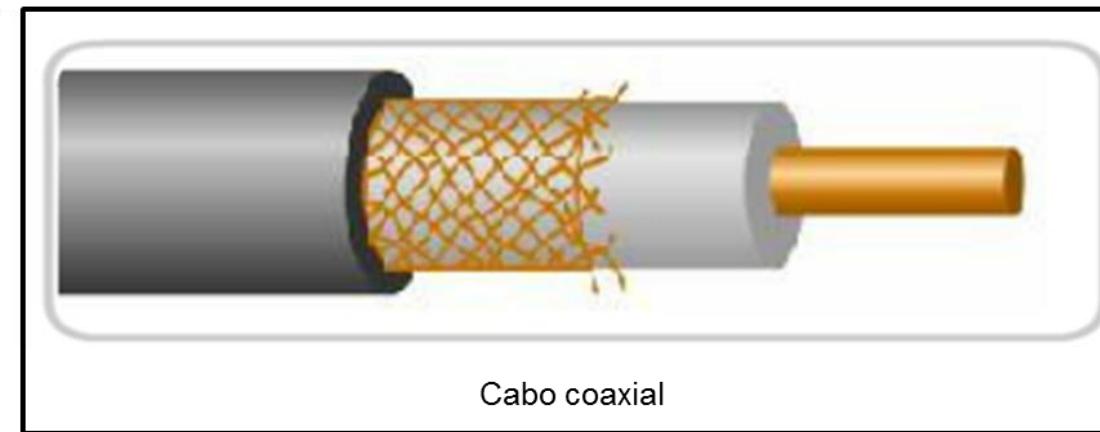


Pulso de Luz –
Cabo de fibra óptica

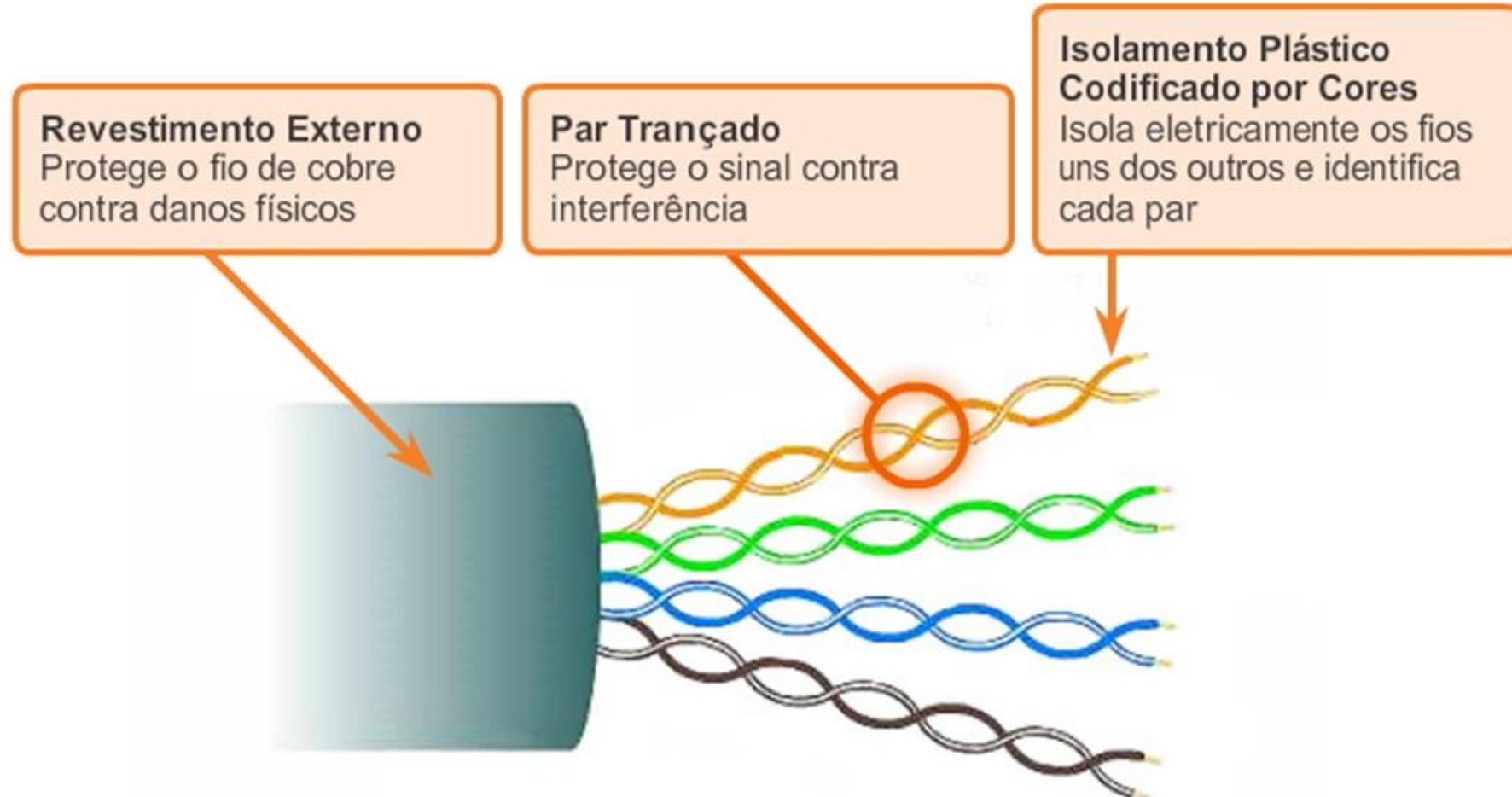


Sinais de Microondas –
Sem fio

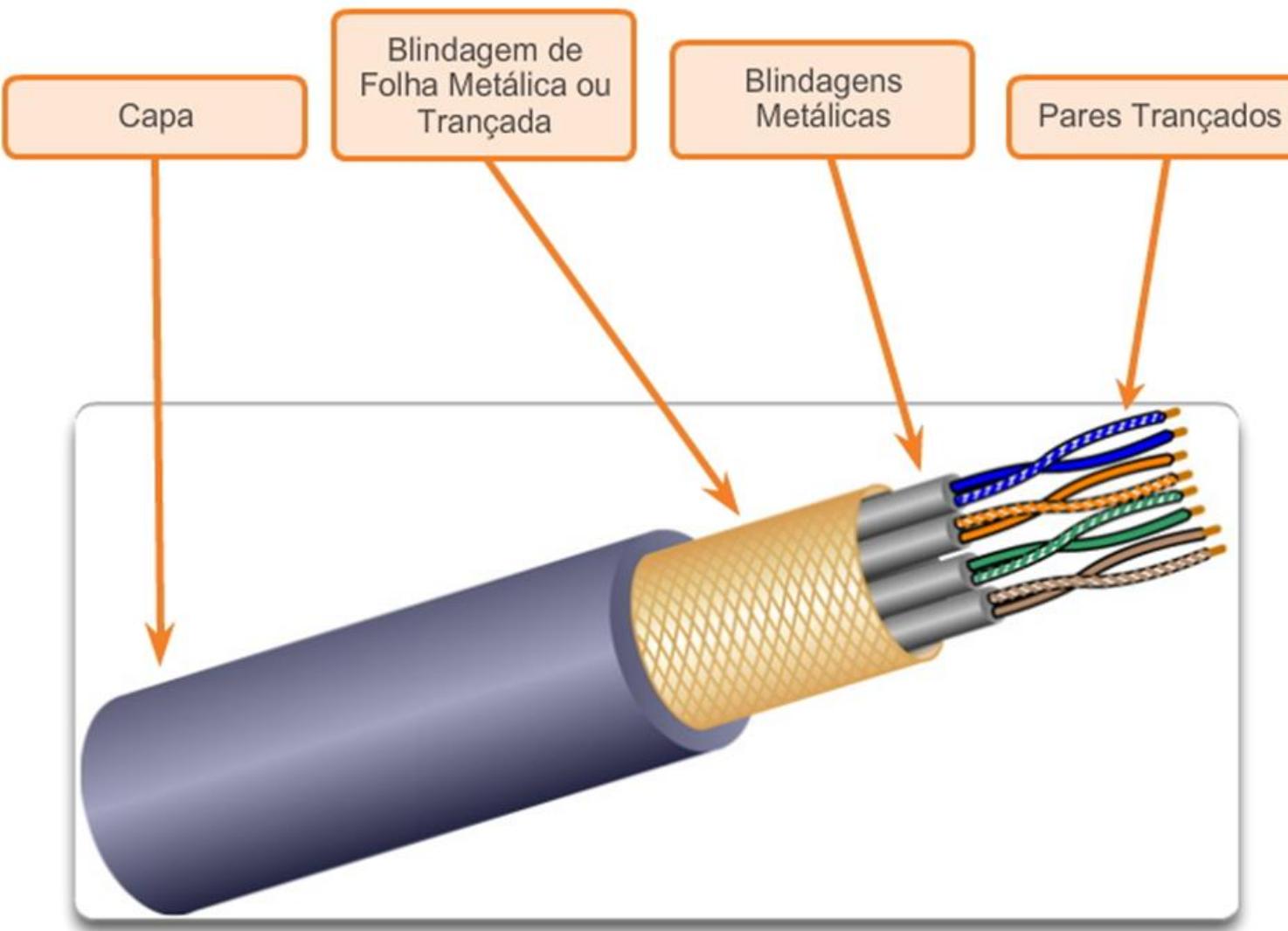


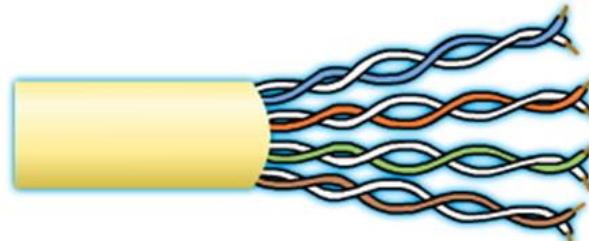


Cabo de Par Trançado Não Blindado (UTP)

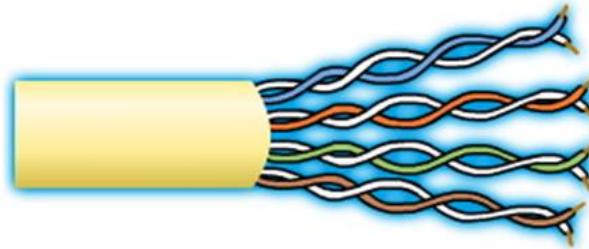


Cabo de Pares Trançados Blindados (STP)

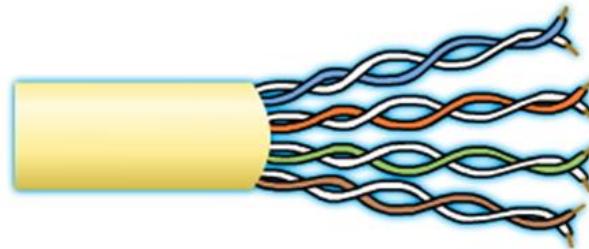




Cabo Categoria 3 (UTP)



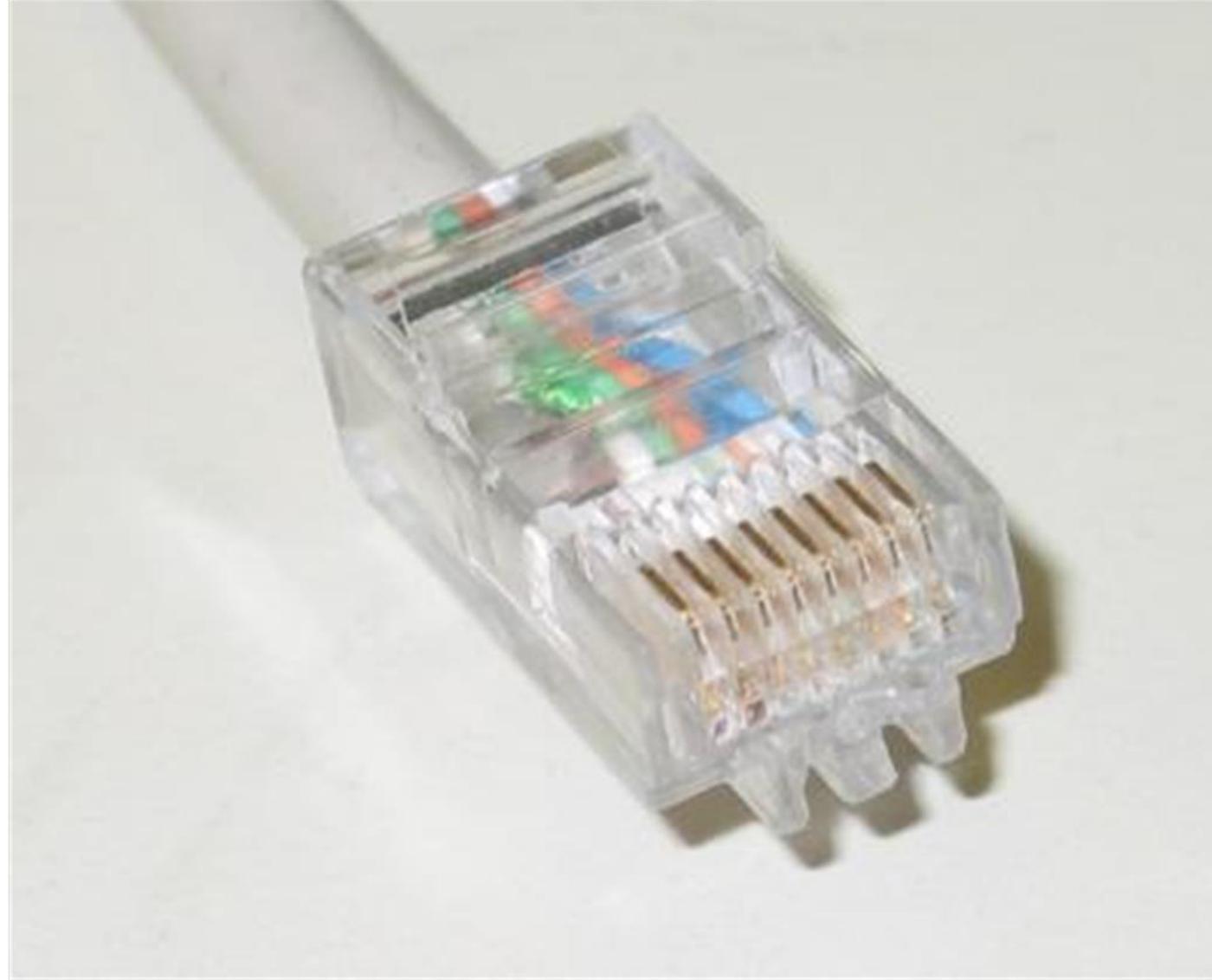
Cabo Categoria 5 e 5e (UTP)

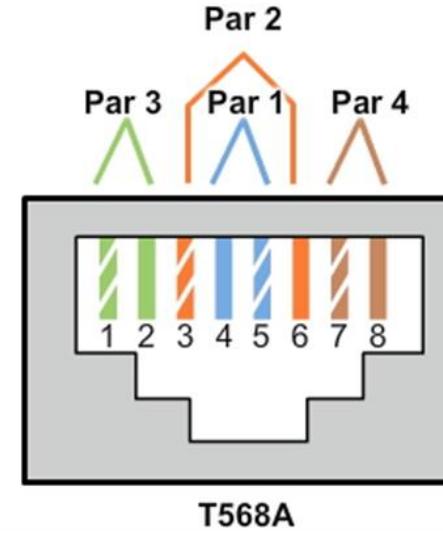


Cabo Categoria 6 (UTP)

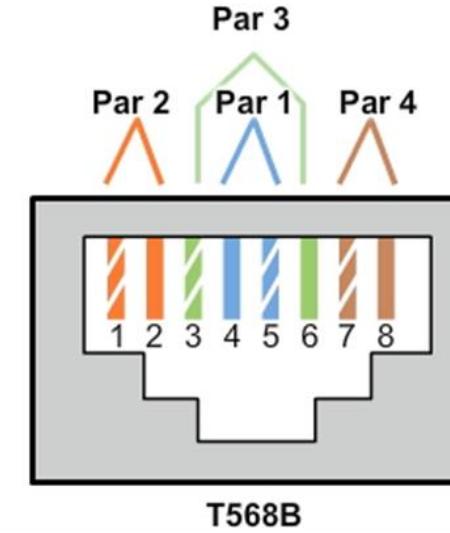
Cabo Categoria 5 e 5e (UTP)

- Usado para transmissão de dados
- A Cat5 suporta 100 Mb/s e pode suportar 1000 Mb/s, mas não é recomendado
- A Cat5e suporta 1000 Mb/s





T568A



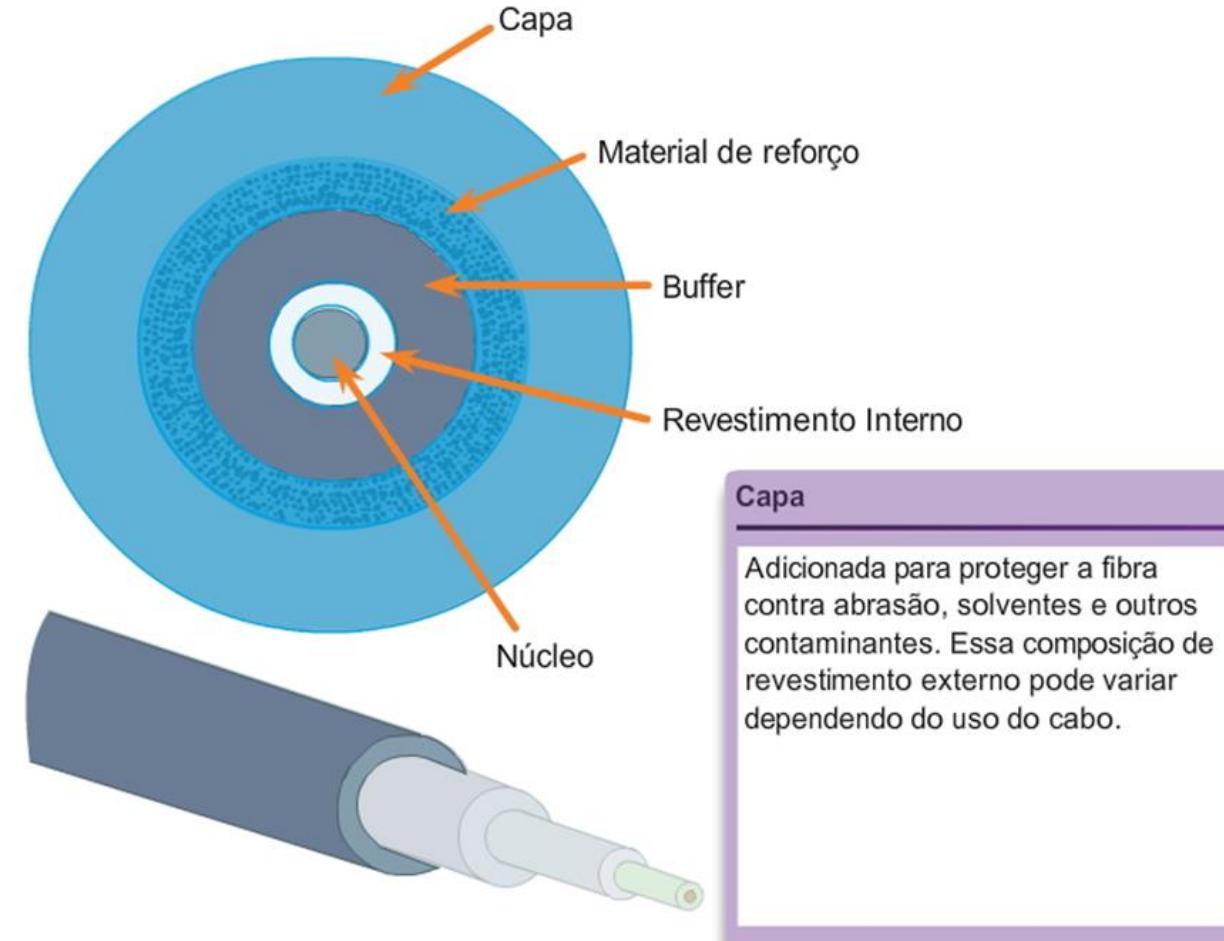
T568B

Tipo de Cabo	Padrão	Aplicação
Ethernet direto	Ambas as extremidades T568A ou ambas as extremidades T568B	Conecta um host de rede a um dispositivo de rede como um switch ou hub.
Ethernet cruzado	Uma extremidade T568A, outra extremidade T568B	<ul style="list-style-type: none">• Conecta dois hosts de rede• Conecta dois dispositivos de rede intermediários (switch com switch ou roteador com roteador)
Console	Cisco proprietário	Conecta uma porta serial da estação de trabalho à porta de console do roteador, usando um adaptador.



Propriedades da cablagem de fibra ótica



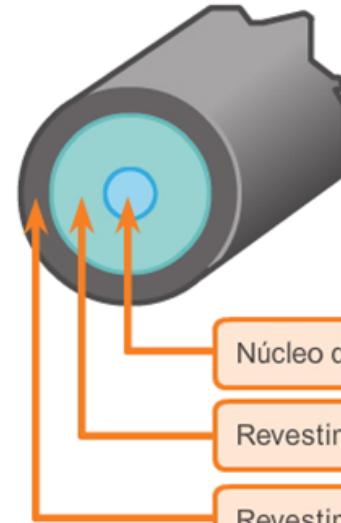


Capa

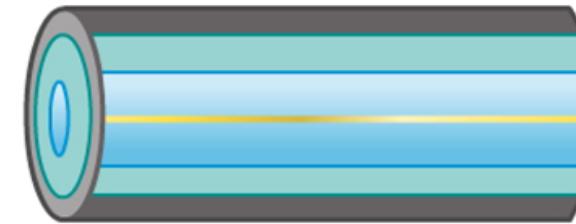
Adicionada para proteger a fibra contra abrasão, solventes e outros contaminantes. Essa composição de revestimento externo pode variar dependendo do uso do cabo.

Clique em cada componente para obter mais informações.

Tipos de meio físico de fibra

**Monomodo**

Produz um único caminho direto para a luz

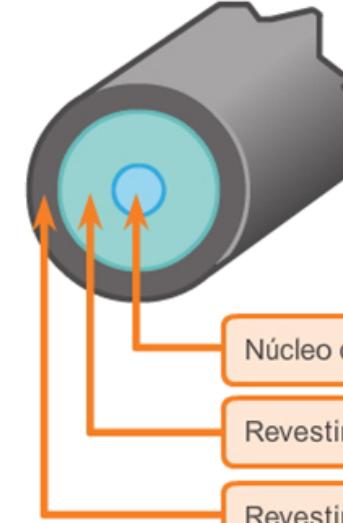


Núcleo de Vidro=9 mícrons

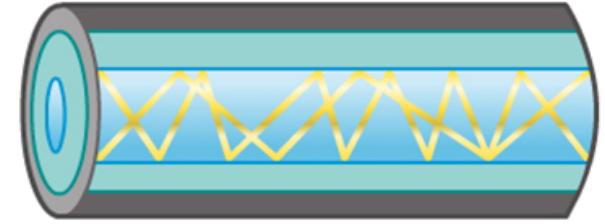
Revestimento interno de vidro com 125 mícrons de diâmetro

Revestimento polimérico

- Núcleo fino
- Menos dispersão
- Adequado para aplicações de longa distância
- Usa lasers como fonte de luz
- Normalmente usado com os backbones de campus para distâncias de vários milhares de metros

**Multimodo**

Permite vários caminhos para a luz



Núcleo de vidro = 50/62,5 mícrons

Revestimento interno de vidro com 125 mícrons de diâmetro

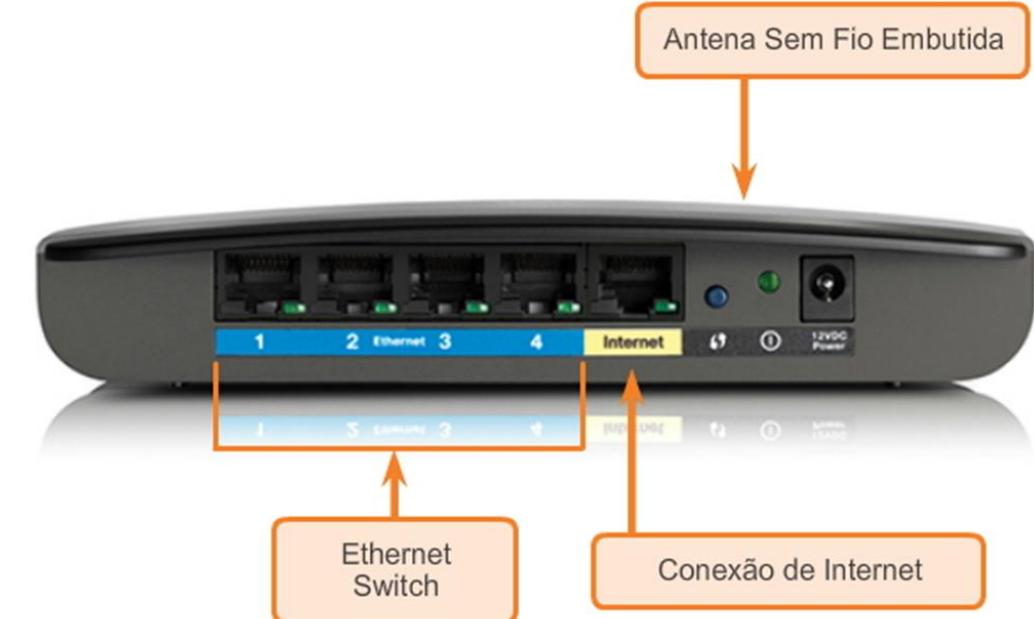
Revestimento

- Núcleo maior do que o cabo monomodo
- Permite maior dispersão e, consequentemente, a perda de sinal
- Adequado para aplicações de longa distância, mas menores que o monomodo
- Usa LEDs como fonte de luz
- Normalmente usado com redes locais ou distâncias de algumas centenas de metros dentro de uma rede de campus

Router Doméstico (Residencial)



Roteador Residencial



Conexāo à Rede Local Com Fio



Ligação à rede local sem fios com um extensor de alcance

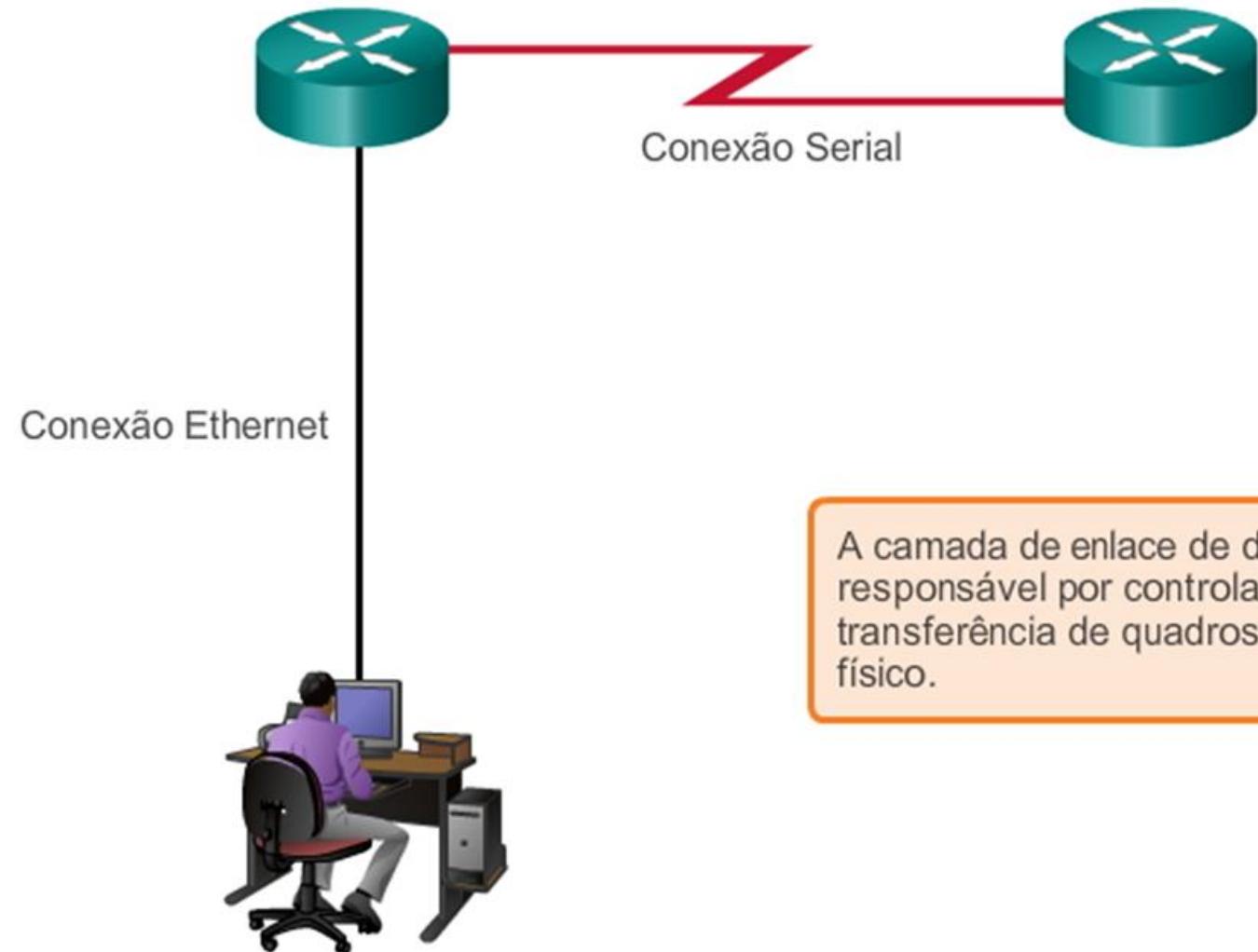


Os protocolos da camada de enlace de dados regem como formatar um quadro para uso em diferentes meios físicos.

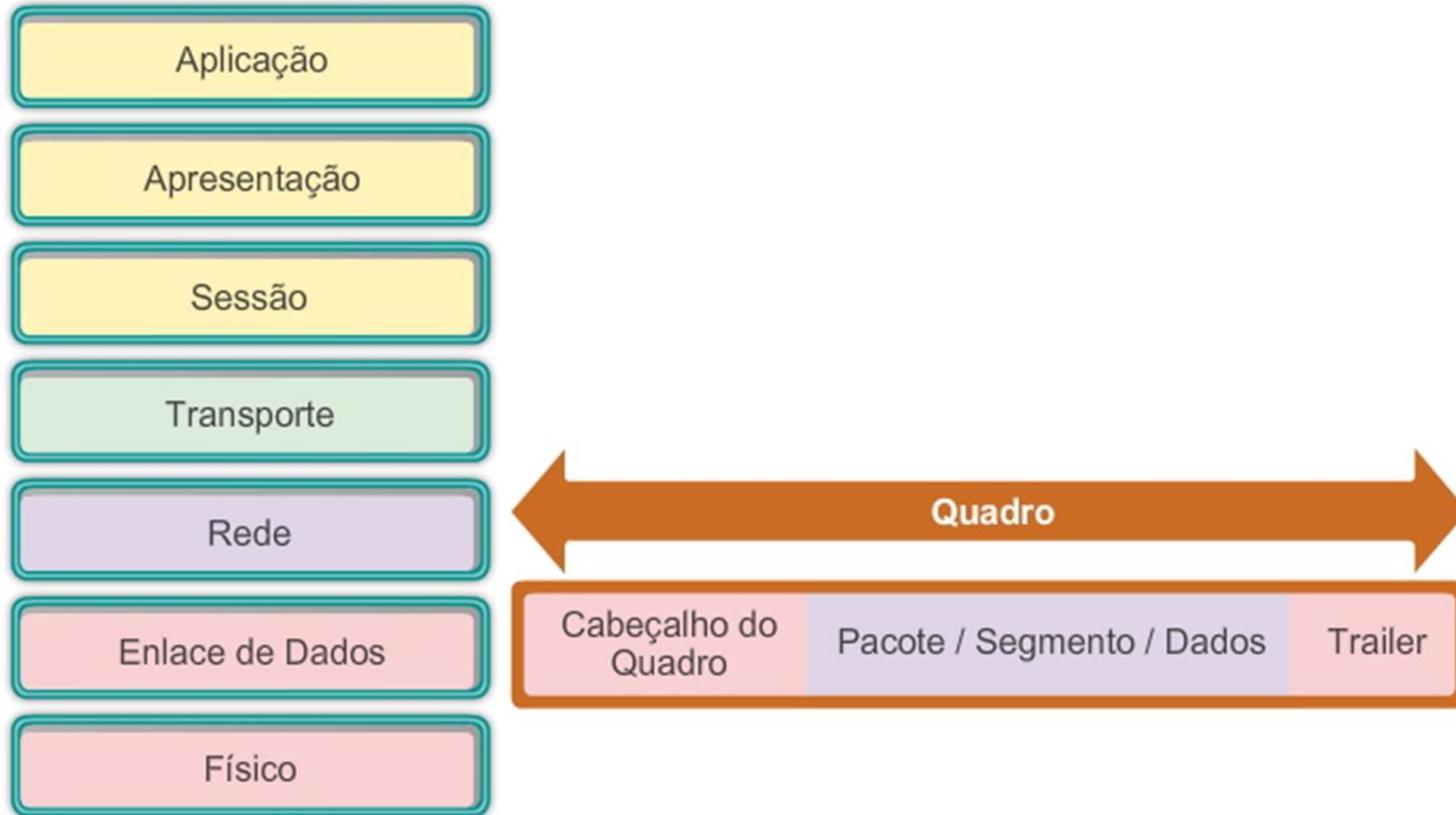


Em cada salto ao longo do caminho, um dispositivo intermediário aceita quadros de um meio, desencapsula o quadro e, em seguida, encaminha os pacotes em um novo quadro. Os cabeçalhos de cada quadro são formatados para o meio específico que o atravessará.

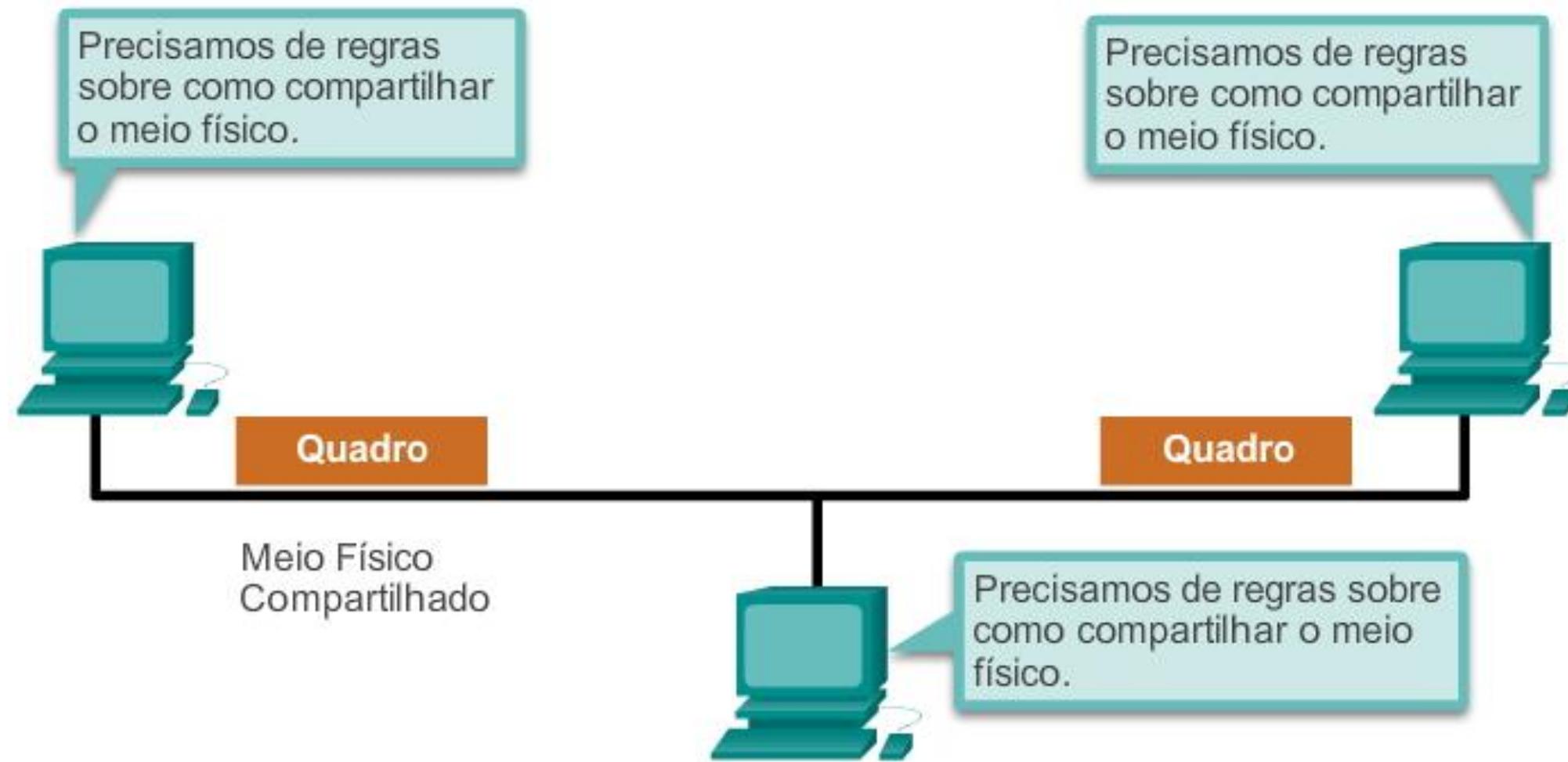


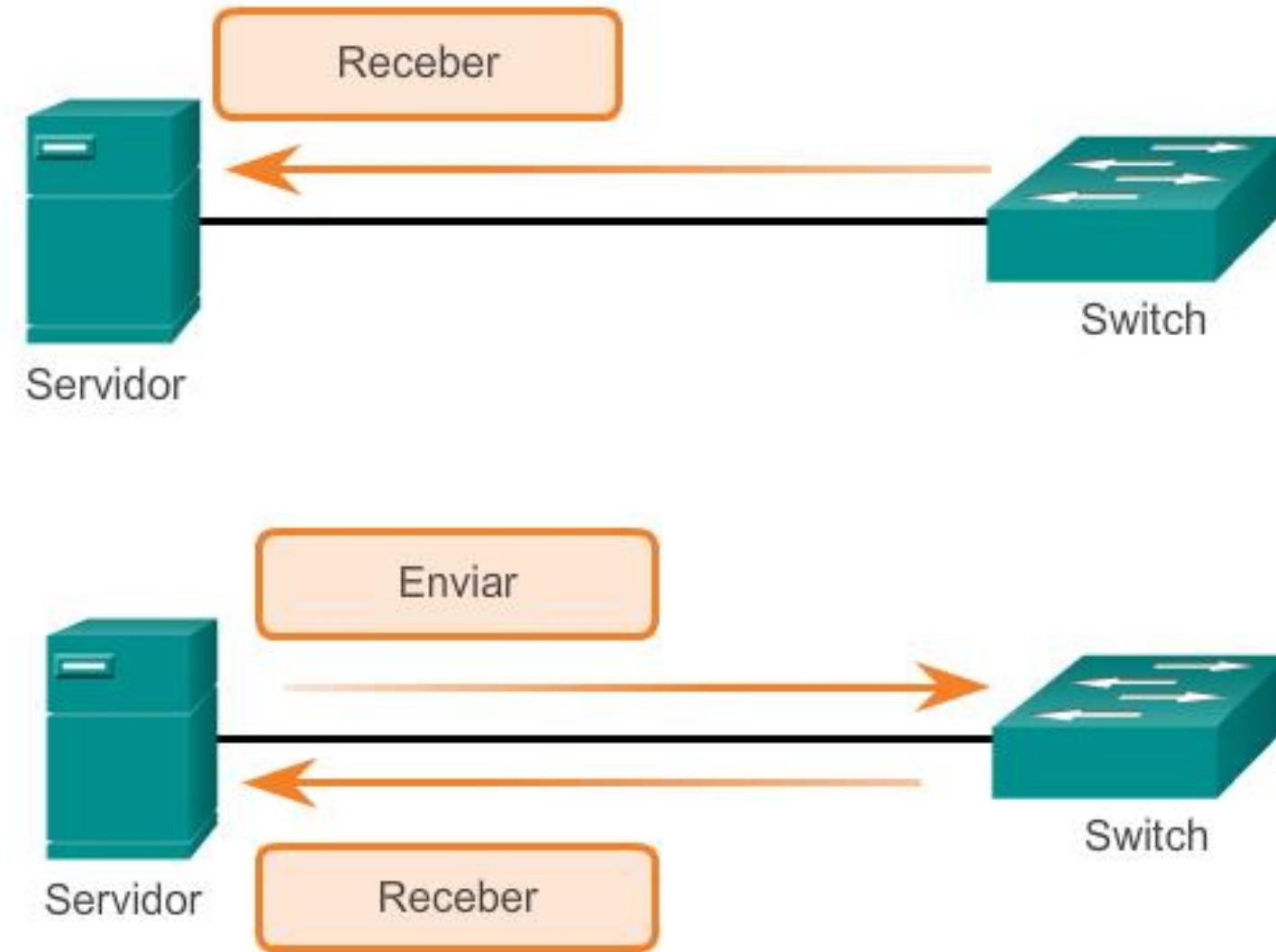


A camada de enlace de dados é responsável por controlar a transferência de quadros pelo meio físico.

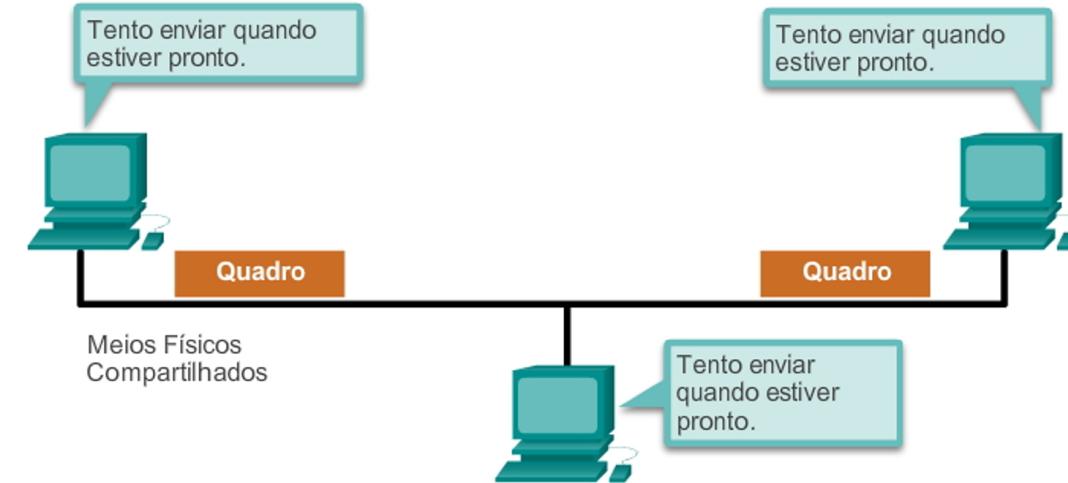


Controlando o acesso ao meio





Acesso Baseado em Contenções

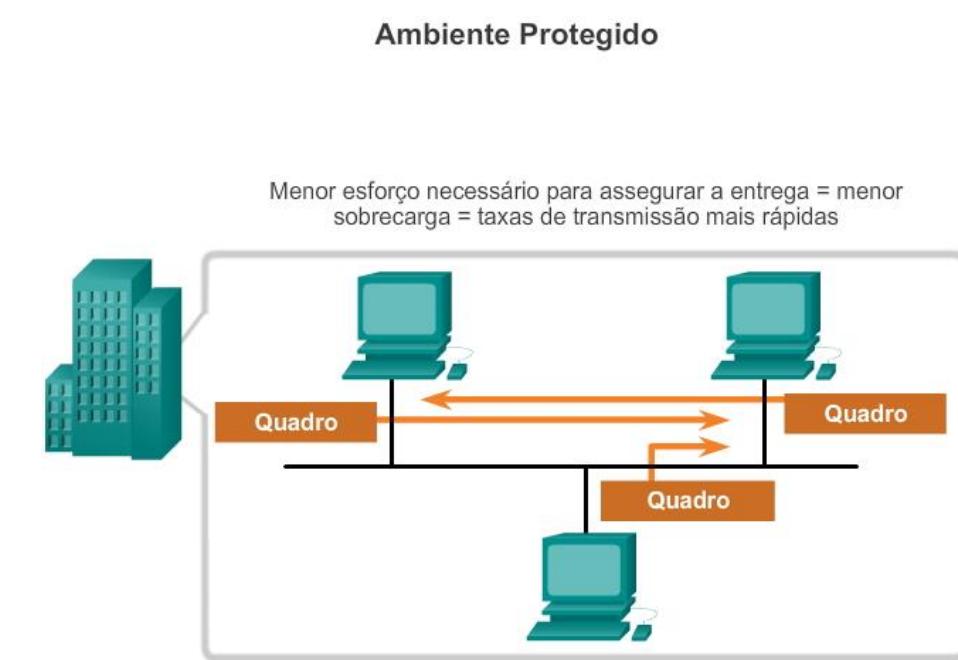


Características	Tecnologias baseadas em contenção
<ul style="list-style-type: none">As estações podem transmitir a qualquer momentoExistem colisõesHá mecanismos para resolver a contenção no meio físico	<ul style="list-style-type: none">CSMA/CD para redes Ethernet 802.3CSMA/CA para redes sem fio 802.11



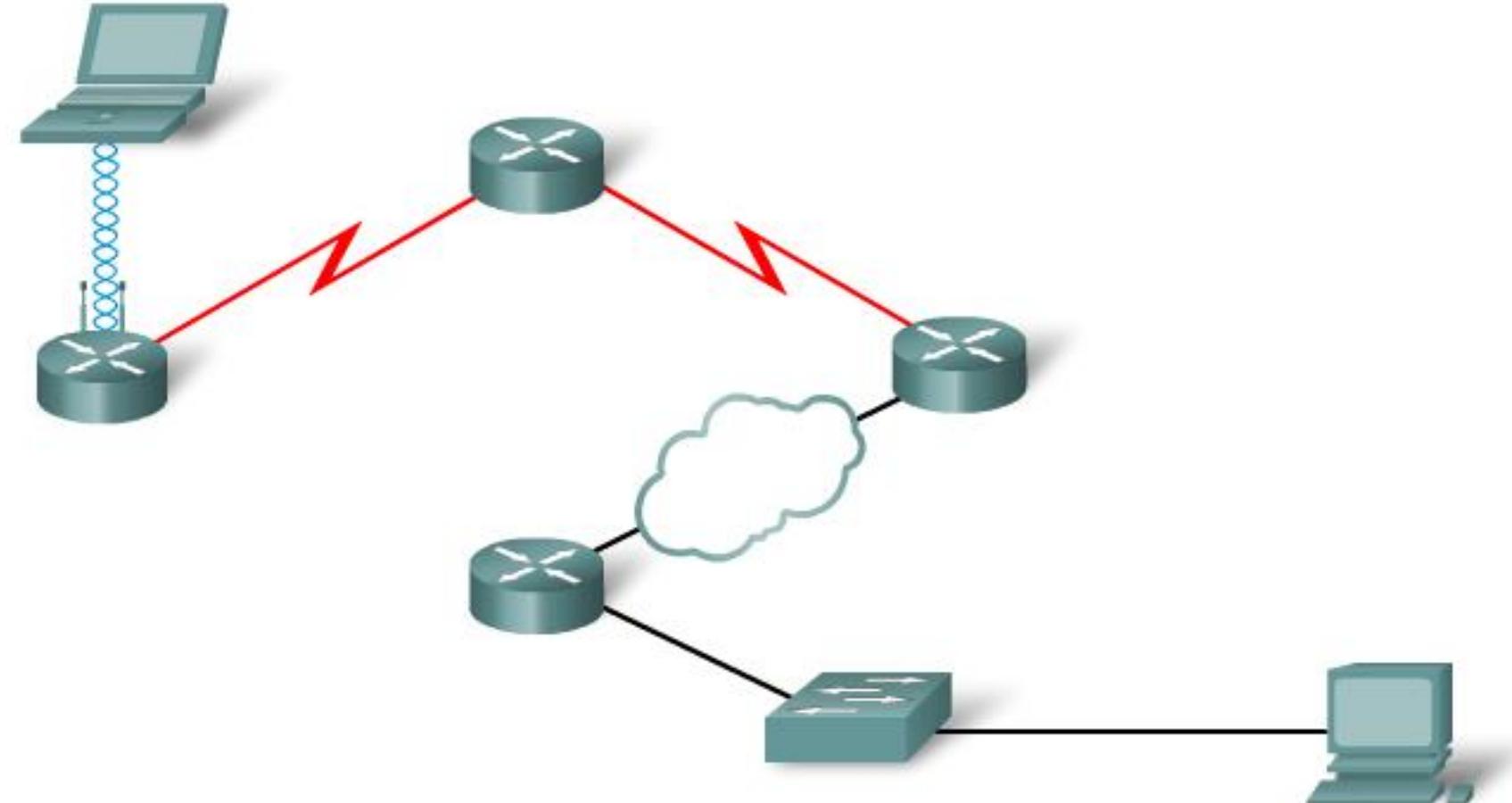
Características	Tecnologias de acesso controlado
<ul style="list-style-type: none"> • Apenas uma estação pode transmitir de cada vez • Os dispositivos que desejam transmitir devem aguardar pela sua vez • Sem colisões • Pode usar um método de passagem de testemunho (token) 	<ul style="list-style-type: none"> • Token Ring (IEEE 802.5) • Fiber Distributed Data Interface – FDDI (IEEE 804.4)

- O formato do quadro depende do protocolo da camada de ligação de dados usado. As três partes de um quadro são: o cabeçalho, os dados e o trailer



Em um **ambiente frágil**, são necessários mais controles para assegurar a entrega. Os campos de cabeçalho e de trailer aumentam à medida que mais informações de controle são necessárias.

Em um **ambiente protegido**, podemos contar com a chegada do quadro ao seu destino. São necessários menos controles, resultando em campos e quadros menores.



Um protocolo de enlace de dados comum para WANs

Quadro						
Nome de Campo	Flag	Endereço	Controle	Protocolo	Dados	FCS
Tamanho	1 byte	1 byte	1 byte	2 bytes	variável	2 ou 4 bytes

Flag - um único byte que indica o início e o fim de um quadro. O campo Flag consiste na sequência binária 01111110.

Endereço - um único byte que contém o endereço de broadcast PPP padrão. O PPP não atribui endereços de estação individuais.

Controle - um único byte que contém a sequência binária 00000011, que requer a transmissão de dados do usuário em um quadro sem sequência.

Protocolo - dois bytes que identificam o protocolo encapsulado no campo de dados do quadro. Os valores mais atualizados do campo de protocolo estão especificados no Assigned Numbers Request For Comments (RFC) mais recente.

Dados - zero ou mais bytes que contenham o datagrama do protocolo especificado no campo de protocolo.

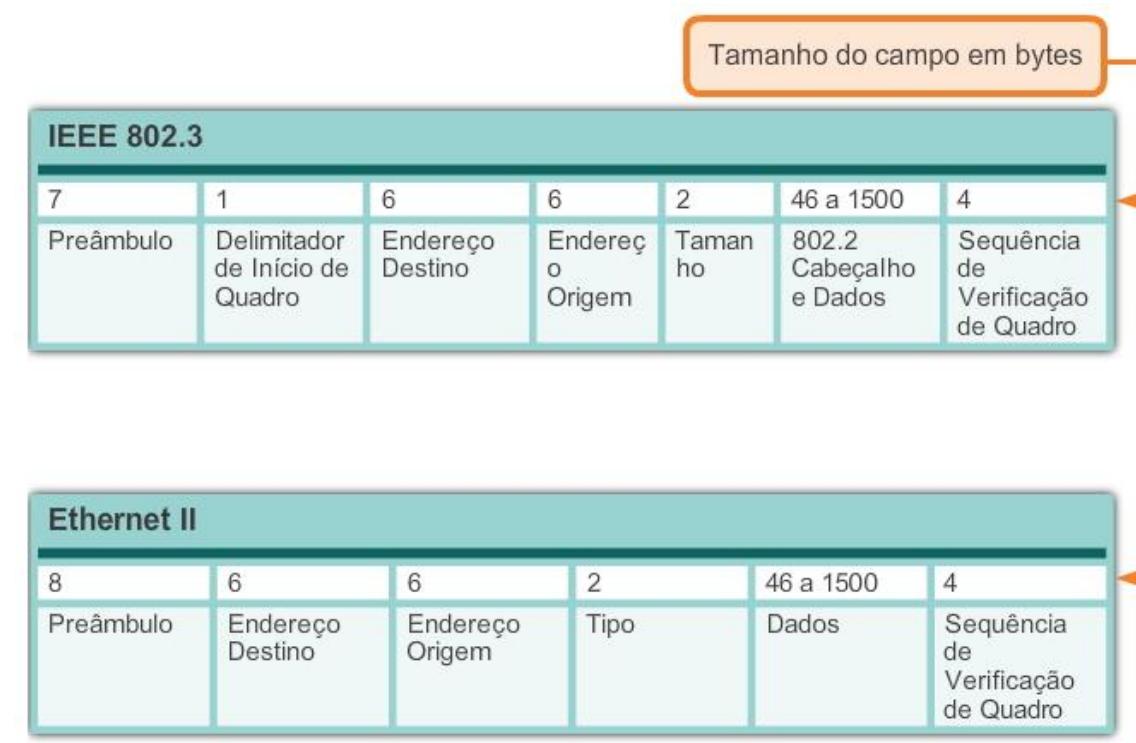
Sequência de verificação de quadro (FCS) - normalmente 16 bits (2 bytes). Por acordo anterior, as implementações que consentem com o PPP podem usar um FCS de 32 bits (4 bytes) para uma melhor detecção de erros.

- Exercício do Packet Tracer
 - 4.6.5 – Fazer ligações com e sem fios numa LAN
 - 2.9.1 - Trabalho prático de consolidação de conhecimentos

Comutação e Switches

- Address Resolution Protocol (ARP)
- Switches LAN

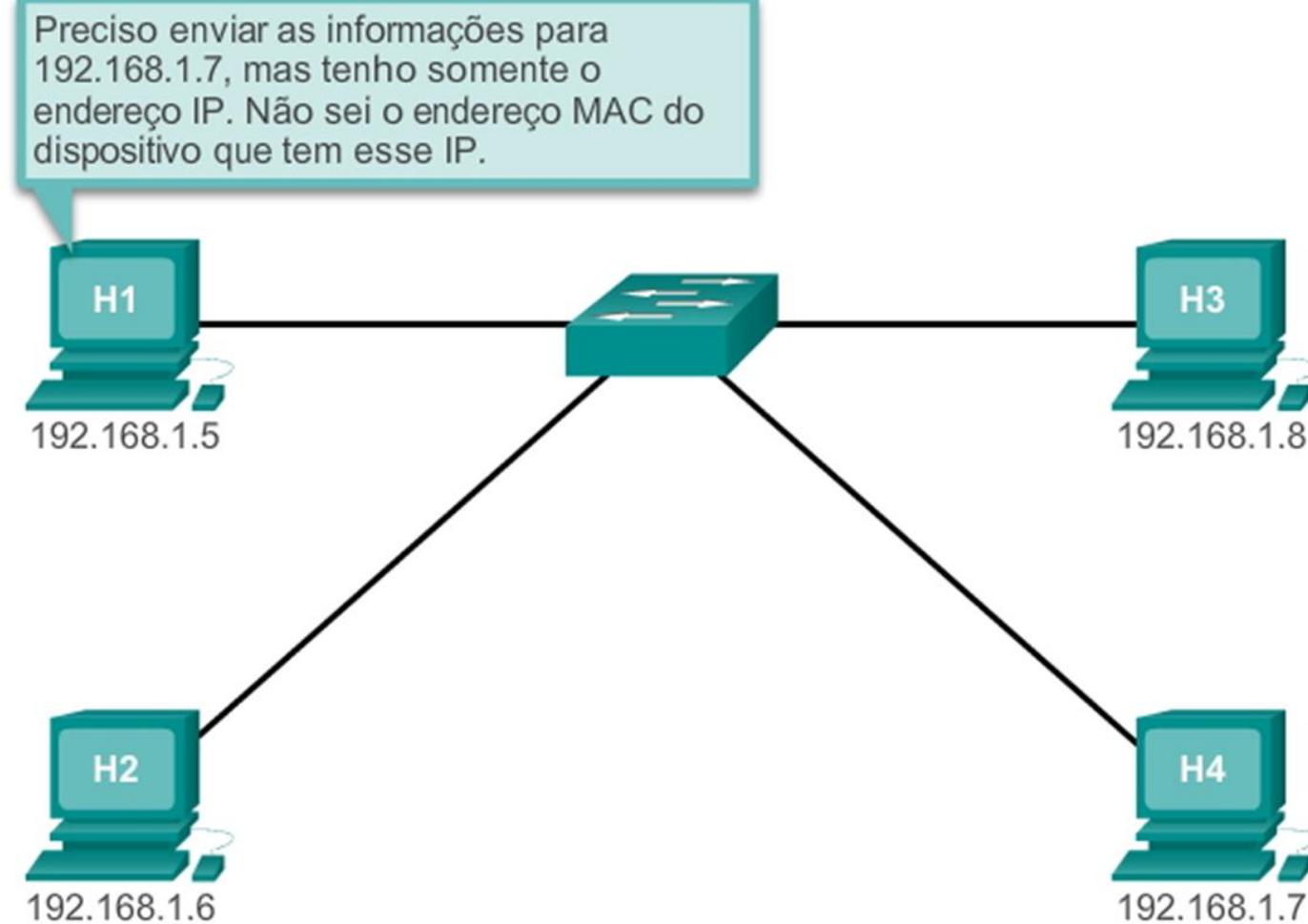
- A estrutura de quadros Ethernet adiciona cabeçalhos e trailers em volta da PDU da Camada 3 para encapsular as mensagens enviadas.
- A Ethernet II é o formato de quadro Ethernet usado em redes TCP/IP.



- Ethernet é a tecnologia mais amplamente usada nas redes locais
- Endereçamento - cada cabeçalho de Ethernet adicionado ao quadro contém o endereço físico (endereço MAC) que permite que um quadro seja entregue a um nó de destino
- Um endereço MAC da Ethernet da Camada 2 é um valor binário de 48 bits expresso como 12 dígitos hexadecimais
- O IEEE exige que um fornecedor siga duas regras simples:
 - ❖ Deve utilizar o OUI atribuído ao fornecedor como os primeiros 3 bytes
 - ❖ Todos os endereços MAC com o mesmo OUI devem receber um valor exclusivo nos últimos 3 bytes.
- Os endereços MAC são atribuídos às estações de trabalho, servidores, impressoras, switches e routers
- Exemplo MACs: 00-05-9A-3C-78-00, 00:05:9A:3C:78:00 ou 0005.9A3C.7800.
- A mensagem encaminhada a uma rede Ethernet, anexa as informações do cabeçalho ao pacote, contém o endereço MAC origem e destino

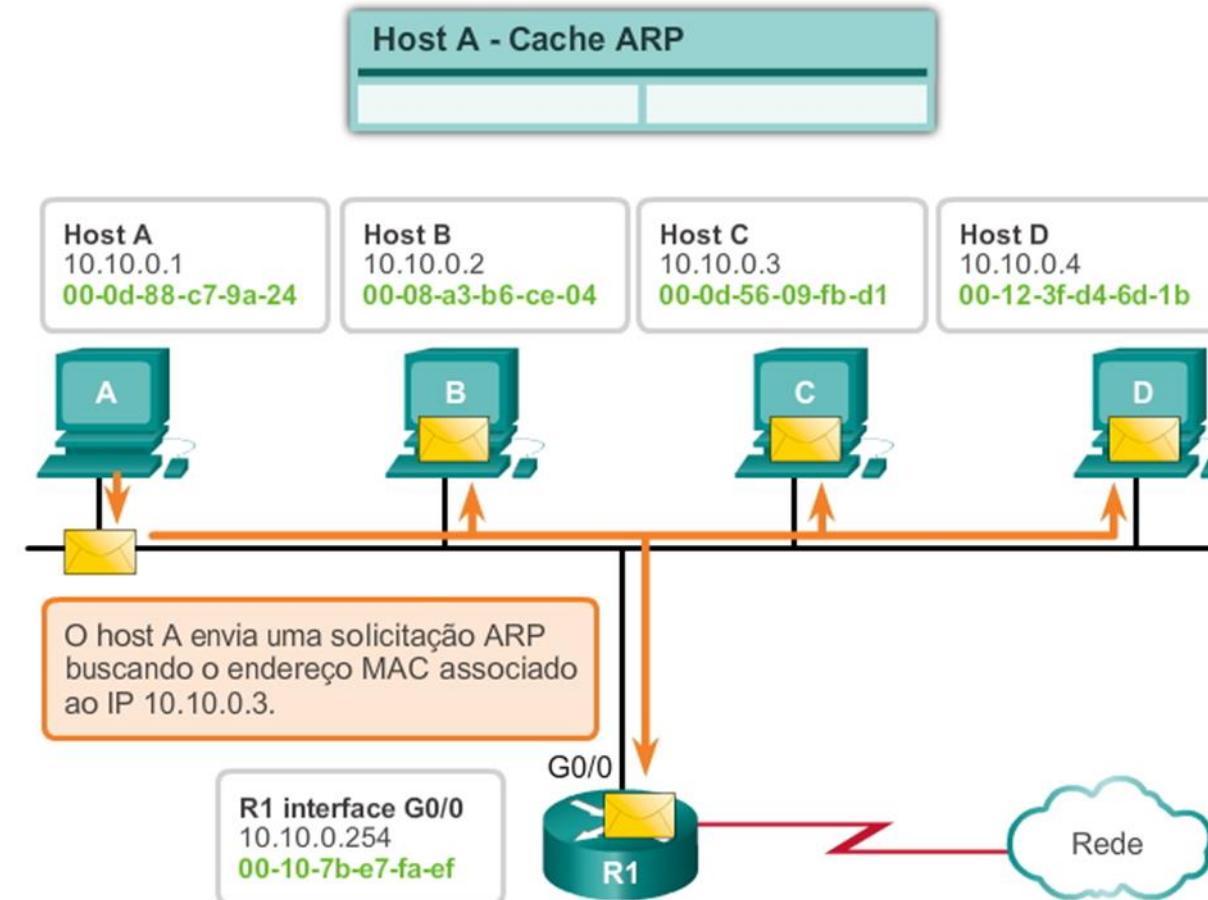
- As primeiras versões de Ethernet eram relativamente lentas a 10 Mbps
- Agora operam a 10 gigabits por segundo e mais rápido
- A Ethernet II e padrões IEEE 802.3 definem o tamanho mínimo de quadro como 64 bytes e o máximo como 1518 bytes
- Endereços MAC
 - ❖ Unicast
 - ❖ Multicast: 01-00-5E-?-?-?-?
 - ❖ Broadcast: FF-FF-FF-FF-FF-FF

- Finalidade ARP
 - ❖ A estação origem precisa de uma maneira de descobrir o endereço MAC do destino
- O protocolo ARP fornece duas funções básicas:
 - ❖ Resolver endereços de IPv4 para endereços MAC
 - ❖ Manter uma tabela de mapeamentos

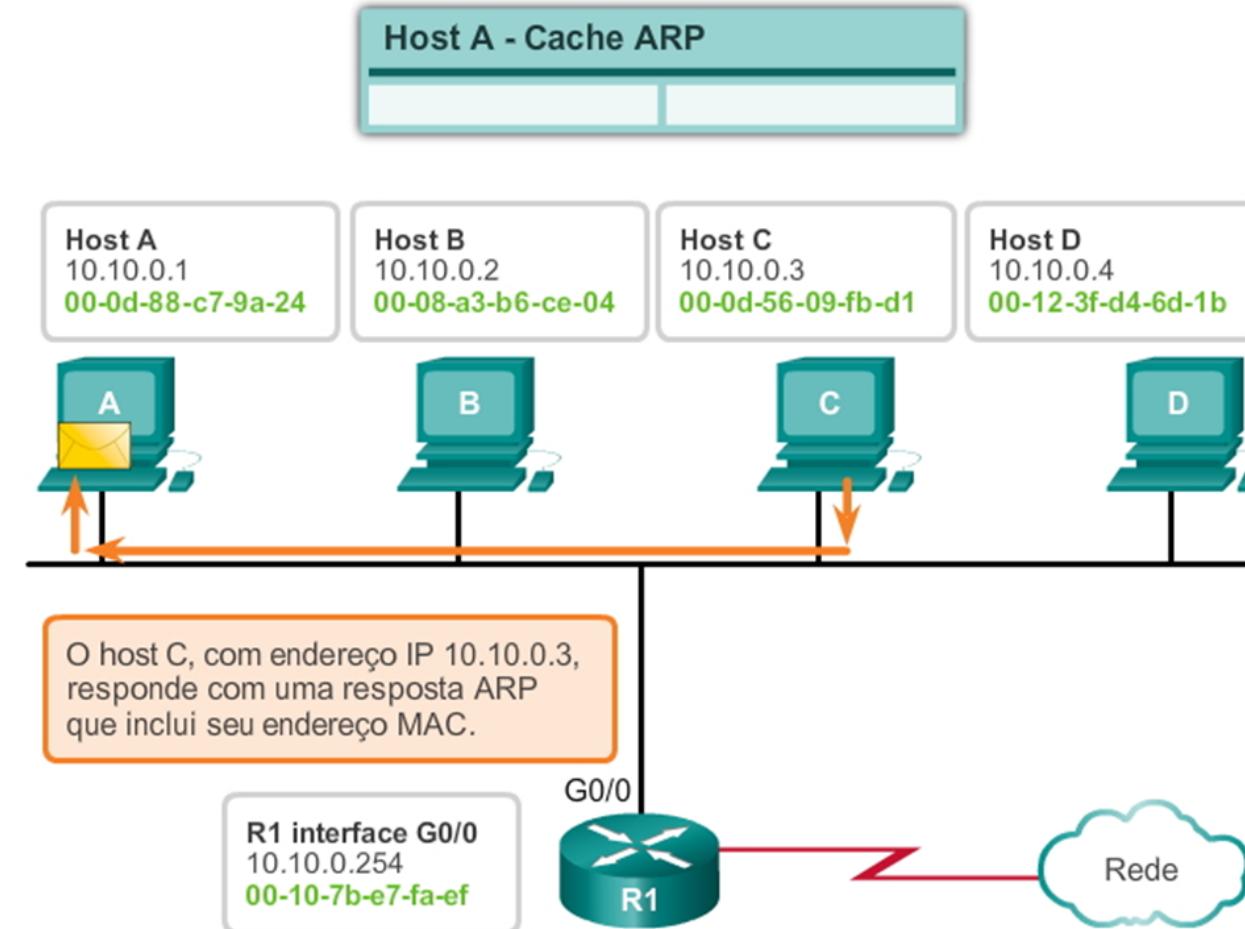


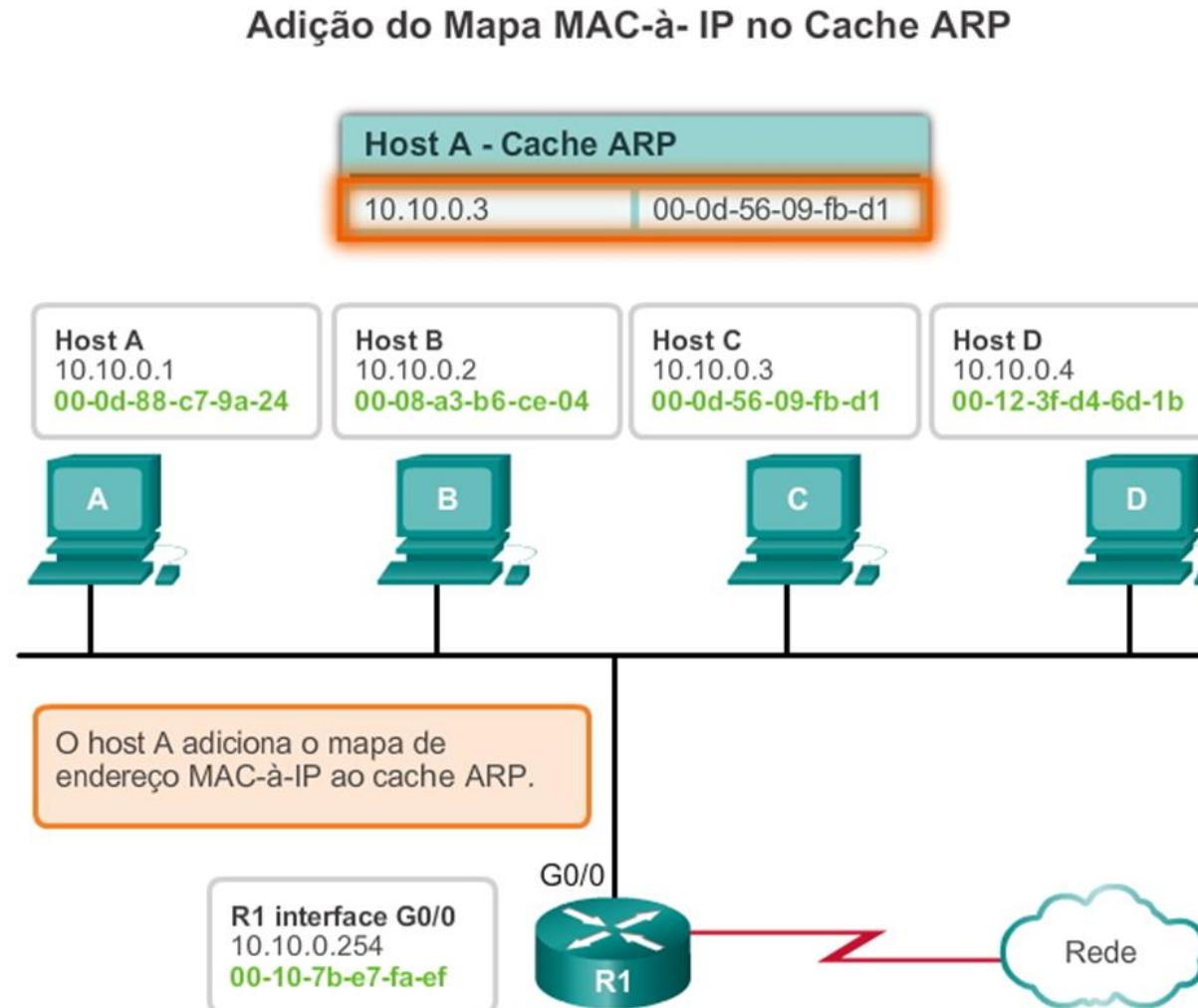
- Tabela ARP
 - ❖ Usada para encontrar o endereço da camada de ligação de dados que é mapeado no endereço IPv4 de destino
 - ❖ À medida que um nó recebe quadros do meio físico, ele pode registrar o IP origem e o endereço MAC como um mapeamento na tabela ARP
- Solicitação ARP
 - ❖ Mensagem de Broadcast (Difusão) de Camada 2 para todos os dispositivos na rede local Ethernet
 - ❖ O nó que corresponde ao endereço IP na mensagem de broadcast responderá
 - ❖ Se nenhum dispositivo responder à solicitação ARP, o pacote é eliminado porque um quadro não pode ser criado
- Entradas de mapeamento estático podem ser inseridas numa tabela ARP, mas isso raramente é feito

Transmissão de uma Solicitação ARP

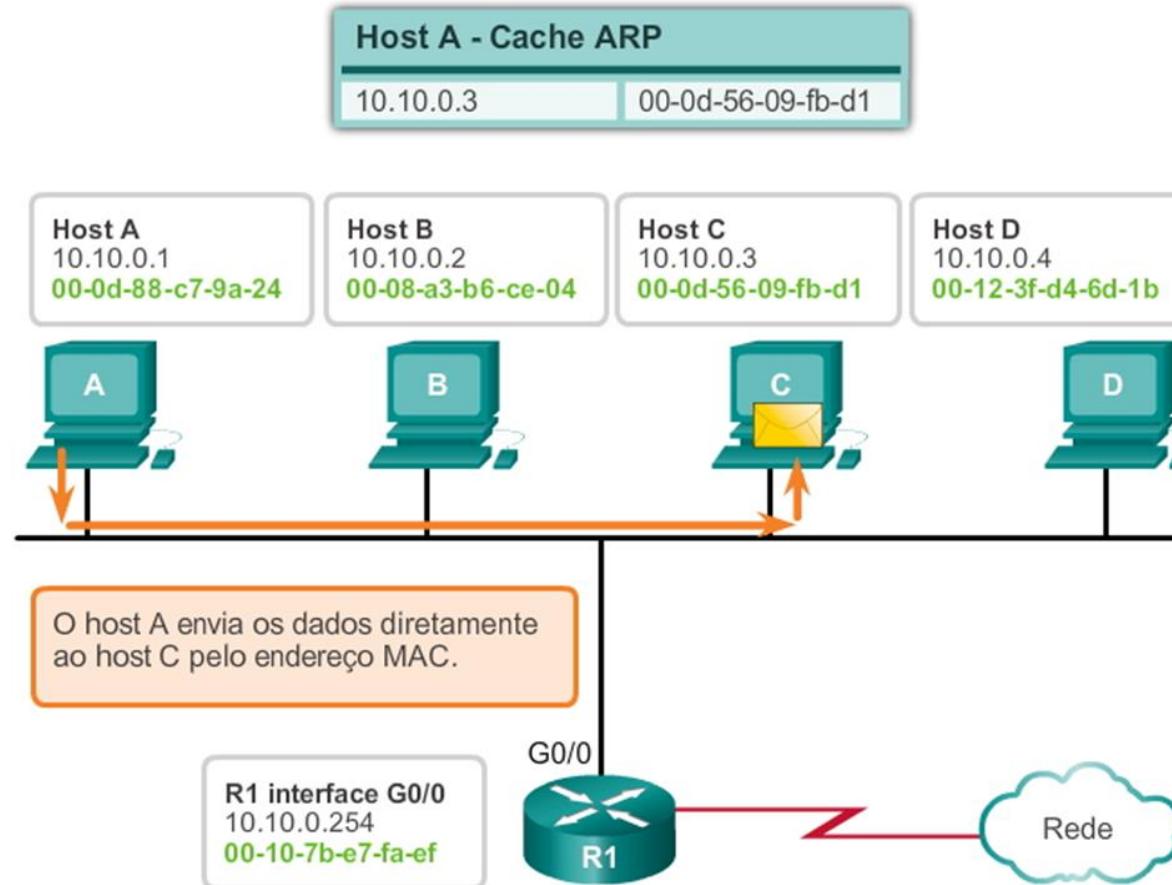


Resposta ARP com Informações MAC





Dados de Encaminhamento com Informações de Endereço MAC



Exemplo de tabelas ARP em dispositivos de rede

```
Router#show ip arp
```

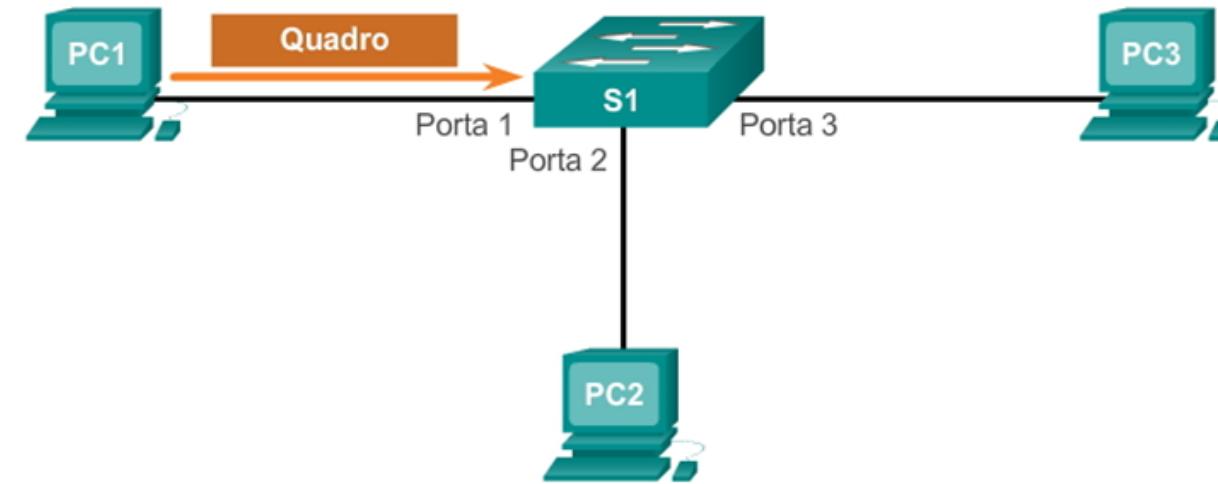
Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	172.16.233.229	-	0000.0c59.f892	ARPA	Ethernet0/0
Internet	172.16.233.218	-	0000.0c07.ac00	ARPA	Ethernet0/0
Internet	172.16.168.11	-	0000.0c63.1300	ARPA	Ethernet0/0
Internet	172.16.168.254	9	0000.0c36.6965	ARPA	Ethernet0/0

```
C:\>arp -a
```

Interface:	---	0xa	Type
Internet Address		Physical Address	
192.168.1.254		64-0f-29-0d-36-91	dynamic
192.168.1.255		ff-ff-ff-ff-ff-ff	static
224.0.0.22		01-00-5e-00-00-16	static
224.0.0.251		01-00-5e-00-00-fb	static
224.0.0.252		01-00-5e-00-00-fc	static
255.255.255.255		ff-ff-ff-ff-ff-ff	static

- Switch LAN de camada 2
 - ❖ Ligação de dispositivos finais a um dispositivo intermediário central, na maioria das redes Ethernet
 - ❖ Executa o switching e a filtragem com base apenas no endereço MAC
 - ❖ Cria uma tabela de endereços MAC que usa para tomar decisões de encaminhamento
 - ❖ Depende dos routers para passar dados entre sub-redes IP

- O switch recebe um quadro de PC 1 na porta 1.
- O switch insere o endereço MAC origem no quadro e a porta do switch que recebeu o quadro na tabela de endereços.
- Como o endereço destino não se encontra na tabela de endereços MAC, o switch inunda o quadro para todas as portas, exceto aquela em que recebeu o quadro.



- O dispositivo a quem o quadro se destinava (vamos supor que era PC 2) é o único a responde com um quadro unicast endereçado ao PC 1.
- O switch insere o endereço MAC origem do PC 2 e o número de porta de switch que recebeu o quadro na tabela de endereços. O endereço destino do quadro e da porta associada já se encontra na tabela de endereços MAC.
- O switch pode agora enviar quadros entre os dispositivos de origem e de destino sem inundar, pois tem as entradas na tabela de endereços que identificam as portas associadas.

Configuração fixa versus modular

Diâmetro Total do Switch



Switches de Configuração Fixos

Os recursos e as opções limitam-se aos fornecidos originalmente com o switch.



Switches de Configuração Modular

O chassi aceita as placas de linha que contêm as portas.

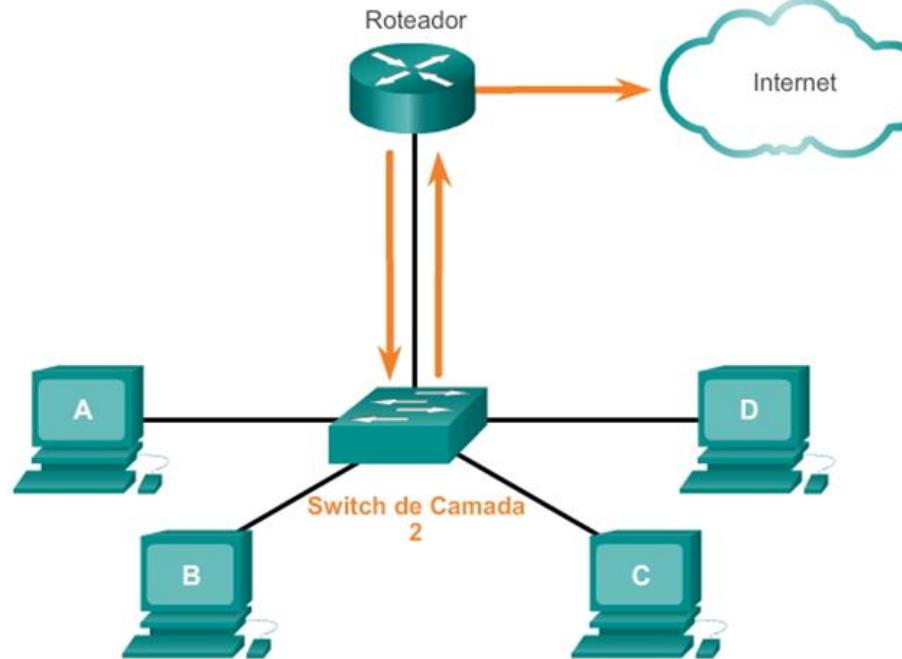


Switches de Configuração Empilhável

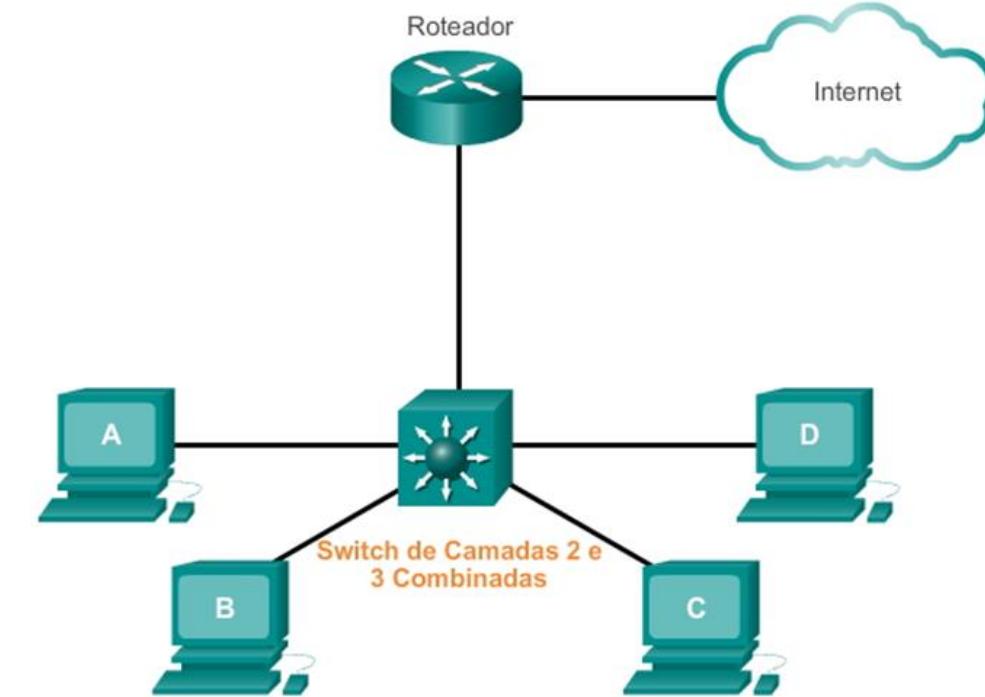
Switches empilháveis, conectados por um cabo especial, opera efetivamente como um grande switch.

switching Camada 2 versus switching de camada 3

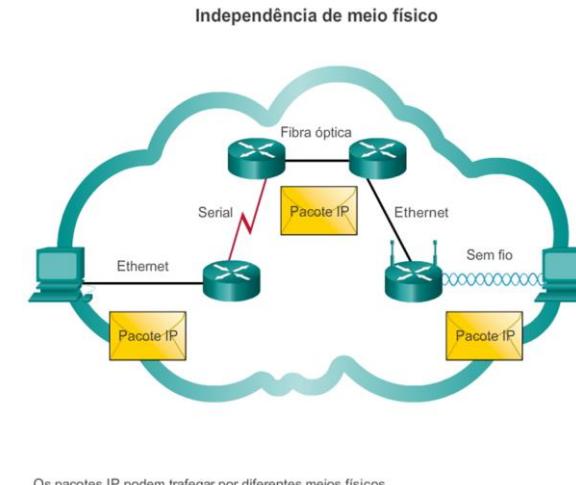
Switching de Camada 2



Switching de Camada 3

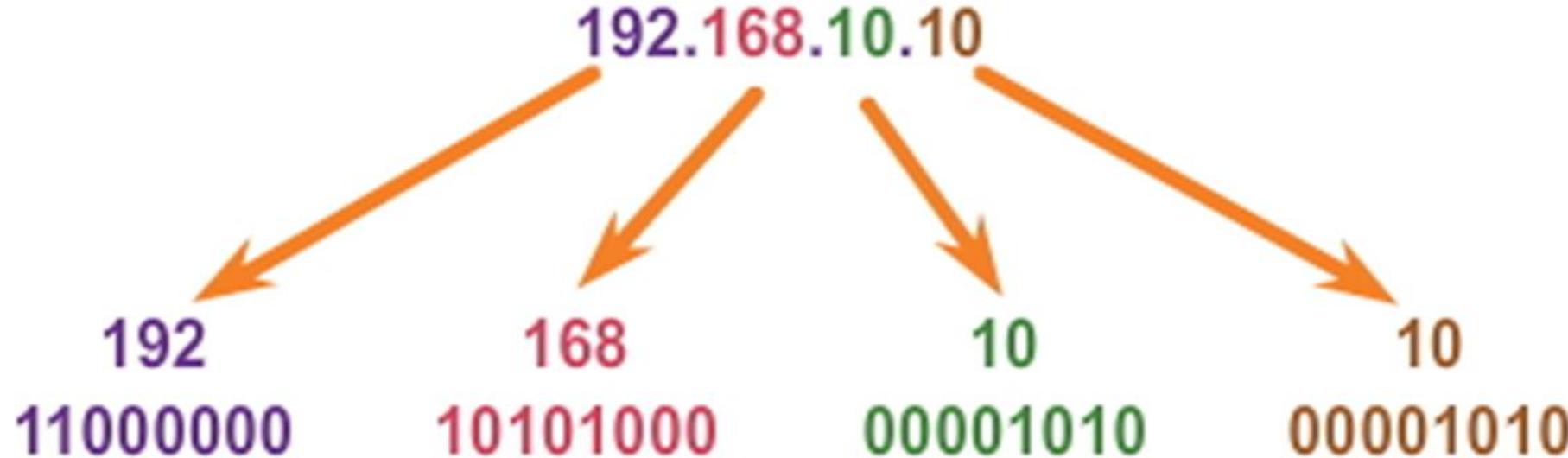


Camada de rede e encaminhamento

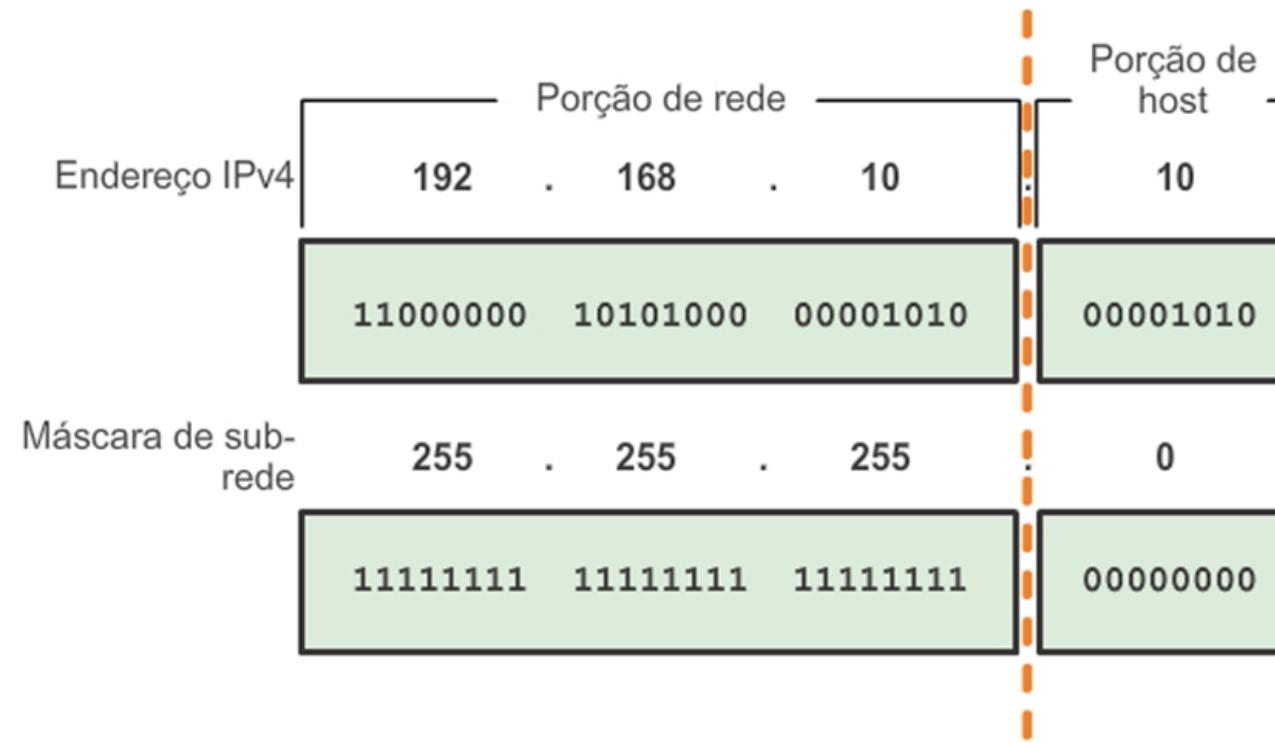


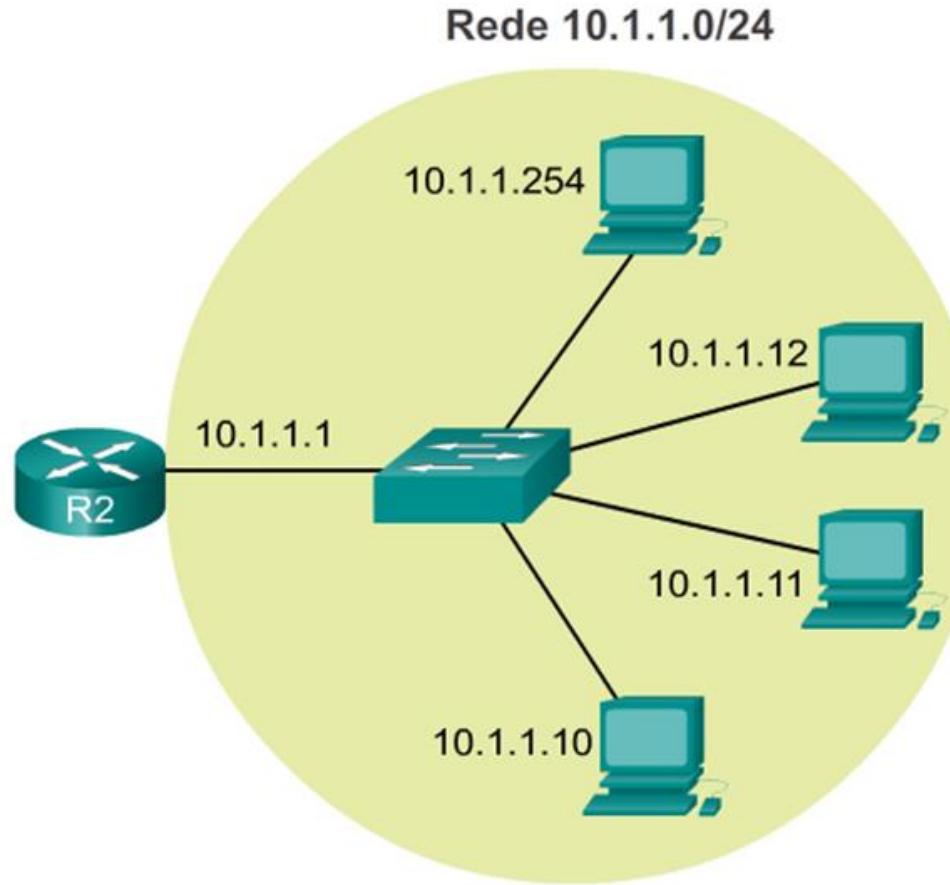
- Endereços IP: Unicast, Multicast e Broadcast

Converter decimal em binário

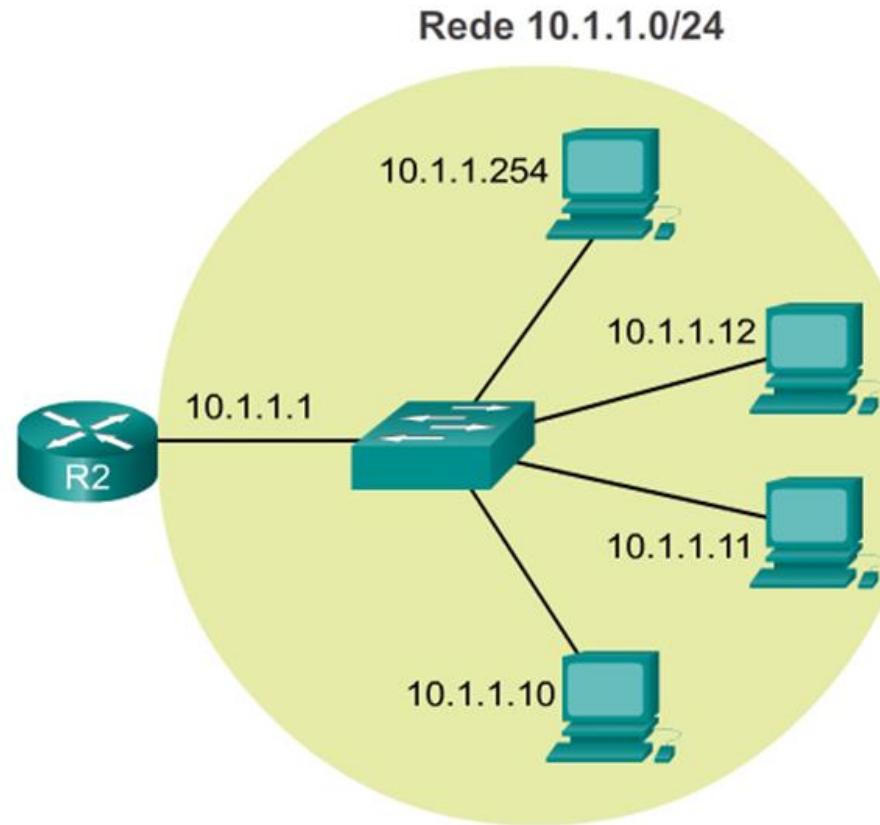


- Para definir a rede e as partes do host de um endereço, os dispositivos utilizam um padrão de 32 bits chamado máscara de sub-rede
- A máscara de sub-rede não contém realmente a rede ou parte do host de um endereço IPv4, ela apenas diz onde procurar essas partes de um endereço IPv4 determinado





Porção de rede	Porção de host
10 00001010	1 00000001
10 00001010	1 00000001
10 00001010	255 11111111



Porção de rede			Porção de host
10	00001010	1	1 00000001
10	00001010	1	254 11111110

- Os blocos de endereços privados são:
 - ❖ 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
 - ❖ 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
 - ❖ 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)
- Hosts que não requerem acesso à Internet poderão usar endereços privados

- O IPv6 é o sucessor do IPv4
- A redução do espaço de endereço IPv4 é o fator de motivação para migrar para IPv6
- Exemplo de endereço IPv6:
2001:0DB8:0000:1111:0000:0000:0200

- 128 bits de comprimento e escrito como uma sequência de valores hexadecimais
- No IPv6, 4 bits representam um único dígito hexadecimal,
32 valores hexadecimais = endereço IPv6
 - 2001:0DB8:0000:1111:0000:0000:0000:0200
 - FE80:0000:0000:0000:0123:4567:89AB:CDEF
- Sexteto (Hextet) usado para referir a um segmento de 16 bits ou de quatro dígitos hexadecimais
- Pode ser escrito em minúsculas ou em maiúsculas

- A primeira regra para ajudar a reduzir a representação dos endereços IPv6, diz que 0s (zeros) mais significativos, em qualquer seção de 16 bits (ou no hextet) podem ser omitidos.
- 01AB pode ser representado como 1AB
- 09F0 pode ser representado como 9F0
- 0A00 pode ser representado como A00
- 00AB pode ser representado como AB

Preferência de	2001: 0 DB8: 000 A:1000: 000 0: 000 0: 000 0: 01 00
Nenhum 0 à esquerda	2001: DB8: A:1000: 0: 0: 0: 100

Regra 2 - Omitir todos os segmentos de 0s

- Dois pontos duplo (::) podem substituir uma única sequência contígua de um ou mais segmentos de 16 bits (hextets) que consistem em tudo a zeros
- O dois pontos duplo (::) pode ser usado apenas uma vez, senão o endereço será ambíguo
- Conhecido como o formato compactado
- Endereço incorreto - 2001:0DB8::ABCD::1234

➤ Exemplos

Preferência de	2001: 0DB8:0000:0000:ABCD:0000:0000:0100
Nenhum 0 à esquerda	2001: DB8: 0: 0: ABCD: 0: 0: 100
Compactado	2001:DB8::ABCD:0:0:100
ou	
Compactado	2001:DB8:0:0:ABCD::100

Apenas um:: pode ser usado.

Preferência de	FE80: 0000:0000:0000:0123:4567:89AB:CDEF
Nenhum 0 à esquerda	FE80: 0: 0: 0: 123:4567:89AB:CDEF
Compactado	FE80::123:4567:89AB:CDEF

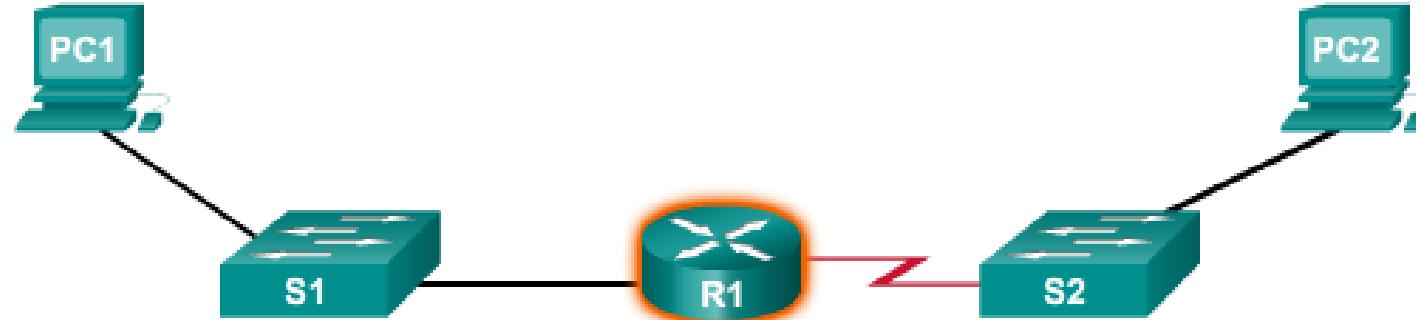
- As técnicas de migração podem ser divididas em três categorias:
- Pilha dual: permite que IPv4 e IPv6 coexistam na mesma rede. Os dispositivos executam as pilhas de protocolo IPv4 e IPv6 simultaneamente.
- Túneis: um método de transporte de um pacote IPv6 numa rede IPv4. O pacote IPv6 é encapsulado dentro de um pacote IPv4.
- Tradução: a Network Address Translation 64 (NAT64) permite que os dispositivos IPv6 comuniquem com os dispositivos IPv4, usando uma técnica de tradução semelhante ao NAT no IPv4. Um pacote IPv6 é traduzido num pacote IPv4, e vice-versa

- Determinam qual o melhor caminho pelo qual enviar os pacotes
 - ✓ Usando a sua tabela de encaminhamento para determinar o caminho
- Encaminham os pacotes em direção do seu destino
 - ✓ Encaminha o pacote para a interface indicada na tabela de encaminhamento
 - ✓ Encapsula o pacote e envia-o na direção do seu destino.
- Routers usam rotas estáticas e protocolos de encaminhamento dinâmico para aprender sobre redes remotas e criar as suas tabelas de encaminhamento

- Configuração das interfaces LAN
- Configurar rotas estáticas e protocolos de encaminhamento dinâmico (não estudado aqui)
- Verificar a configuração da interface

Tabela de encaminhamento após configurar as interfaces

Routers Route Packets



```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
      i - IS-IS, 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

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0
```

Cisco IOS command line interface (CLI) can be used to view the route table.

Tabela de Encaminhamento – noções básicas

- Tabela de encaminhamento é um arquivo armazenado na memória RAM contendo informações sobre
 - ✓ Redes diretamente ligadas
 - ✓ Redes remotas
 - ✓ Agrupamentos de redes ou de próximos saltos

- As primeiras tarefas básicas que devem ser efetuadas num router ou switch Cisco:
 - ✓ Atribuir nome ao dispositivo – Distingue o equipamento de outros routers
 - ✓ Configurar o acesso seguro para gestão

```
R1(config)#enable secret class
R1(config)#
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#service password-encryption
R1(config)#
```

- Para ficar disponível uma interface do router deve ser:
 - ✓ Configurado com uma endereço IP e máscara de sub-rede.
 - ✓ Ativado – por omissão, interfaces LAN e WAN não são ativados.
Deve ser ativado usando o comando no shutdown

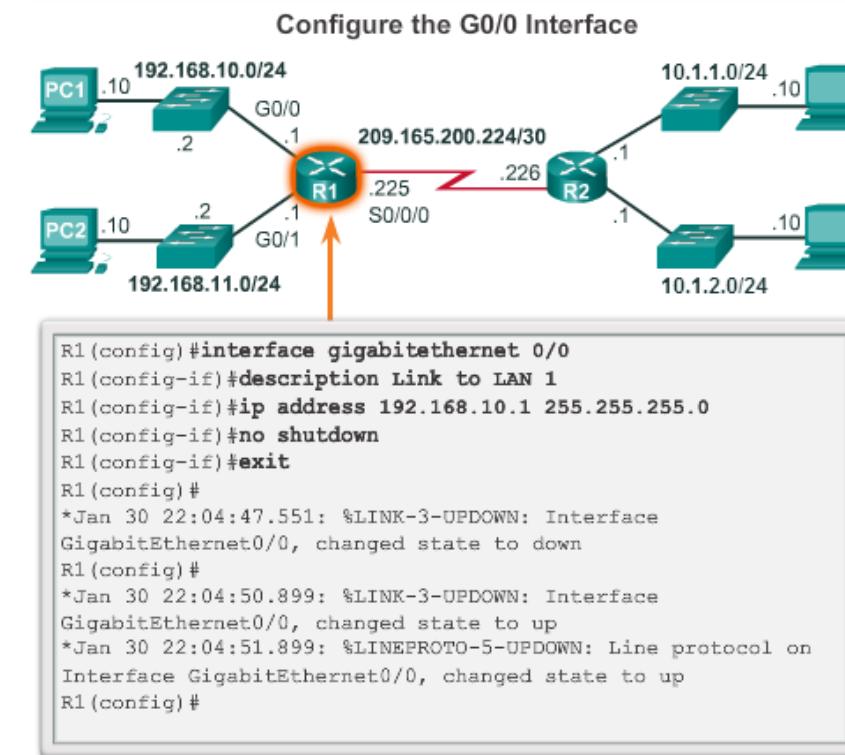
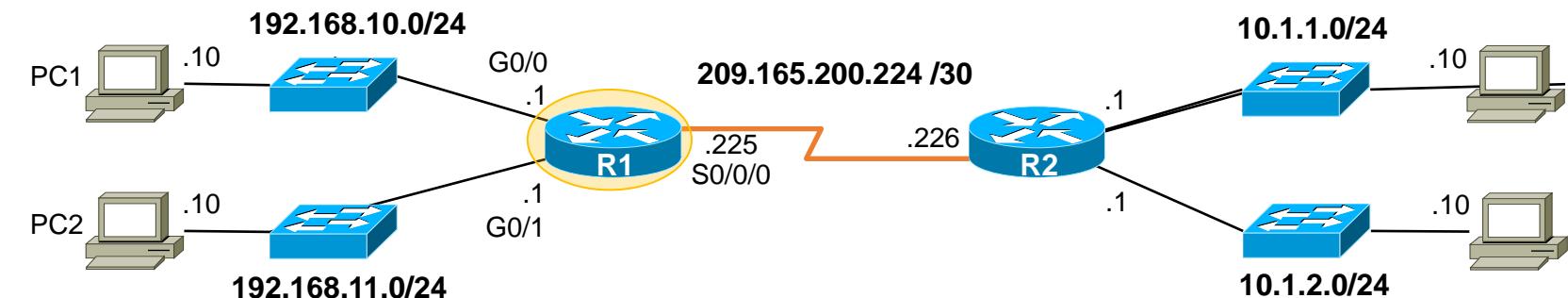


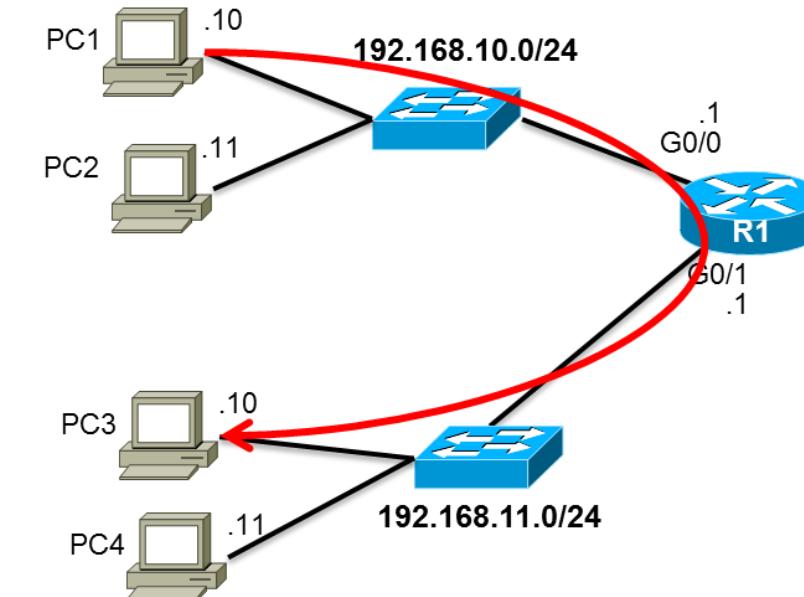
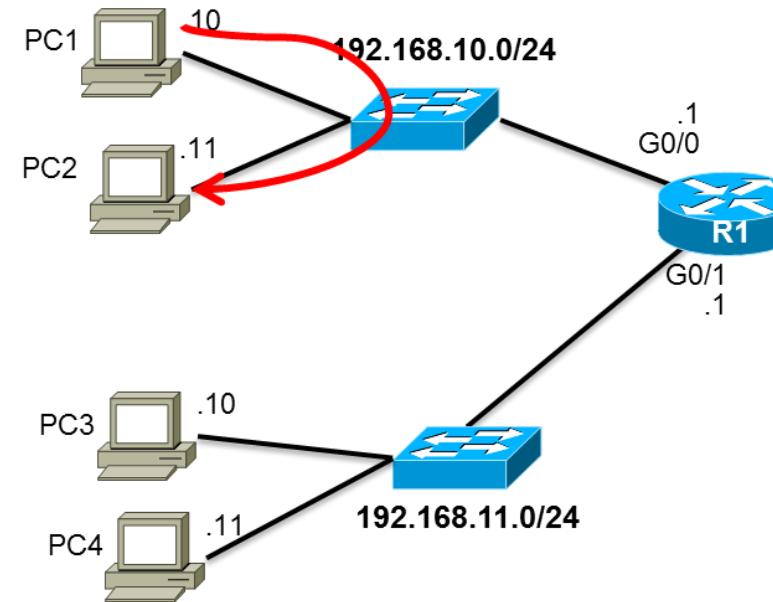
Tabela de encaminhamento do router IPv4

```
R1#show ip route
Codes: L - local, C - connected, 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, E - EGP
      i - IS-IS, 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

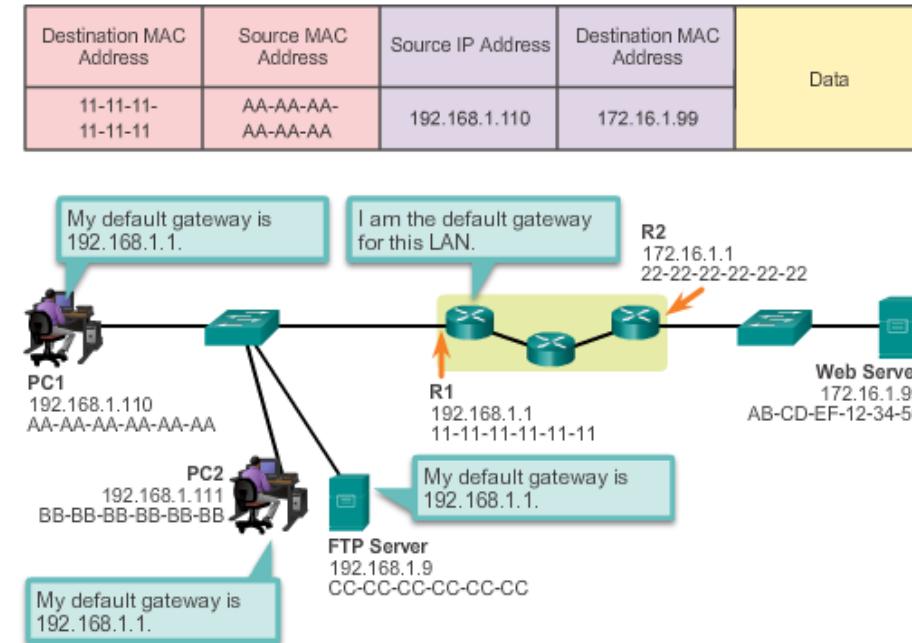
Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D        10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
D        10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
  192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0
  192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/1
  209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C        209.165.200.224/30 is directly connected, Serial0/0/0
L        209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

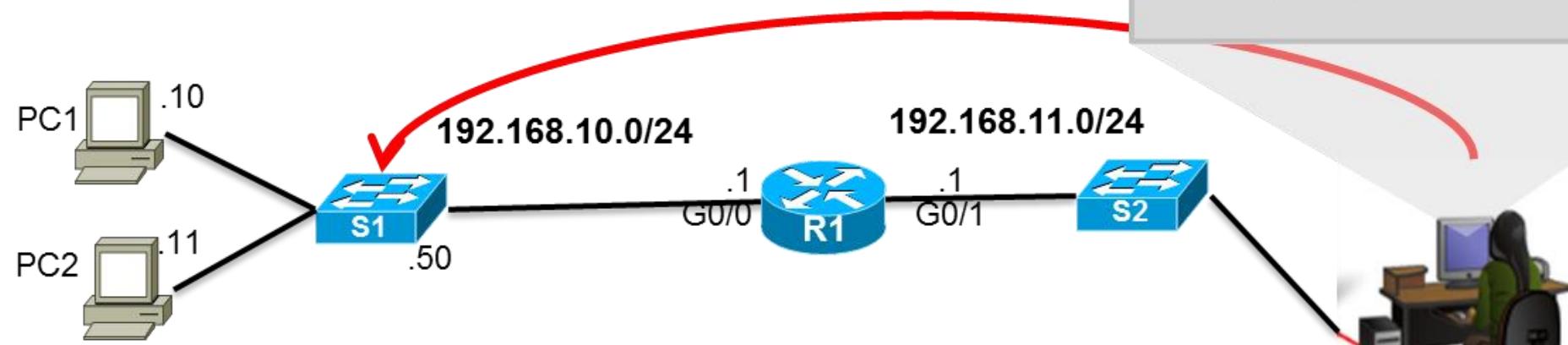




- Para permitir o acesso à rede, os dispositivos devem ser configurado com as seguintes informações sobre o endereço IP:
 - ✓ Endereço IP - Identifica um host numa rede local.
 - ✓ Máscara de sub-rede - Identifica a sub-rede do host.
 - ✓ Gateway por omissão (default gateway) - Identifica o router para o qual um pacote é enviado quando o destino não está na mesma sub-rede local



Gateway padrão num switch

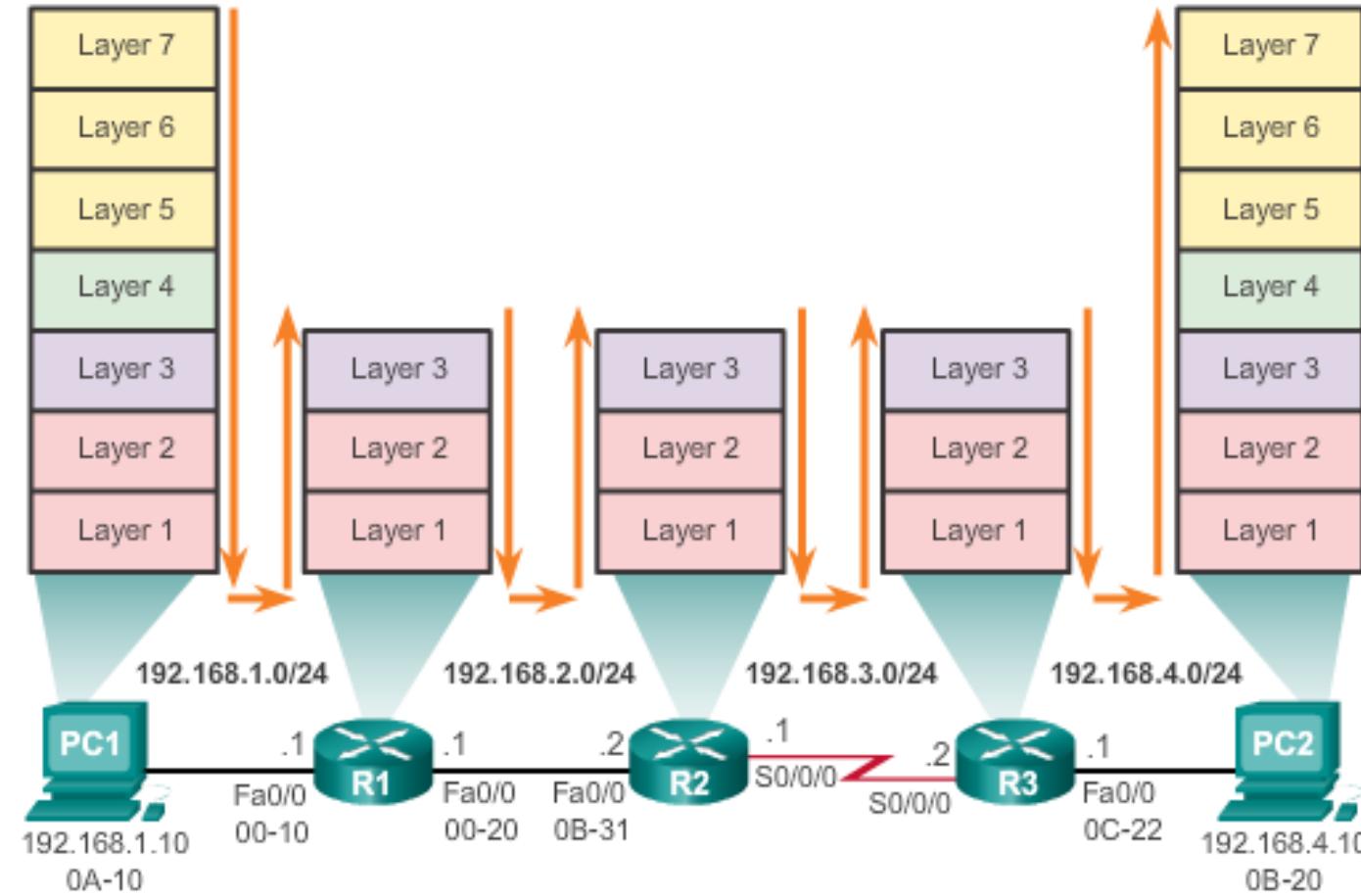


```
S1#show running-config
Building configuration...
!
<output omitted>
service password-encryption
!
hostname S1
!
Interface Vlan1
ip address 192.168.10.50
!
ip default-gateway 192.168.10.1
<output omitted>
```

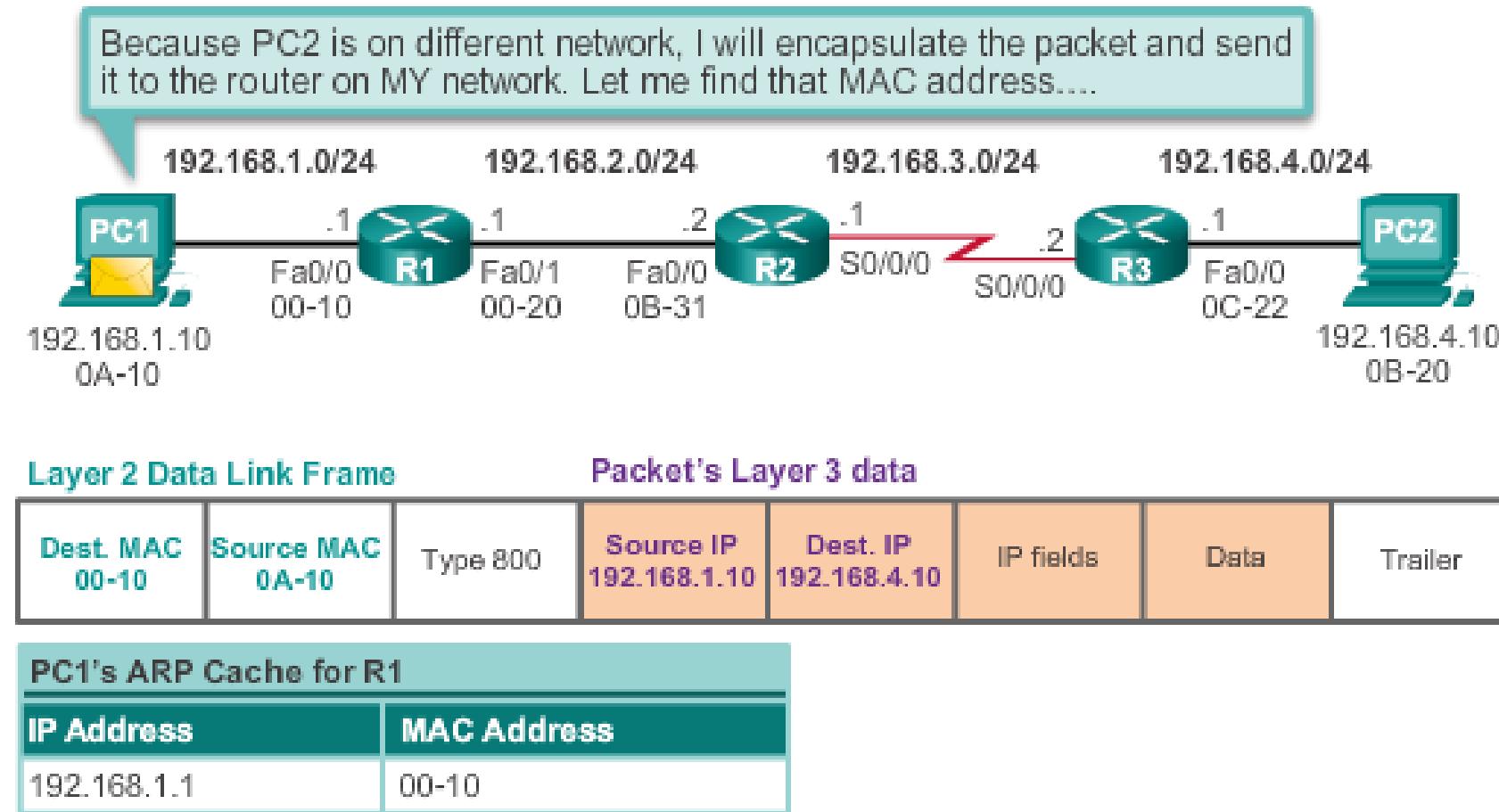
Se o gateway padrão não for configurado em S1, os pacotes de resposta de S1 não poderão chegar ao administrador de 192.168.11.10. O administrador não conseguirá gerir remotamente o dispositivo.



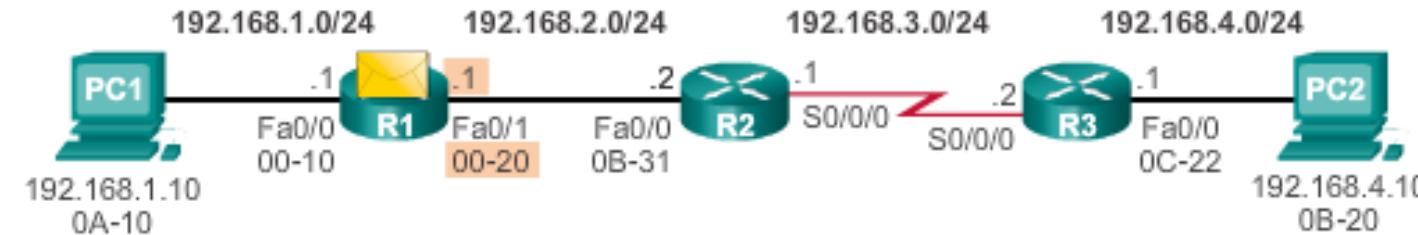
Encapsulating and De-Encapsulating Packets



PC1 Sends a Packet to PC2



R3 Forwards the Packet to PC2



Layer 2 Data Link Frame

Dest. MAC 0B-31	Source MAC 00-20	Type 800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

R1's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	0	Dir. Connect.	Fa0/0
192.168.2.0/24	0	Dir. Connect.	Fa0/1
192.168.3.0/24	1	192.168.2.2	Fa0/1
192.168.4.0/24	2	192.168.2.2	Fa0/1

Encaminhando pacotes entre redes - IV

R2 Forwards the Packet to R3



Layer 2 Data Link Frame

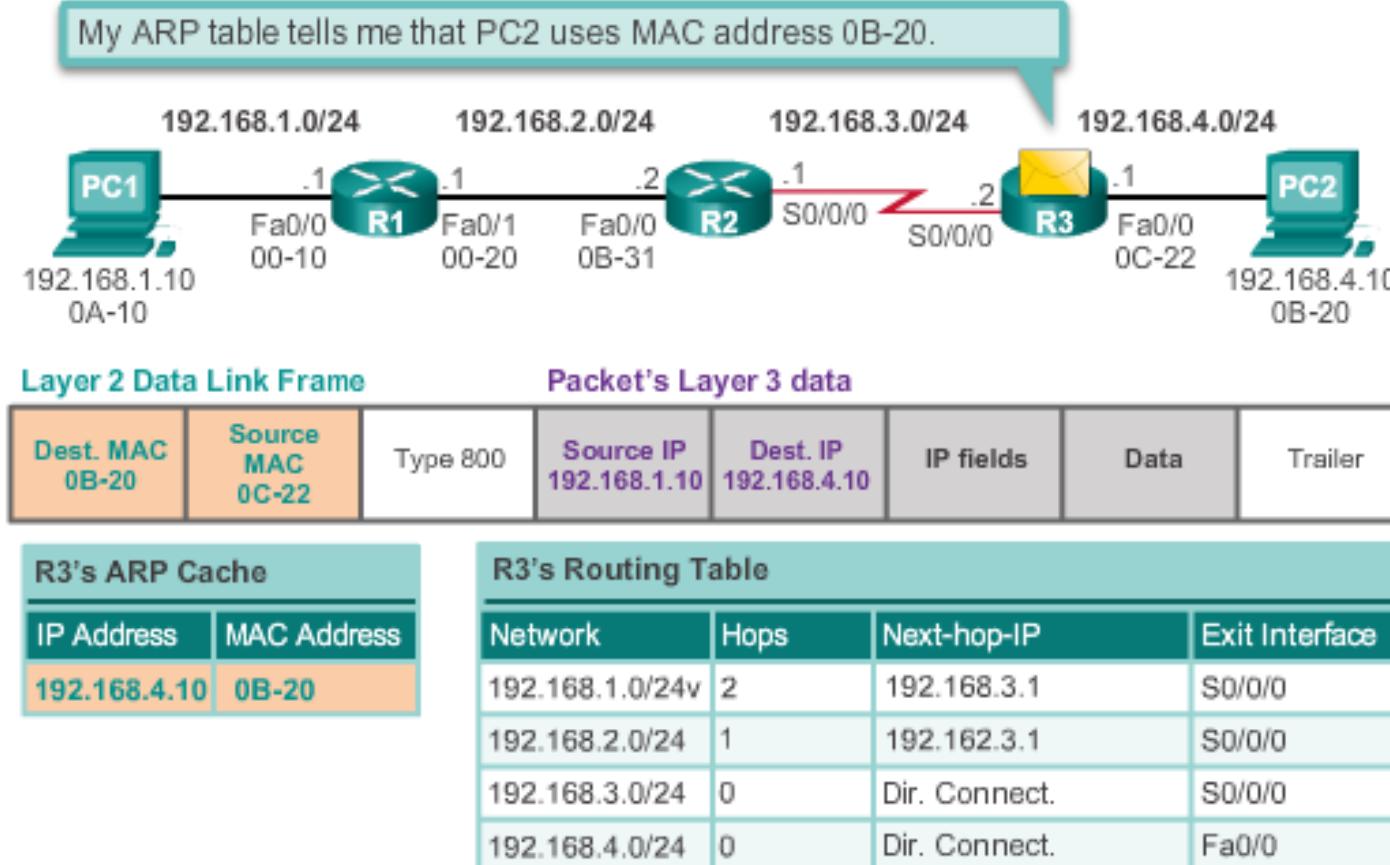
Packet's Layer 3 data

Address 0x8F	Control 0x00	Type 800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

R2's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	1	192.168.3.1	Fa/0/0
192.168.2.0/24	0	Dir. Connect.	Fa/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	1	192.168.3.2	S0/0/0

R3 Forwards the Packet to PC2

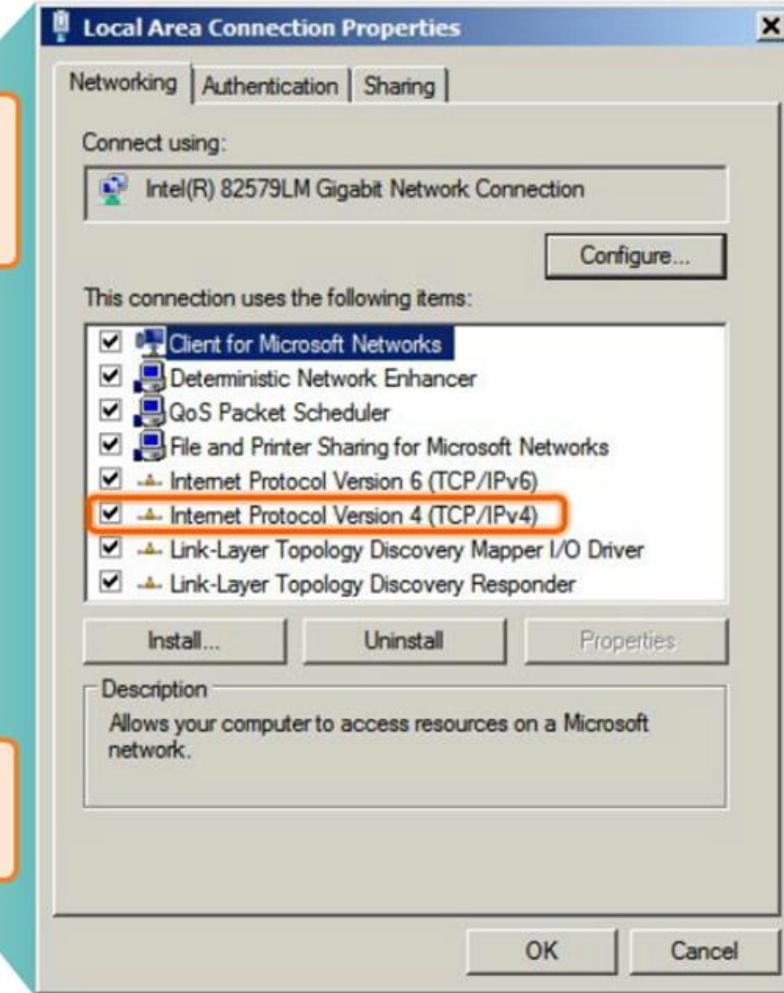


Teste da pilha TCP/IP local

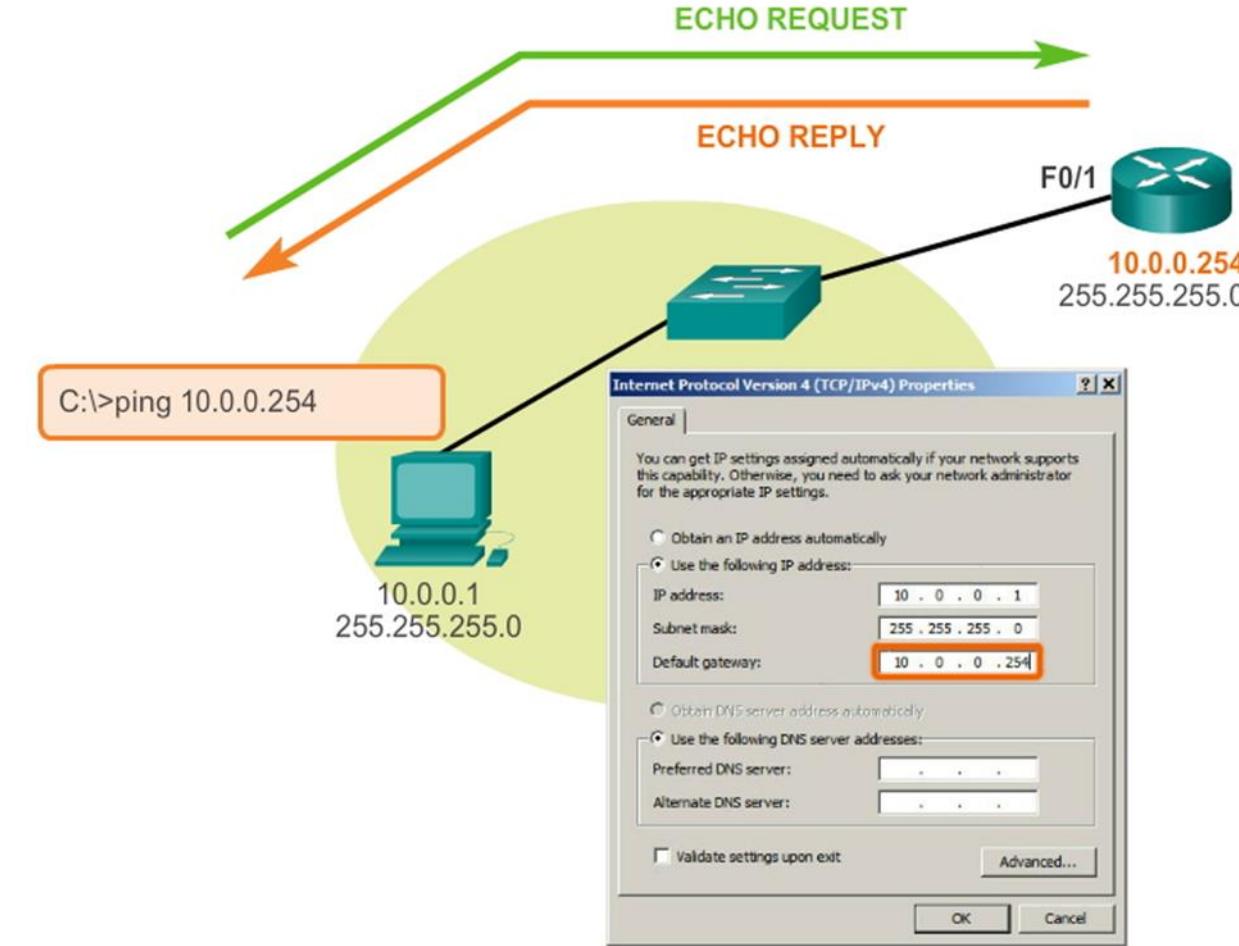
Fazer ping no host local
confirmou que o TCP/IP está
instalado e funcionando no
host local.



Fazer ping **127.0.0.1** faz com
que um dispositivo faça ping
em si mesmo.

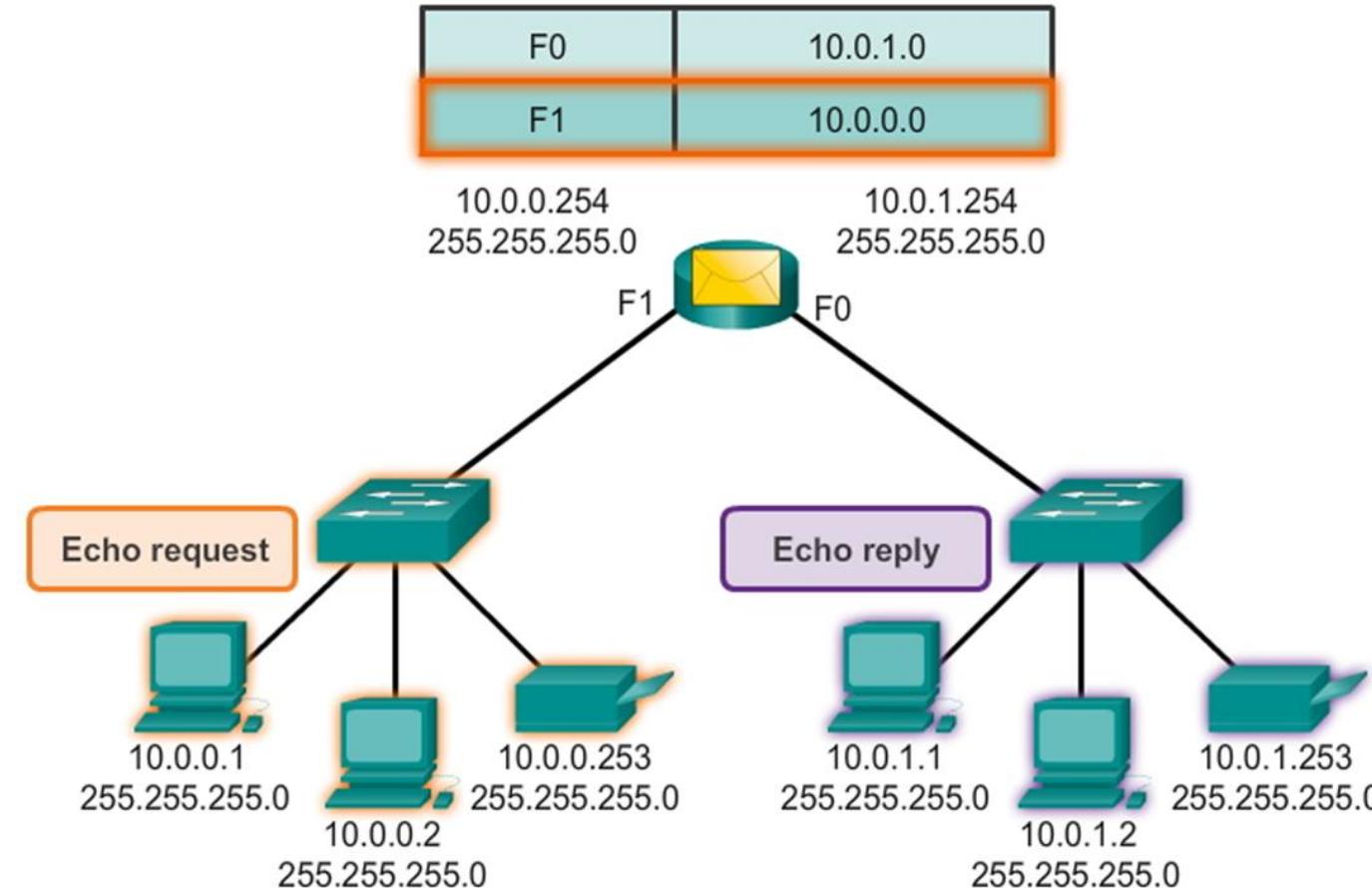


Teste da conectividade IPv4 na rede local



Ping - Teste de conectividade para uma rede remota

Teste de conectividade da LAN remota Ping de um host remoto



➤ Traceroute (tracert)

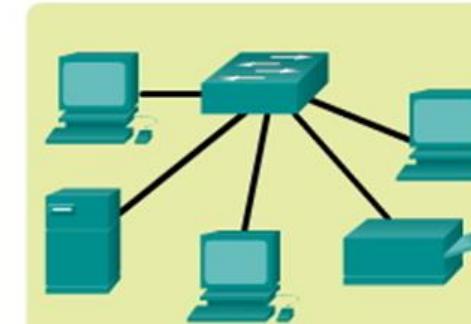
- ✓ Gera uma lista dos saltos que foram bem-sucedidos ao longo do caminho.
- ✓ Fornece informações valiosas para verificação e solução de problemas
- ✓ Se os dados atingirem o destino, listará a interface de cada router no caminho entre os hosts
- ✓ Se os dados falham em algum salto ao longo do caminho, o endereço do último router que respondeu ao trace pode fornecer uma indicação de onde o problema ou as restrições de segurança são encontradas
- ✓ Usar o traceroute fornece o tempo de ida e volta para cada salto ao longo do caminho e indica se um salto deixou de responder

- Exercício do Packet Tracer
 - 10.3.4 - Ligar um router a uma LAN
 - 10.1.4 – Configurações básicas de um router
 - 10.3.5 – Identificação e resolução de problemas no DG
 - 13.2.7 – Problemas de conetividade

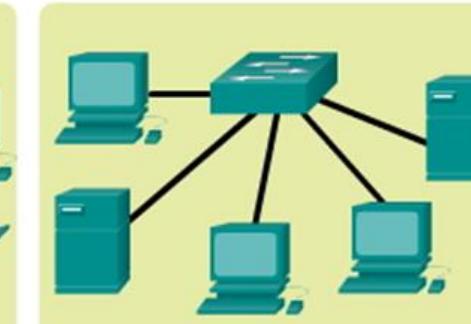
Divisão de redes IP em sub-redes

- As redes grandes precisam ser segmentadas em sub-redes menores, criando grupos menores de dispositivos e serviços para:
 - ✓ Controlar o tráfego, contendo o tráfego de broadcast dentro de uma sub-rede
 - ✓ Reduzir o tráfego total da rede e melhorar o desempenho da rede
- Divisão em sub-redes - o processo de segmentação de uma rede em várias redes menores chamadas Sub-redes.
- Comunicação entre sub-redes
 - ✓ É necessário um router para os dispositivos em diferentes redes e sub-redes poderem comunicar.
 - ✓ Cada interface do router deve ter um endereço IPv4 pertencente à rede ou à sub-rede à qual a interface está ligada.
 - ✓ Os dispositivos em uma rede e sub-rede utilizam a interface do router ligada à rede local como o gateway padrão

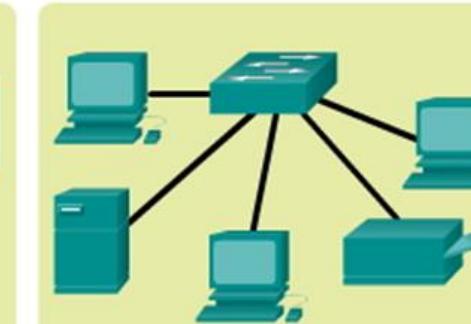
A divisão de uma rede IP em sub-redes é fundamental



LAN de Estudantes



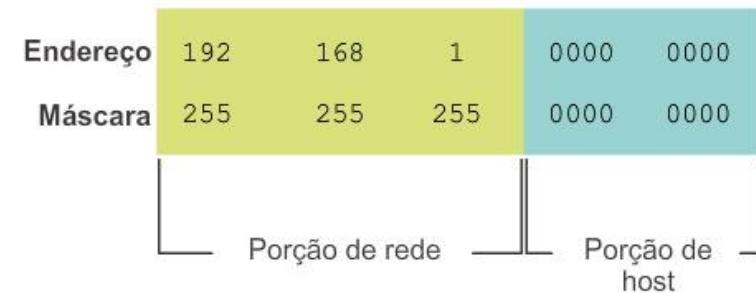
LAN do Corpo Docente



Rede Local da Admin.

O planejamento requer resoluções sobre cada sub-rede em termos de tamanho, o número de hosts por sub-rede e como os endereços de host serão atribuídos.

- Pedir bits emprestados para criar sub-redes
- Pedir 1 bit emprestado, $2^1 = 2$ sub-redes



Sinal	192.	168.	1.	0	000	0000	Rede: 192.168.1.0/24
Máscara	255.	255.	255.	0	000	0000	Máscara: 255.255.255.0

O empréstimo de 1 bits da parte do host cria 2 sub-redes com a mesma máscara de sub-rede

Sub-rede 0

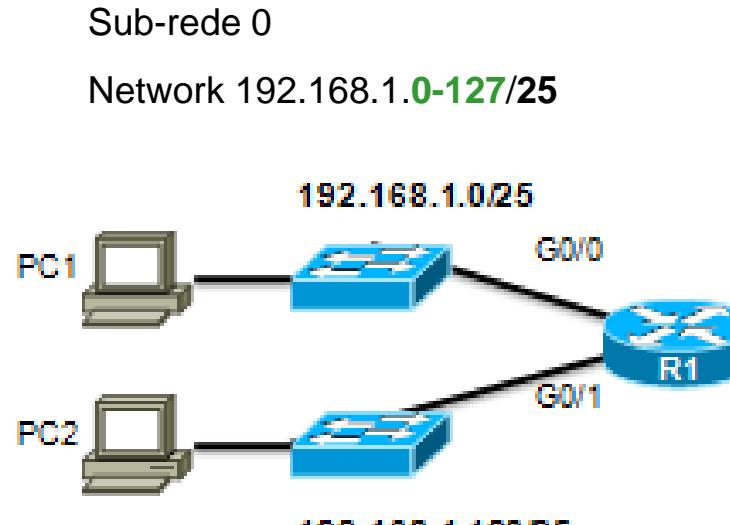
Network 192.168.1.**0-127**/25

Máscara: 255.255.255.**128**

Sub-rede 1

Rede 192.168.1.**128-255**/25

Máscara: 255.255.255.**128**



Sub-rede 1

Rede 192.168.1.128-255/25

Intervalo de Endereços da Sub-rede 192.168.1.0/25			
Endereço de rede			= 192.168.1.0
192.	168.	1.	0 000 0000
Primeiro endereço de host			= 192.168.1.1
192.	168.	1.	0 000 0001
Último endereço de host			= 192.168.1.126
192.	168.	1.	0 111 1110
Endereço de broadcast			= 192.168.1.127
192.	168.	1.	0 111 1111
Intervalo de Endereços da Sub-rede 192.168.1.128/25			
Endereço de rede			= 192.168.1.128
192.	168.	1.	1 000 0000
Primeiro endereço de host			= 192.168.1.129
192.	168.	1.	1 000 0001
Último endereço de host			= 192.168.1.254
192.	168.	1.	1 111 1110
Endereço de broadcast			= 192.168.1.255
192.	168.	1.	1 111 1111

Fórmulas da divisão de uma rede em sub-redes

- Calcule o número de sub-redes

Sub-redes = 2^n
(onde n = bits emprestados)

192. 168. 1. 0 000 0000



$$2^1 = 2 \text{ sub-redes}$$

- Calcule o número de hosts

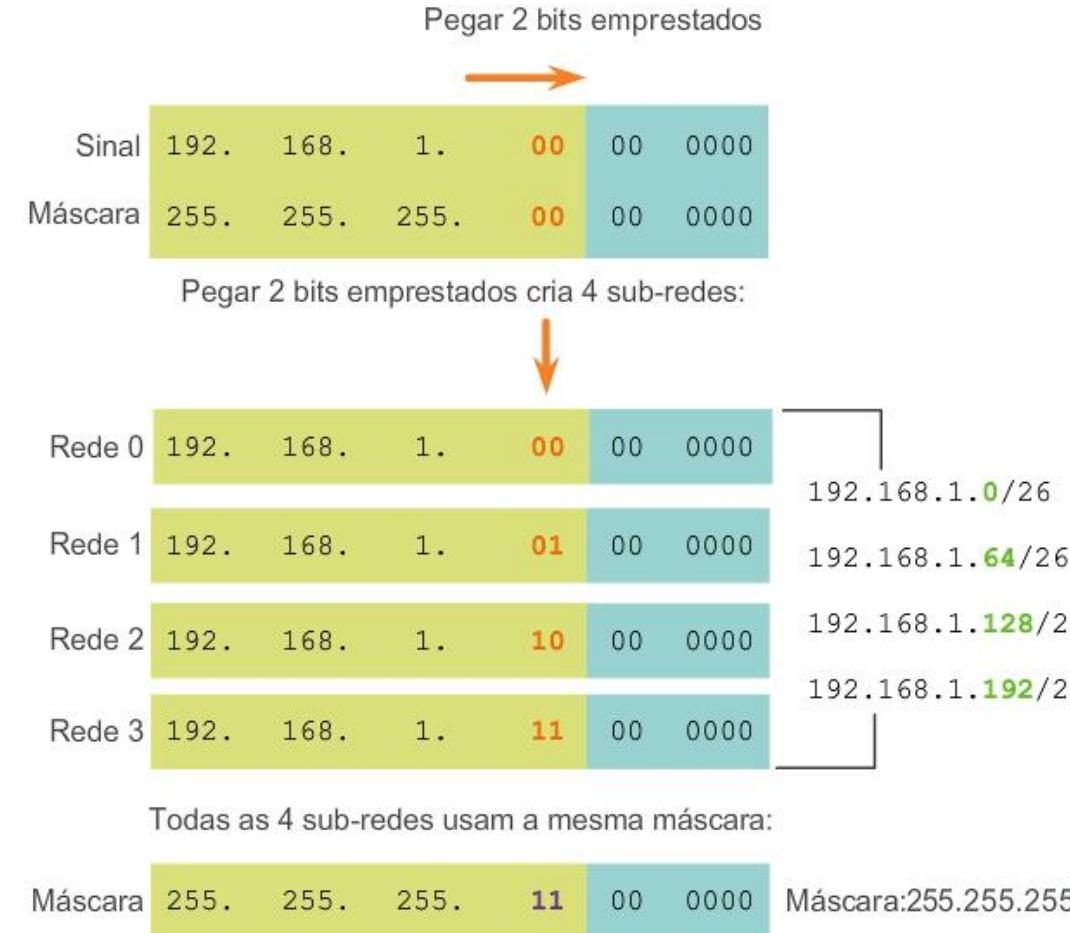
Hosts = 2^n
(onde n = bits de host restantes)

192. 168. 1. 0 000 0000



$$\begin{aligned} 2^7 &= 128 \text{ hosts por sub-rede} \\ 2^7 - 2 &= 126 \text{ hosts válidos por sub-rede} \end{aligned}$$

- Empréstimo de 2 bits para criar 4 sub-redes. $2^2 = 4$ sub-redes

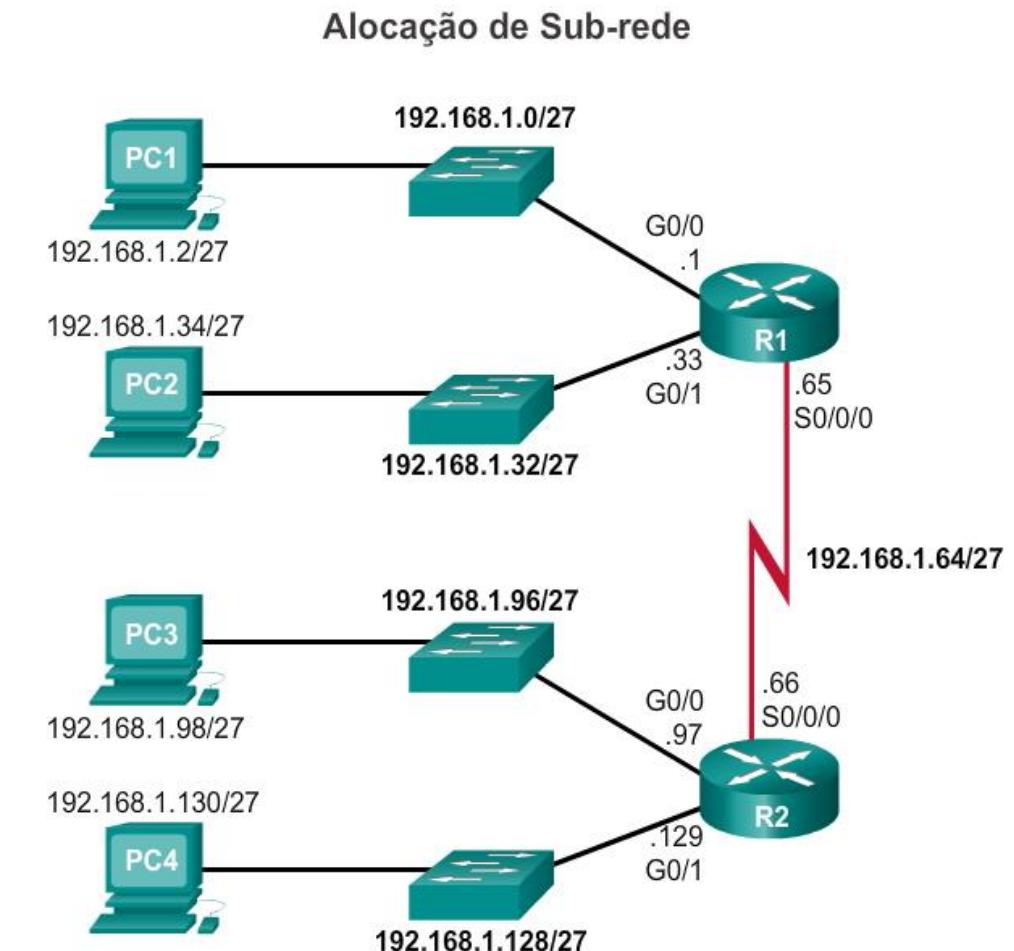


- Empréstimo de 3 bits para criar 8 sub-redes. $2^3 = 8$ sub-redes

	Rede	192.	168.	1.	000	0	0000	192.168.1.0
Rede 0	Nome	192.	168.	1.	000	0	0001	192.168.1.1
	Sobrenome	192.	168.	1.	000	1	1110	192.168.1.30
	Broadcast	192.	168.	1.	000	1	1111	192.168.1.31
<hr/>								
	Rede	192.	168.	1.	001	0	0000	192.168.1.32
Rede 1	Nome	192.	168.	1.	001	0	0001	192.168.1.33
	Sobrenome	192.	168.	1.	001	1	1110	192.168.1.62
	Broadcast	192.	168.	1.	001	1	1111	192.168.1.63
<hr/>								
	Rede	192.	168.	1.	010	0	0000	192.168.1.64
Rede 2	Nome	192.	168.	1.	010	0	0001	192.168.1.65
	Sobrenome	192.	168.	1.	010	1	1110	192.168.1.94
	Broadcast	192.	168.	1.	010	1	1111	192.168.1.95
<hr/>								
	Rede	192.	168.	1.	011	0	0000	192.168.1.96
Rede 3	Nome	192.	168.	1.	011	0	0001	192.168.1.97
	Sobrenome	192.	168.	1.	011	1	1110	192.168.1.126
	Broadcast	192.	168.	1.	011	1	1111	192.168.1.127

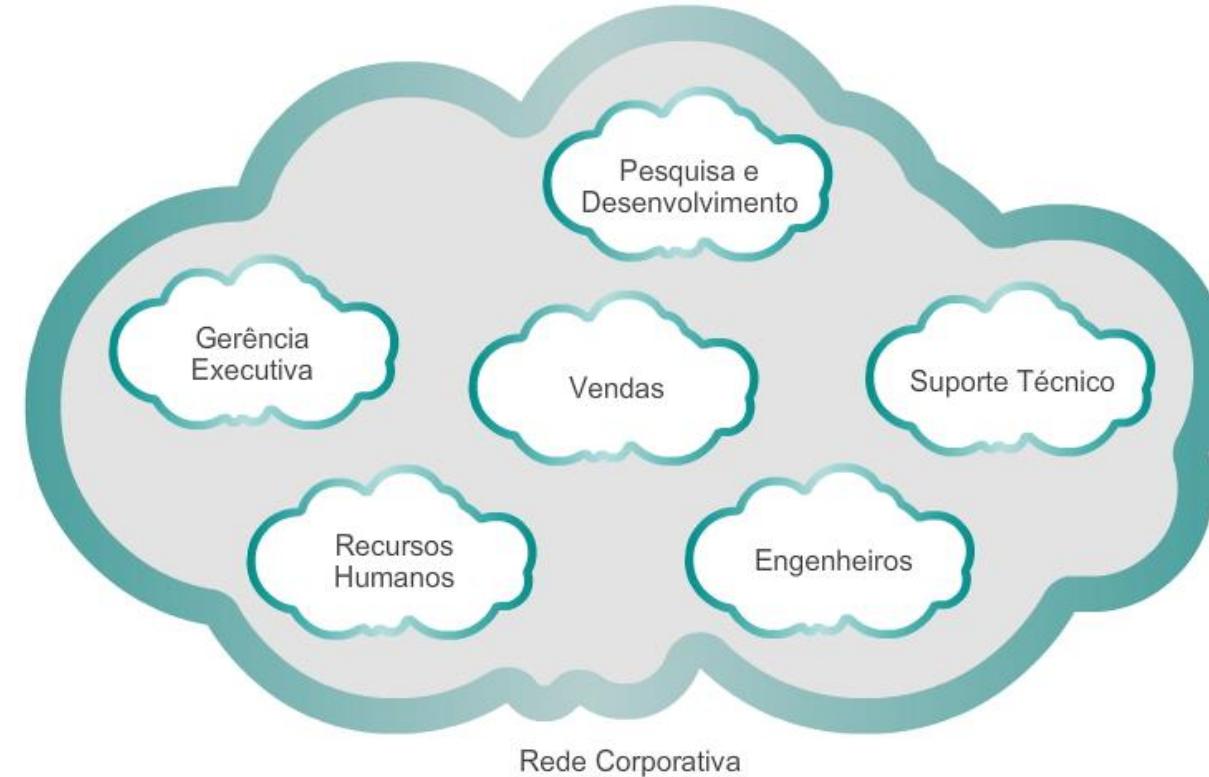
Criando 8 sub-redes (continuação)

	Rede	192.	168.	1.	000	0	0000	192.168.1.0
Rede 0	Nome	192.	168.	1.	000	0	0001	192.168.1.1
	Sobrenome	192.	168.	1.	000	1	1110	192.168.1.30
	Broadcast	192.	168.	1.	000	1	1111	192.168.1.31
Rede 1	Rede	192.	168.	1.	001	0	0000	192.168.1.32
	Nome	192.	168.	1.	001	0	0001	192.168.1.33
	Sobrenome	192.	168.	1.	001	1	1110	192.168.1.62
	Broadcast	192.	168.	1.	001	1	1111	192.168.1.63
Rede 2	Rede	192.	168.	1.	010	0	0000	192.168.1.64
	Nome	192.	168.	1.	010	0	0001	192.168.1.65
	Sobrenome	192.	168.	1.	010	1	1110	192.168.1.94
	Broadcast	192.	168.	1.	010	1	1111	192.168.1.95
Rede 3	Rede	192.	168.	1.	011	0	0000	192.168.1.96
	Nome	192.	168.	1.	011	0	0001	192.168.1.97
	Sobrenome	192.	168.	1.	011	1	1110	192.168.1.126
	Broadcast	192.	168.	1.	011	1	1111	192.168.1.127



- Há duas considerações no planeamento de sub-redes:
 - ✓ Número de sub-redes necessárias
 - ✓ Número exigido de endereços de host em cada sub-rede
 - ✓ Fórmula para determinar o número de hosts que podem ser usados
$$2^n -$$
$$2^n \text{ (onde } n \text{ é o número de bits de host restantes)} \text{ é usado para calcular o número de hosts}$$
$$-2 \text{ a ID da sub-rede e o endereço de broadcast não podem ser usados em cada sub-rede}$$

- Calcule o número de sub-redes
- Fórmula 2^n (onde n é o número de bits emprestados)
- Sub-rede necessária para cada departamento no gráfico



- Exercício do Packet Tracer
 - 11.5.5 e 11.7.5 – Sub-redes da mesma dimensão

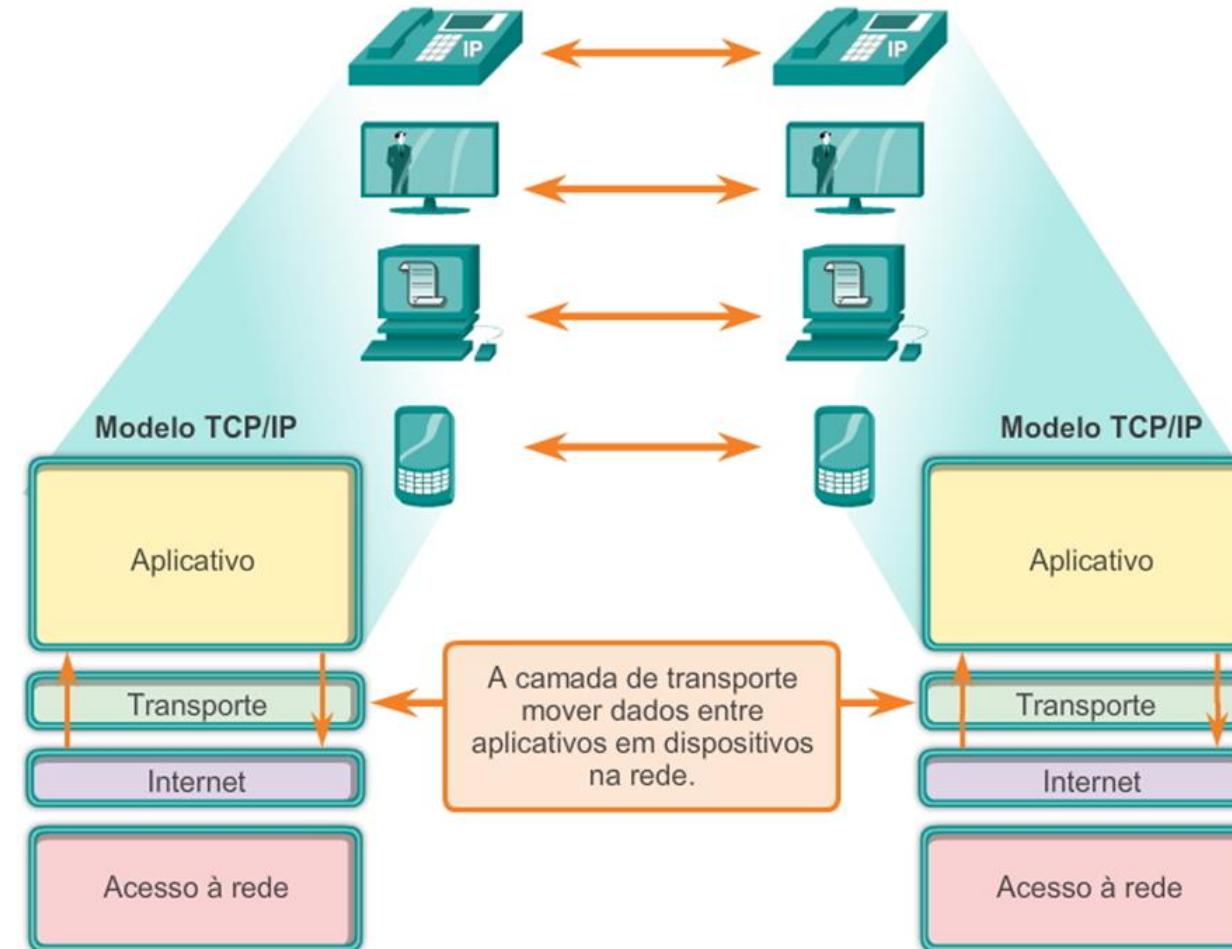
Camada de transporte

Objetivos da Camada de Transporte

Protocolos TCP e UDP

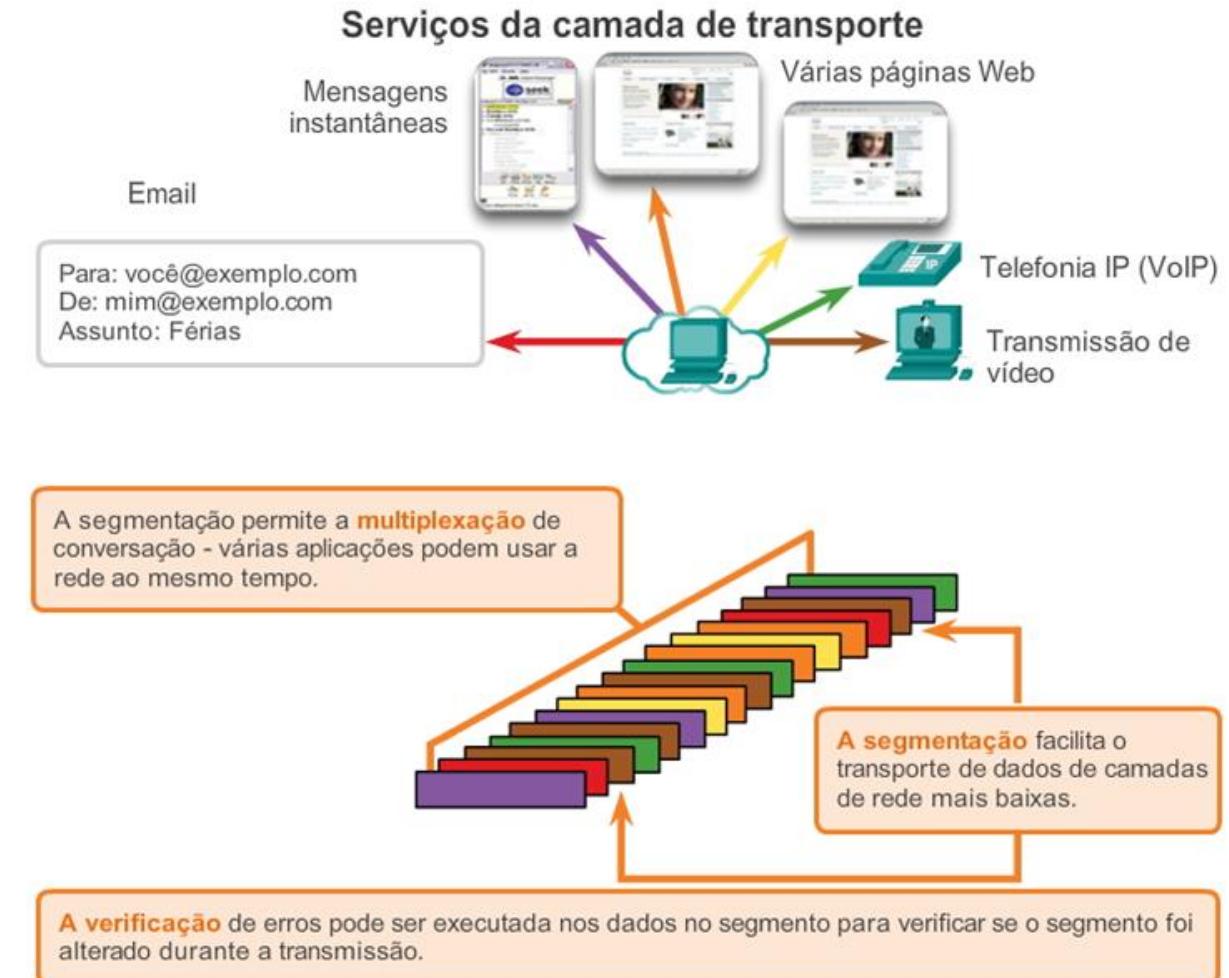
- A camada de transporte é responsável para estabelecer de comunicação temporária entre duas aplicações e entregar dados entre elas. O TCP/IP usa dois protocolos para fazer isso:
 - ✓ Protocolo TCP (Transmission Control Protocol)
 - ✓ Protocolo UDP (User Datagram Protocol)
- Responsabilidades principais dos protocolos de camada de transporte
 - ✓ Rastrear uma comunicação individual entre as aplicações nos hosts de origem e destino.
 - ✓ Segmentar dados para tratamento adequado e reassemblegem dos dados segmentados em fluxos de dados para a aplicação no destino
 - ✓ Identificando a aplicação apropriada para cada comunicação

Permitir que aplicativos em dispositivos se comuniquem



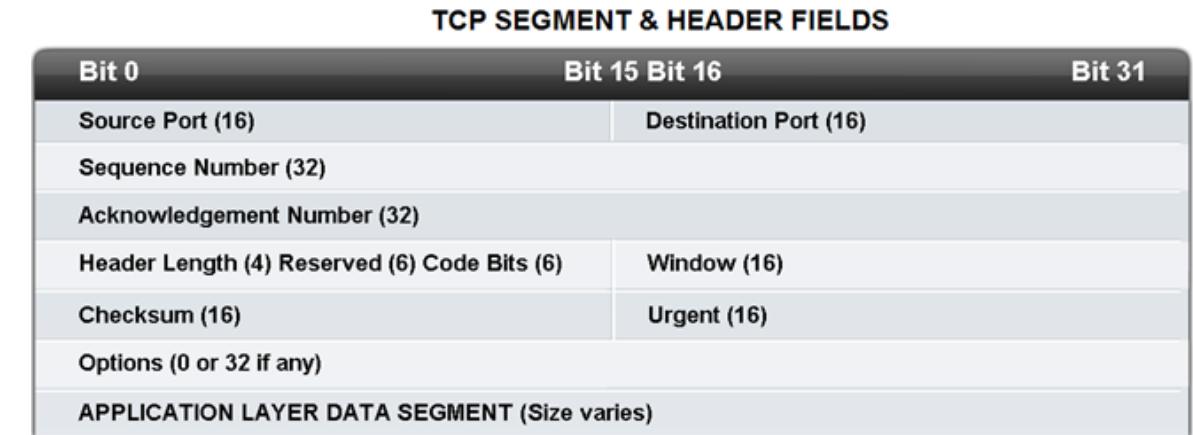
➤ Segmentar os dados

- ✓ Permitir muitas comunicações diferentes, de vários utilizadores diferentes, que podem ser intercaladas (multiplexadas) na mesma rede, ao mesmo tempo.
- ✓ Fornece os meios para enviar e receber dados quando várias aplicações estão a ser executar.
- ✓ O cabeçalho adicionado a cada segmento permite identificá-lo



- Diferentes aplicações têm diferentes requisitos de confiabilidade de transporte.
- Protocolos de Camada de Transporte TCP/IP, **TCP** e **UDP**
 - ✓ **TCP**
 - ❖ Fornece a **entrega confiável** para assegurar que todos os dados cheguem ao destino.
 - ❖ Usa a entrega confirmada e outros processos para garantir a entrega
 - ❖ Coloca maiores exigências sobre a rede – mais sobrecarga
 - ✓ **UDP (User Datagram Protocol)**
 - ❖ **Protocolo** Fornece apenas as **funções básicas para a entrega** – nenhuma confiabilidade
 - ❖ Menos sobrecarga
- **Usar TCP ou UDP**
 - Isso cria um dilema entre o valor de confiabilidade e a carga que ela coloca sobre a rede.
 - Os desenvolvedores das aplicações escolhem o protocolo de transporte com base nos requisitos das aplicações.

- **Protocolo TCP (Transmission Control Protocol)**
 - ✓ Orientado para conexão – criando uma sessão entre a origem e o destino
 - ✓ Entrega confiável – retransmissão de dados perdidos ou corrompidos
 - ✓ Reconstrução de dados ordenados – numeração e a sequência de segmentos
 - ✓ Controle de fluxo - regulando a quantidade de dados transmitida
 - ✓ Protocolo stateful– rastrear a sessão



➤ Protocolo UDP (User Datagram Protocol)

- ✓ O **protocolo simples** que fornece as funções de camada de transporte básica
 - ❖ Sem conexão.
 - ❖ **Entrega não confiável**.
 - ❖ Nenhuma reconstrução de dados ordenados.
 - ❖ **Sem controle de fluxo**.
 - ❖ Protocolo sem estado.
 - ❖ Baixa sobrecarga
- ✓ Usado pelas aplicações que podem tolerar uma **perda pequena de dados**
- ✓ Usado pelas aplicações que não toleram o **atraso**



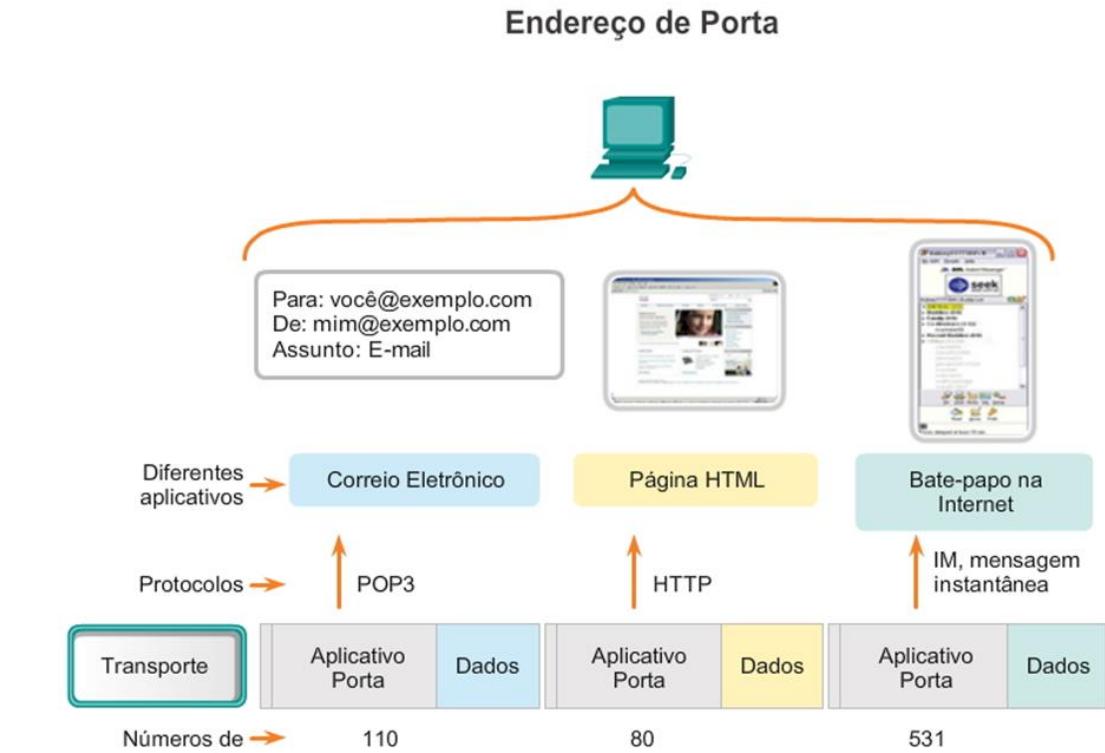
➤ **Aplicações que usam UDP:**

- ✓ Domain Name System (DNS)
- ✓ Simple Network Management Protocol (SNMP)
- ✓ Dynamic Host Configuration Protocol (DHCP)
- ✓ Trivial File Transfer Protocol (TFTP)
- ✓ Telefonia IP ou Voz sobre IP (VoIP)
- ✓ Jogos on-line
- ✓ Streaming de Vídeo

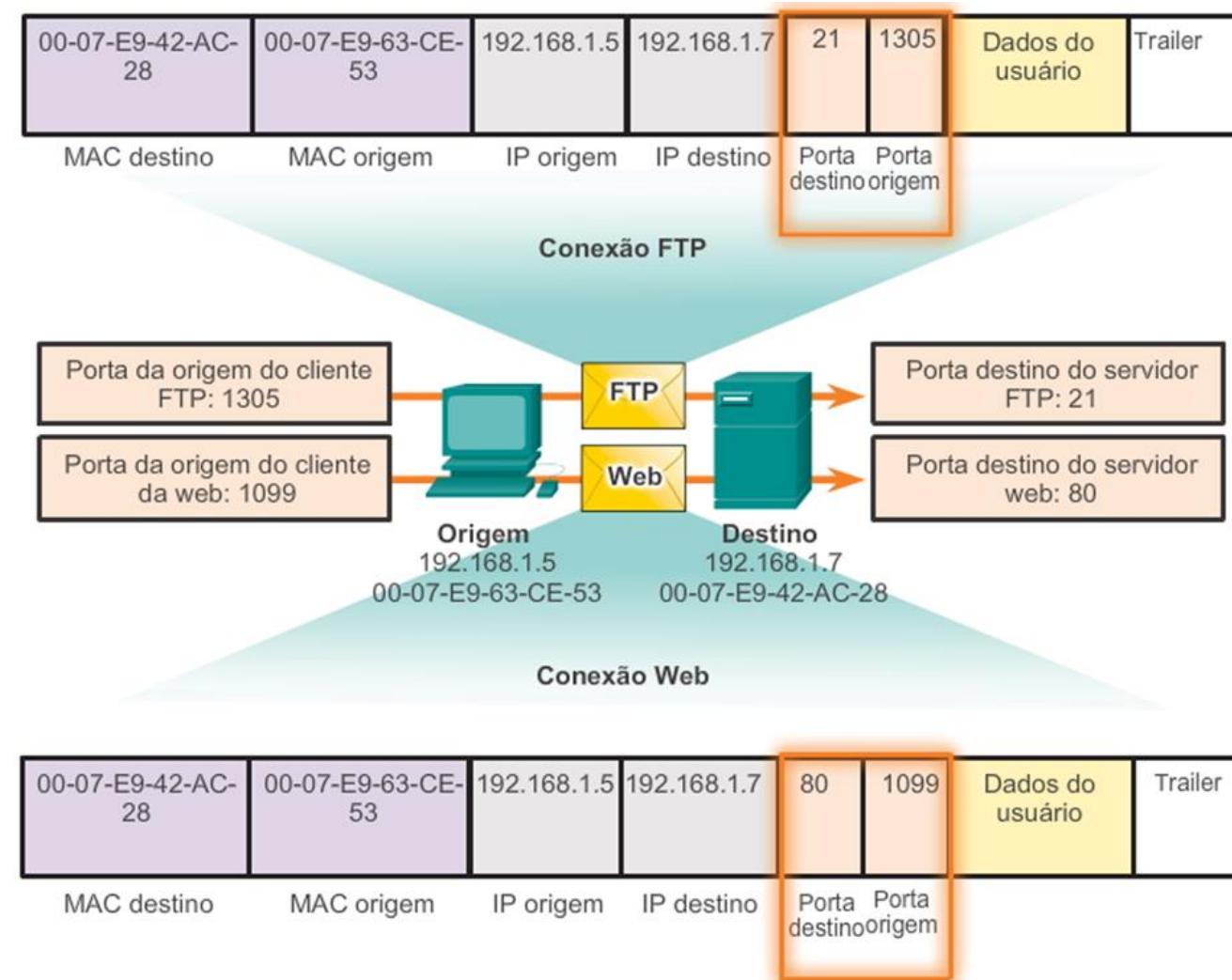


Separação das várias comunicações

- Os números de porta são usados pelo TCP e pelo UDP para distinção das várias aplicações



Os dados de diferentes aplicativos são direcionados para o aplicativo correto porque cada aplicativo tem um número de porta único.



Endereço de porta do TCP e UDP

Números de portas

Intervalo do números da porta	Grupo de portas
0 a 1023	Portas conhecidas
1024 a 49151	Portas registradas
49152 a 65535	Portas dinâmicas e/ou privadas

Legenda

Portas TCP registradas:
1863 MSN Messenger
2000 Cisco SCCP (VoIP)
8008 Alternate HTTP
8080 Alternate HTTP

Portas TCP conhecidas:
21 FTP
23 Telnet
25 SMTP
80 HTTP
143 IMAP
194 Internet Relay Chat (IRC)
443 Secure HTTP (HTTPS)

Legenda

Portas UDP registradas:
1812 RADIUS Authentication Protocol
5004 RTP (Voice and Video Transport Protocol)
5040 SIP (VoIP)

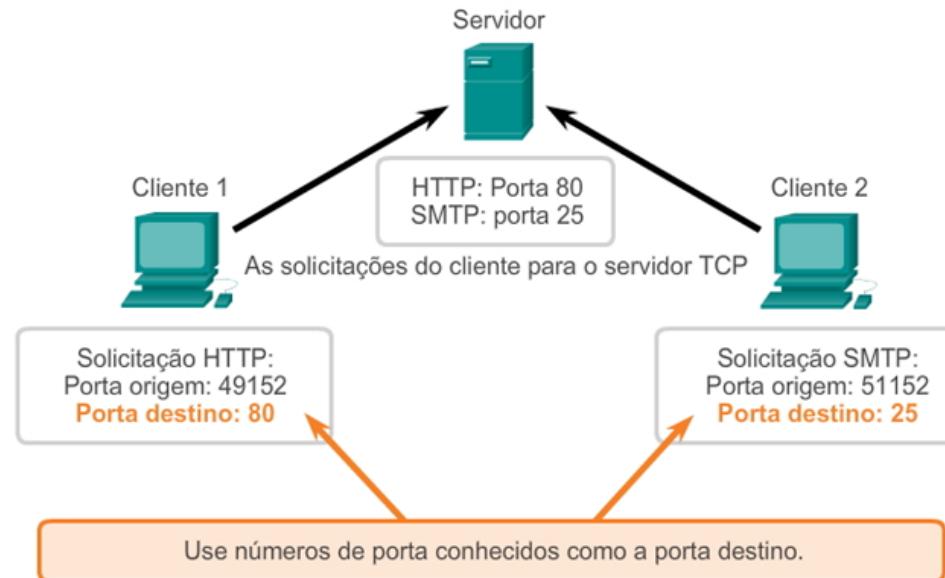
Portas UDP conhecidas:
69 TFTP
520 RIP

Legenda

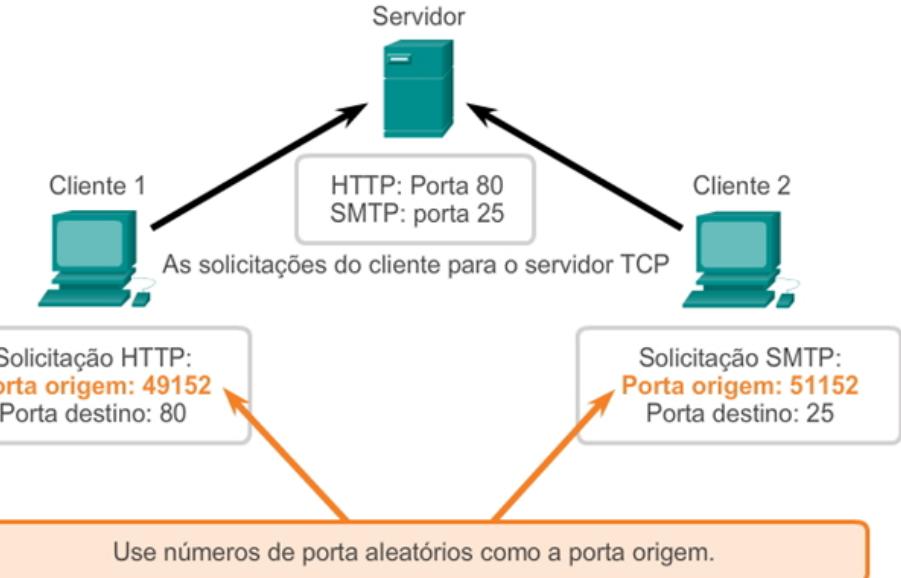
Portas TCP/UDP comuns registradas:
1433 MS SQL
2948 WAP (MMS)

Portas TCP/UDP comuns conhecidas:
53 DNS
161 SNMP
531 AOL Instant Messenger, IRC

Portas destino de solicitação

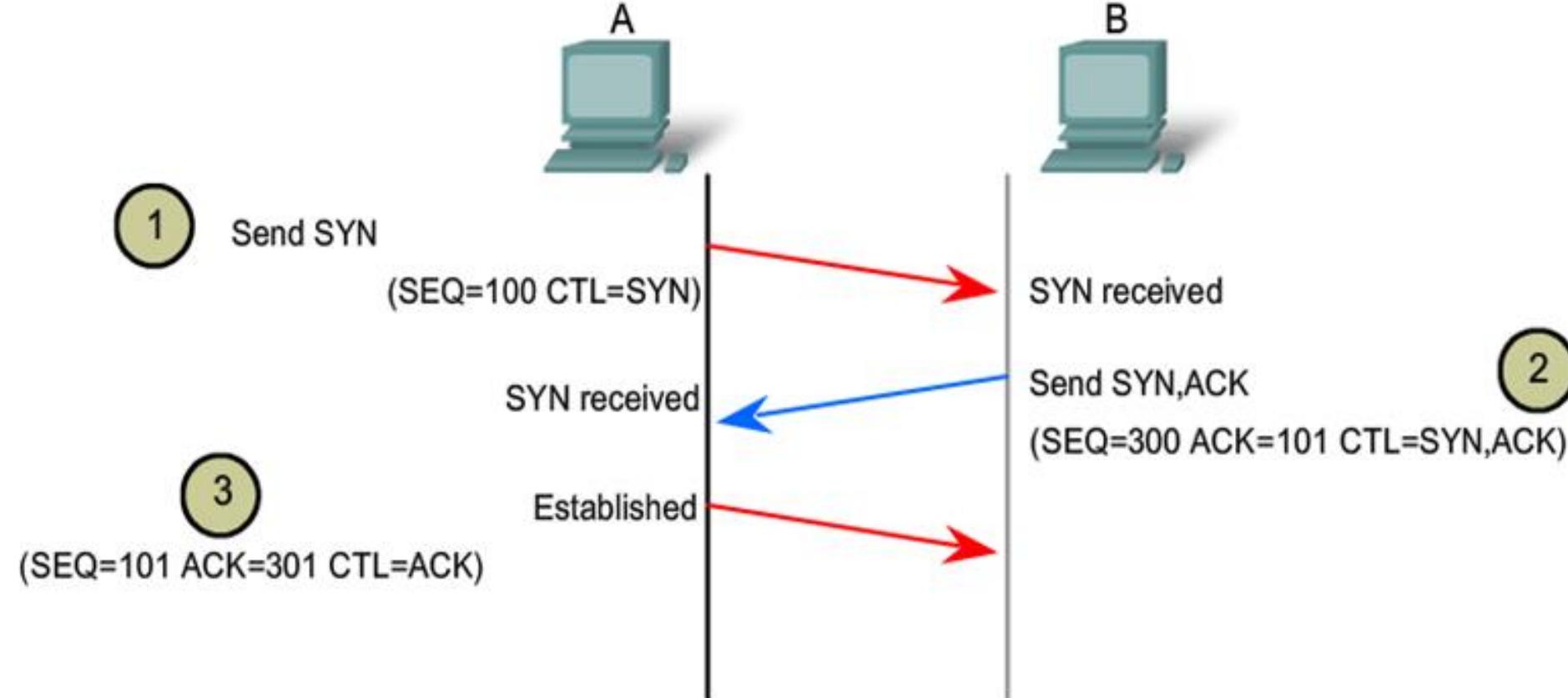


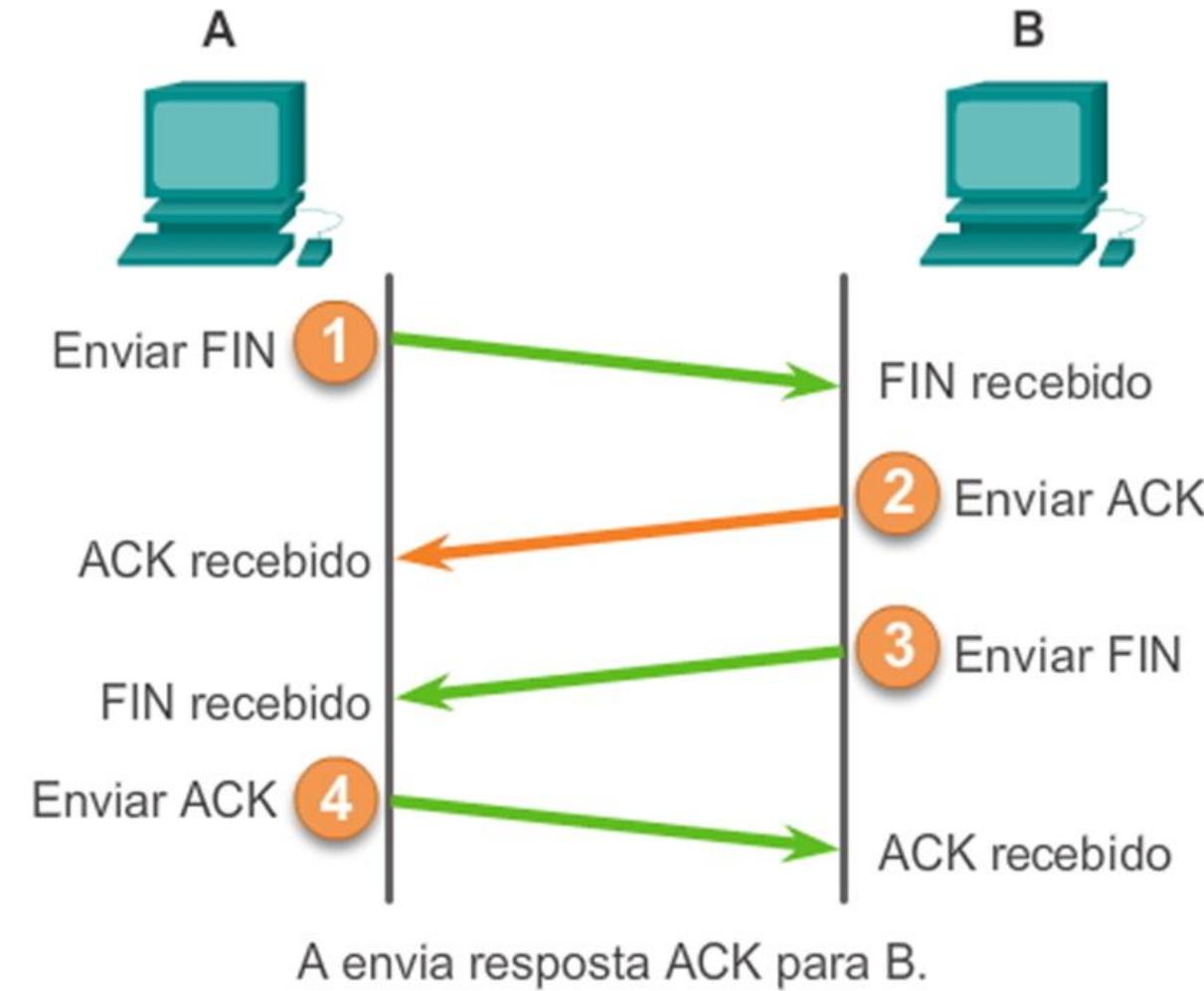
Portas origem de solicitação



► Handshake Triplo

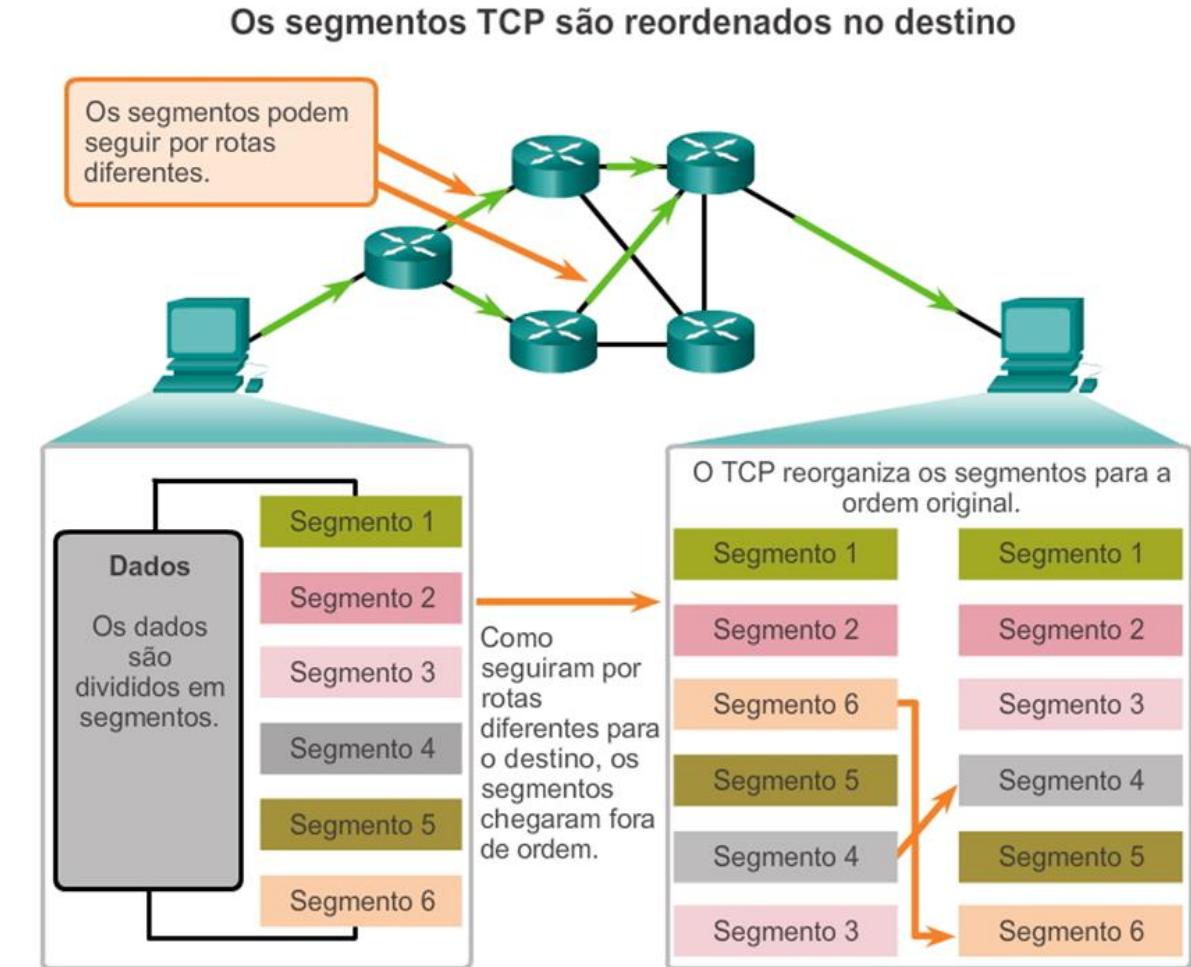
- ▶ Estabelece que o **dispositivo destino** está presente na rede.
- ▶ Verifica se o **dispositivo destino** tem um **serviço ativo** e está a aceitar solicitações no número de porta destino que o cliente pretende usar para a sessão.
- ▶ Informa o dispositivo destino que o **cliente** pretende estabelecer uma sessão de comunicação nesse número de porta





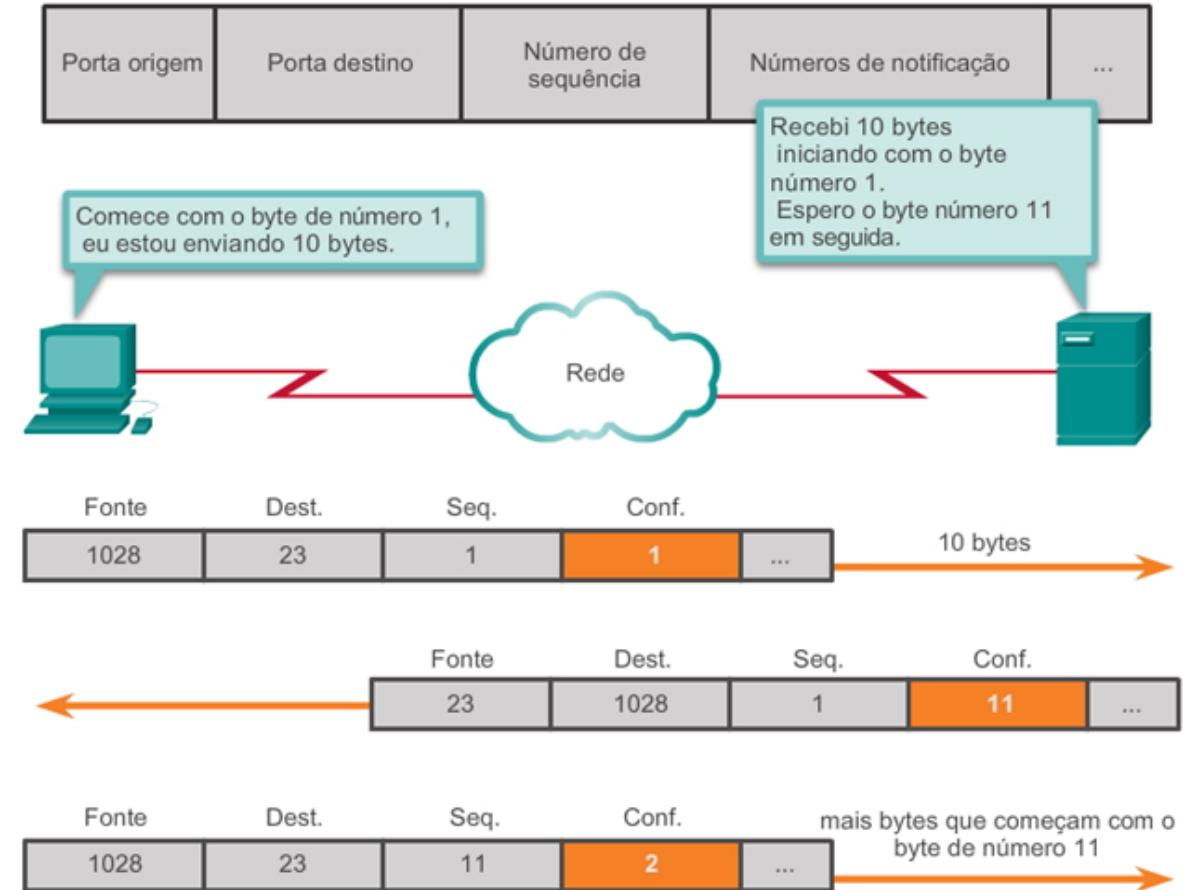
Confiabilidade de TCP - entrega ordenada

- Números de sequência usados para reagrupar segmentos na ordem original

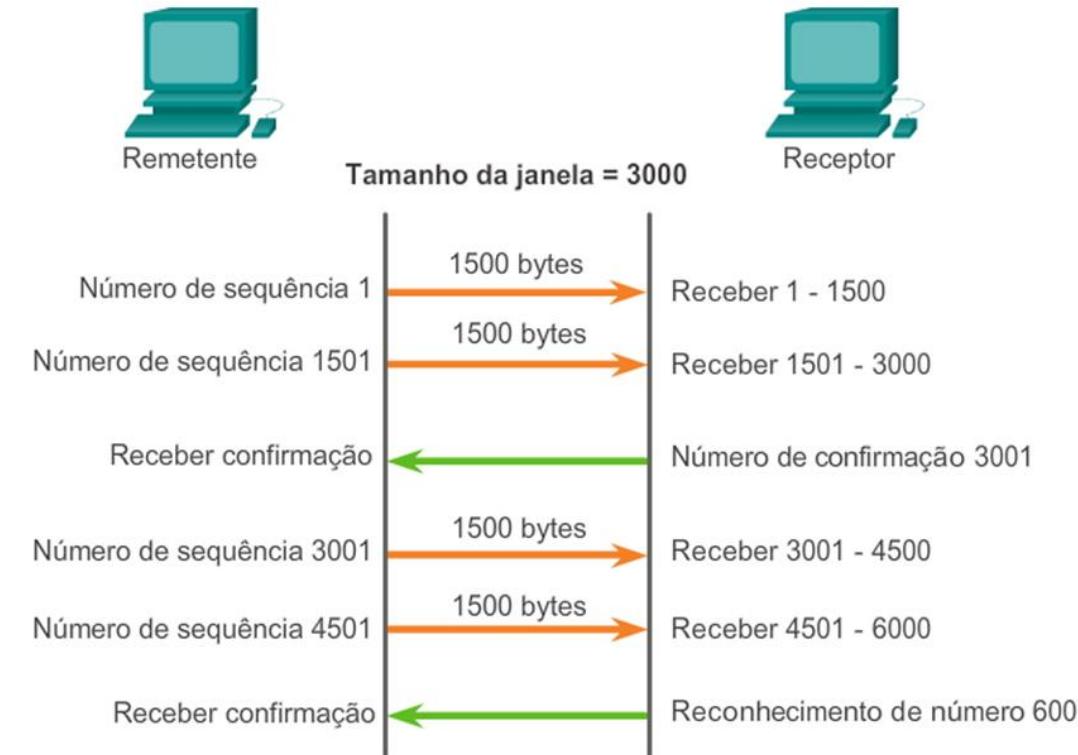


- O número de sequência e o número de confirmação são usados em conjunto para confirmar a receção.
- Tamanho da janela - A quantidade de dados que a fonte pode transmitir sem a confirmação ser recebida

Reconhecimento de segmentos TCP



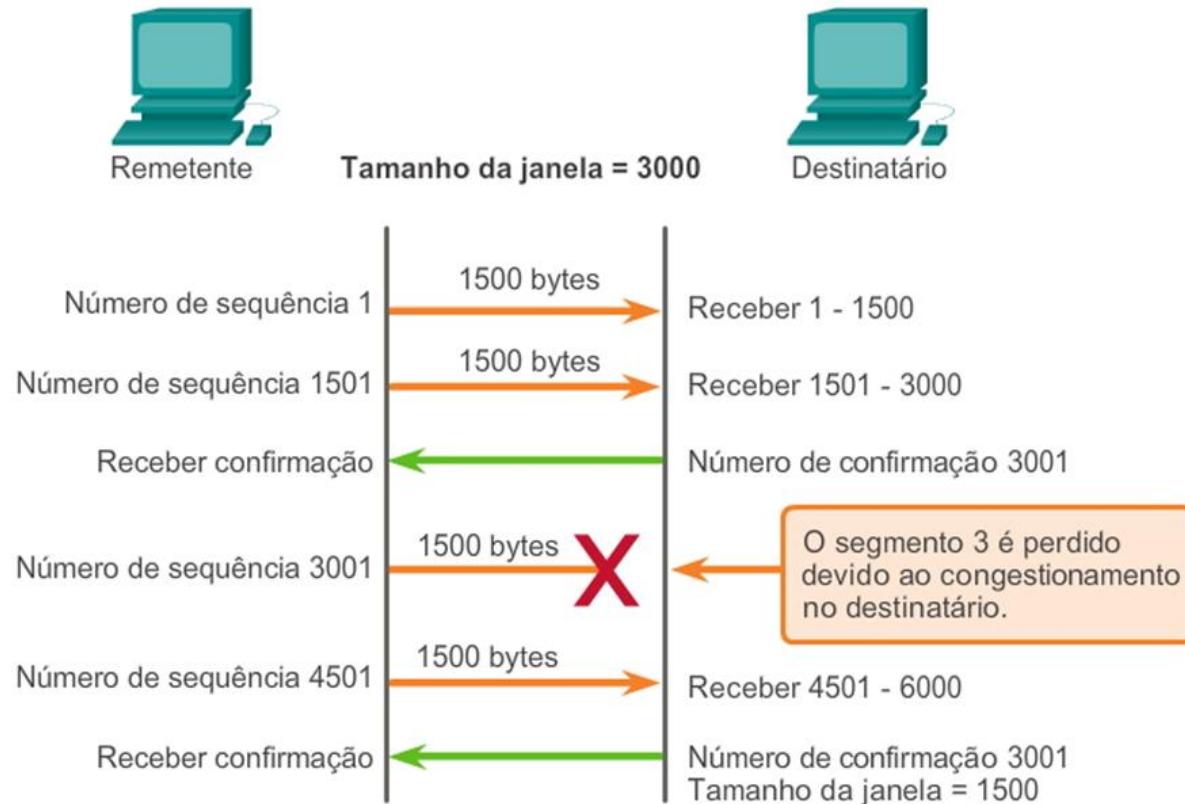
Confirmação do segmento TCP e tamanho da janela



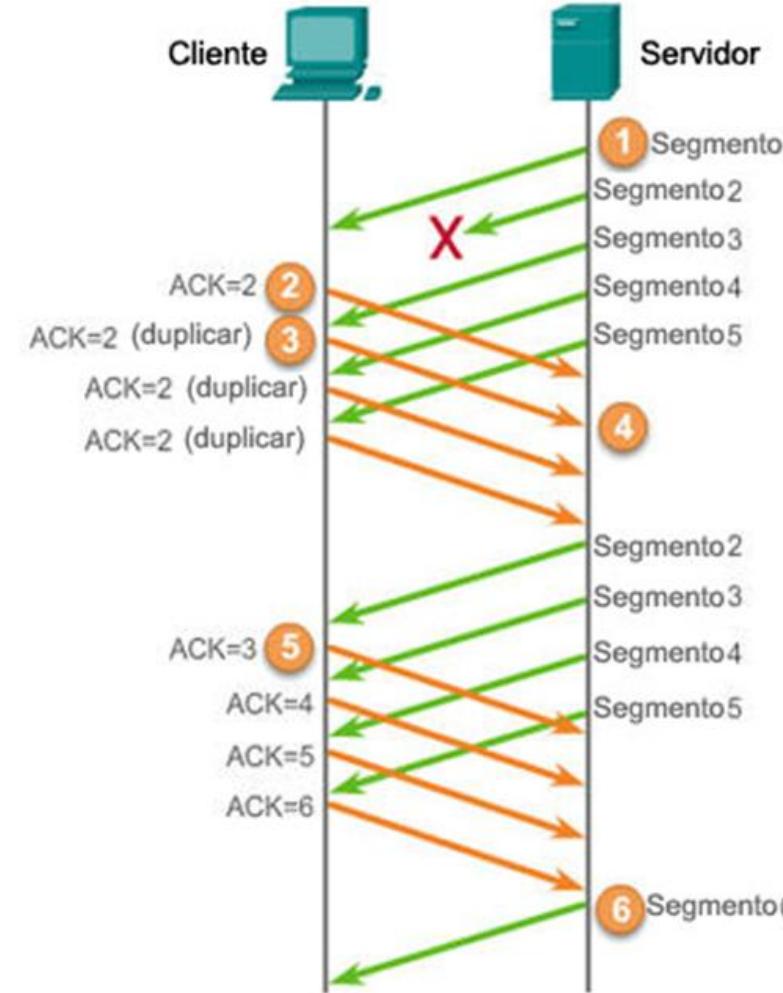
O **tamanho da janela** determina o número de bytes enviados antes que uma confirmação seja esperada.

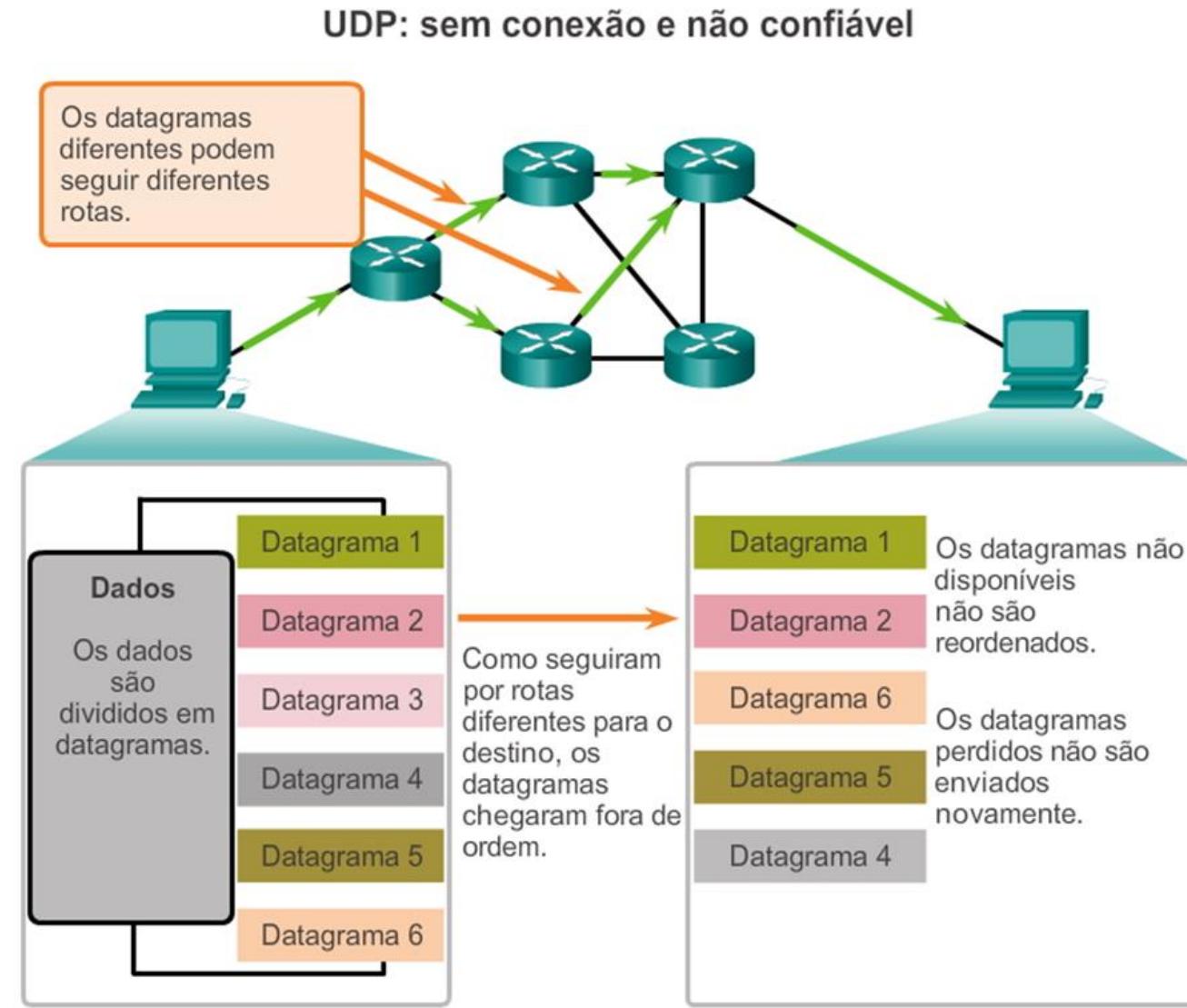
O **número de confirmação** é o número de bytes esperados.

Congestionamento e controle de fluxo TCP



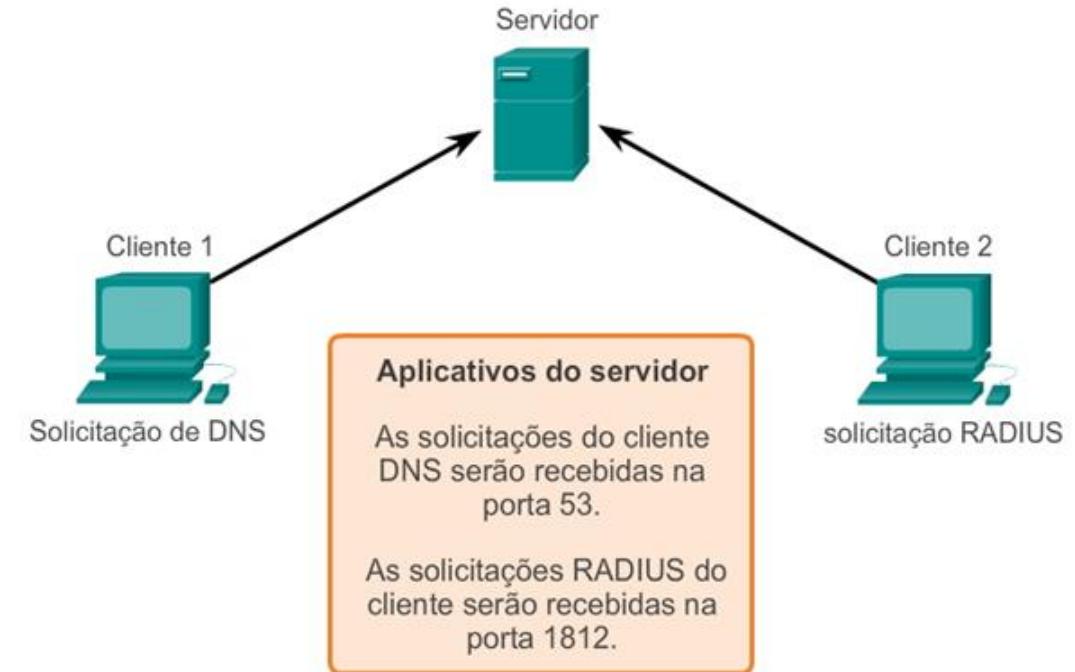
Se os segmentos são perdidos devido ao congestionamento, o recipiente reconhece o último segmento sequencial recebido e responde com um tamanho de janela reduzido.



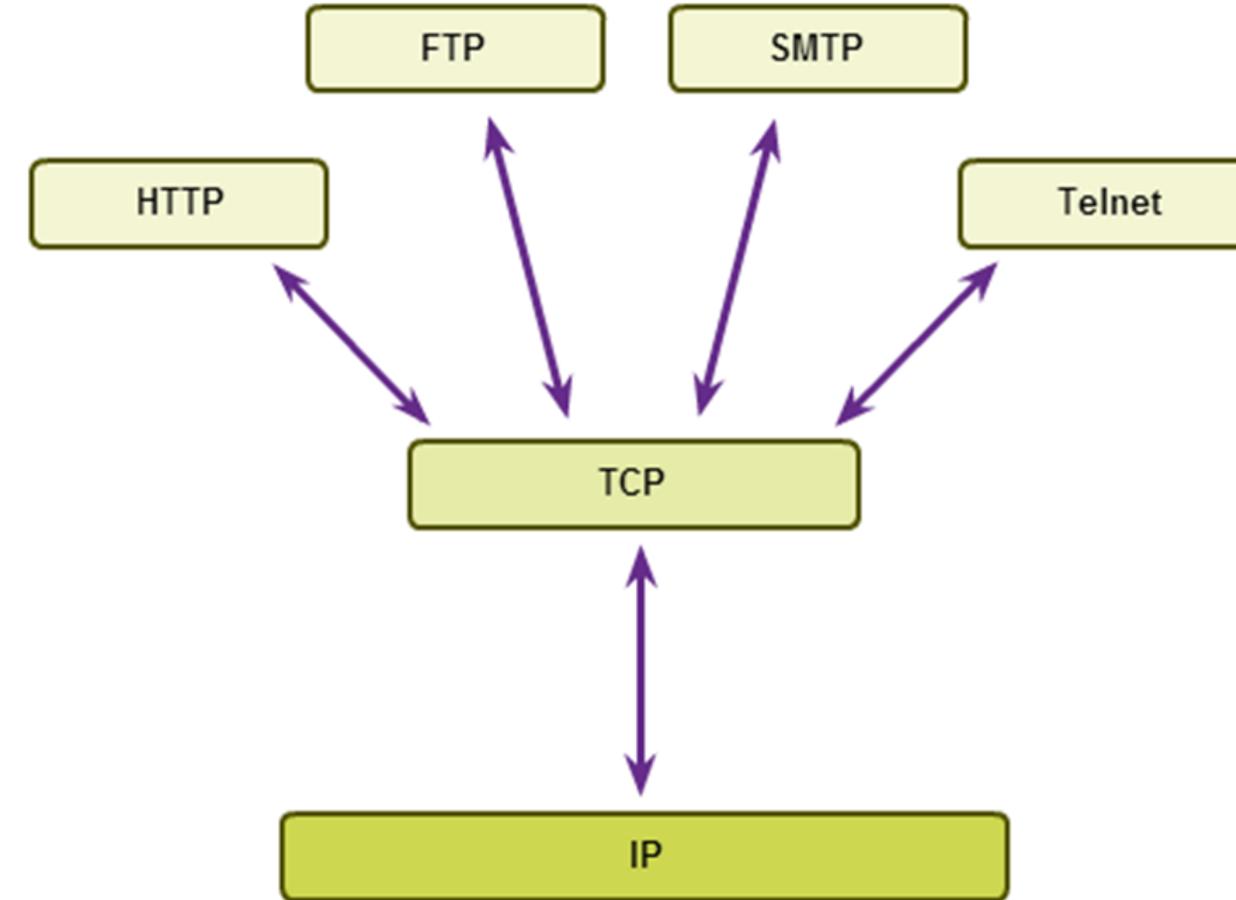


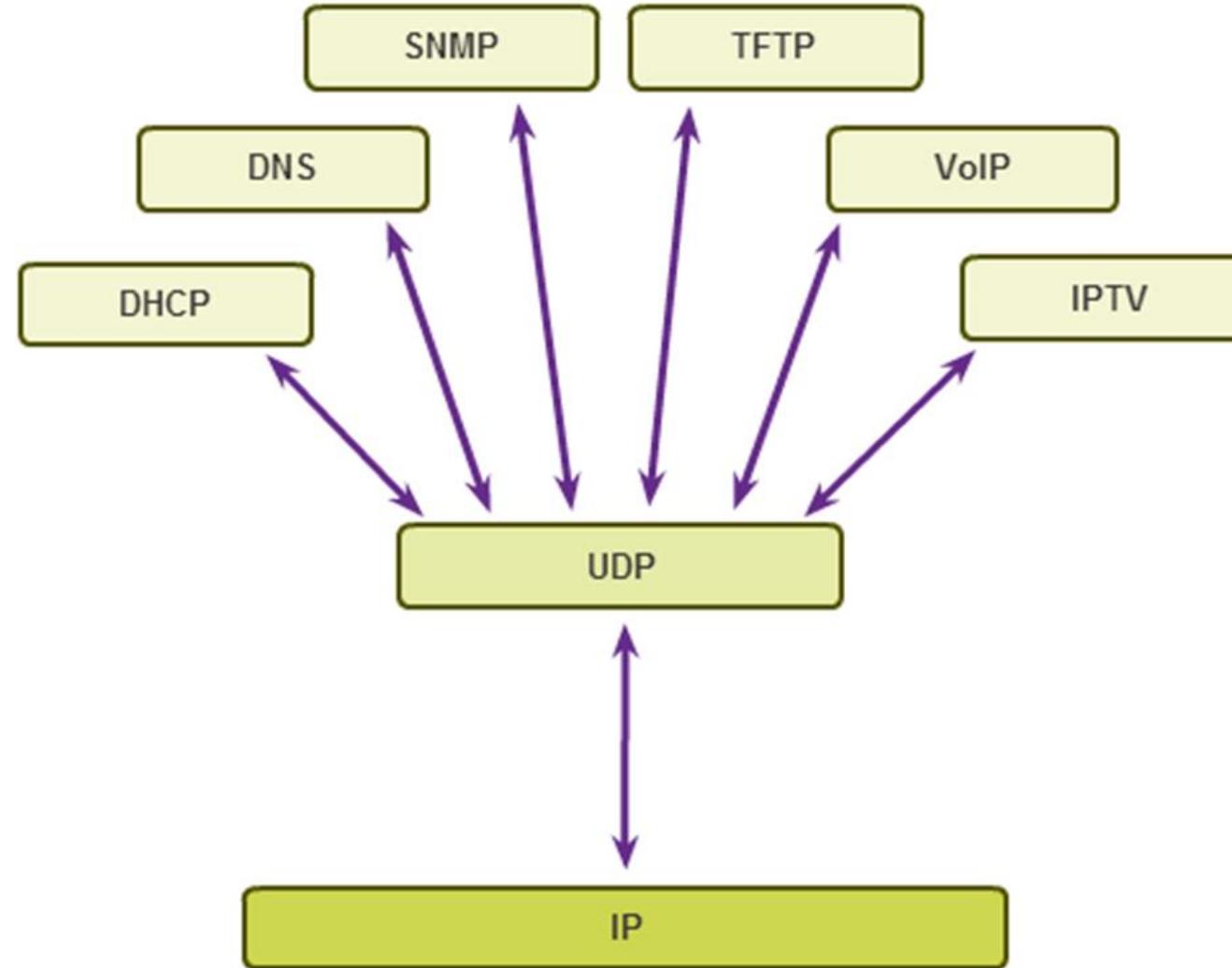
- Aplicações de servidor baseados em UDP são atribuídos a números de portas conhecidos ou registrados.
- O processo do cliente UDP seleciona aleatoriamente o número da porta do intervalo de números de porta dinâmico como a porta origem

Servidor UDP ouve solicitações



As solicitações do cliente para servidores possuem números de porta conhecidos como a porta destino.

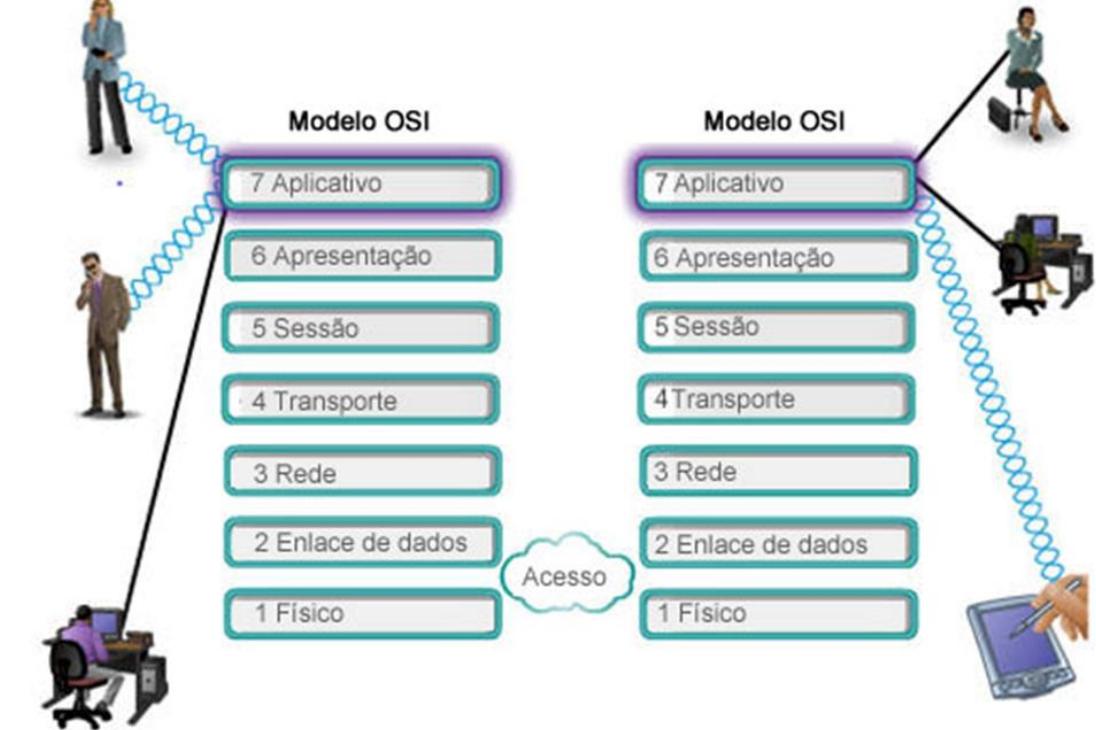


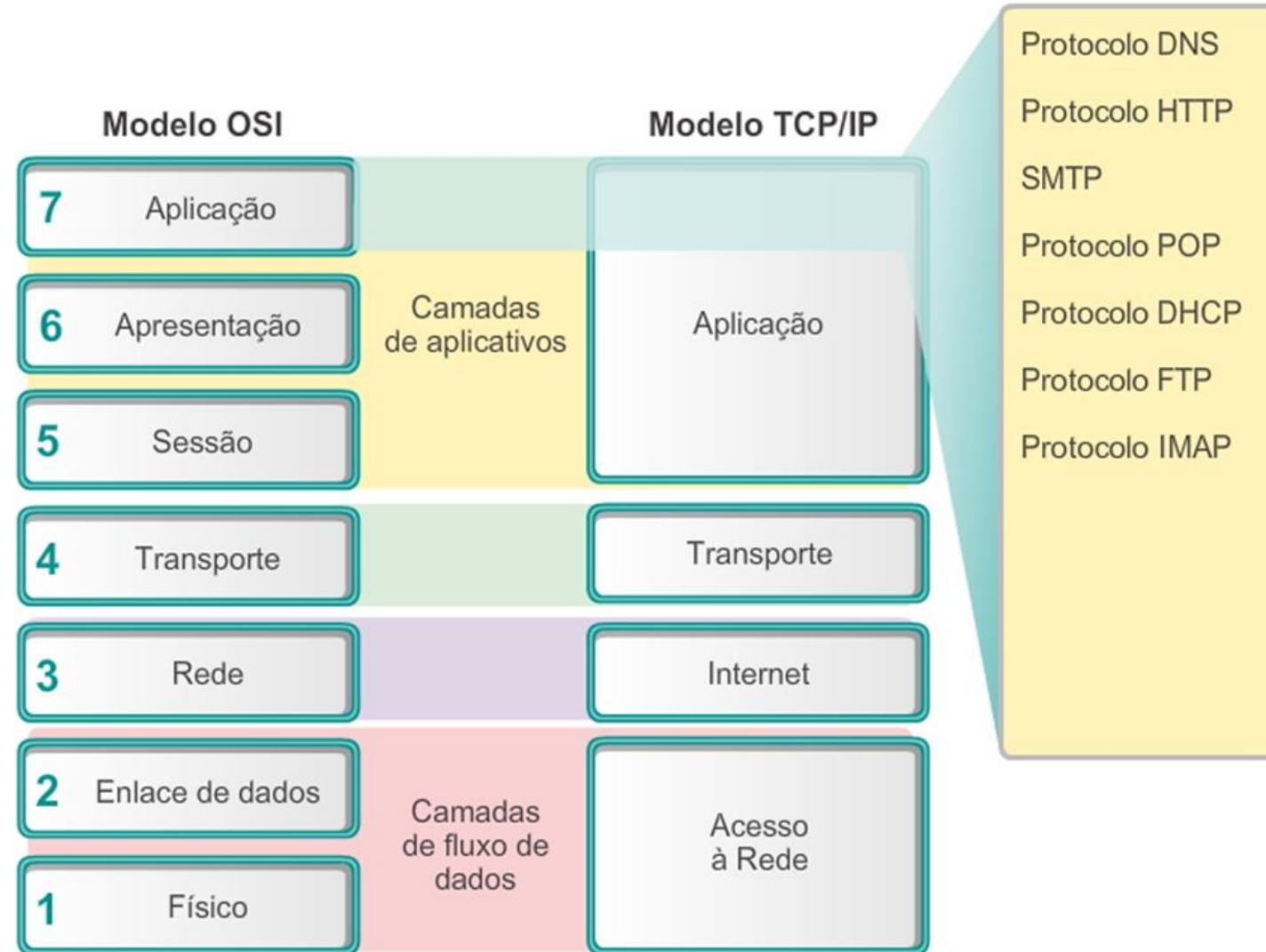


- Exercício do Packet Tracer
 - 14.8.1 - Análise de tráfego para identificação e análise dos campos do cabeçalho TCP e do cabeçalho UDP

Serviços e protocolos da camada de aplicação

- A camada de aplicação fornece o interface entre as aplicações usadas para comunicar e a rede subjacente na qual as mensagens são transmitidas

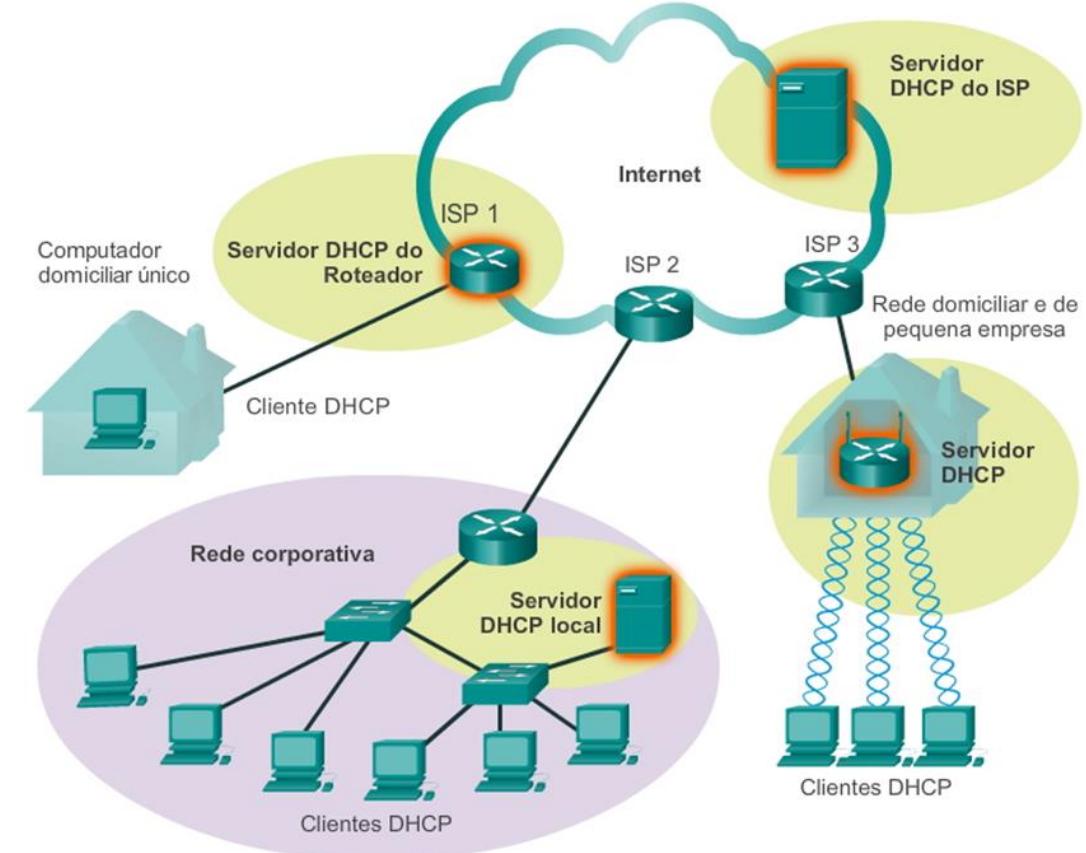




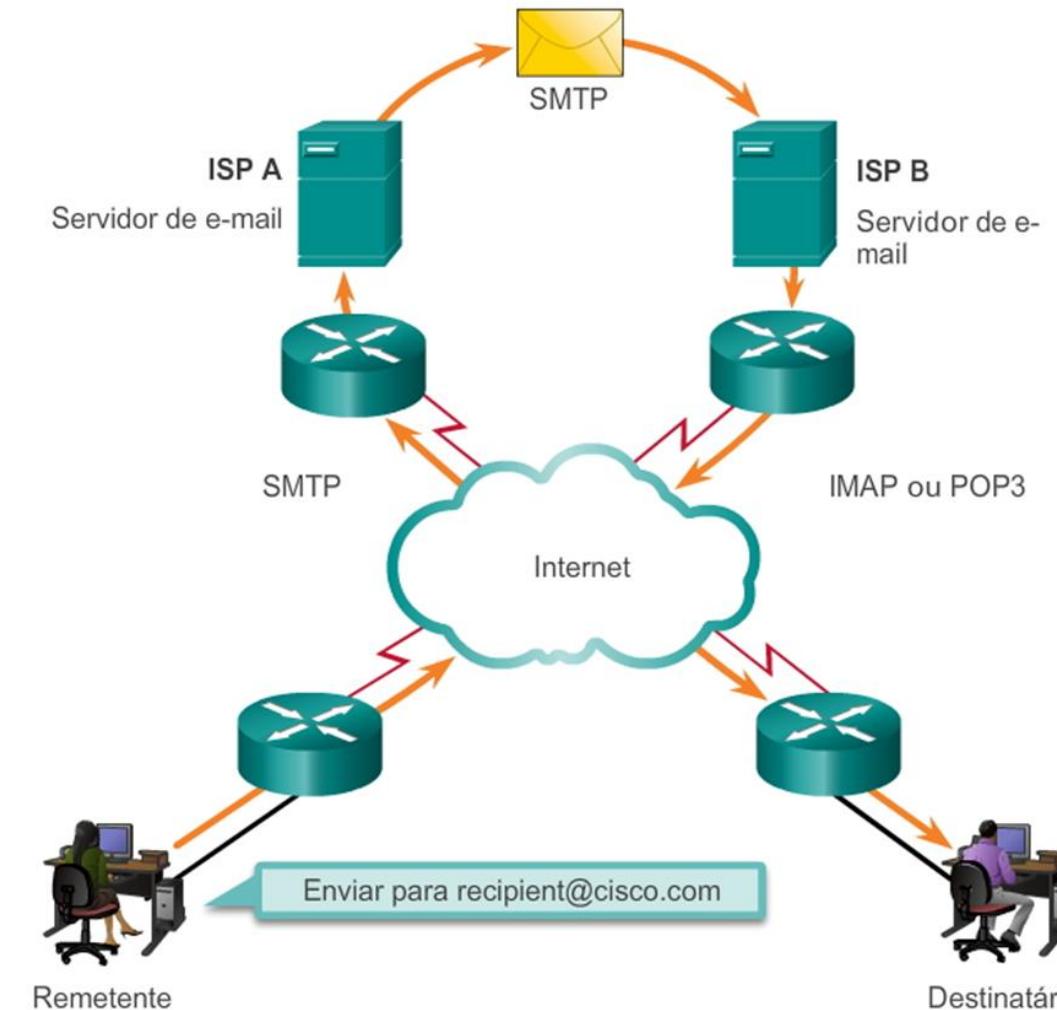
- **Protocolo de serviço de nome de domínio (Domain Name Service Protocol - DNS)** - utilizado para resolver nomes de Internet em endereços IP.
- **Telnet** - um protocolo de simulação de terminal que é utilizado para fornecer acesso remoto a servidores e dispositivos de rede.
- **Protocolo de Controle Dinâmico de Host (Dynamic Host Control Protocol - DHCP)** - usado para atribuir um endereço IP, a máscara de sub-rede, o gateway padrão e o servidor DNS a um host
- **Protocolo de transferência de hipertexto (Hypertext Transfer Protocol – HTTP)** - usado para transferir ficheiros que compõem as páginas Web da World Wide Web.

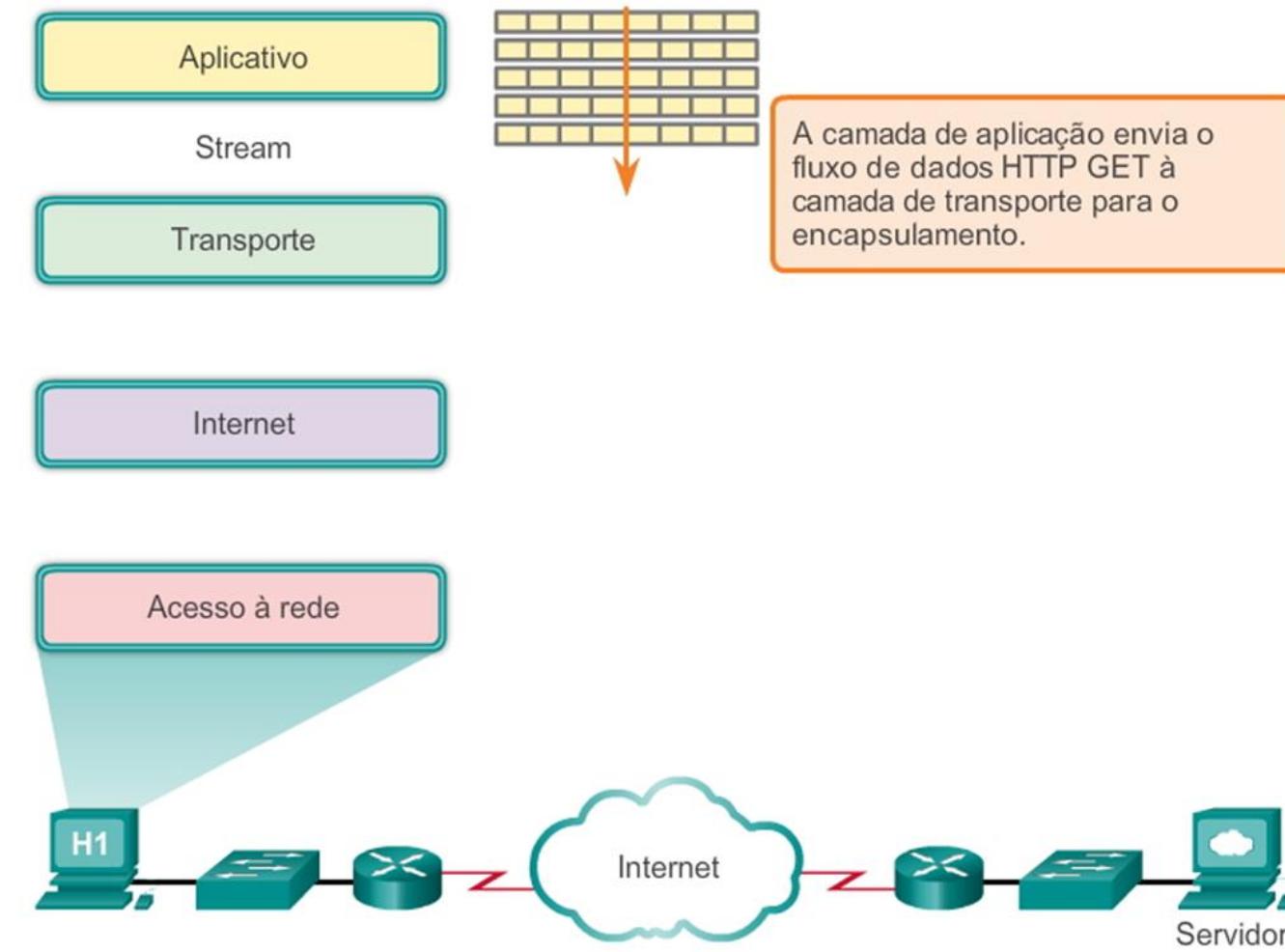
- **Protocolo de transferência de ficheiros (File Transfer Protocol - FTP)** - usado para transferência interativa de ficheiros entre sistemas
- **Protocolo de transferência de correio (Simple Mail Transfer Protocol – SMTP)** - usado para transferência de mensagens e anexos de e-mail.
- **Protocolo POP (Post Office Protocol)** - usado por clientes de e-mail para recuperar e-mail de um servidor remoto, o e-mail é transferido do servidor ao cliente e excluído do servidor
- **Protocolo de acesso a mensagens de Internet (Internet Message Access Protocol - IMAP)** - outro protocolo para a recuperação do e-mail de um servidor remoto, ao contrário do POP as mensagens originais são mantidas no servidor até que sejam excluídas manualmente

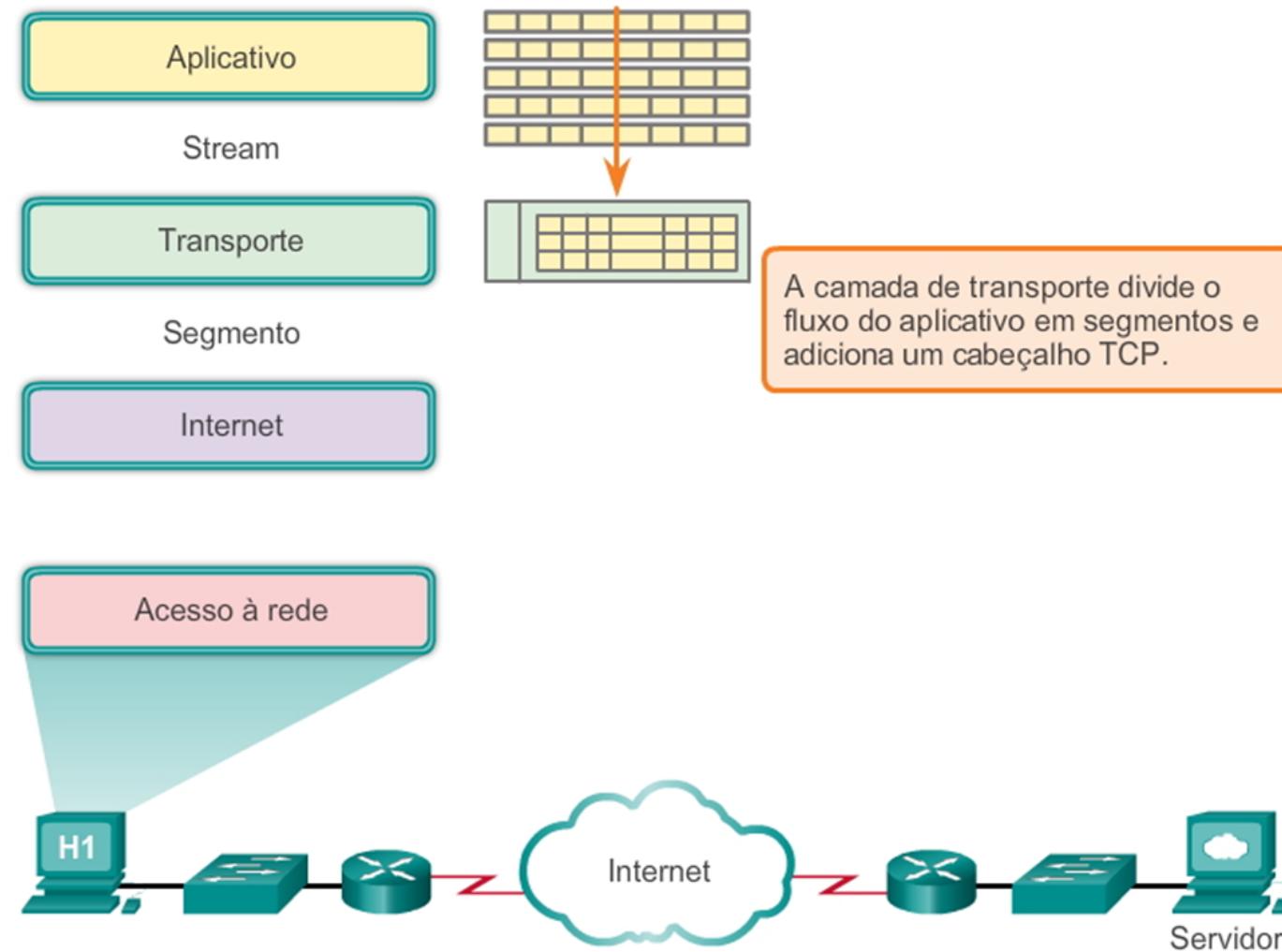
- O DHCP permite que um host obtenha um endereço IP de forma dinâmica
- O servidor DHCP é contatado e o endereço é solicitado - escolhe o endereço de uma lista configurada de endereços chamada pool e "arrenda-o" ao host por um período definido
- O DHCP é utilizado por hosts de uso geral, como dispositivos de utilizador final e o endereçamento estático, é usado em dispositivos de rede, como gateways, switches, servidores e impressoras.

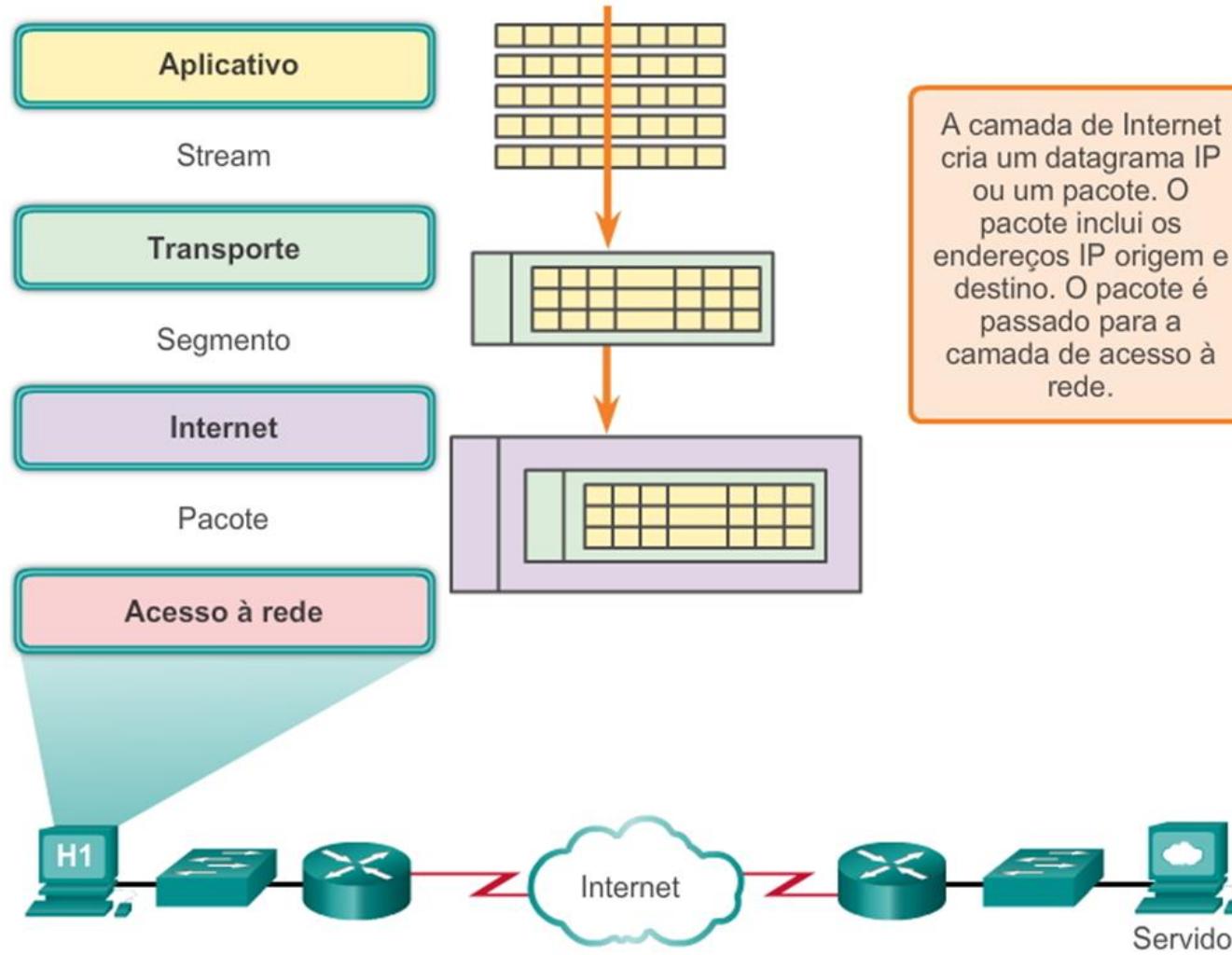


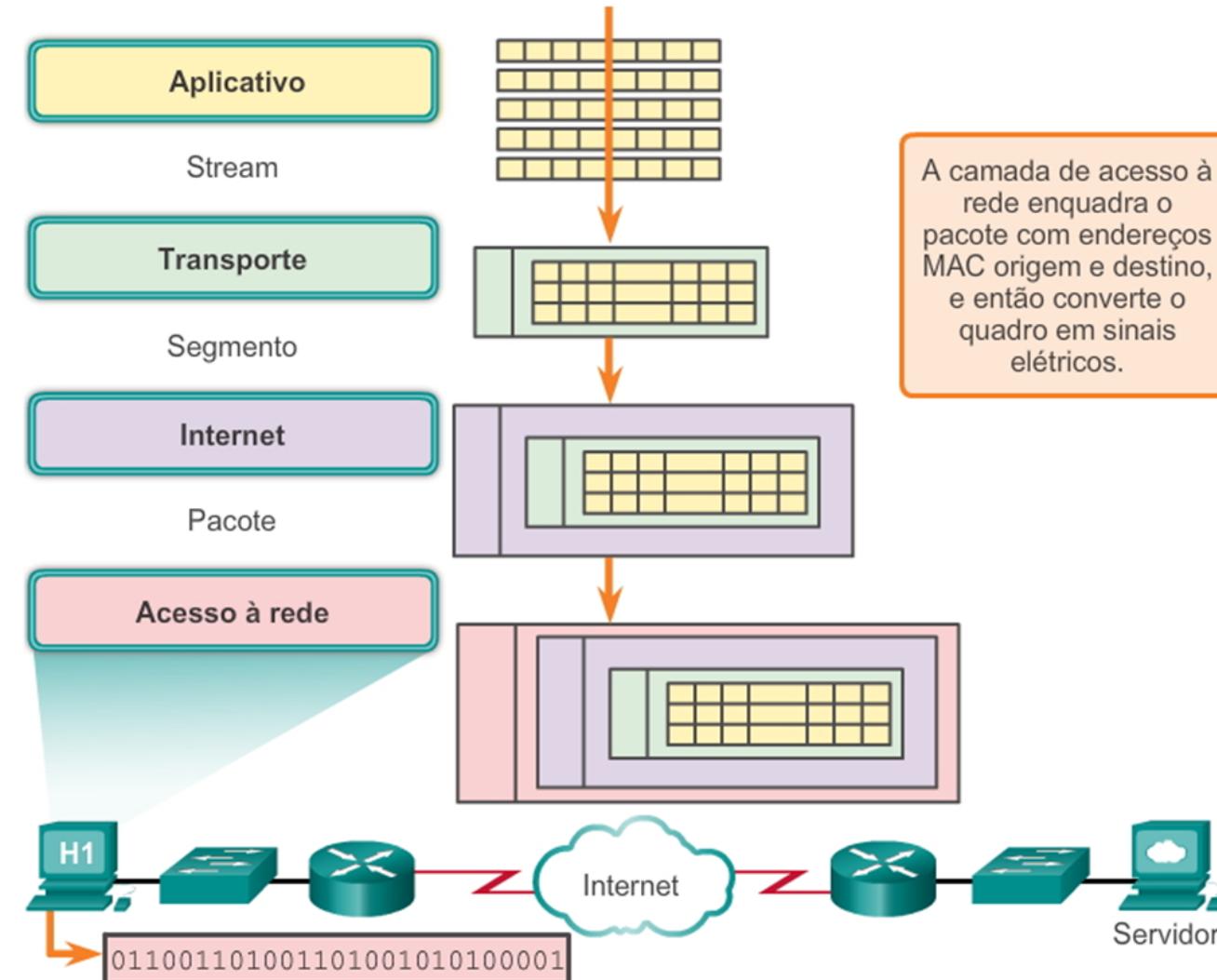
- O servidor DNS armazena diferentes tipos de registros de recursos utilizados para resolver nomes
- Contém nome, endereço e tipo de registro
- Não é possível resolver o nome utilizando os registros armazenados, então entra em contato com outros servidores
- O servidor armazena temporariamente o endereço numerado que corresponde ao nome na memória cache
- Windows **ipconfig /displaydns** exibe todos os DNS em cache

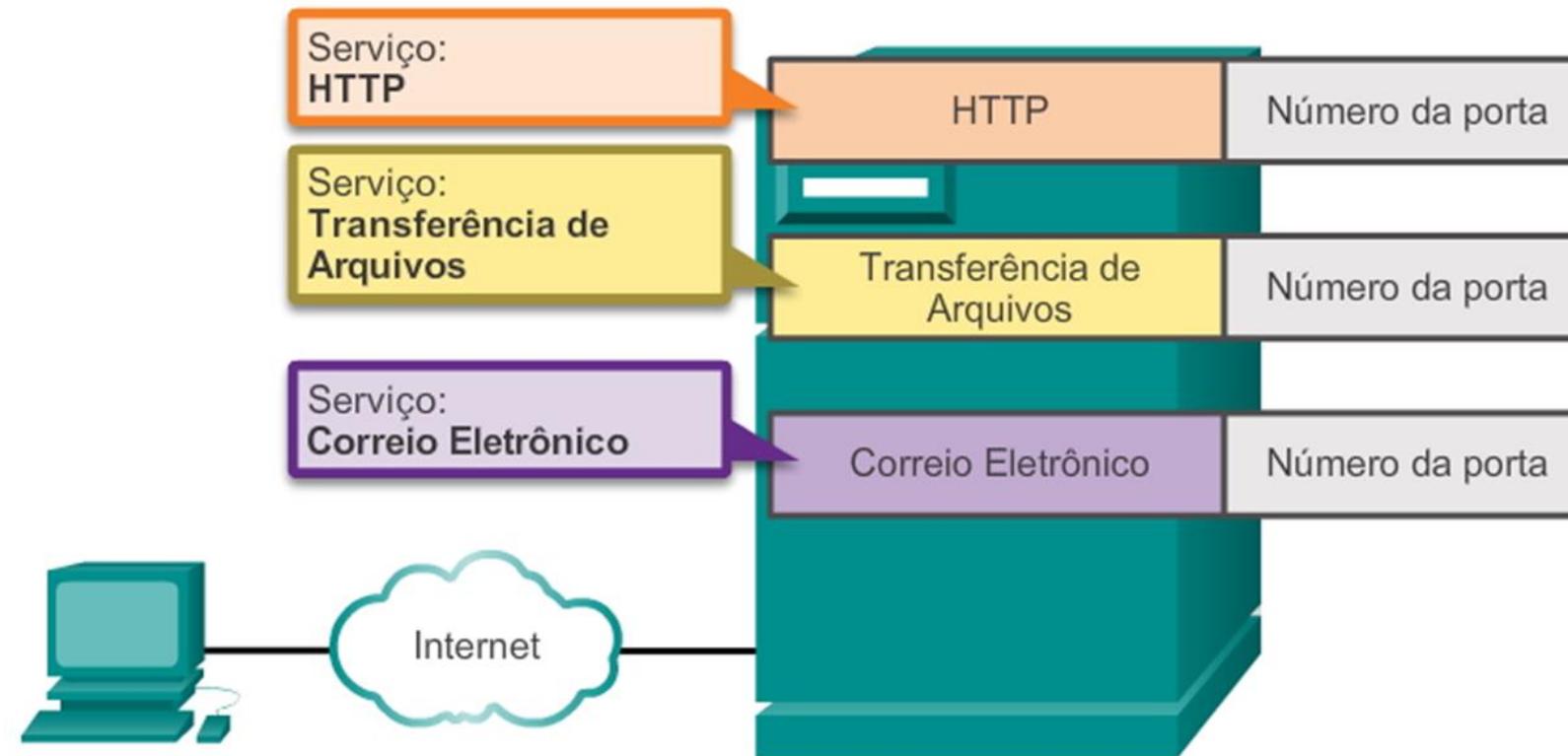












No dispositivo final, o número de porta de serviço direciona os dados da conversa correta.